NOA-3570

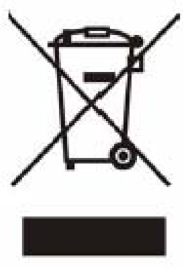
Outdoor Access Point

User's Guide

Version 3.50
12/2005

Certifications

1 Select the certification you wish to view from this page.



Interference Statements and Warnings

FCC Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antennas or antenna connector cable. Only use the included antennas or antenna connector cable.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to corrosive liquids.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

Table of Contents

List of Figures

List of Tables

CHAPTER 1
Getting to Know Your NOA-3570

This chapter introduces the main features and applications of the NOA-3570.

1.1 Introducing the NOA-3570

The NOA-3570 is an enterprise level, outdoor IEEE 802.11g compliant business access point, bridge and repeater with excellent wireless performance. Wireless Distribution System (WDS) support provides flexibility in building an extended wireless network with bridge and repeater applications. IEEE 802.1x, Wi-Fi Protected Access, WEP data encryption and MAC address filtering offer highly secured wireless connectivity.

Rugged die-cast, watertight construction, built-in lightening protection, and grounding make the NOA-3570 perfect for outdoors applications.

It is easy to install and configure the NOA-3570. The web-based configurator allows remote configuration and management of your NOA-3570. The Power over Ethernet (PoE) feature means that power can be delivered to the NOA-3570 over an Ethernet line. This allows you to mount the NOA-3570 in areas where there are no nearby power sources.

1.2 NOA-3570 Features

The following sections describe the features of the NOA-3570

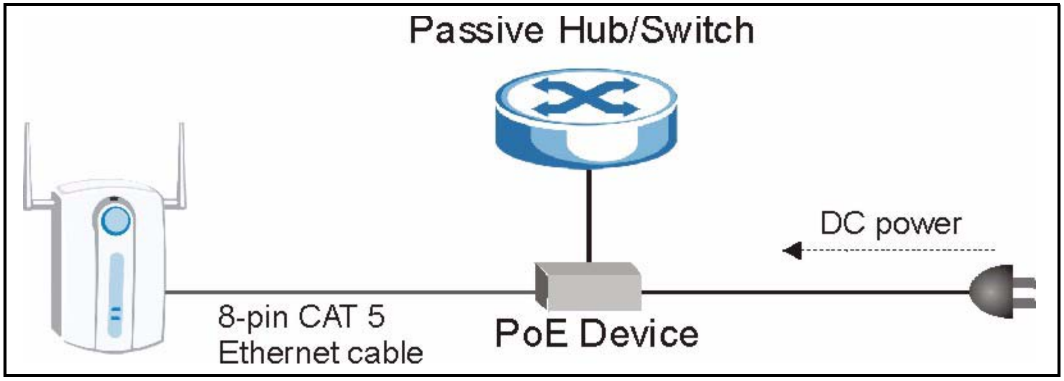
10/100M Auto-negotiating Ethernet/Fast Ethernet Interface

This auto-negotiating feature allows the NOA-3570 to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Power over Ethernet (PoE)

Power over Ethernet (PoE) is the ability to provide power to your NOA-3570 via an 8-pin CAT 5 Ethernet cable, eliminating the need for a nearby power source. The NOA-3570 includes a special high current power injector that allows the NOA-3570 to be located farther away. This feature allows increased flexibility in the locating of your NOA-3570.

Figure 1 PoE Installation Example



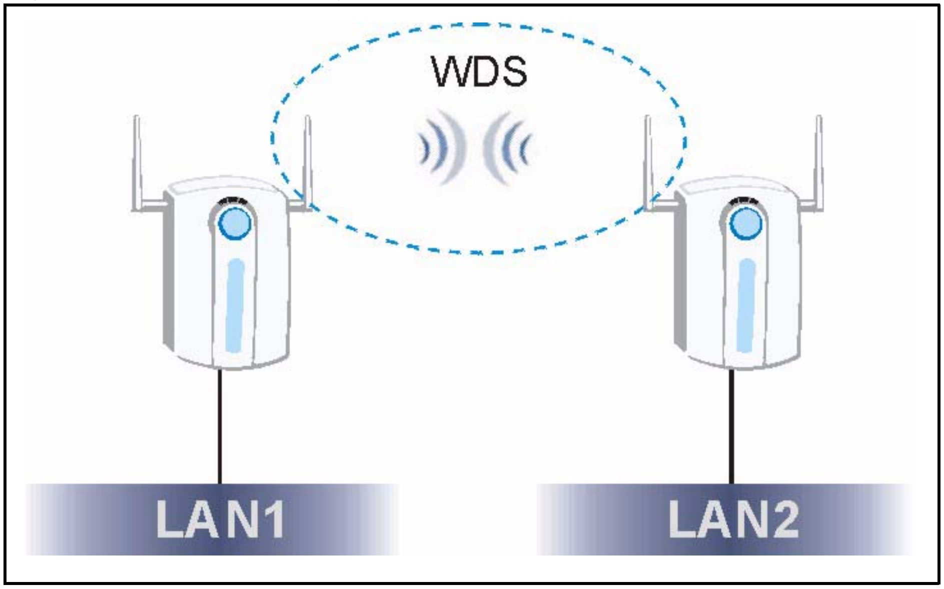
Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption.

WDS Functionality

A Distribution System (DS) is a wired connection between two or more APs, while a Wireless Distribution System (WDS) is a wireless connection. Your NOA-3570 supports WDS, providing a cost-effective solution for wireless network expansion. The NOA-3570 supports up to five wireless links with other APs.

Figure 2 WDS Functionality Example



IEEE 802.11g Wireless LAN Standard

The NOA-3570 complies with the IEEE 802.11g wireless standard. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows. The modulation technique defines how bits are encoded onto radio waves.

Table 1 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Note: The NOA-3570 may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

IEEE 802.11b Wireless LAN Standard

The NOA-3570 also fully complies with the IEEE 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g device (and vice versa) at 11 Mbps or lower depending on range.

The IEEE 802.11b data rate and corresponding modulation techniques are shown in the table below.

Table 2 IEEE 802.11b

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)

STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network.

SSL Passthrough

SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https” instead of “http”. The NOA-3570 allows SSL connections to take place through the NOA-3570.

VPN Passthrough

VPN (Virtual Private Network) connections use data encryption to provide secure communications over unsecure networks (like the Internet). The NOA-3570 allows VPN connections to go through it.

Wireless LAN MAC Address Filtering

Your NOA-3570 checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.

WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.

IEEE 802.1x Network Security

The NOA-3570 supports the IEEE 802.1x standard to enhance user authentication. This allows you to use a RADIUS (RFC2138, 2139 - Remote Authentication Dial In User Service) server to authenticate users.

Embedded RADIUS Server

The NOA-3570's embedded RADIUS server eliminates the need to purchase and maintain a standalone external RADIUS server. Use the embedded RADIUS server to authenticate up to 32 users. You can also use an external RADIUS server to authenticate a potentially unlimited number of users.

Backup RADIUS Server

You can configure the NOA-3570 to use backup external RADIUS servers and accounting servers in case the primary external RADIUS or accounting server does not respond.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your NOA-3570 supports SNMP agent functionality, which allows a manger station to manage and monitor the NOA-3570 through the network. The NOA-3570 supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

Full Network Management

The web configurator is an HTML-based management interface that allows easy setup and management via Internet browser. Most functions of the NOA-3570 are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator over a telnet connection.

Logging and Tracing

- Built-in message logging and packet tracing.
- Syslog facility support.

Embedded FTP and TFTP Servers

The NOA-3570's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

Wireless Association List

With the wireless association list, you can see the list of the wireless stations that are currently using the NOA-3570 to access your wired network.

Wireless LAN Channel Usage

The **Wireless Channel Usage** screen displays which radio channels are being used by other wireless devices within the transmission range of the NOA-3570. This allows you to select the channel with minimum interference for your NOA-3570.

1.3 Applications for the NOA-3570

The NOA-3570 can be configured using the following WLAN operating modes

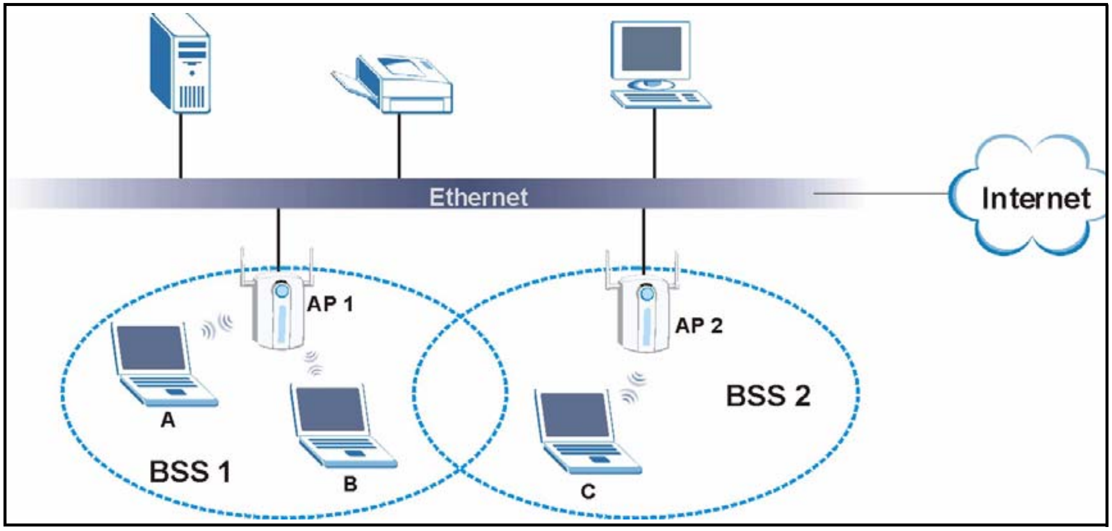
1. AP
2. AP+Bridge
3. Bridge/Repeater

Applications for each operating mode are shown below.

1.3.1 Access Point

The NOA-3570 is an ideal access solution for wireless Internet connection. A typical Internet access application for your NOA-3570 is shown as follows. Stations A, B and C can access the wired network through the NOA-3570s.

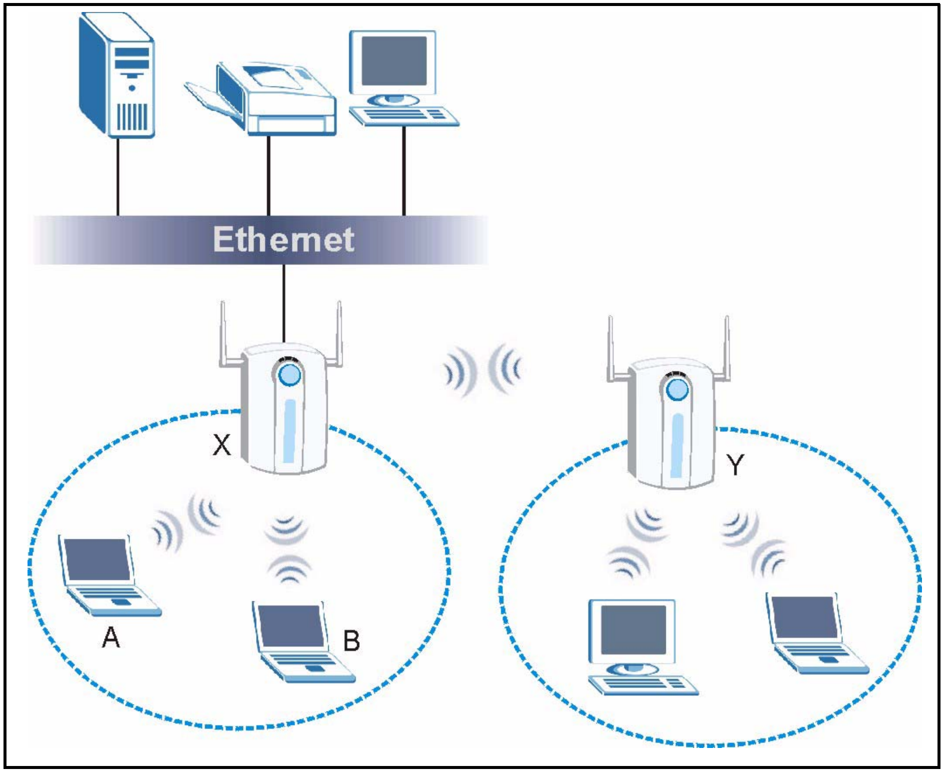
Figure 3 Access Point Application



1.3.2 AP + Bridge

In **AP+Bridge** mode, the NOA-3570 supports both AP connections (**A** and **B** can connect to the wired network through **X**) and bridge connections (**X** can communicate with **Y**) at the same time.

Figure 4 AP+Bridge Application



1.3.3 Bridge / Repeater

The NOA-3570 can act as a wireless network bridge and establish wireless links with other APs. In bridge mode, the NOA-3570s (see **A** and **B** in Figure 5 on page 35) are connected to independent wired networks and have a bridge (**A** can communicate with **B**) connection at the same time. A NOA-3570 without a wired connection can act as a repeater (see **C** in Figure 6 on page 36).

Figure 5 Bridge Application

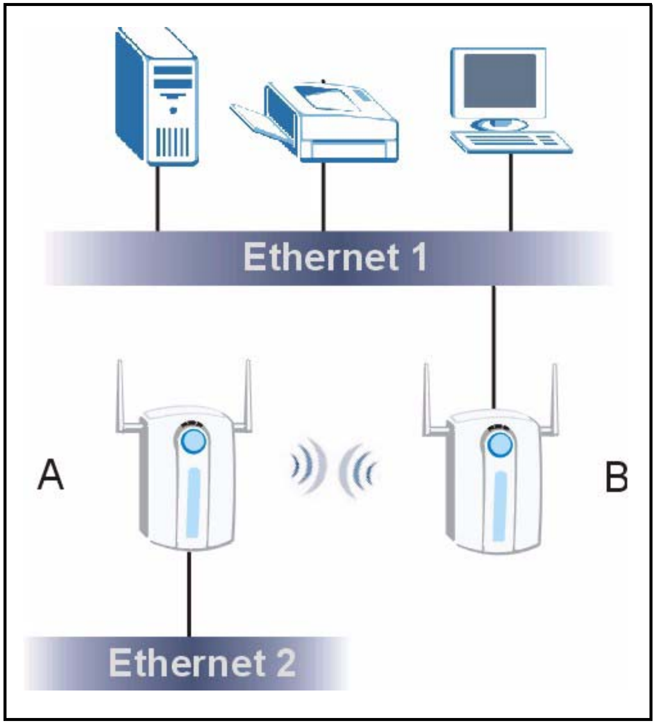
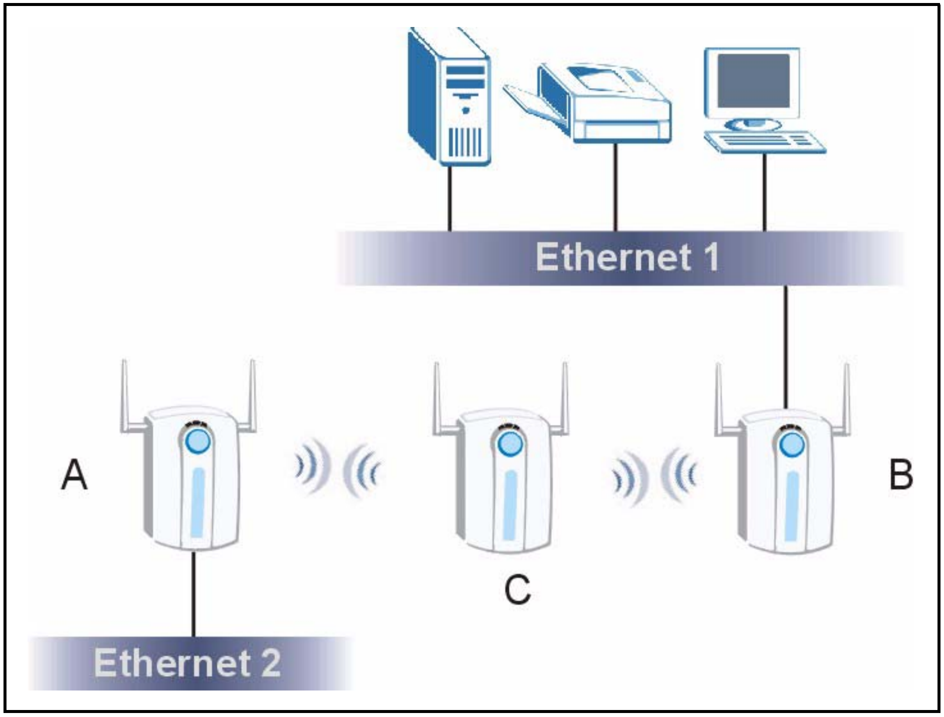


Figure 6 Repeater Application



CHAPTER 2
Introducing the Web Configurator

This chapter describes how to access the NOA-3570 web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The embedded web configurator allows you to manage the NOA-3570 from anywhere through a browser such as Microsoft Internet Explorer. Use Internet Explorer 6.0 and later versions with JavaScript enabled.

It is recommended that you set your screen resolution to 1024 by 768 pixels.

2.2 Accessing the NOA-3570 Web Configurator

1 Make sure your NOA-3570 hardware is properly connected (refer to the Quick Start Guide).

2 Prepare your computer/computer network to connect to the NOA-3570 (refer to Appendix D on page 201).

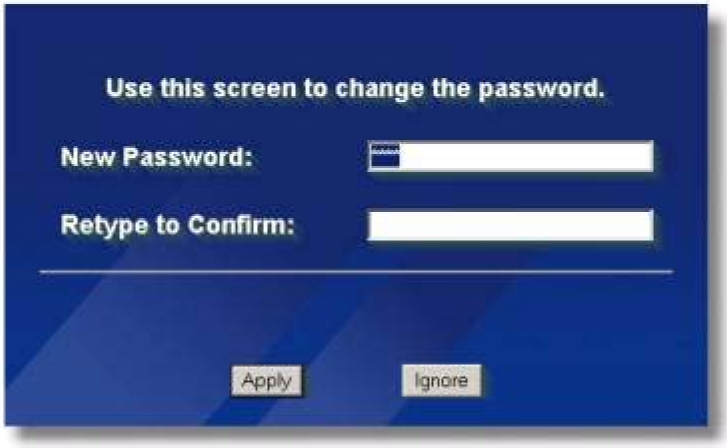
3 Launch your web browser.

4 Type "192.168.1.2" (the default IP address of the NOA-3570) as the URL.

5 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

6 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore** to allow access without password change.

Figure 7 Change Password Screen



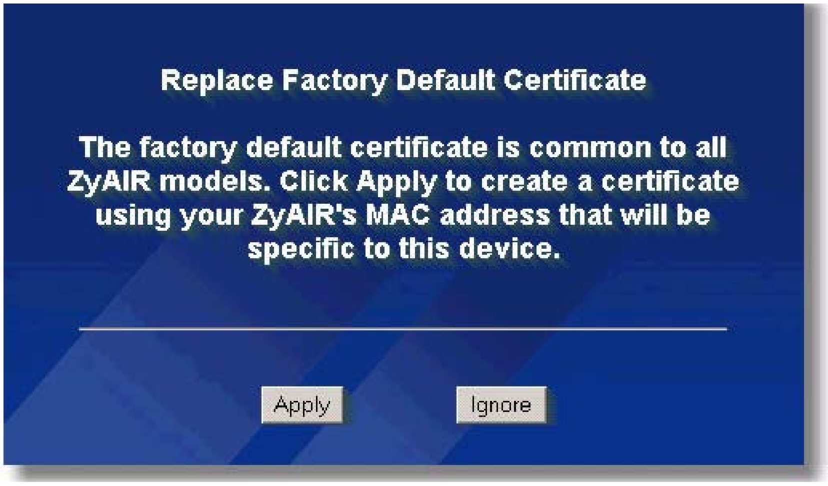
Use this screen to change the password.

New Password:

Retype to Confirm:

7 Click **Apply** in the **Replace Certificate** screen to create a certificate using your NOA-3570’s MAC address that will be specific to this device.

Figure 8 Replace Certificate Screen.



Replace Factory Default Certificate

The factory default certificate is common to all ZyAIR models. Click Apply to create a certificate using your ZyAIR's MAC address that will be specific to this device.

8 You should now see the **MAIN MENU** screen (see Figure 10 on page 40).

Note: The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the NOA-3570 if this happens to you.

2.3 Resetting the NOA-3570

If you forget your password or cannot access the NOA-3570, you will need to reload the factory-default configuration file. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to “1234” and the IP address will be reset to 192.168.1.2.

Do the following to erase the current configuration and restore factory defaults.

Obtain the default configuration file, unzip it and save it in a folder. Use a console cable to connect a computer with terminal emulation software to the NOA-3570's console port. Turn the NOA-3570 off and then on to begin a session. When you turn on the NOA-3570 again, you will see the initial screen. When you see the message "Press any key to enter Debug Mode within 3 seconds" press a key to enter debug mode.

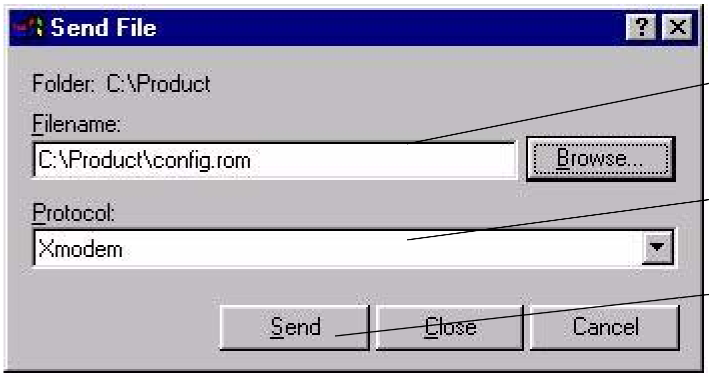
To upload the configuration file, do the following:

1 Type "atlc" after the Enter Debug Mode message.

2 Wait for the Starting XMODEM upload message before activating XMODEM upload on your terminal.

3 This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer,** then **Send File** to display the following screen.

Figure 9 Example Xmodem Upload



Folder: C:\Product

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

4 After a successful configuration file upload, type "atgo" to restart the NOA-3570.

The NOA-3570 is now reinitialized with a default configuration file including the default password of "1234" and IP address of 192.168.1.2.

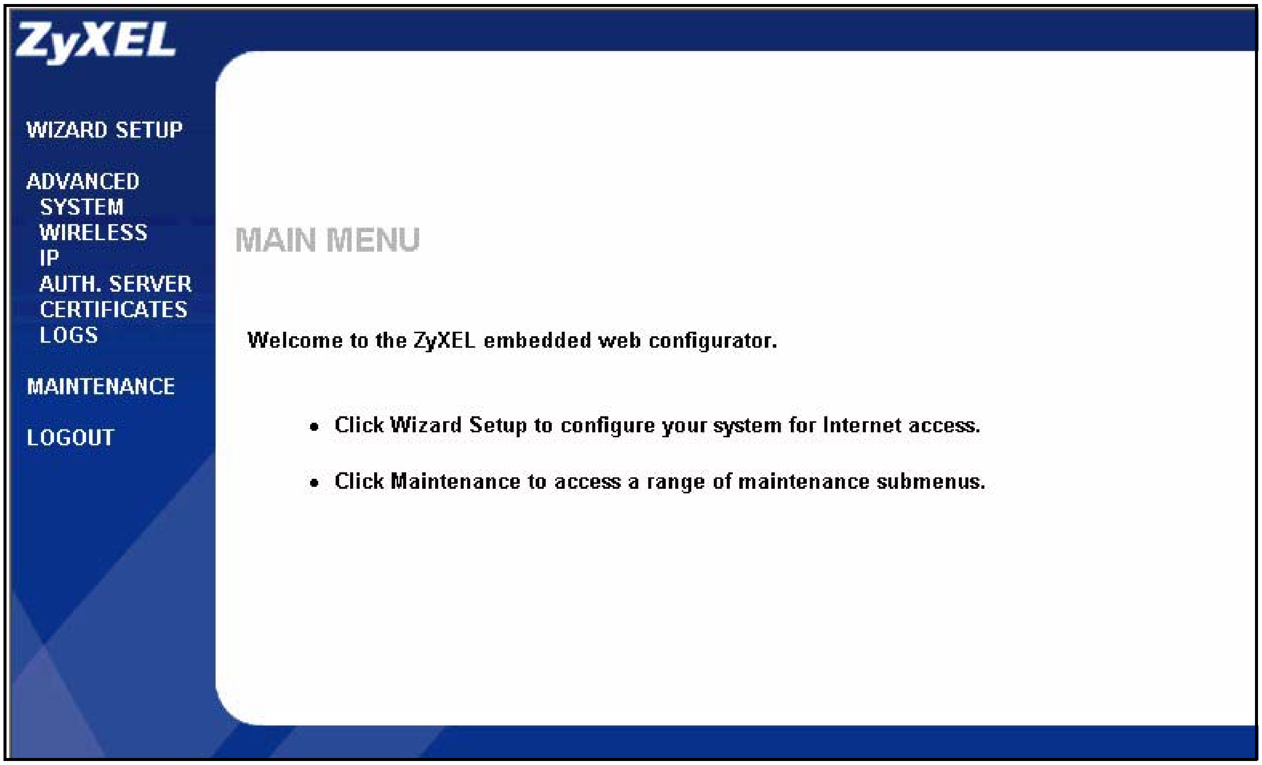
2.4 Navigating the NOA-3570 Web Configurator

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.

Note: Follow the instructions you see in the MAIN MENU screen or click the HELP ? icon (located in the top right corner of most screens) to view online help.

The HELP ? icon does not appear in the MAIN MENU screen.

Figure 10 The MAIN MENU Screen of the Web Configurator



MAIN MENU

Welcome to the ZyXEL embedded web configurator.

- Click Wizard Setup to configure your system for Internet access.
- Click Maintenance to access a range of maintenance submenus.

Use submenus to configure NOA-3570 features.

Click **LOGOUT** at any time to exit the web configurator.

The following table describes the sub-menus.

Table 3 Screens SummaryNOA-3570

LINK	TAB	FUNCTION
WIZARD SETUP		Click **WIZARD SETUP** for initial configuration including general setup, wireless LAN setup and IP address assignment.
SYSTEM	General	This screen contains administrative and system-related information.
	Password	Use this screen to change your password.
	Time Setting	Use this screen to change your NOA-3570’s time and date settings.
WIRELESS	Wireless	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	MAC Filter	Use this screen to change MAC filter settings on the NOA-3570
	Roaming	Use this screen to configure the NOA-3570 to allow wireless users to roam seamlessly between APs that are within the same subnet.
	802.1x/WPA	Use this screen to configure wireless LAN security.
IP	IP	Use this screen to configure IP address settings.

Table 3 Screens SummaryNOA-3570

LINK	TAB	FUNCTION
AUTH. SERVER	Setting	Configure this screen to use the internal server to authenticate wireless users.
	Trusted AP	Configure this screen to allow specified AP’s to communicate with the NOA-3570.
	Trusted Users	Use this screen to configure the local user account(s) on the NOA-3570.
CERTIFICATES	My Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CAs	Use this screen to view and manage the list of the trusted CAs.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your NOA-3570’s log settings.
MAINTENANCE	Status	This screen contains administrative and system-related information.
	Association List	Use this screen to view a list of wireless clients that are connected to the NOA-3570.
	Channel Usage	Use this screen to see which APs are using which wireless channels within range of your NOA-3570.
	F/W Upload	Use this screen to upload firmware to your NOA-3570
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NOA-3570.
	Restart	This screen allows you to reboot the NOA-3570 without turning the power off.
LOGOUT		Click **LOGOUT** to exit the web configurator.

CHAPTER 3 Wizard Setup

This chapter provides information on the **WIZARD SETUP** screens in the web configurator.

3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your NOA-3570 for wireless stations to access your wired LAN.

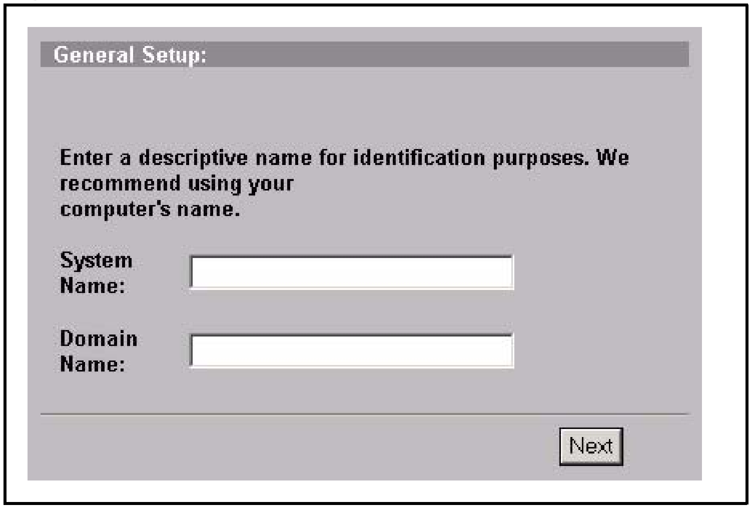
Note: Click **Next** in each screen to continue or click **Back** to return to the previous screen.

Your settings are not saved when you click **Back**.

3.2 Wizard Setup: General Setup

General Setup contains administrative and system-related information.

Figure 11 Wizard: General Setup



General Setup:

Enter a descriptive name for identification purposes. We recommend using your computer's name.

System Name:

Domain Name:

The following table describes the labels in this screen.

Table 4 Wizard: General Setup

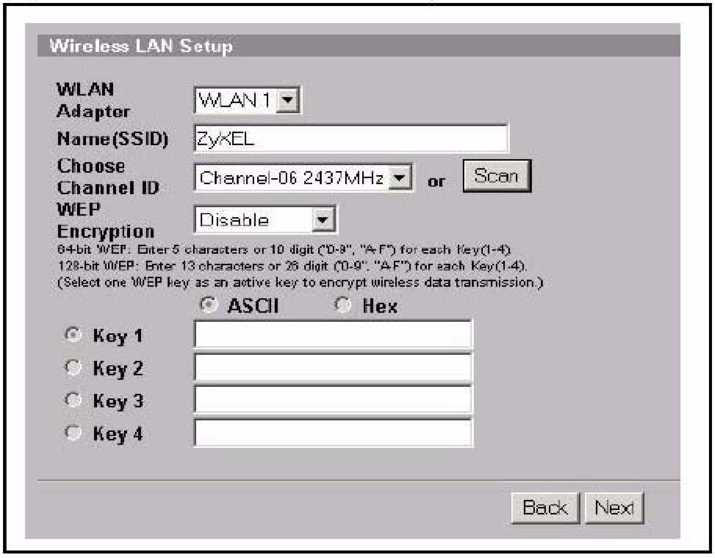
LABEL	DESCRIPTION
System Name	It is recommended you type your computer's "Computer name". In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**. In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**. In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the NOA-3570 **System Name**. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Next	Click **Next** to proceed to the next screen.

3.3 Wizard Setup: Wireless LAN

Use this wizard screen to configure one of the NOA-3570's two wireless LAN (WLAN) adapters to function as an AP (**WLAN 1** is recommended). Use the **ADVANCED WIRELESS** screens to configure a WLAN adapter for bridge/repeater functions.

Note: The wireless clients and NOA-3570 must use the same SSID, channel ID and WEP encryption key (if you enable WEP) for wireless communication.

Figure 12 Wizard: Wireless LAN Setup



Wireless LAN Setup

WLAN Adapter: WLAN 1

Name(SSID): ZyXEL

Choose Channel ID: Channel-06 2437MHz or Scan

WEP Encryption: Disable

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1

○ Key 2

○ Key 3

○ Key 4

The channel only can setup in Channel 01 ~ 11.

The following table describes the labels in this screen.

Table 5 Wizard: Wireless LAN Setup

LABEL	DESCRIPTION
Wireless LAN Setup	
WLAN Adapter	Select which WLAN adapter you want to configure (**WLAN 1** recommended).
Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NOA-3570, make sure all wireless stations use the same Name (SSID) in order to access the network.
Choose Channel ID	To manually set the NOA-3570 to use a channel, select the channel from the drop-down list box. To have the NOA-3570 automatically select a channel, click **Scan** instead.
Scan	Click this button to have the NOA-3570 automatically scan for and select a channel with the least interference.
WEP Encryption	Select **Disable** allows all wireless computers to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to use data encryption. Note: Use the **ADVANCED WIRELESS** screens to configure stronger types of security (such as WPA).
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding 0x is entered automatically.

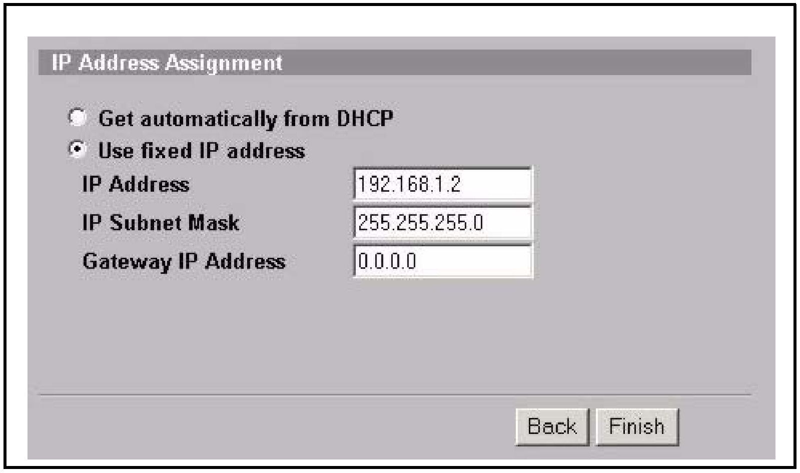
Table 5 Wizard: Wireless LAN Setup

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NOA-3570 and the wireless stations must use the same WEP key. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.4 Wizard Setup: IP Address Assignment

Use this wizard screen to configure IP address assignment for the NOA-3570.

Figure 13 Wizard: IP Address Assignment



IP Address Assignment

○ Get automatically from DHCP

● Use fixed IP address

IP Address: 192.168.1.2

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

Table 6 Wizard: IP Address Assignment

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option to have the NOA-3570 use a dynamically assigned IP address from a DHCP server. **Note:** You must know the IP address assigned to the NOA-3570 (by the DHCP server) to access the NOA-3570 again.
Use fixed IP address	Select this option if your NOA-3570 is using a static IP address. When you select this option, fill in the fields below.

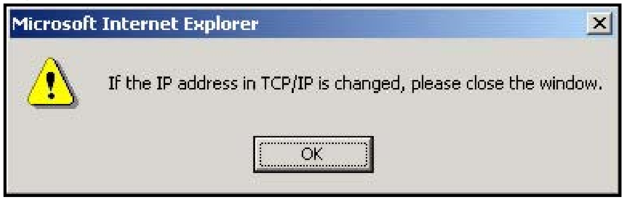
Table 6 Wizard: IP Address Assignment

LABEL	DESCRIPTION
IP Address	Enter the IP address of your NOA-3570 in dotted decimal notation. **Note:** If you changed the NOA-3570's IP address, you must use the new IP address if you want to access the web configurator again.
IP Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your NOA-3570 that will forward the packet to the destination. The gateway must be a router on the same segment as your NOA-3570's LAN or WAN port.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to proceed to complete the Wizard setup.

3.5 Basic Setup Complete

When you click **Finish** in the **Wizard IP Address Assignment** screen, a warning window displays as shown. Click **OK** to close the window. Log into the web configurator again using the new IP address if you change the default IP address (192.168.1.2).

Figure 14 TCP/IP Warning Screen

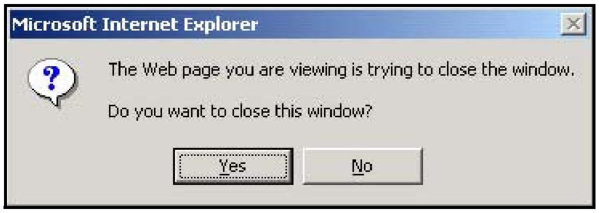


Microsoft Internet Explorer

If the IP address in TCP/IP is changed, please close the window.

The following screen displays prompting you to close the web browser.

Figure 15 Close Browser Screen



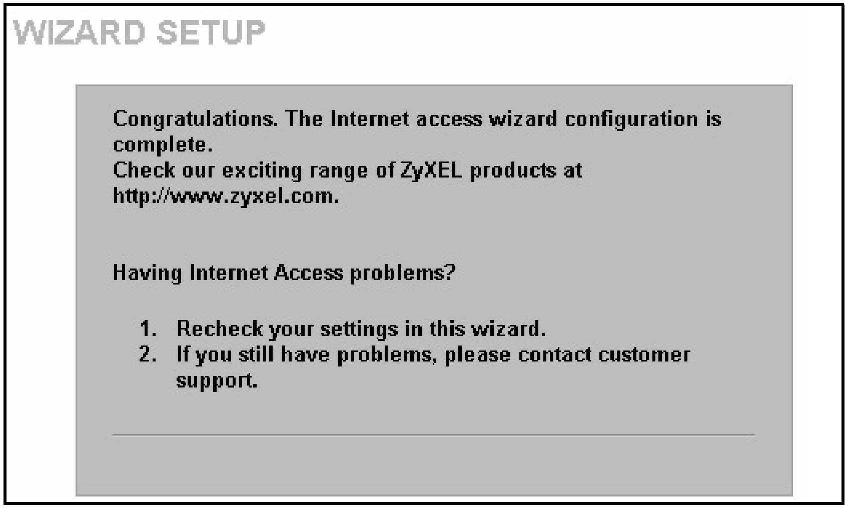
Microsoft Internet Explorer

The Web page you are viewing is trying to close the window.

Do you want to close this window?

Click **Yes** to close the web configurator. Otherwise, click **No** to use the **ADVANCED** screens to configure other features (the congratulations screen shows next).

Figure 16 Wizard: Setup Complete



Congratulations. The Internet access wizard configuration is complete.
Check our exciting range of ZyXEL products at http://www.zyxel.com.

Having Internet Access problems?

1. Recheck your settings in this wizard.
2. If you still have problems, please contact customer support.

Well done! You have set up your NOA-3570 to operate on your network and access the Internet.

CHAPTER 4
System Screens

This section provides information on general system setup.

4.1 System Overview

This chapter describes how to configure the NOA-3570’s general, DNS, password and time settings.

4.2 General Screen

The **General** screen contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the NOA-3570 **System Name**.

4.2.1 Domain Name

You can manually enter a domain name or the NOA-3570 can get it automatically by DHCP.

4.2.2 DNS Server Address Assignment

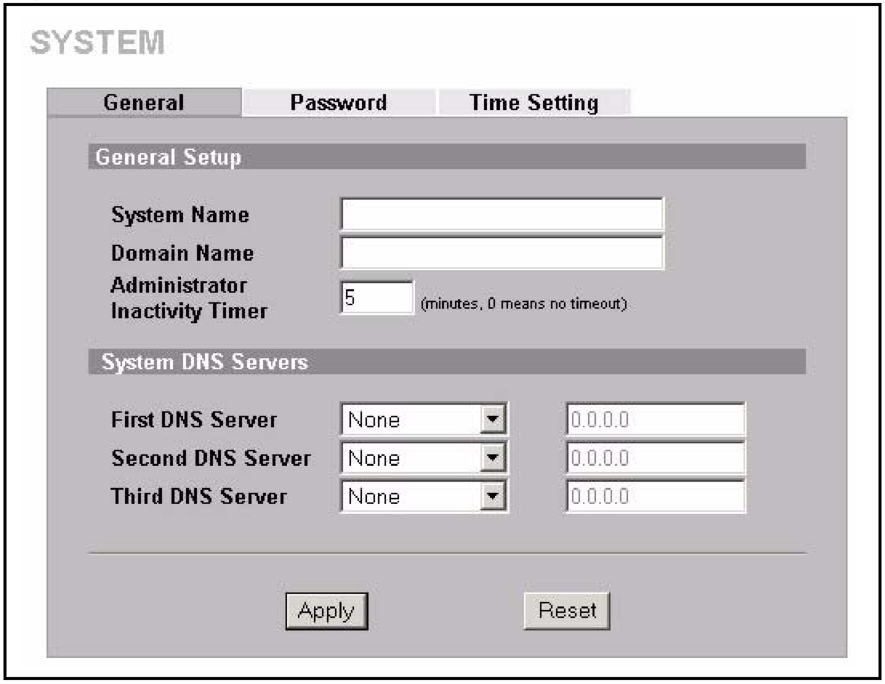
Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

You can manually configure DNS server addresses if you know them or the NOA-3570 can receive them automatically through DHCP.

4.3 Configuring General Setup

Click the **SYSTEM** link under **ADVANCED** to open the **General** screen.

Figure 17 System General



SYSTEM

General Setup

System Name:

Domain Name:

Administrator Inactivity Timer: 5 (minutes, 0 means no timeout)

System DNS Servers

First DNS Server: None 0.0.0.0

Second DNS Server: None 0.0.0.0

Third DNS Server: None 0.0.0.0

The following table describes the labels in this screen.

Table 7 System General Setup NOA-3570

LABEL	DESCRIPTION
General Setup	
System Name	Type a descriptive name to identify the NOA-3570 in the Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
System DNS Servers	

Table 7 System General Setup NOA-3570

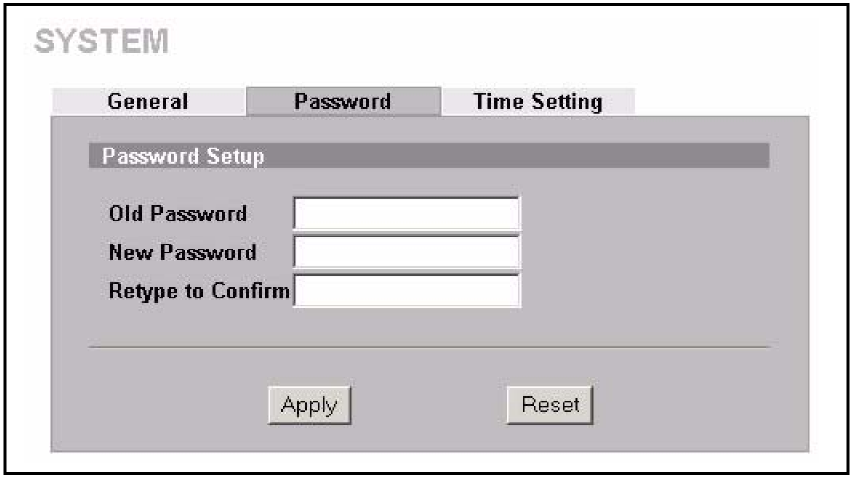
LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **From DHCP** if your ISP dynamically assigns DNS server information. The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is **None**.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.4 Configuring Password

To change your NOA-3570's password (recommended), click the **SYSTEM** link under **ADVANCED** and then the **Password** tab. The screen appears as shown. This screen allows you to change the NOA-3570's password.

If you forget your password (or the NOA-3570 IP address), you will need to reset the NOA-3570. See Section 2.3 on page 38 for details.

Figure 18 Password.



The following table describes the labels in this screen.

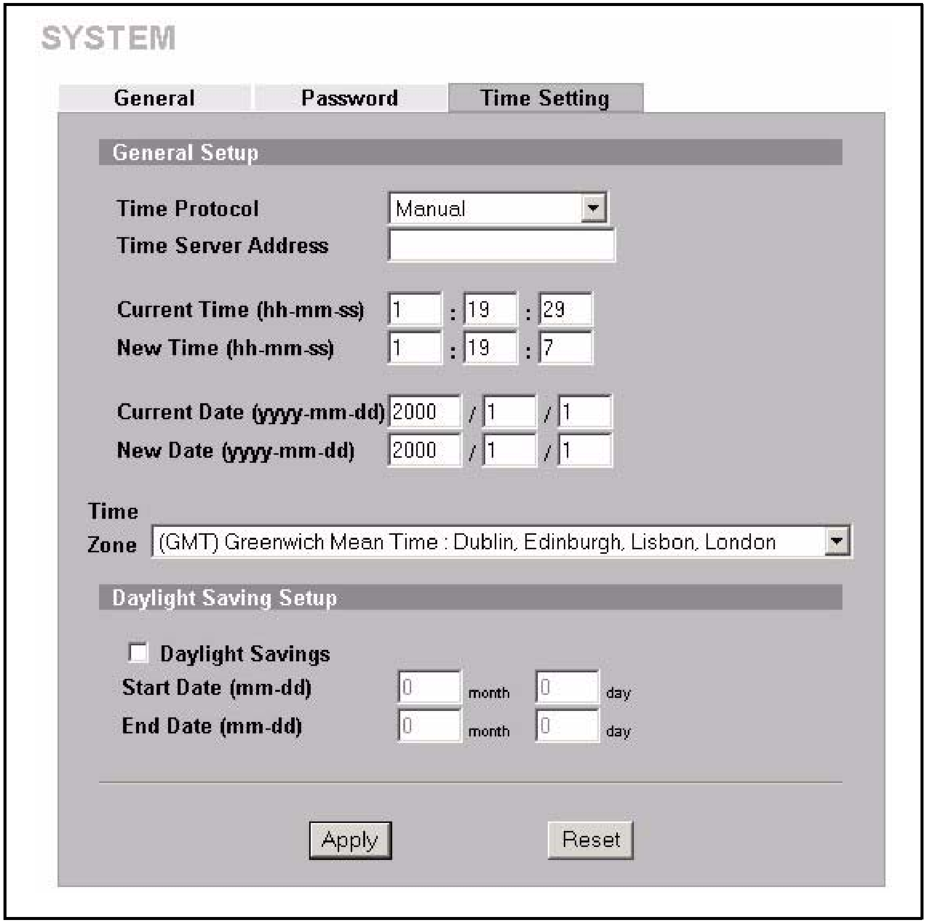
Table 8 Password

LABEL	DESCRIPTIONS
Old Password	Type in your existing system password (1234 is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to reload the previous configuration for this screen.

4.5 Configuring Time Setting

To change your NOA-3570’s time and date, click the **SYSTEM** link under **ADVANCED** and then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the NOA-3570’s time based on your local time zone.

Figure 19 Time Setting



SYSTEM

General Setup

Time Protocol: Manual
Time Server Address:
Current Time (hh-mm-ss): 1 : 19 : 29
New Time (hh-mm-ss): 1 : 19 : 7
Current Date (yyyy-mm-dd): 2000 / 1 / 1
New Date (yyyy-mm-dd): 2000 / 1 / 1
Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Daylight Saving Setup

□ Daylight Savings
Start Date (mm-dd): 0 month 0 day
End Date (mm-dd): 0 month 0 day

The following table describes the labels in this screen.

Table 9 Time Setting NOA-3570

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC 1305),** is similar to Time (RFC 868). Select **Manual** to enter the time and date manually.
Time Server Address	Enter the IP address or the URL of your time server. Check with your ISP/ network administrator if you are unsure of this information.
Current Time (hh:mm:ss)	This field displays the time of your NOA-3570. Each time you reload this page, the NOA-3570 synchronizes the time with the time server.
New Time (hh:mm:ss)	This field displays the last updated time from the time server. When you select **None** in the **Time Protocol** field, enter the new time in this field and then click **Apply**.
Current Date (yyyy/ mm/dd)	This field displays the date of your NOA-3570. Each time you reload this page, the NOA-3570 synchronizes the date with the time server.
New Date (yyyy/mm/ dd)	This field displays the last updated date from the time server. When you select **None** in the **Time Protocol** field, enter the new date in this field and then click **Apply**.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight saving time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date (mm-dd)	Enter the month and day that your daylight-saving time starts on if you selected **Daylight Savings**.
End Date (mm-dd)	Enter the month and day that your daylight-saving time ends on if you selected **Daylight Savings**.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to reload the previous configuration for this screen.

CHAPTER 5 Wireless LAN

This chapter discusses how to configure wireless LAN.

5.1 Introduction

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

Note: See the WLAN appendix for more detailed information on WLANs.

5.2 Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless stations, access points and the wired network.

Wireless security methods available on the NOA-3570 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NOA-3570 identity.

5.2.1 Encryption

- Use WPA security if you have WPA-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK if you have WPA-aware wireless clients but no RADIUS server.
- If you don't have WPA-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off.

5.2.2 Authentication

WPA has user authentication and you can also configure IEEE 802.1x to use the built-in database (Local User Database) or a RADIUS server to authenticate wireless clients before joining your network.

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the NOA-3570.

- Use the Local User Database if you have less than 32 wireless clients in your network. The NOA-3570 uses MD5 encryption when a client authenticates with the Local User Database

5.2.3 Restricted Access

The **MAC Filter** screen allows you to configure the AP to give exclusive access to devices (**Allow Association**) or exclude them from accessing the AP (**Deny Association**).

5.2.4 Hide NOA-3570 Identity

If you hide the SSID, then the NOA-3570 cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the NOA-3570 may be inconvenience for some valid WLAN clients. If you don't hide the ESSID, at least you should change the default one.

5.2.5 Configuring Wireless LAN on the NOA-3570

1. Configure the **ESSID** and **WEP** in the **Wireless** screen.
2. Use the **MAC Filter** screen to restrict access to your wireless network by MAC address.
3. Configure **WPA** or **WPA-PSK** in the **802.1x/WPA** screen. You can also configure 802.1x wireless client authentication in the **802.1x/WPA** screen.
4. Configure the RADIUS settings in the **AUTH. SERVER** screens.

The following table shows the relative effectiveness of these wireless security methods available on your NOA-3570.

Table 10 NOA-3570 Wireless Security Levels

Security Level	Security Type
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
Most Secure	Wi-Fi Protected Access (WPA)

Note: You must enable the same wireless security settings on the NOA-3570 and on all wireless clients that you want to associate with it.

If you do not enable any wireless security on your NOA-3570, your network is accessible to any wireless networking device that is within range.

5.3 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

5.3.1 Rapid STP

The NOA-3570 uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

5.3.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

Table 11 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

5.3.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

5.3.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 12 STP Port States

PORT STATES	DESCRIPTIONS
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

5.4 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

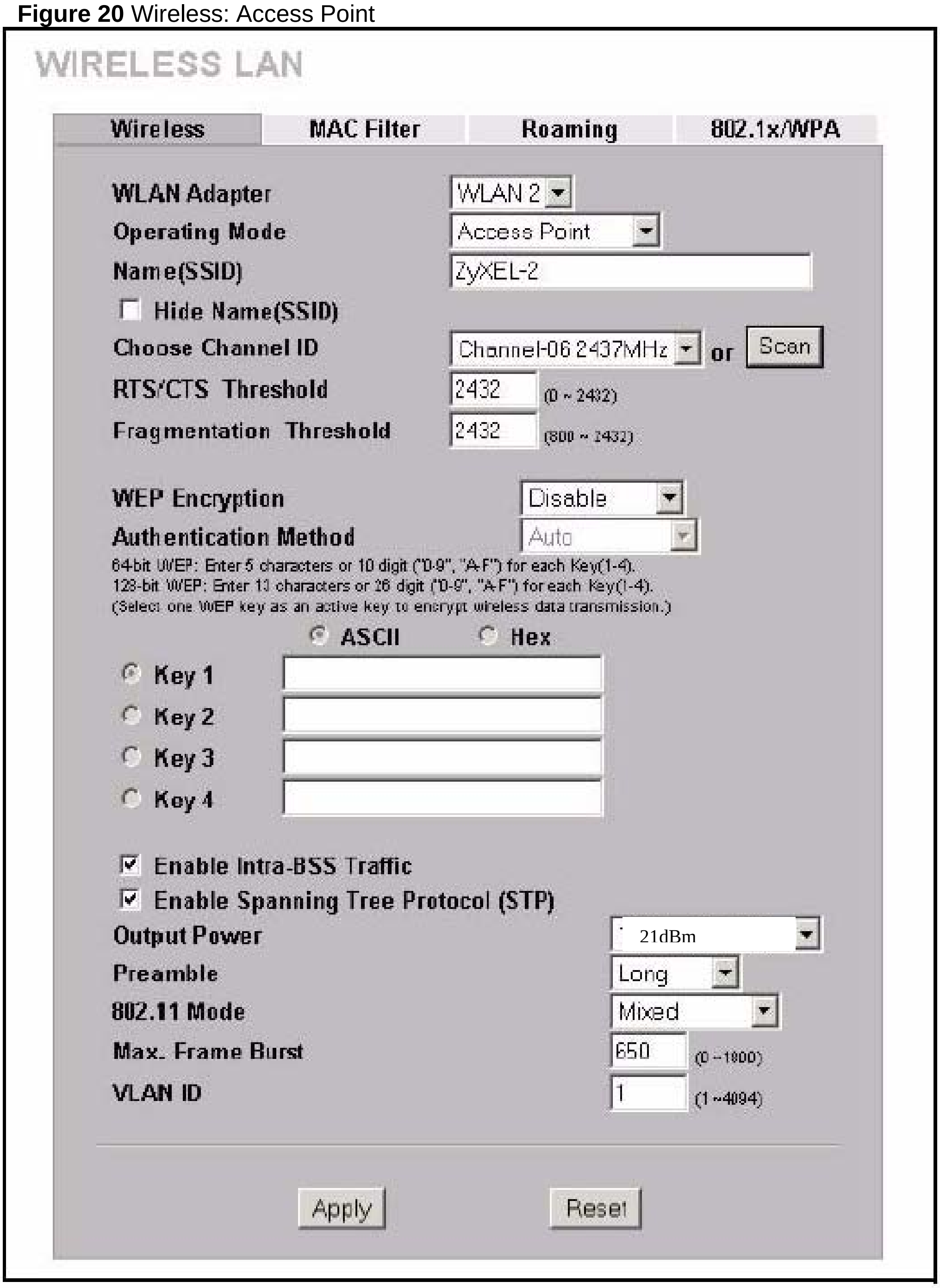
5.5 Configuring the Wireless Screen

Click the **WIRELESS** link under **ADVANCED** to display the **Wireless** screen. The screen varies depending upon the operating mode you select.

5.5.1 Access Point Mode

Select **Access Point** in the **Operating Mode** drop-down list box to display the screen as shown next.
Channel selection only can choose 1~11ch.

Figure 20 Wireless: Access Point



WLAN Adapter: WLAN 2
Operating Mode: Access Point
Name(SSID): ZyXEL-2
□ Hide Name(SSID)
Choose Channel ID: Channel-06 2437MHz or Scan
RTS/CTS Threshold: 2432 (0 ~ 2432)
Fragmentation Threshold: 2432 (800 ~ 2432)

WEP Encryption: Disable
Authentication Method: Auto
64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

☑ Enable Intra-BSS Traffic
☑ Enable Spanning Tree Protocol (STP)
Output Power: 21dBm
Preamble: Long
802.11 Mode: Mixed
Max. Frame Burst: 650 (0 ~1800)
VLAN ID: 1 (1 ~4094)

Table 13 Wireless: Access Point NOA-3570

LABEL	DESCRIPTION
WLAN Adapter	Select which WLAN adapter you want to configure. It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.
Operating Mode	Select the operating mode from the drop-down list. The options are **Access Point**, **Bridge/Repeater** and **AP+Bridge**.
Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. **Note:** If you are configuring the NOA-3570 from a computer connected to the wireless LAN and you change the NOA-3570's SSID or WEP settings, you will lose your wireless connection when you click **Apply** to confirm. You must then change the wireless settings of your computer to match the NOA-3570's new settings.
Hide Name (SSID)	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through passive scanning using a site survey tool.
Choose Channel ID	Set the operating frequency/channel depending on your particular region. To manually set the NOA-3570 to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the NOA-3570 automatically select a channel, click **Scan** instead.
Scan	Click this button to have the NOA-3570 automatically scan for and select a channel with the least interference.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **800** and **2432**.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	If you use WEP encryption, select **Auto**, **Open System** or **Shared Key** from the drop-down list box.

Table 13 Wireless: Access Point NOA-3570

LABEL	DESCRIPTION
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations. The preceding “0x” is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Enable Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the same BSS. Enable Intra-BSS traffic to allow wireless stations connected to the NOA-3570 to communicate with each other. Disable Intra-BSS traffic to only allow wireless stations to communicate with the wired network, not with each other.
Enable Spanning Tree Protocol (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP - compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the NOA-3570.
Output Power	Set the output power of the NOA-3570 in this field. If there is a high density of APs within an area, decrease the output power of the NOA-3570 to reduce interference with other APs. The options are **21dBm**, **19dBm**, **17dBm** or **15dBm**.
Preamble	Preamble is used to signal that data is coming to the receiver. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless adapters support long preamble, but not all support short preamble. Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks. Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications. Select **Dynamic** to have the NOA-3570 automatically use short preamble when all wireless clients support it, otherwise the NOA-3570 uses long preamble. **Note:** The NOA-3570 and the wireless stations MUST use the same preamble mode in order to communicate.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the NOA-3570. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the NOA-3570. Select **Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NOA-3570. The transmission rate of your NOA-3570 might be reduced.
Max. Frame Burst	Enable Maximum Frame Burst to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. Maximum Frame Burst sets the maximum time, in microseconds, that the NOA-3570 transmits IEEE 802.11g wireless traffic only. Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature.

Table 13 Wireless: Access Point NOA-3570

LABEL	DESCRIPTION
VLAN ID	The NOA-3570 supports IEEE 802.1 tagged VLAN for partioning a physical network into multiple logical networks. Enter a number from 1 to 4094 to set the VLAN ID tag that the NOA-3570 adds to the Ethernet frames that this WLAN adapter receives from wireless clients or other APs. Use the **VLAN** screen to enable or disable the NOA-3570's VLAN feature.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

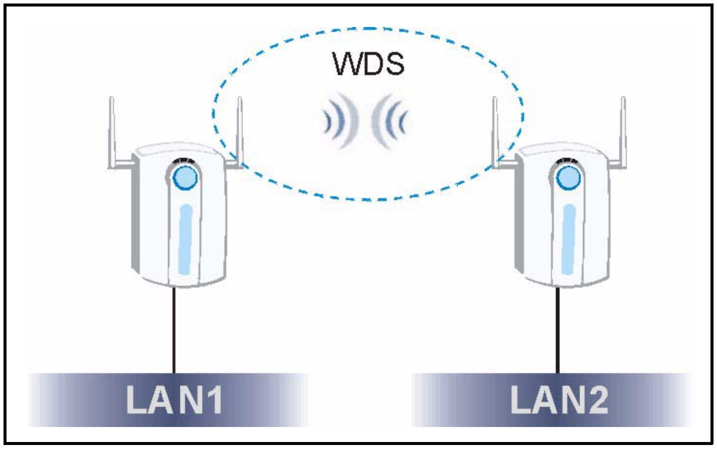
5.5.2 Bridge/Repeater Mode

The NOA-3570 can act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

The NOA-3570 can establish wireless links with other APs.

In the example below, when both NOA-3570s are in Bridge/Repeater mode, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

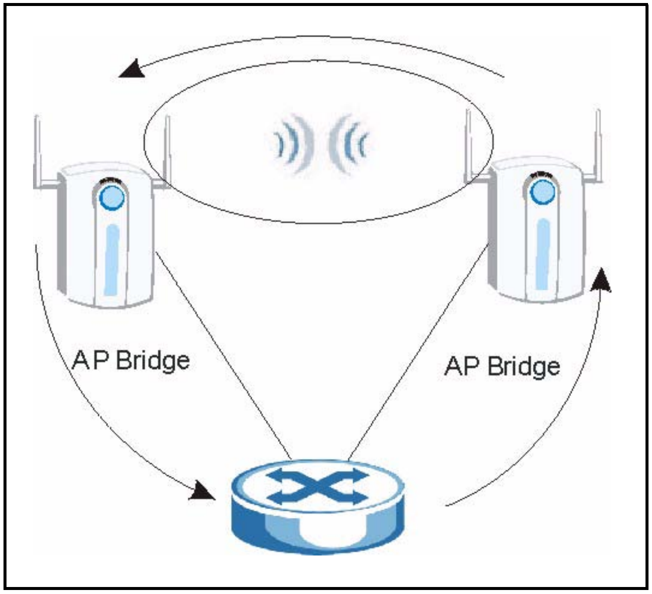
Figure 21 Bridging Example



Be careful to avoid bridge loops when you enable bridging in the NOA-3570. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

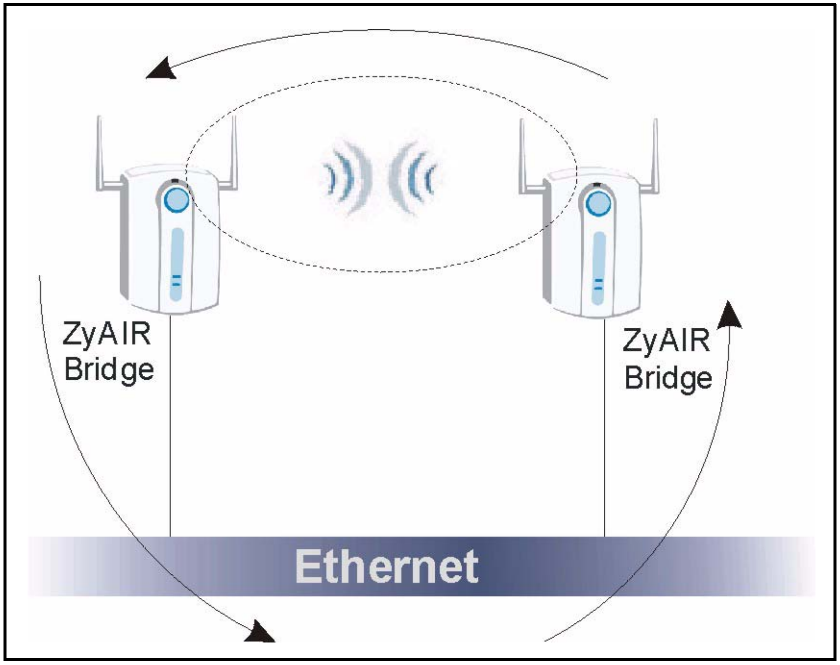
If two or more NOA-3570s (in bridge mode) are connected to the same hub as shown next.

Figure 22 Bridge Loop: Two Bridges Connected to Hub



If your NOA-3570 (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN as shown next.

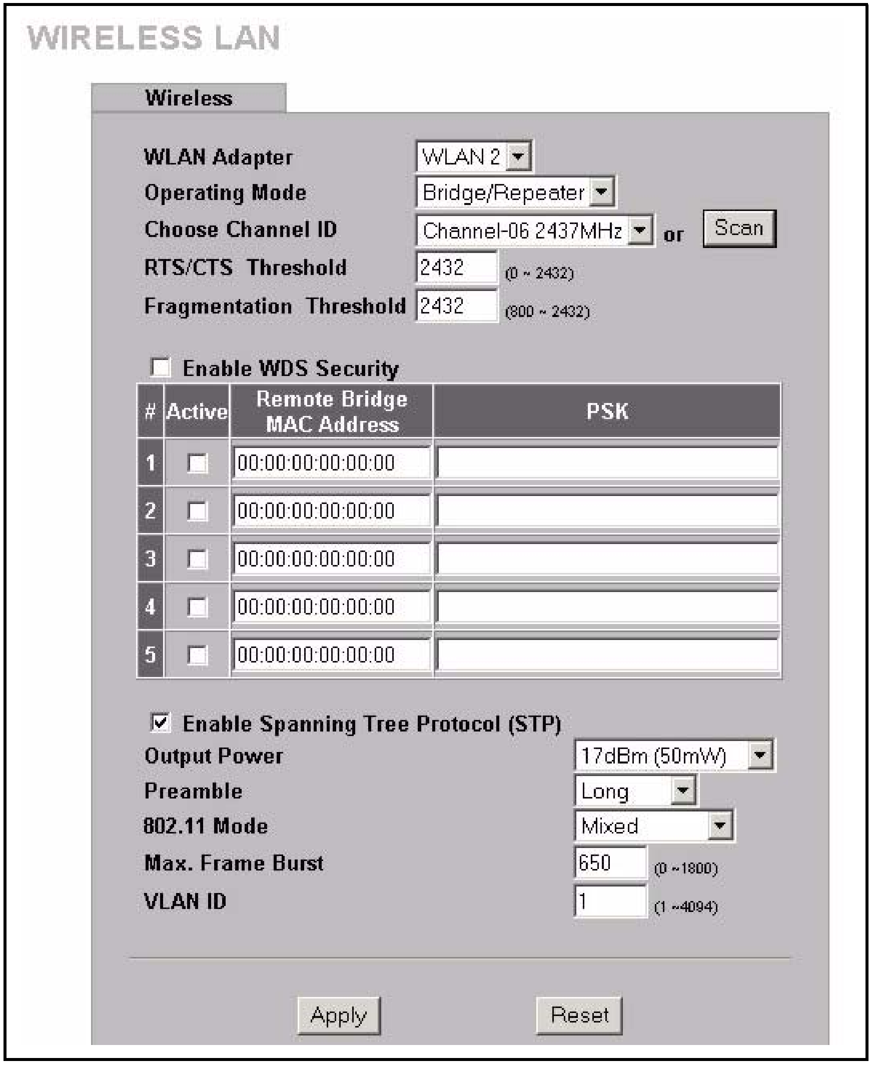
Figure 23 Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that you enable STP in the **Wireless** screen or your NOA-3570 is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

Click the **WIRELESS** link under **ADVANCED**. Select **Bridge/Repeater** in the **Operating Mode** drop-down list box to have the NOA-3570 act as a wireless bridge only.

Figure 24 Wireless: Bridge/Repeater



WIRELESS LAN

Wireless

WLAN Adapter	WLAN 2	
Operating Mode	Bridge/Repeater	
Choose Channel ID	Channel-06 2437MHz	or Scan
RTS/CTS Threshold	2432	(0 ~ 2432)
Fragmentation Threshold	2432	(800 ~ 2432)

□ Enable WDS Security

#	Active	Remote Bridge MAC Address	PSK
1	□	00:00:00:00:00:00	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	

☑ Enable Spanning Tree Protocol (STP)

Output Power	17dBm (50mW)	
Preamble	Long	
802.11 Mode	Mixed	
Max. Frame Burst	650	(0 ~1800)
VLAN ID	1	(1 ~4094)

The following table describes the labels in this screen that are specific to bridge/repeater mode.

Table 14 Wireless: Bridge/Repeater NOA-3570

LABEL	DESCRIPTIONS
WLAN Adapter	Select which WLAN adapter you want to configure. It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.
Operating Mode	Select **Bridge/Repeater** in this field to display the screen shown above.
Enable WDS Security	A Wireless Distribution System (WDS) is a wireless connection between two or more APs. Select the check box to use TKIP to encrypt traffic on the WDS between APs. When you enable WDS security, type a Pre-Shared Key (PSK) for each link. **Note:** Other APs must use the same encryption method in order to communicate with the NOA-3570 when you enable WDS security.

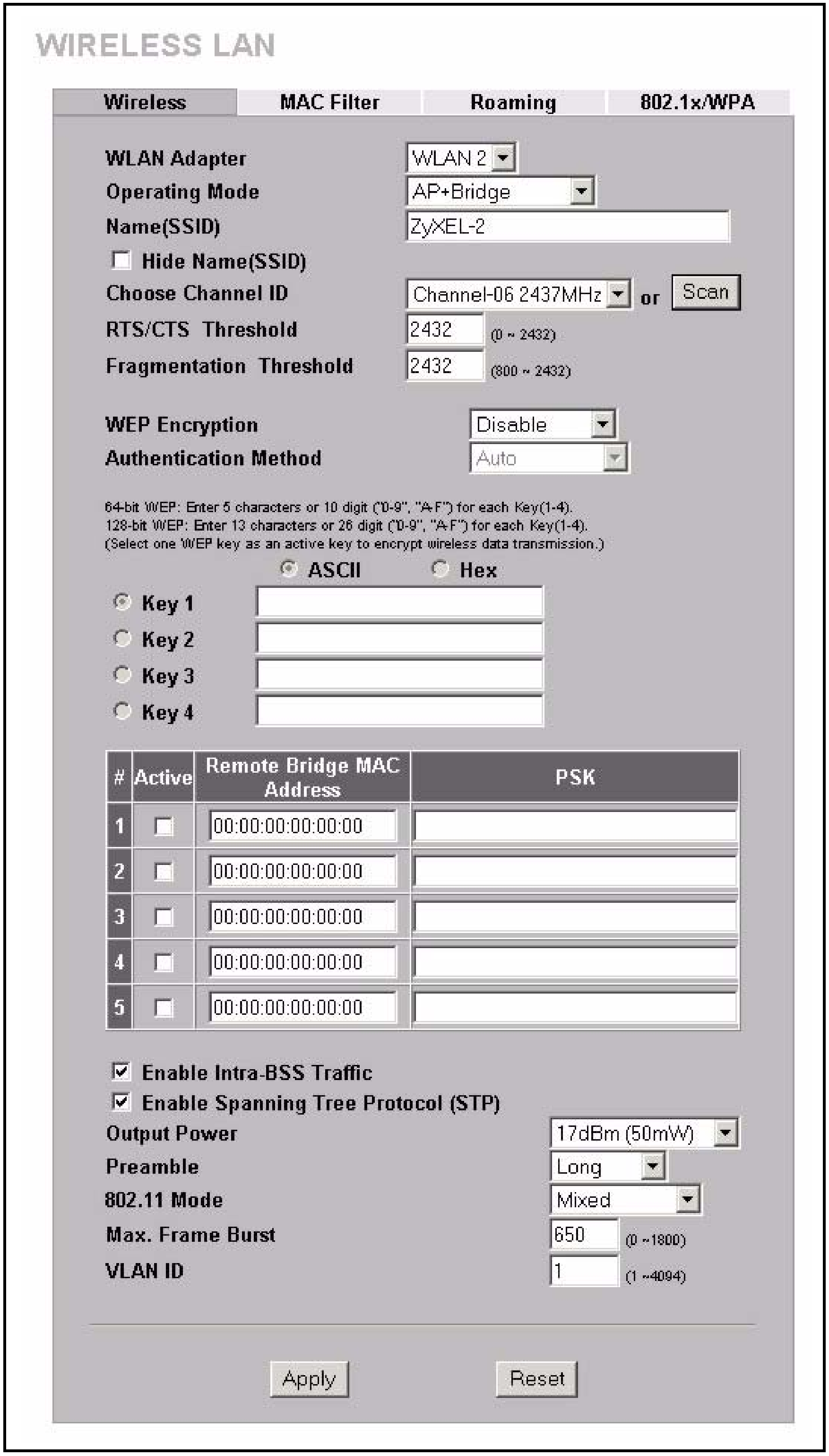
Table 14 Wireless: Bridge/Repeater NOA-3570

LABEL	DESCRIPTIONS
#	This is the index number of the bridge connection.
Active	Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.
Remote Bridge MAC Address	Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). When the NOA-3570 is in **Bridge/Repeater** mode, you don't have to enter a pre-shared key, but the traffic between devices won't be encrypted if you don't. The peer bridge must use the same pre-shared key and encryption method.
Enable Spanning Tree Protocol (STP)	Select the check box to activate STP on the NOA-3570.

5.5.3 AP+Bridge Mode

Click the **WIRELESS** link under **ADVANCED**. Select **AP+Bridge** in the **Operating Mode** drop-down list box to display the screen as shown next. In this screen, you can configure the NOA-3570 to function as an AP and bridge simultaneously. See the section on NOA-3570 applications for more information.

Figure 25 Wireless: AP+Bridge



WIRELESS LAN

WLAN Adapter: WLAN 2

Operating Mode: AP+Bridge

Name(SSID): ZyXEL-2

□ Hide Name(SSID)

Choose Channel ID: Channel-06 2437MHz or Scan

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (800 ~ 2432)

WEP Encryption: Disable

Authentication Method: Auto

64-bit WEP: Enter 5 characters or 10 digit ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 characters or 26 digit ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

● ASCII ○ Hex

● Key 1
○ Key 2
○ Key 3
○ Key 4

#	Active	Remote Bridge MAC Address	PSK
1	□	00:00:00:00:00:00	
2	□	00:00:00:00:00:00	
3	□	00:00:00:00:00:00	
4	□	00:00:00:00:00:00	
5	□	00:00:00:00:00:00	

☑ Enable Intra-BSS Traffic

☑ Enable Spanning Tree Protocol (STP)

Output Power: 17dBm (50mW)

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 650 (0 ~1800)

VLAN ID: 1 (1 ~4094)

See Table 13 on page 60 and Table 14 on page 64 descriptions of the fields in the **Access Point** and **Bridge/Repeater** operating modes for descriptions of the fields in this screen.

When you enable WEP encryption, you can also specify MAC addresses and pre-shared keys of peer bridges in order to use TKIP (see Appendix F on page 221 for more on TKIP) to encrypt traffic between the bridges.

Note: The following screens are configurable only in Access Point and AP+Bridge operating modes.

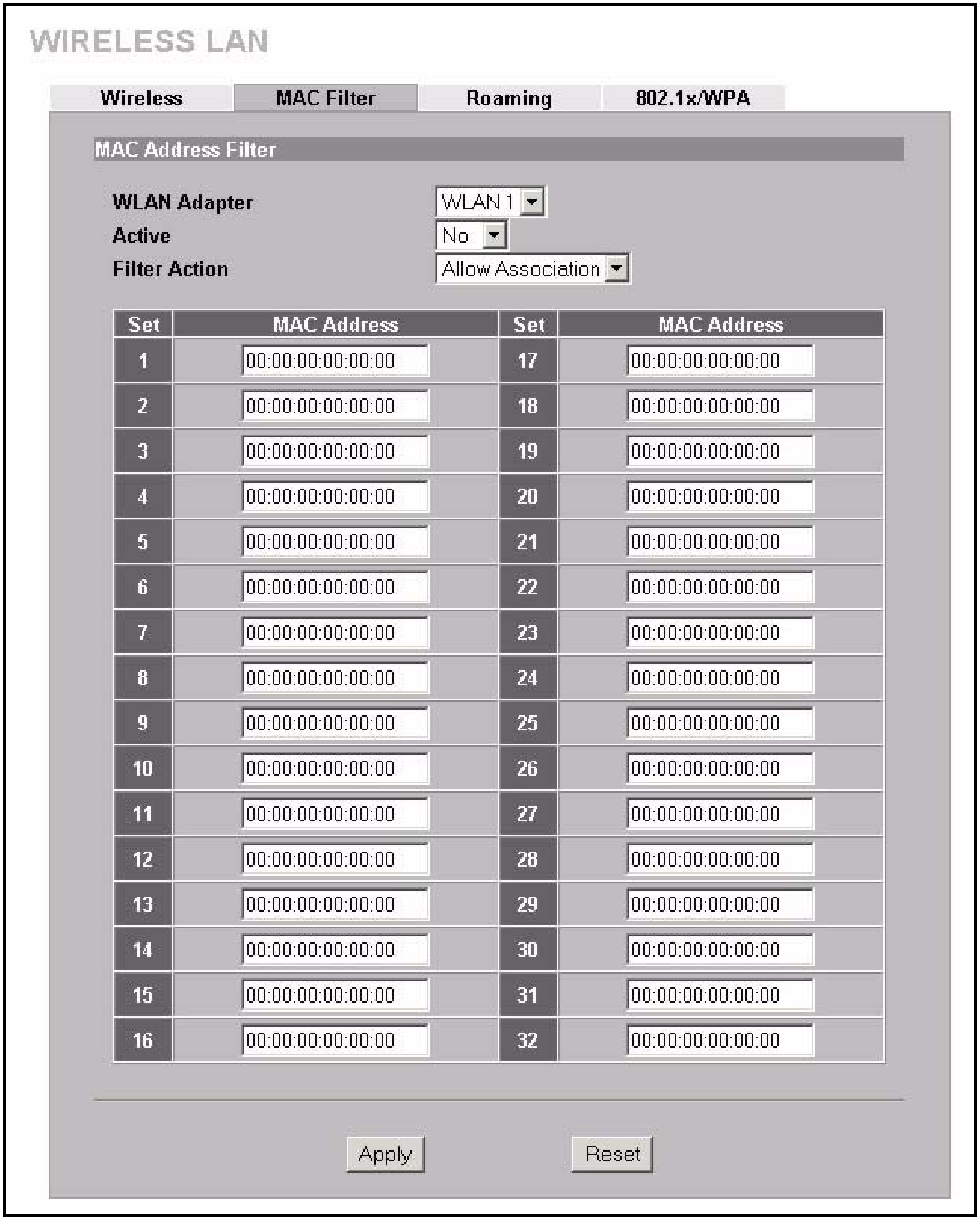
5.6 Configuring MAC Filters

The MAC filter screen allows you to configure the NOA-3570 to give exclusive access to up to 32 devices (**Allow Association**) or exclude up to 32 devices from accessing the NOA-3570 (**Deny Association**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your NOA-3570's MAC filter settings, click the **WIRELESS** link under **ADVANCED** and then the **MAC Filter** tab. The screen appears as shown.

Note: Be careful not to list your computer's MAC address and set the **Action** field to **Deny Association** when managing the NOA-3570 via a wireless connection. This would lock you out.

Figure 26 MAC Address Filter



MAC Address Filter

WLAN Adapter	WLAN 1
Active	No
Filter Action	Allow Association

Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

The following table describes the labels in this screen.

Table 15 MAC Address Filter NOA-3570

LABEL	DESCRIPTION
WLAN Adapter	Select the WLAN adapter for which you want to configure MAC address filtering.
Active	Select **Yes** from the drop down list box to enable MAC address filtering.

Table 15 MAC Address Filter NOA-3570

LABEL	DESCRIPTION
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the NOA-3570 in these address fields.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

5.7 Configuring Roaming

A wireless station is a device with an IEEE 802.11b or an IEEE 802.11g compliant wireless interface. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

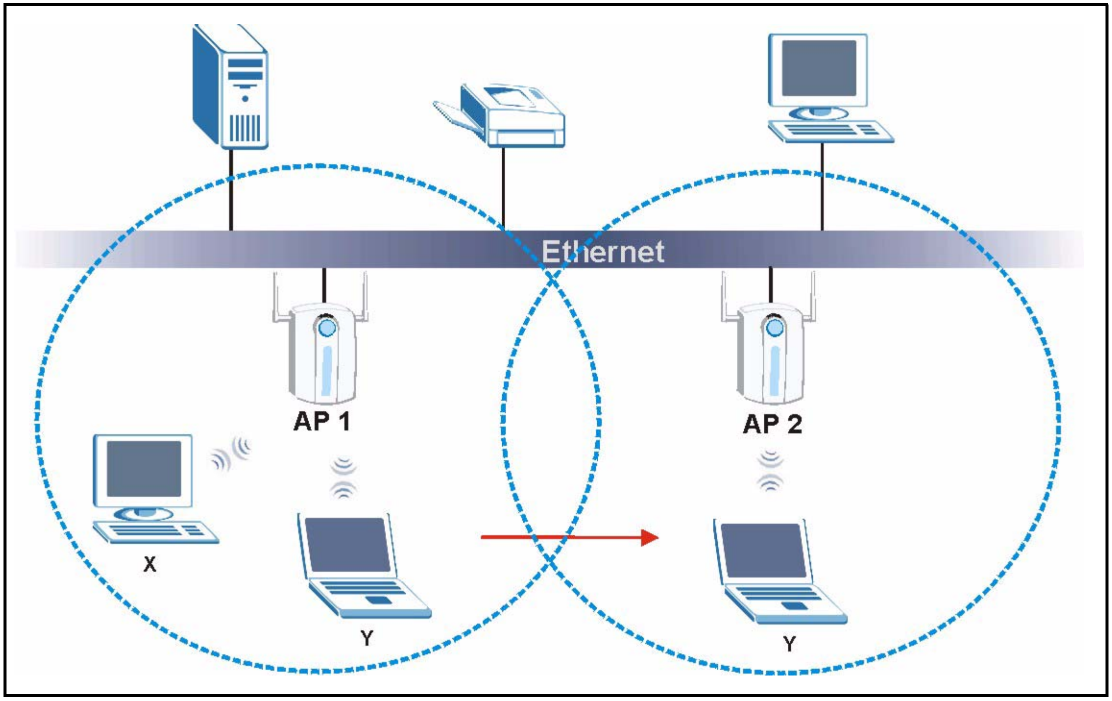
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in Figure 27 on page 70.

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this). IEEE 802.1x authentication information is not exchanged (at the time of writing).

Figure 27 Roaming Example



The steps below describe the roaming process.

1 As wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point

2 **AP 2**, it scans and uses the signal of access point **AP 2**.

3 Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.

4 Access point **AP 1** updates the new position of wireless station.

5 Wireless station **Y** sends a request to access point **AP 2** for reauthentication.

5.7.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1 All the access points must be on the same subnet and configured with the same SSID.

2 If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.

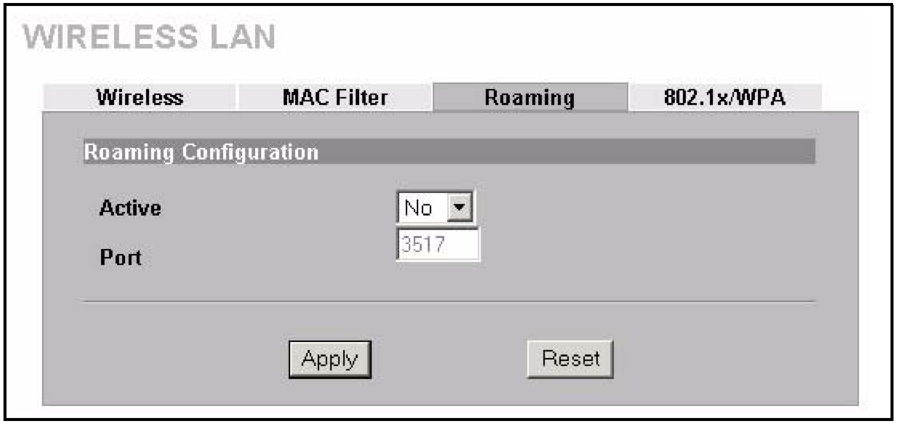
3 The adjacent access points should use different radio channels when their coverage areas overlap.

4 All access points must use the same port number to relay roaming information.

5 The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your NOA-3570, click the **WIRELESS** link under **ADVANCED** and then the **Roaming** tab. The screen appears as shown.

Figure 28 Roaming



Roaming Configuration

Active: No

Port: 3517

The following table describes the labels in this screen.

Table 16 Roaming

LABEL	DESCRIPTION
Active	Select **Yes** from the drop-down list box to enable roaming on the NOA-3570 if you have two or more APs on the same subnet. **Note:** All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Port	Enter the port number to communicate roaming information between access points. The port number must be the same on all access points. The default is 3517. Make sure this port is not used by other services.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

5.8 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption.

5.9 WPA-PSK Application Example

A WPA-PSK application looks as follows.

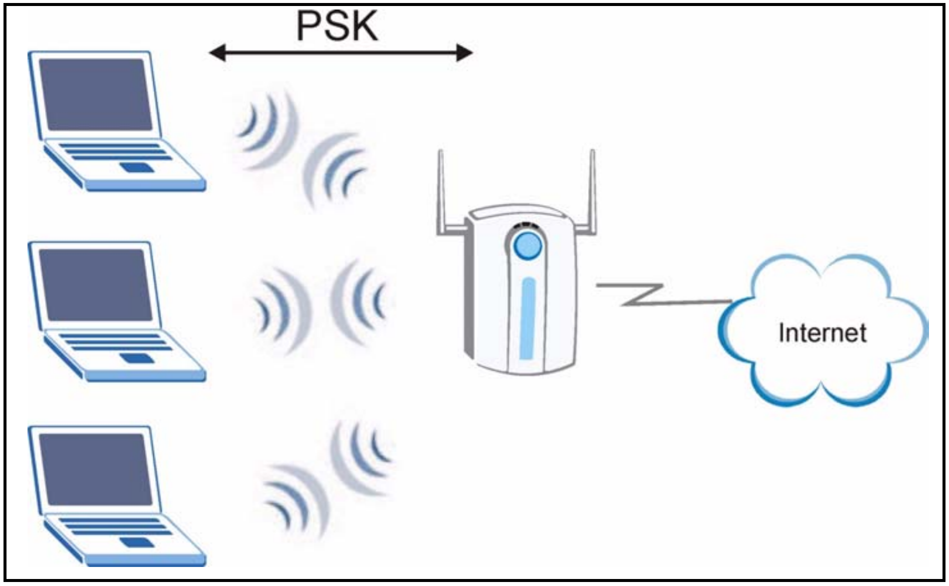
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).

2 The AP checks each client's password and (only) allows it to join the network if it matches its password.

3 The AP derives and distributes keys to the wireless clients.

4 The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

Figure 29 WPA - PSK Authentication



5.10 WPA with RADIUS Application Example

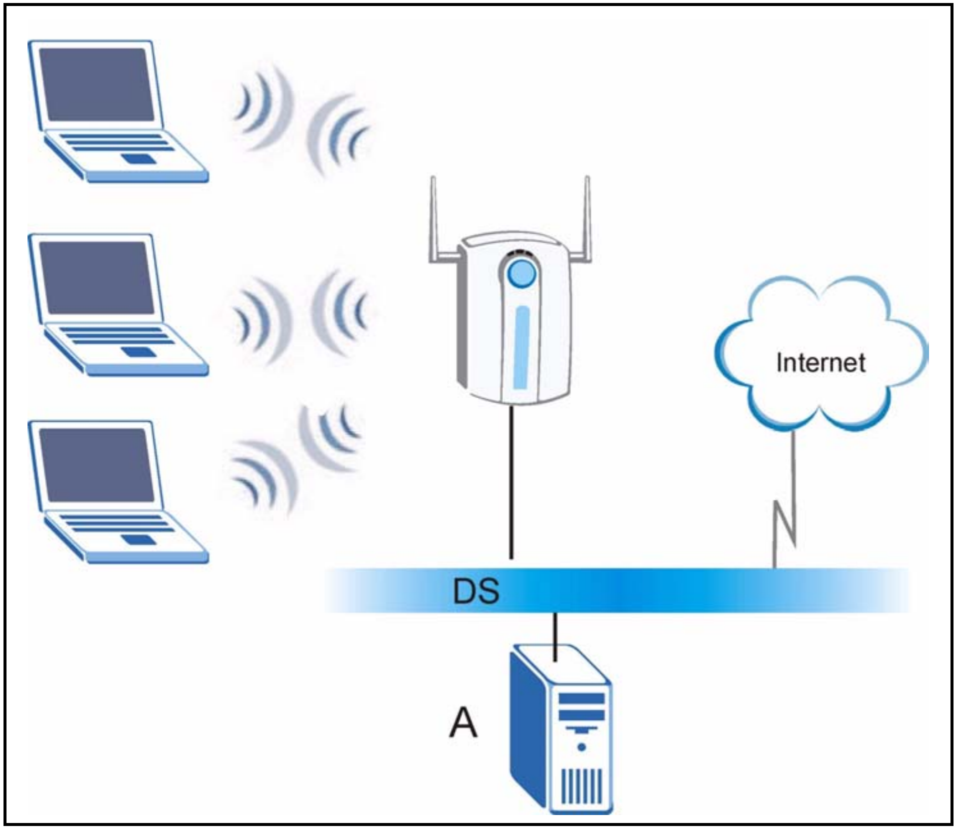
This example is for using WPA with an external RADIUS server. You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1 The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 30 WPA with RADIUS Application Example



5.11 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

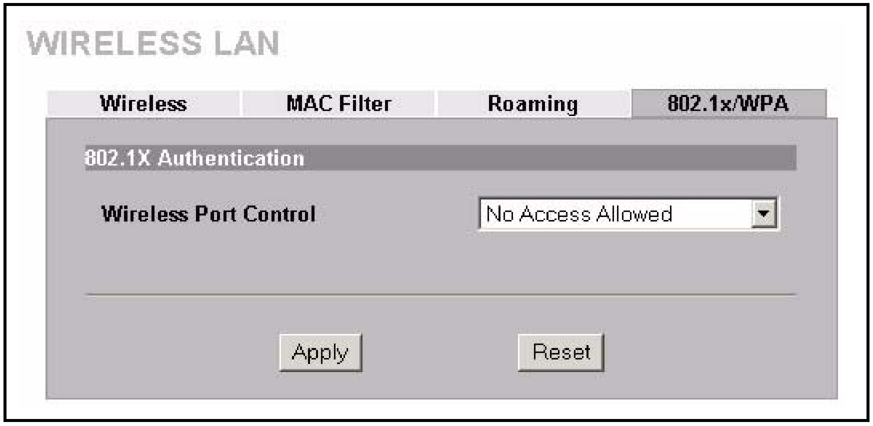
The Funk Software's Odyssey client is bundled free (at the time of writing) with some of ZyXEL’s client wireless adapter(s).

5.12 Configuring 802.1x and WPA

To change your NOA-3570’s authentication settings, click the **WIRELESS** link under **ADVANCED** and then the **802.1x/WPA** tab. The screen varies by the key management protocol you select. The WPA function is not available on all NOA-3570 models.

You see the next screen when you select **No Access Allowed** or **No Authentication Required** in the **Wireless Port Control** field.

Figure 31 Wireless LAN: 802.1x/WPA



802.1X Authentication

Wireless Port Control: No Access Allowed

The following table describes the labels in this screen.

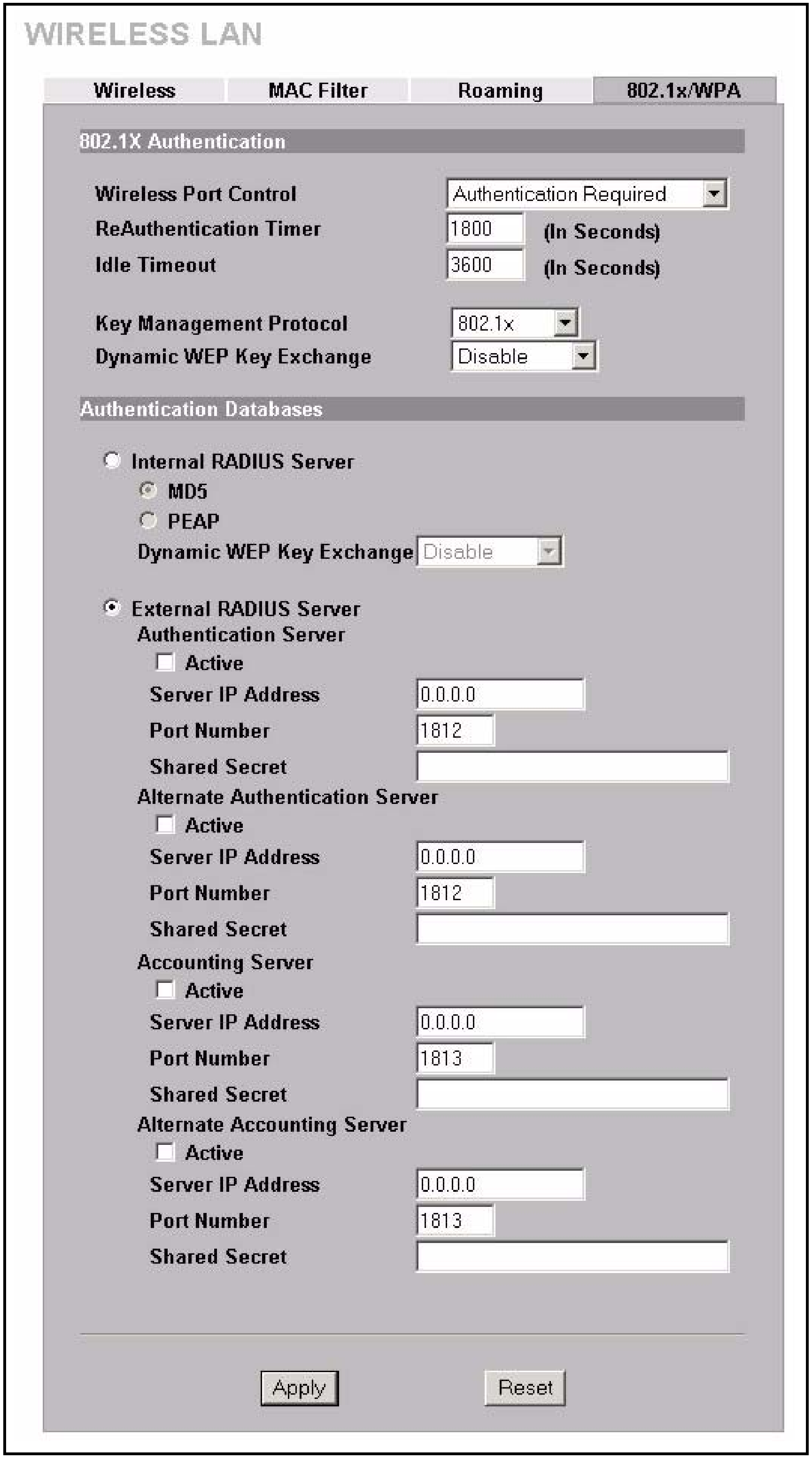
Table 17 Wireless LAN: 802.1x/WPA

LABEL	DESCRIPTION
Wireless Port Control	To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Access Allowed**, **No Authentication Required** and **Authentication Required**. **No Access Allowed** blocks all wireless stations access to the wired network. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **Authentication Required** to configure **Key Management Protocol** and other related fields.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

5.13 Authentication Required: 802.1x

Select **Authentication Required** in the **Wireless Port Control** field and **802.1x** in the **Key Management Protocol** field to display the next screen.

Figure 32 Wireless LAN: 802.1x/WPA for 802.1x Protocol



802.1X Authentication

Wireless Port Control	Authentication Required
ReAuthentication Timer	1800 (In Seconds)
Idle Timeout	3600 (In Seconds)
Key Management Protocol	802.1x
Dynamic WEP Key Exchange	Disable

Authentication Databases

○ Internal RADIUS Server
● MD5
○ PEAP
Dynamic WEP Key Exchange: Disable

● External RADIUS Server

Authentication Server
□ Active

Server IP Address	0.0.0.0
Port Number	1812
Shared Secret	

Alternate Authentication Server
□ Active

Server IP Address	0.0.0.0
Port Number	1812
Shared Secret	

Accounting Server
□ Active

Server IP Address	0.0.0.0
Port Number	1813
Shared Secret	

Alternate Accounting Server
□ Active

Server IP Address	0.0.0.0
Port Number	1813
Shared Secret	

The following table describes the labels in this screen.

Table 18 Wireless LAN: 802.1x/WPA for 802.1x Protocol NOA-3570

LABEL	DESCRIPTION
Wireless Port Control	To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Authentication Required**, **Authentication Required** and **No Access Allowed**. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. **No Access Allowed** blocks all wireless stations access to the wired network. The following fields are only available when you select **Authentication Required**.
ReAuthentication Timer (In Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). **Note:** If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (In Seconds)	The NOA-3570 automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).
Key Management Protocol	Choose **802.1x** from the drop-down list.
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**.
Authentication Databases	The authentication database contains wireless station login information.
Internal RADIUS Server	Select this radio button to use the NOA-3570’s **Internal RADIUS Server**. Select the **MD5** radio button to use this EAP authentication type to authenticate other APs or wireless clients in other wireless networks. Select the **PEAP** radio button to use this EAP authentication type to authenticate other APs or wireless clients in other wireless networks. Use the drop-down list box to select **Disable**, **64-bit WEP** or **128-bit WEP** for Dynamic WEP Exchange. **Note:** MD5 cannot be used with Dynamic WEP Key Exchange.
External RADIUS Server	Select the radio button to use an external radius server to authenticate the NOA-3570’s wireless clients. Configure the server(s) details in the following fields.

Table 18 Wireless LAN: 802.1x/WPA for 802.1x Protocol NOA-3570

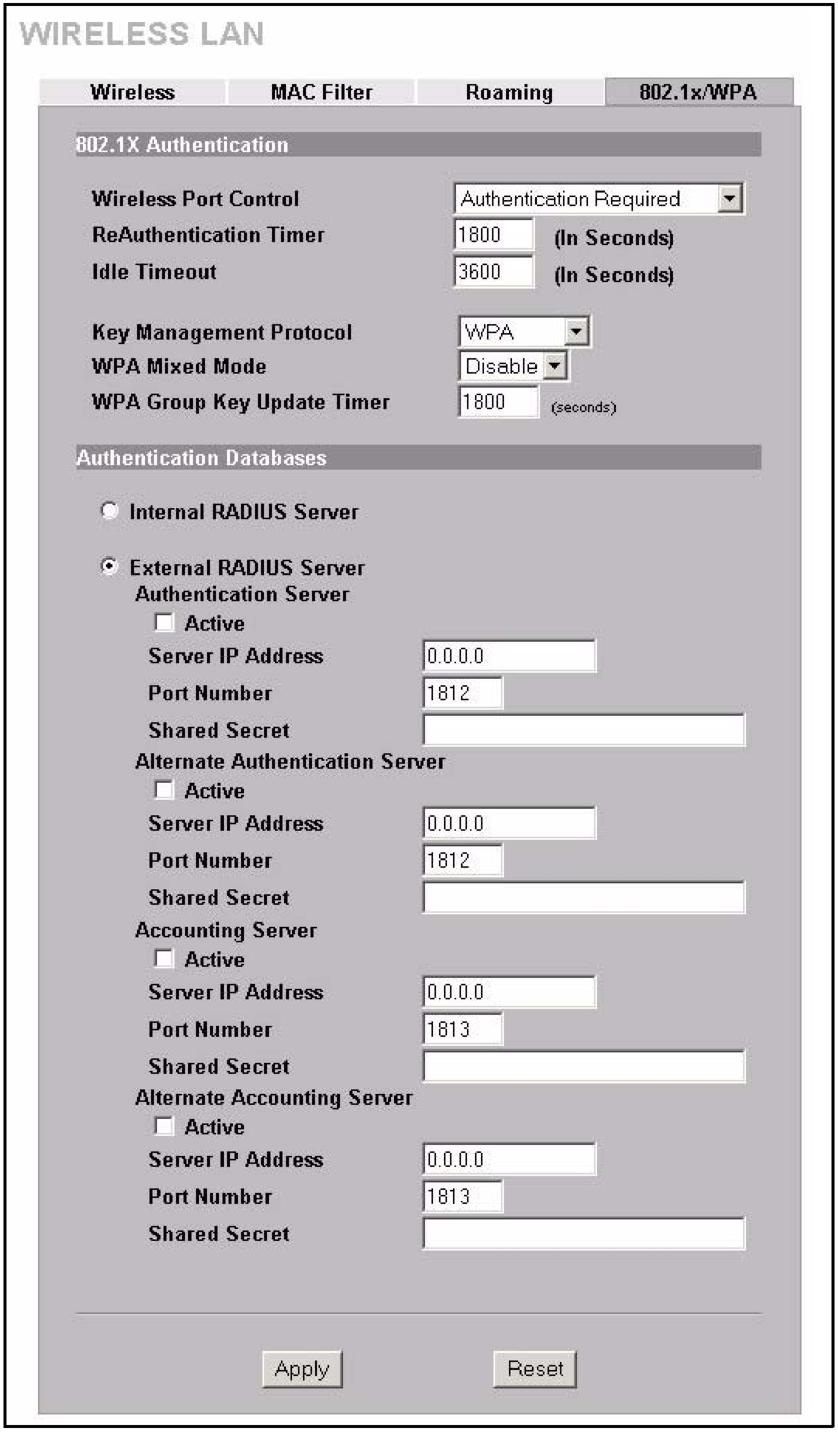
LABEL	DESCRIPTION
Authentication Server /Alternate	The NOA-3570 will make three attempts to authenticate wireless users using the authentication server before attempting to use the alternate authentication server. Requests can be issued from the client interface to use the alternate authentication server. The length of time for each authentication is decided by the wireless client or based on the configuration of the **ReAuthentication Timer** field. **Note:** You can use the command line interface to configure the NOA-3570 to use up to four alternate authentication servers.
Active	Select **Active** to enable user authentication through this external authentication server. Clear the **Active** check box to not use this to not perform user authentication through this external authentication server.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the NOA-3570. The key must be the same on the external authentication server and your NOA-3570. The key is not sent over the network.
Accounting Server /Alternate	The NOA-3570 will make three attempts to communicate with the accounting server before attempting to use the alternate accounting server. **Note:** You can use the command line interface to configure the NOA-3570 to use up to four alternate accounting servers.
Active	Select **Active** to enable user accounting through this external accounting server. Clear the **Active** check box to not use this to not perform user accounting through this external accounting server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the NOA-3570. The key must be the same on the external accounting server and your NOA-3570. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

Note: If you enable the NOA-3570's internal RADIUS server, configure trusted user accounts in the **AUTH SERVER Trusted Users** screen.

5.14 Authentication Required: WPA

Select **Authentication Required** in the **Wireless Port Control** field and **WPA** in the **Key Management Protocol** field to display the next screen.

Figure 33 Wireless LAN: 802.1x/WPA for WPA Protocol



802.1X Authentication

Wireless Port Control: Authentication Required
ReAuthentication Timer: 1800 (In Seconds)
Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA
WPA Mixed Mode: Disable
WPA Group Key Update Timer: 1800 (seconds)

Authentication Databases

○ Internal RADIUS Server

● External RADIUS Server

Authentication Server
□ Active
Server IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Alternate Authentication Server
□ Active
Server IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Accounting Server
□ Active
Server IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:

Alternate Accounting Server
□ Active
Server IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:

The following table describes the labels not previously discussed.

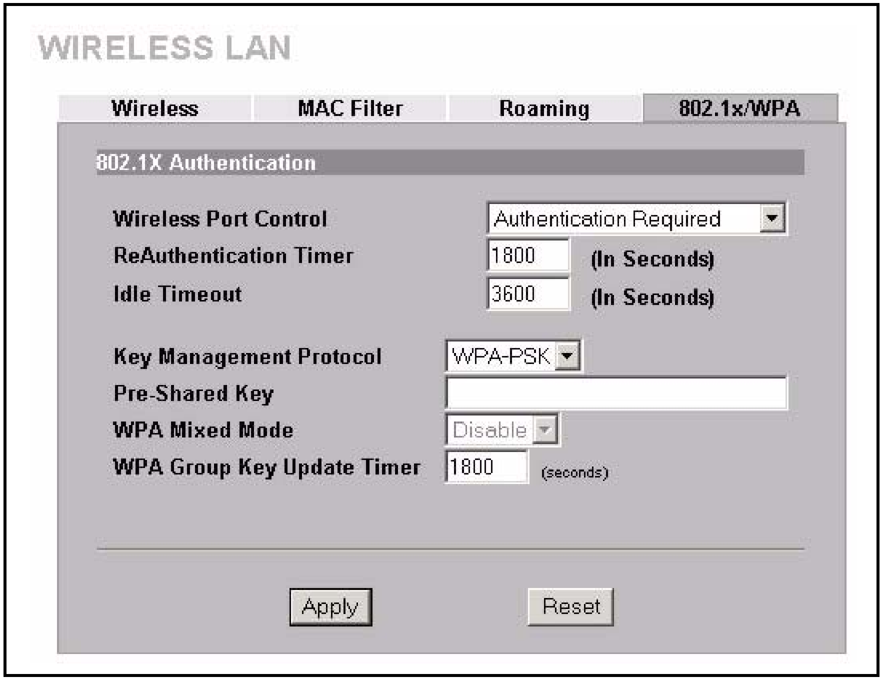
Table 19 Wireless LAN: 802.1x/WPA for WPA Protocol

LABEL	DESCRIPTIONS
Key Management Protocol	Choose **WPA** in this field.
WPA Mixed Mode	The NOA-3570 can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with IEEE 802.1x in the same Wi-Fi network. Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable**.
WPA Group Key Update Timer	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The NOA-3570 default is 1800 seconds (30 minutes).
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

5.15 Authentication Required: WPA-PSK

Select **Authentication Required** in the **Wireless Port Control** field and **WPA-PSK** in the **Key Management Protocol** field to display the next screen.

Figure 34 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol



WIRELESS LAN

802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: WPA-PSK

Pre-Shared Key:

WPA Mixed Mode: Disable

WPA Group Key Update Timer: 1800 (seconds)

The following table describes the labels not previously discussed.

Table 20 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

LABEL	DESCRIPTION
Key Management Protocol	Choose **WPA-PSK** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 6
Internal RADIUS Server

The NOA-3570 can use its internal RADIUS server to authenticate wireless clients. It can also serve as a RADIUS server to authenticate other APs and their wireless clients. For more background information on RADIUS, see the *Introduction to RADIUS* section.

6.1 Internal RADIUS Overview

The NOA-3570 has a built-in RADIUS server that can authenticate wireless clients or other APs (that are configured as trusted APs).

The NOA-3570 can function as an AP and as a RADIUS server at the same time.

PEAP (Protected EAP) and MD5 authentication is implemented on the internal RADIUS server using simple username and password methods over a secure TLS connection. See the appendices for more information on the types of EAP authentication and the internal RADIUS authentication method used in your NOA-3570.

Figure 35 NOA-3570 Authenticates Wireless Stations

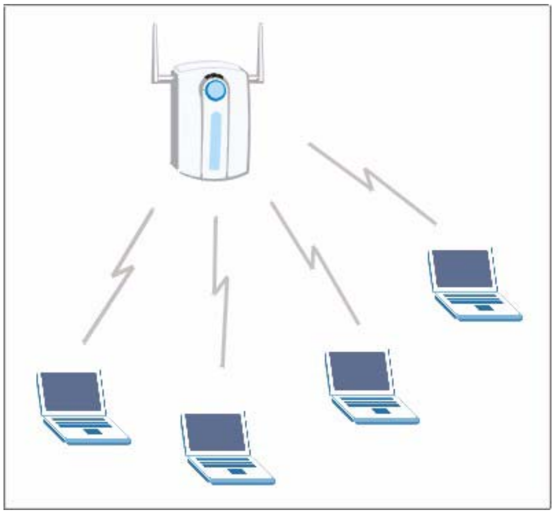


Figure 36 NOA-3570 Authenticates Trusted APs

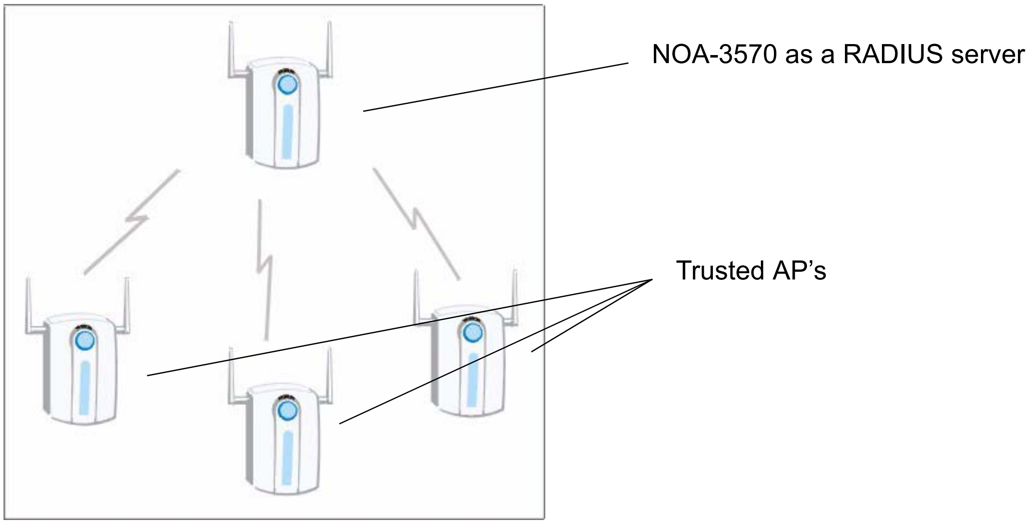


Table 21 Internal RADIUS Server Screens Overview

LABEL	DESCRIPTION
Setting	Use the **Setting** screen to turn the NOA-3570’s internal RADIUS server off or on and to view information about the NOA-3570’s certificates.
Trusted AP	Use the **Trusted AP** screen to specify APs as trusted APs so they can use the NOA-3570’s internal RADIUS server to authenticate wireless clients. You can set up to 31 trusted AP’s.
Trusted Users	Use the **Trusted Users** screen to configure a list of wireless client user names and passwords for the NOA-3570 to authenticate. The NOA-3570 internal RADIUS server can authenticate up to 32 wireless clients.

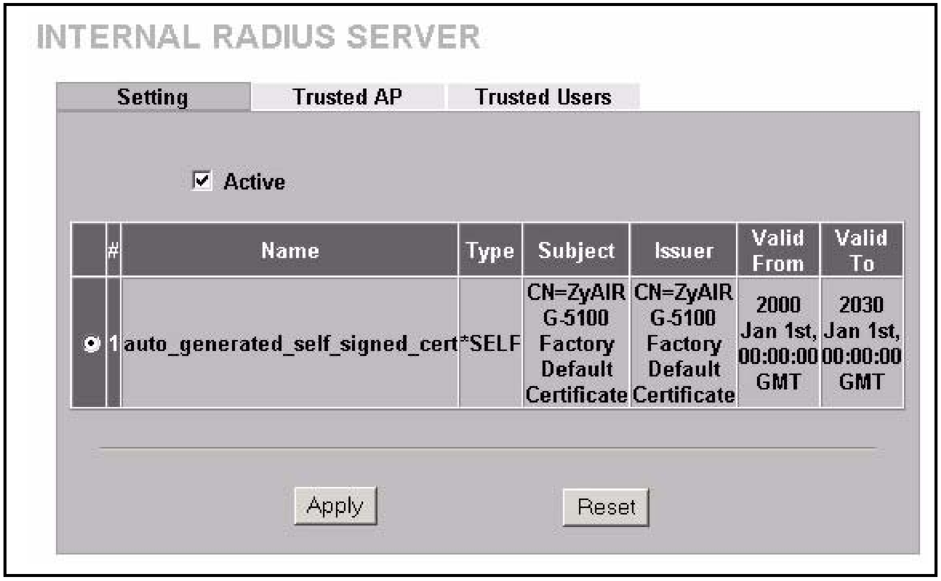
6.2 Internal RADIUS Server Setting

The **INTERNAL RADIUS SERVER Setting** screen displays information about certificates. The certificates are used by wireless clients to authenticate the RADIUS server. Information matching the certificate is held on the wireless clients utility, for example, Funk Software’s Odyssey client. A password and user name on the utility must match the **Trusted Users** list so that the RADIUS server can be authenticated.

Note: The internal RADIUS server does not support domain accounts (DOMAIN/ user). When you configure your Windows XP SP2 Wireless Zero Configuration PEAP/ MS-CHAPv2 settings, deselect the **Use Windows logon name and password** check box. When authentication begins, a pop-up dialog box requests you to type a **Name**, **Password** and **Domain** of the RADIUS server. Specify a name and password only, do not specify a domain.

Click the **AUTH SERVER** link under **ADVANCED** and then the **Setting** tab. The screen appears as shown.

Figure 37 Internal RADIUS Server Setting Screen



☑ Active

	#	Name	Type	Subject	Issuer	Valid From	Valid To
●	1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-5100 Factory Default Certificate	CN=ZyAIR G-5100 Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

The following table describes the labels in this screen.

Table 22 My CertificatesNOA-3570

LABEL	DESCRIPTION
Active	Select the **Active** check box to have the NOA-3570 use its internal RADIUS server to authenticate wireless clients or other APs.
#	This field displays the certificate index number. The certificates are listed in alphabetical order. Use the **CERTIFICATES** screens to manage certificates. The internal RADIUS server uses one of the certificates listed in this screen to authenticate each wireless client. The exact certificate used, depends on the certificate information configured on the wireless client.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. **auto_generated_self_signed_cert** is the factory default certificate common to all NOA-3570’s that use certificates. **Note:** ZyXEL recommends that you replace the factory default certificate with one that uses your NOA-3570's MAC address. Do this when you first log in to the NOA-3570 or in the **CERTIFICATES My Certificates** screen.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the NOA-3570 uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate’s owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.

Table 22 My CertificatesNOA-3570

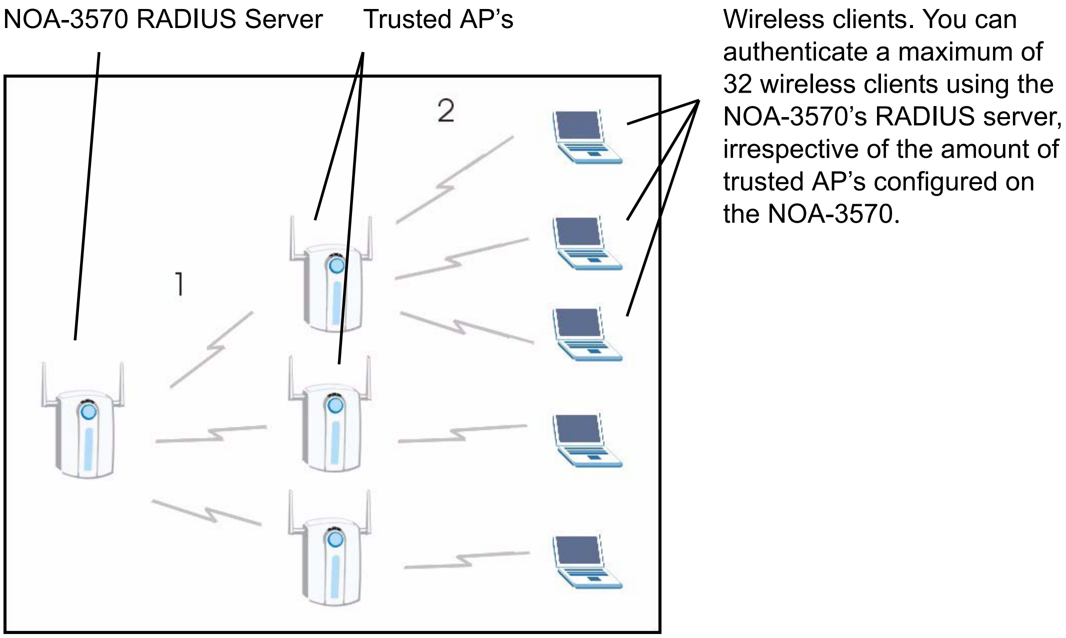
LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Apply	Click **Apply** to have the NOA-3570 use certificates to authenticate wireless clients.
Reset	Click **Reset** to start configuring this screen afresh.

6.3 Trusted AP Overview

A trusted AP is an AP that uses the NOA-3570's internal RADIUS server to authenticate its wireless clients. Each wireless client must have a user name and password configured in the **Trusted Users** screen.

The following figure shows how this is done in two phases.

Figure 38 Trusted AP Overview


NOA-3570 RADIUS Server
Trusted AP's
Wireless clients. You can authenticate a maximum of 32 wireless clients using the NOA-3570's RADIUS server, irrespective of the amount of trusted AP's configured on the NOA-3570.
2
1

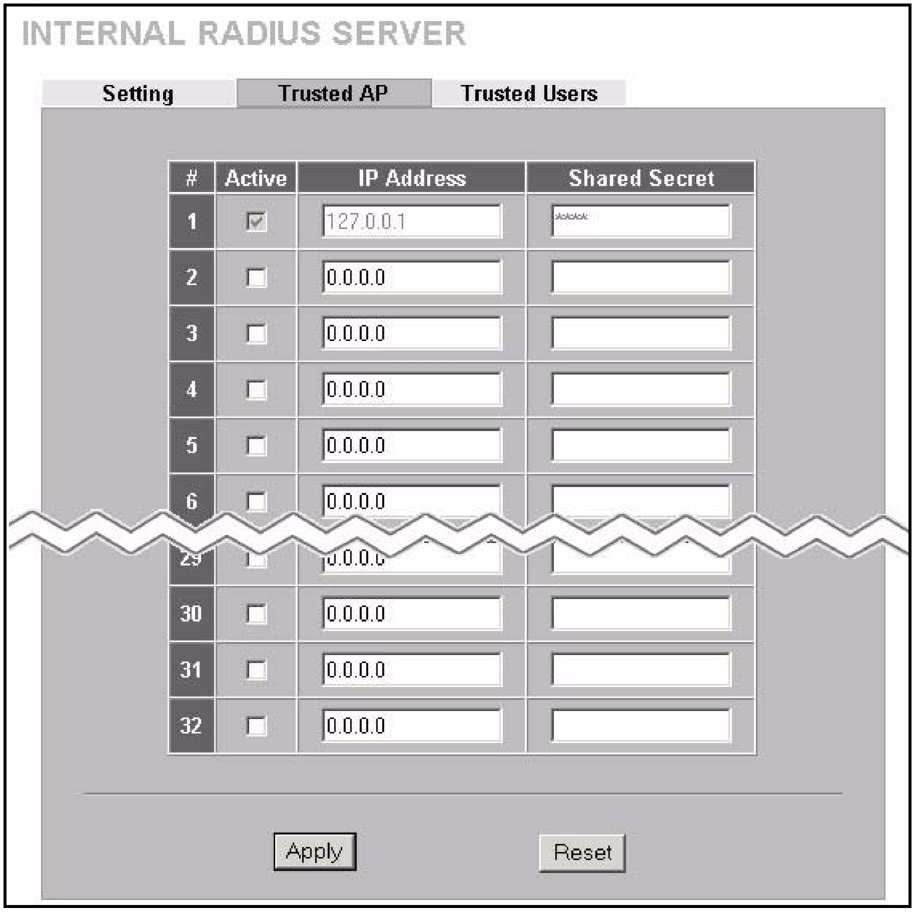
1 Configure an IP address and shared secret in the **Trusted AP** database to authenticate an AP as a trusted AP.

2 Configure wireless client user names and passwords in the **Trusted Users** database to use a trusted AP as a relay between the NOA-3570's internal RADIUS server and the wireless clients. The wireless clients can then be authenticated by the NOA-3570's internal RADIUS server.

6.4 Configuring Trusted AP

To specify APs as trusted APs so they can use the NOA-3570's internal RADIUS server to authenticate wireless clients, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted AP** tab. The screen appears as shown.

Figure 39 Trusted AP Screen



#	Active	IP Address	Shared Secret
1	☑	127.0.0.1	****
2	□	0.0.0.0	
3	□	0.0.0.0	
4	□	0.0.0.0	
5	□	0.0.0.0	
6	□	0.0.0.0	
29	□	0.0.0.0	
30	□	0.0.0.0	
31	□	0.0.0.0	
32	□	0.0.0.0	

The following table describes the labels in this screen.

Table 23 Trusted AP

LABEL	DESCRIPTION
#	This field displays the trusted AP index number.
Active	Select this check box to have the NOA-3570 use the **IP Address** and **Shared Secret** to authenticate a trusted AP.

Table 23 Trusted AP

LABEL	DESCRIPTION
IP Address	Type the IP address of the trusted AP in dotted decimal notation.
Shared Secret	Enter a password (up to 31 alphanumeric characters, no spaces) as the key for encrypting communications between the AP and the NOA-3570. The key is not sent over the network. This key must be the same on the AP and the NOA-3570. Both the NOA-3570's IP address and this shared secret must also be configured in the "external RADIUS" server fields of the trusted AP. **Note:** The first trusted AP fields are for the NOA-3570 itself. Use SMT menu 23.2 to configure them.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

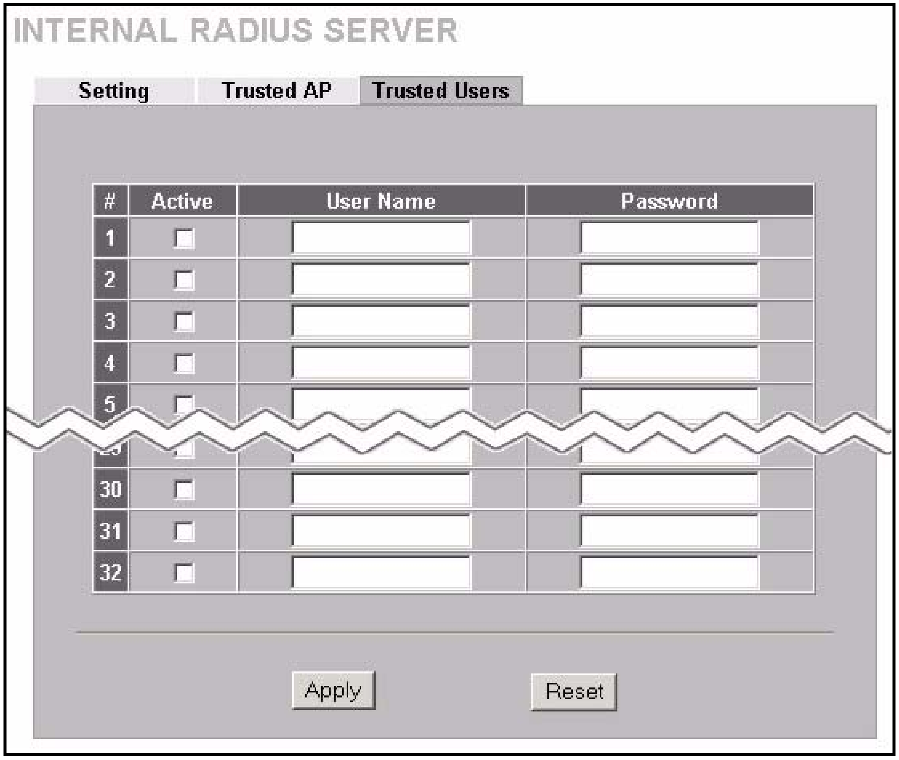
6.5 Trusted Users Overview

A trusted user entry consists of a wireless client user name and password

6.6 Configuring Trusted Users

To configure trusted user entries, click the **AUTH SERVER** link under **ADVANCED** and then the **Trusted Users** tab. The screen appears as shown.

Figure 40 Trusted Users Screen



INTERNAL RADIUS SERVER

#	Active	User Name	Password
1	□		
2	□		
3	□		
4	□		
5	□		
30	□		
31	□		
32	□		

The following table describes the labels in this screen.

Table 24 Trusted Users

LABEL	DESCRIPTION
#	This field displays the trusted user index number.
Active	Select this check box to have the NOA-3570 authenticate wireless clients with the same user name and password activated on their wireless utilities.
User Name	Enter the user name for this user account. This name can be up to 31 alphanumeric characters long, including spaces. The wireless client’s utility must use this name as its login name.
Password	Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. The password on the wireless client’s utility must be the same as this password. **Note:** If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 7 VLAN

This chapter discusses how to configure VLAN on the NOA-3570

7.1 VLAN

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network can belong to one or more groups. Only stations within the same group can talk to each other.

The NOA-3570 supports IEEE 802.1q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The NOA-3570 can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.

7.1.1 Management VLAN ID

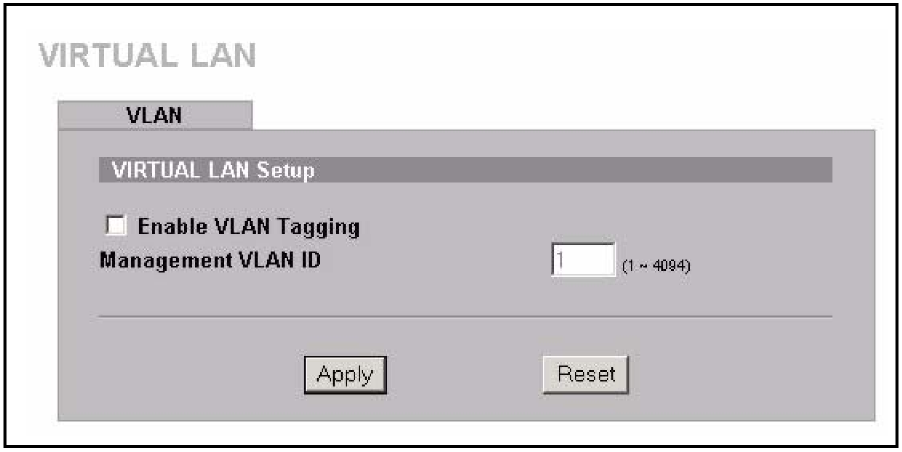
The management VLAN ID identifies the "management VLAN". A computer must be a member of this "management VLAN" in order to access and manage the NOA-3570. A computer that is not a member of this VLAN, then that device cannot manage the NOA-3570.

If no devices are in the management VLAN, then you will only be able to access the NOA-3570 through the console port (not through the network).

7.2 Configuring VLAN

Click **ADVANCED** and then **VLAN**. The screen appears as shown next.

Figure 41 VLAN



VIRTUAL LAN

The following table describes the labels in this screen.

Table 25 VLAN

LABEL	DESCRIPTION
Enable VLAN Tagging	Select this check box to turn on VLAN tagging. Use the **Wireless** screen to set the VLAN ID tag that the NOA-3570 adds to the Ethernet frames that a WLAN adapter receives from wireless clients or APs.
Management VLAN ID	Enter a number from 1 to 4094 to define this VLAN group. Your management computer must belong to this VLAN group in order to manage the NOA-3570. This can be done in the following ways: • The management computer could be a wireless client of the NOA-3570 if the NOA-3570's WLAN adapter is set to add the add the management VLAN ID tag to Ethernet frames received from wireless clients. • The management computer could be on the wired network, behind a VLAN-aware switch that is configured to add the management VLAN ID tag to Ethernet frames from the computer before sending them to NOA-3570. **Note:** Mail and FTP servers must have the same management VLAN ID to communicate with the NOA-3570.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 8
IP Screen

This chapter discusses how to configure IP on the NOA-3570

8.1 Factory Ethernet Defaults

The Ethernet parameters of the NOA-3570 are preset in the factory with the following values:

1. IP address of 192.168.1.2
2. Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

8.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your NOA-3570, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NOA-3570 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the NOA-3570 unless you are instructed to do otherwise.

8.2.1 IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 26 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

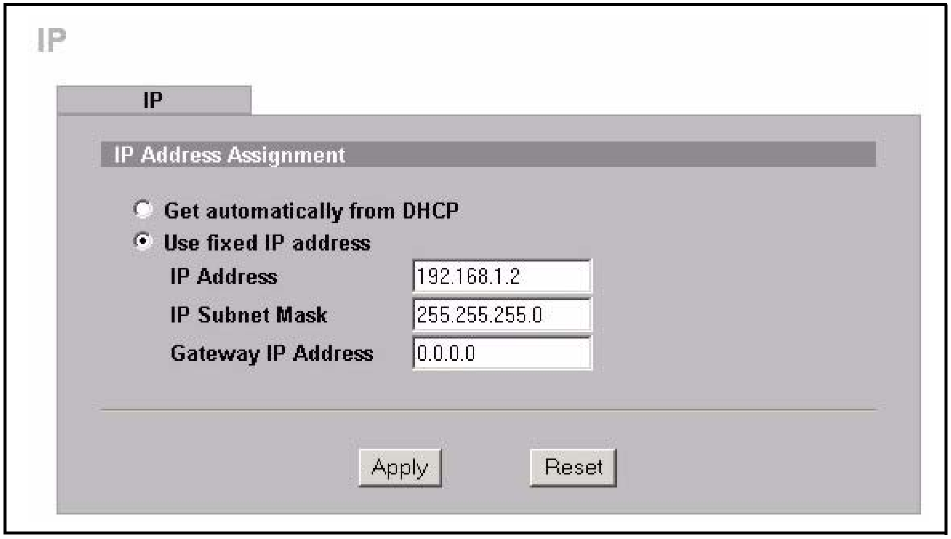
You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

8.3 Configuring IP

Click **ADVANCED** and then **IP** to display the screen shown next.

Figure 42 IP Setup



IP

IP Address Assignment

○ Get automatically from DHCP

● Use fixed IP address

IP Address: 192.168.1.2

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 0.0.0.0

The following table describes the labels in this screen.

Table 27 IP Setup NOA-3570

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option to have the NOA-3570 use a dynamically assigned IP address from a DHCP server. **Note:** You must know the IP address assigned to the NOA-3570 (by the DHCP server) to access the NOA-3570 again.
Use fixed IP address	Select this option if your NOA-3570 is using a static IP address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your NOA-3570 in dotted decimal notation. **Note:** If you change the NOA-3570's IP address, you must use the new IP address if you want to access the web configurator again.
IP Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is a router or switch on the same network segment as the NOA-3570. The gateway helps forward packets to their destinations. Leave this field as 0.0.0.0 if you do not know it.
Apply	Click **Apply** to save your changes back to the NOA-3570.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 9
Certificates

This chapter gives background information about public-key certificates and explains how to use them.

9.1 Certificates Overview

The NOA-3570 can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner’s identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the NOA-3570 to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim’s public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny’s public key to decrypt the message.

The NOA-3570 uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority’s public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The NOA-3570 does not trust a certificate if any certificate on its path has expired or been revoked.

9.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The NOA-3570 only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

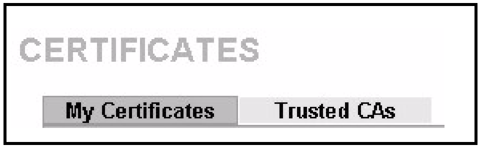
9.2 Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the NOA-3570 act as a certification authority and sign its own certificates.

9.3 Configuration Summary

This section summarizes how to manage certificates on the NOA-3570.

Figure 43 Certificate Configuration Overview



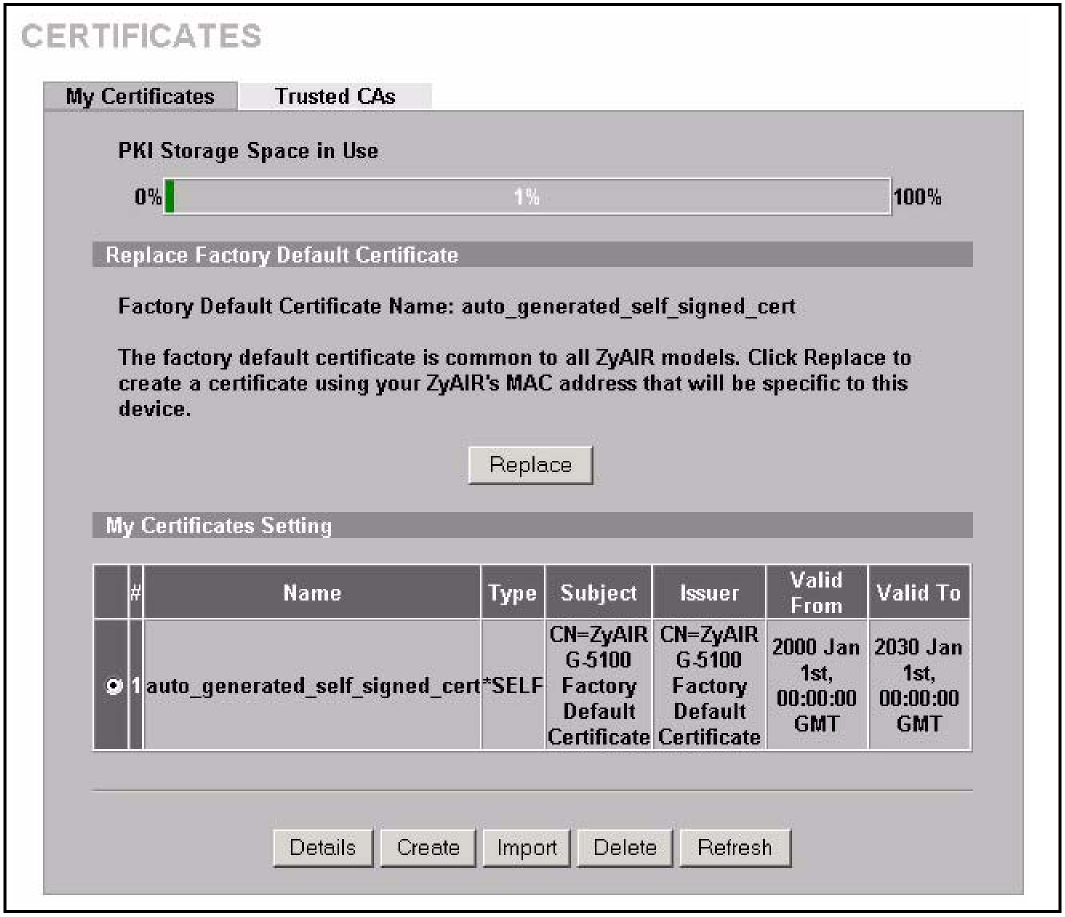
Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the NOA-3570s' CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the NOA-3570.

9.4 My Certificates

Click **CERTIFICATES**, **My Certificates** to open the NOA-3570's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

Figure 44 My Certificates



Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyAIR models. Click Replace to create a certificate using your ZyAIR's MAC address that will be specific to this device.

My Certificates Setting

	#	Name	Type	Subject	Issuer	Valid From	Valid To
●	1	auto_generated_self_signed_cert	*SELF	CN=ZyAIR G-5100 Factory Default Certificate	CN=ZyAIR G-5100 Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT

The following table describes the labels in this screen.

Table 28 My CertificatesNOA-3570

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the NOA-3570’s PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the NOA-3570 has the factory default certificate. The factory default certificate is common to all NOA-3570s that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your NOA-3570's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

Table 28 My CertificatesNOA-3570

LABEL	DESCRIPTION
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the NOA-3570 uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Details	Select a certificate's radio button and click **Details** to open a screen with an in-depth list of information about the certificate.
Create	Click **Create** to go to the screen where you can have the NOA-3570 generate a certificate or a certification request.
Import	Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the NOA-3570.
Delete	Select a certificate's radio button and click **Delete** to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no features are configured to use the ***SELF** certificate. 2. Select the radio button of another self-signed certificate and click **Details** (see the description on the **Create** button if you need to create a self-signed certificate). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. Subsequent certificates move up by one when you take this action.
Refresh	Click **Refresh** to display the current validity status of the certificates.

9.5 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

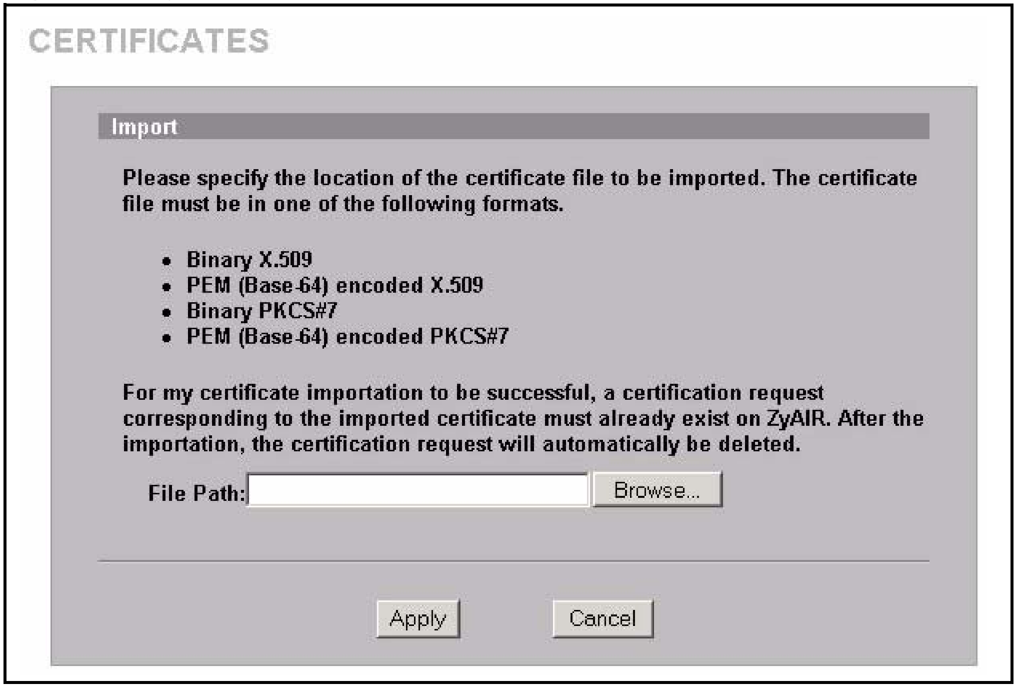
- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The NOA-3570 currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

9.6 Importing a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the NOA-3570, see the following figure.

Note: 1. You can only import a certificate that matches a corresponding certification request that was generated by the NOA-3570.
Note: 2. The certificate you import replaces the corresponding request in the **My Certificates** screen.
Note: 3. You must remove any spaces from the certificate's filename before you can import it.

Figure 45 My Certificate Import



Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyAIR. After the importation, the certification request will automatically be deleted.

File Path:

The following table describes the labels in this screen.

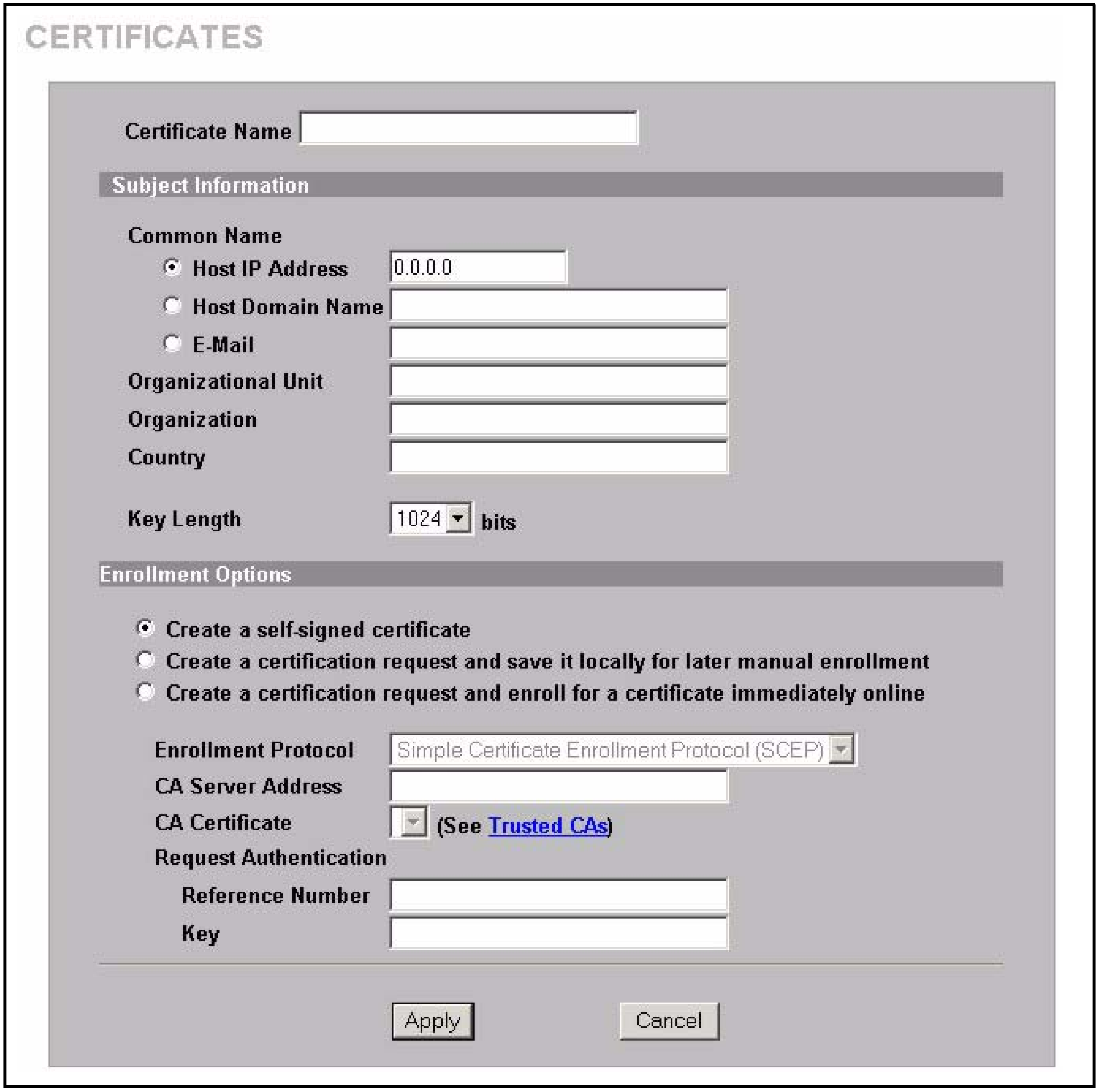
Table 29 My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the NOA-3570.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

9.7 Creating a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the NOA-3570 create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request, see the following figure.

Figure 46 My Certificate Create



CERTIFICATES

Certificate Name

Subject Information

Common Name

● Host IP Address 0.0.0.0

○ Host Domain Name

○ E-Mail

Organizational Unit

Organization

Country

Key Length 1024 bits

Enrollment Options

● Create a self-signed certificate

○ Create a certification request and save it locally for later manual enrollment

○ Create a certification request and enroll for a certificate immediately online

Enrollment Protocol Simple Certificate Enrollment Protocol (SCEP)

CA Server Address

CA Certificate (See Trusted CAs)

Request Authentication

Reference Number

Key

The following table describes the labels in this screen.

Table 30 My Certificate CreateNOA-3570

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate’s owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.

Table 30 My Certificate CreateNOA-3570

LABEL	DESCRIPTION
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the NOA-3570 drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the NOA-3570 drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the NOA-3570 drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the NOA-3570 generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the NOA-3570 generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 9.8 on page 103) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the NOA-3570 generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority’s certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority’s enrollment protocol and the certification authority’s certificate from the drop-down list boxes and enter the certification authority’s server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	Select the certification authority’s enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority’s certificate from the **CA Certificate** drop-down list box. You must have the certification authority’s certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the NOA-3570's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol.

Table 30 My Certificate CreateNOA-3570

LABEL	DESCRIPTION
Key	Type the key that the certification authority gave you.
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the NOA-3570 is generating the self-signed certificate or certification request.

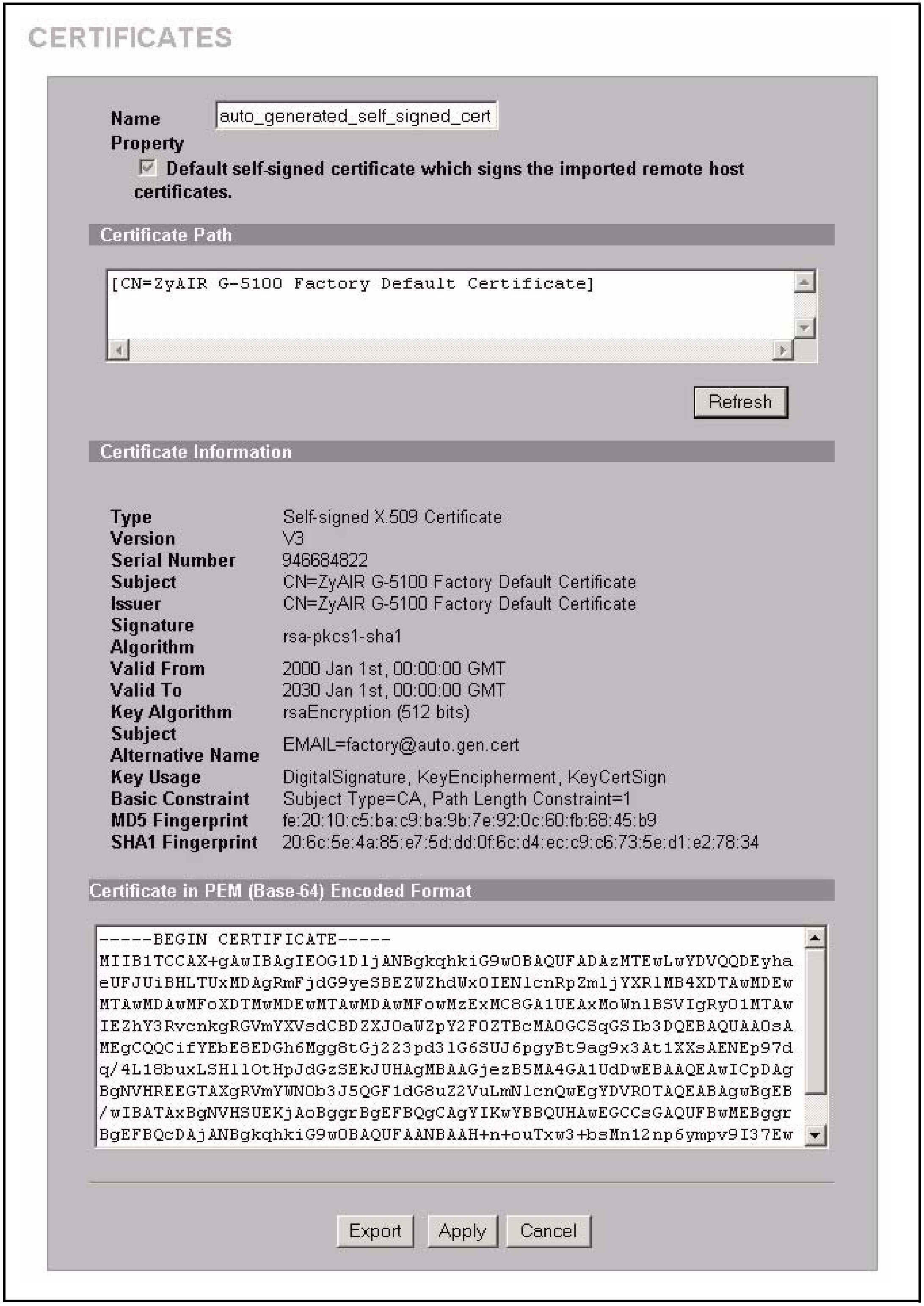
After the NOA-3570 successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the NOA-3570 enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the NOA-3570 to enroll a certificate online.

9.8 My Certificate Details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see Figure 44 on page 97). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate’s name. In the case of a self-signed certificate, you can set it to be the one that the NOA-3570 uses to sign the trusted remote host certificates that you import to the NOA-3570.

Figure 47 My Certificate Details



Name: auto_generated_self_signed_cert

Property

☑ Default self-signed certificate which signs the imported remote host certificates.

```
[CN=ZyAIR G-5100 Factory Default Certificate]
```

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946684822
Subject	CN=ZyAIR G-5100 Factory Default Certificate
Issuer	CN=ZyAIR G-5100 Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=factory@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	fe:20:10:c5:ba:c9:ba:9b:7e:92:0c:60:fb:68:45:b9
SHA1 Fingerprint	20:6c:5e:4a:85:e7:5d:dd:0f:6c:d4:ec:c9:c6:73:5e:d1:e2:78:34

```
-----BEGIN CERTIFICATE-----
MIIB1TCCAX+gAwIBAgIEOG1D1jANBgkqhkiG9w0BAQUFADAzMTEwLwYDVQQDEyha
eUFJUiBHLTUxMDAgRmFjdG9yeSBEZWZhdWx0IENlcnRpZmljYXRlMB4XDTAwMDEw
MTAwMDAwMFoXDTMwMDEwMTAwMDAwMFowMzExMC8GA1UEAxMoWnlBSVIgRy01MTAw
IEZhY3RvcnkgRGVmYXVsdCBDZXJ0aWZpY2F0ZTBcMA0GCSqGSIb3DQEBAQUAA0sA
MEgCQQCifYEbE8EDGh6Mgg8tGj223pd31G6SUJ6pgyBt9ag9x3At1XXsAENEp97d
q/4L18buxLSH11OtHpJdGzSEkJUHAgMBAAGjezB5MA4GA1UdDwEBAAQEAwICpDAg
BgNVHREEGTAXgRVmYWN0b3J5QGF1dG8uZ2VuLmNlcnQwEgYDVR0TAQEABAgwBgEB
/wIBATAxBgNVHSUEKjAoBggrBgEFBQgCAgYIKwYBBQUHAwEGCCsGAQUFBwMEBggr
BgEFBQcDAjANBgkqhkiG9w0BAQUFAANBAAH+n+ouTxw3+bsMn12np6ympv9I37Ew
```

The following table describes the labels in this screen.

Table 31 My Certificate DetailsNOA-3570

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the NOA-3570 use this certificate to sign the trusted remote host certificates that you import to the NOA-3570. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certification Path	Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The NOA-3570 does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the NOA-3570.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (**CN**), Organizational Unit (**OU**), Organization (**O**) and Country (**C**).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The NOA-3570 uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

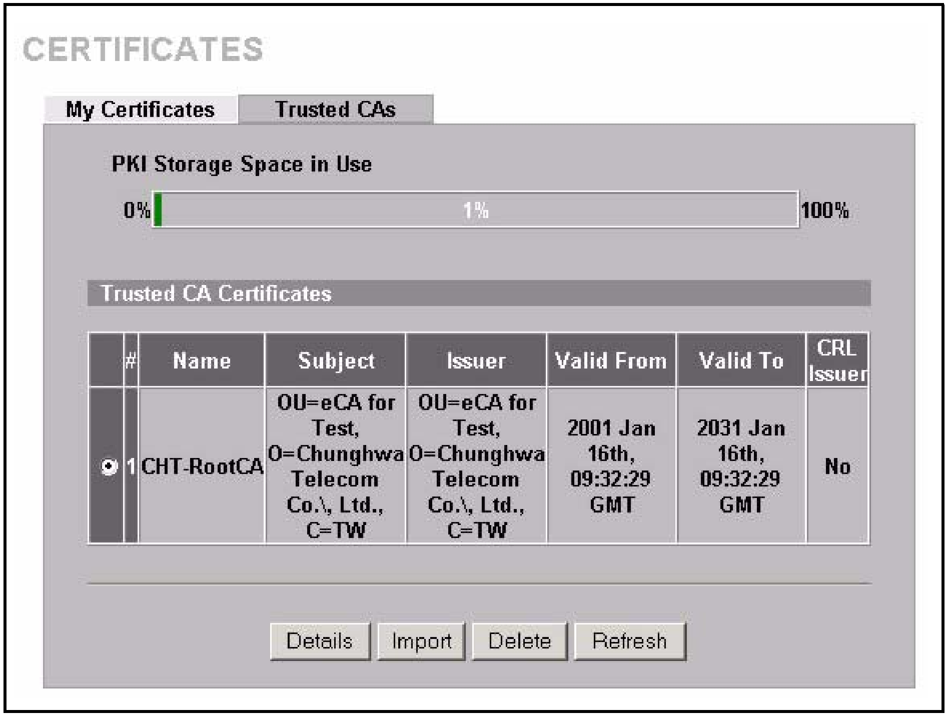
Table 31 My Certificate DetailsNOA-3570

LABEL	DESCRIPTION
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate’s key pair (the NOA-3570 uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner‘s IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path.
MD5 Fingerprint	This is the certificate’s message digest that the NOA-3570 calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate’s message digest that the NOA-3570 calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority’s web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. **Note:** When you are saving your certificate, use "cer" or "cert" as the file name extension.
Apply	Click **Apply** to save your changes back to the NOA-3570. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

9.9 Trusted CAs

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the NOA-3570 to accept as trusted. The NOA-3570 accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities. See the following figure.

Figure 48 Trusted CAs



PKI Storage Space in Use

0% 1% 100%

Trusted CA Certificates

	#	Name	Subject	Issuer	Valid From	Valid To	CRL Issuer
●	1	CHT-RootCA	OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW	OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW	2001 Jan 16th, 09:32:29 GMT	2031 Jan 16th, 09:32:29 GMT	No

The following table describes the labels in this screen.

Table 32 Trusted CAsNOA-3570

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the NOA-3570’s PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate’s owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate’s issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

Table 32 Trusted CAsNOA-3570

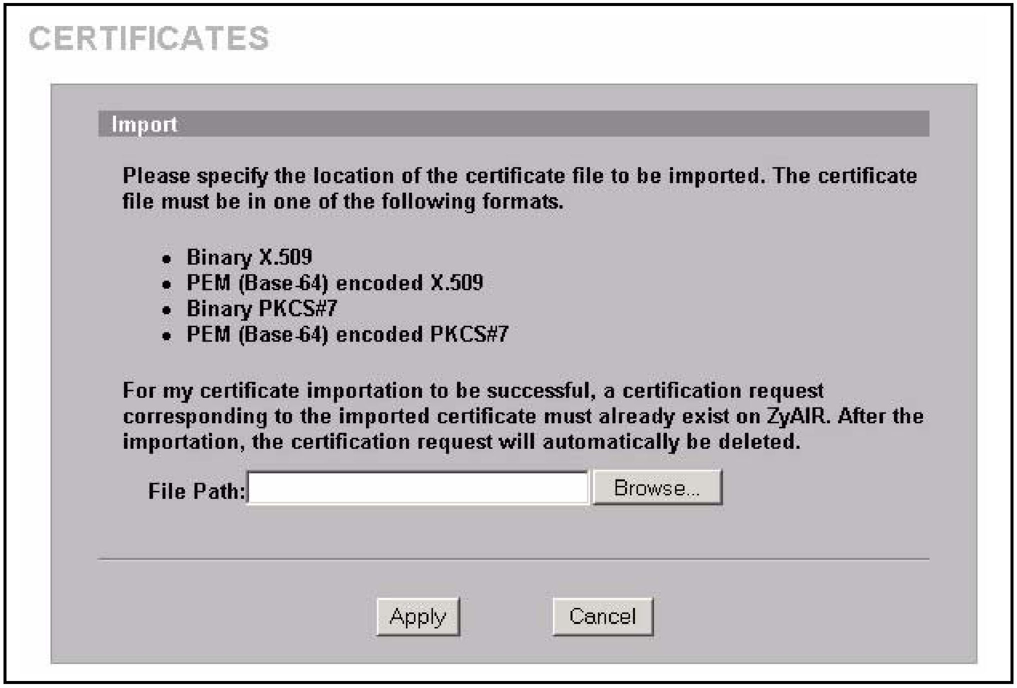
LABEL	DESCRIPTION
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the NOA-3570 check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Details	Select a certificate's radio button and click **Details** to open a screen with an in-depth list of information about the certificate where you can change the certificate's name and set whether or not you want the NOA-3570 to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the NOA-3570.
Delete	Select a certificate's radio button and click **Delete** to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Subsequent certificates move up by one when you take this action.
Refresh	Click this button to display the current validity status of the certificates.

9.10 Importing a Trusted CA's Certificate

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the NOA-3570, see the following figure.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 49 Trusted CA Import



CERTIFICATES

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyAIR. After the importation, the certification request will automatically be deleted.

File Path:

The following table describes the labels in this screen.

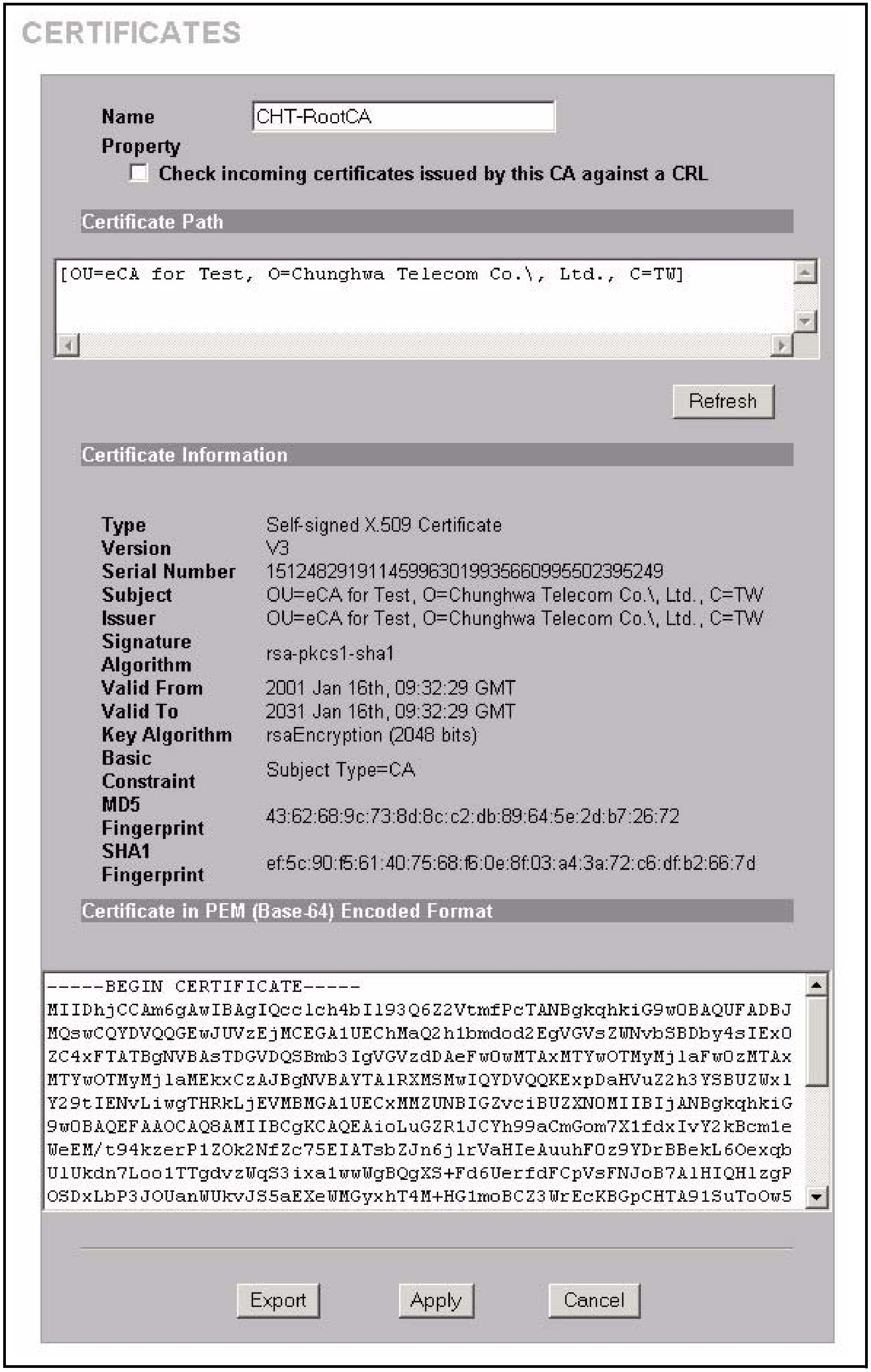
Table 33 Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the NOA-3570.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

9.11 Trusted CA Certificate Details

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the NOA-3570 to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 50 Trusted CA Details



Name	CHT-RootCA
Property	

□ **Check incoming certificates issued by this CA against a CRL**

```
[OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW]
```

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	151248291911459963019935660995502395249
Subject	OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW
Issuer	OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2001 Jan 16th, 09:32:29 GMT
Valid To	2031 Jan 16th, 09:32:29 GMT
Key Algorithm	rsaEncryption (2048 bits)
Basic Constraint	Subject Type=CA
MD5 Fingerprint	43:62:68:9c:73:8d:8c:c2:db:89:64:5e:2d:b7:26:72
SHA1 Fingerprint	ef:5c:90:f5:61:40:75:68:f6:0e:8f:03:a4:3a:72:c6:df:b2:66:7d

```
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIQcclch4bI193Q6Z2VtmfPcTANBgkqhkiG9w0BAQUFADBJ
MQswCQYDVQQGEwJUVzEjMCEGA1UEChMaQ2h1bmdod2EgVGVsZWNvbSBDby4sIExO
ZC4xFTATBgNVBAsTDGVDQSBmb3IgVGVzdDAeFw0wMTAxMTYwOTMyMjlaFw0zMTAx
MTYwOTMyMjlaMEkxCzAJBgNVBAYTAlRXMSMwIQYDVQQKExpDaHVuZ2h3YSBUZWxl
Y29tIENvLiwgTHRkLjEVMBMGA1UECxMMZUNBIGZvciBUZXN0MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAioLuGZR1JCYh99aCmGom7X1fdxIvY2kBcm1e
WeEM/t94kzerP1ZOk2NfZc75EIATsbZJn6jlrVaHIeAuuhF0z9YDrBBekL6Oexqb
UlUkdn7Loo1TTgdvzWqS3ixa1wwWgBQgXS+Fd6UerfdFCpVsFNJoB7AlHIQHlzgP
OSDxLbP3JOUanWUkvJS5aEXeWMGyxhT4M+HG1moBCZ3WrEcKBGpCHTA91SuToOw5
```

The following table describes the labels in this screen.

Table 34 Trusted CA DetailsNOA-3570

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the NOA-3570 check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the NOA-3570 not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certificate Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The NOA-3570 does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the NOA-3570 uses RSA encryption) and the length of the key set in bits (1024 bits for example).

Table 34 Trusted CA DetailsNOA-3570

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate’s owner‘s IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate’s message digest that the NOA-3570 calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate’s message digest that the NOA-3570 calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Apply	Click **Apply** to save your changes back to the NOA-3570. You can only change the name and/or set whether or not you want the NOA-3570 to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

CHAPTER 10 Log Screens

This chapter contains information about configuring general log settings and viewing the NOA-3570’s logs. Refer to Appendix K on page 249 for example log message explanations.

10.1 Configuring View Log

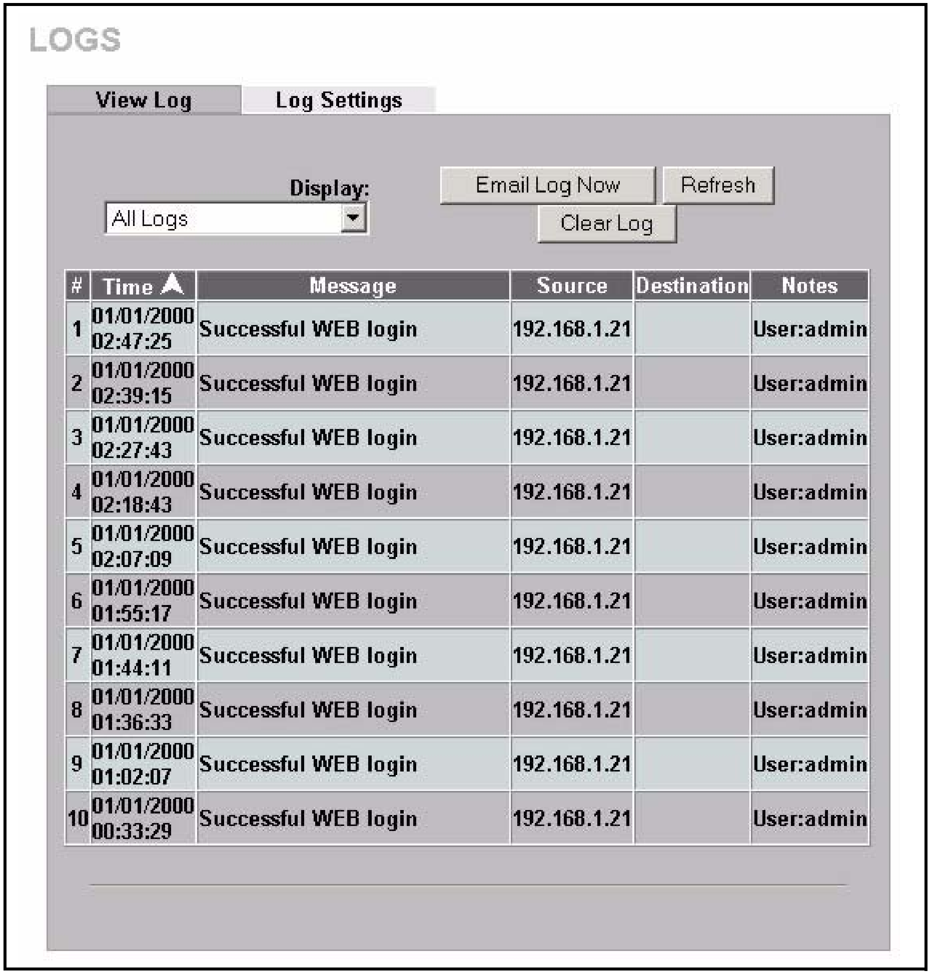
The web configurator allows you to look at all of the NOA-3570’s logs in one location.

Click **LOGS** to open the **View Log** screen. The **View Log** screen displays logs for the categories that you selected in the **Log Settings** screen (see Figure 52 on page 116).

You can view logs and alert messages in this screen. Log entries in red indicate alerts. Once the log table is full, old logs are deleted as new logs are created.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

Figure 51 View Log



#	Time	Message	Source	Destination	Notes
1	01/01/2000 02:47:25	Successful WEB login	192.168.1.21		User:admin
2	01/01/2000 02:39:15	Successful WEB login	192.168.1.21		User:admin
3	01/01/2000 02:27:43	Successful WEB login	192.168.1.21		User:admin
4	01/01/2000 02:18:43	Successful WEB login	192.168.1.21		User:admin
5	01/01/2000 02:07:09	Successful WEB login	192.168.1.21		User:admin
6	01/01/2000 01:55:17	Successful WEB login	192.168.1.21		User:admin
7	01/01/2000 01:44:11	Successful WEB login	192.168.1.21		User:admin
8	01/01/2000 01:36:33	Successful WEB login	192.168.1.21		User:admin
9	01/01/2000 01:02:07	Successful WEB login	192.168.1.21		User:admin
10	01/01/2000 00:33:29	Successful WEB login	192.168.1.21		User:admin

The following table describes the labels in this screen.

Table 35 View Log NOA-3570

LABEL	DESCRIPTION
Display	Select a log category from the drop down list box to display logs within the selected category. To view all logs, select **All Logs**. The number of categories shown in the drop down list box depends on the selection in the **Log Settings** page.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.

Table 35 View Log NOA-3570

LABEL	DESCRIPTION
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

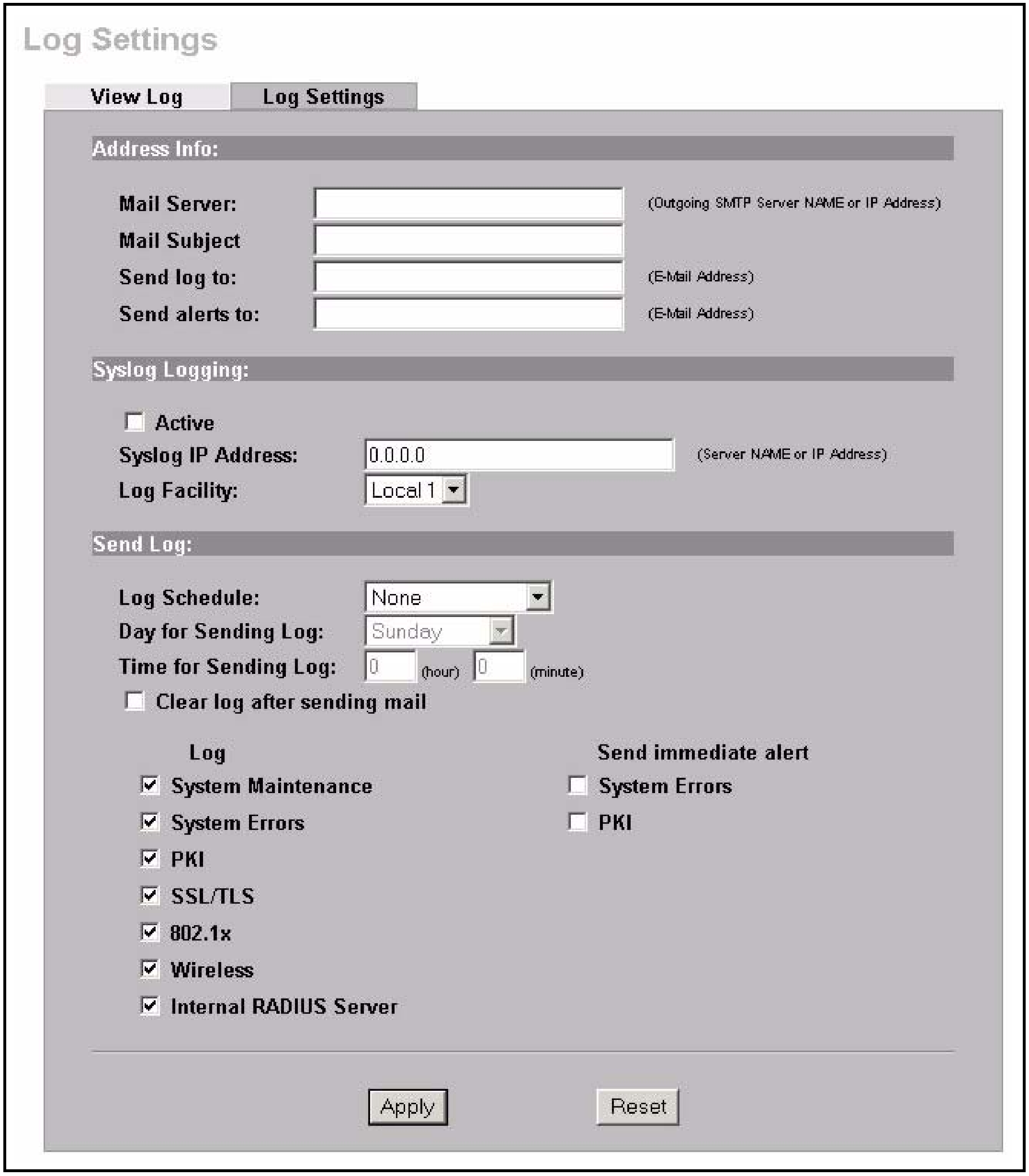
10.2 Configuring Log Settings

To change your NOA-3570’s log settings, click **LOGS** and then **Log Settings**. The **Log Settings** screen opens.

Use the **Log Settings** screen to configure to where the NOA-3570 is to send the logs; the schedule for when the NOA-3570 is to send the logs and which logs and/or immediate alerts the NOA-3570 is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

Figure 52 Log Settings



Address Info:

Mail Server: (Outgoing SMTP Server NAME or IP Address)

Mail Subject

Send log to: (E-Mail Address)

Send alerts to: (E-Mail Address)

Syslog Logging:

□ Active

Syslog IP Address: 0.0.0.0 (Server NAME or IP Address)

Log Facility: Local 1

Send Log:

Log Schedule: None

Day for Sending Log: Sunday

Time for Sending Log: 0 (hour) 0 (minute)

□ Clear log after sending mail

Log	Send immediate alert
☑ System Maintenance	□ System Errors
☑ System Errors	□ PKI
☑ PKI	
☑ SSL/TLS	
☑ 802.1x	
☑ Wireless	
☑ Internal RADIUS Server	

The following table describes the labels in this screen.

Table 36 Log Settings NOA-3570

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the NOA-3570 sends.

Table 36 Log Settings NOA-3570

LABEL	DESCRIPTION
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts to	Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	Select the categories of logs that you want to record.
Send immediate alert	Select the categories of alerts for which you want the NOA-3570 to immediately send e-mail alerts.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to reconfigure all the fields in this screen.

CHAPTER 11 Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

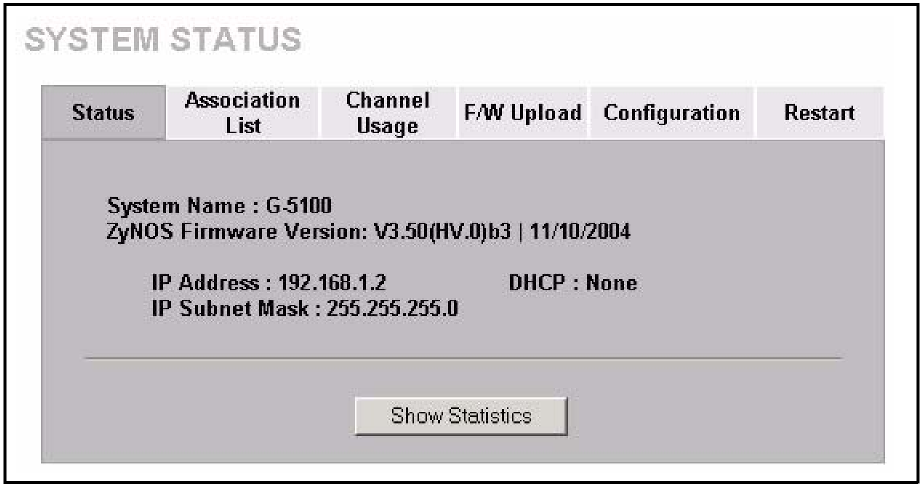
11.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your NOA-3570.

11.2 System Status Screen

Click **MAINTENANCE** to open the **System Status** screen, where you can use to monitor your NOA-3570. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.

Figure 53 System Status



System Name : G-5100
ZyNOS Firmware Version: V3.50(HV.0)b3 | 11/10/2004

IP Address : 192.168.1.2 DHCP : None
IP Subnet Mask : 255.255.255.0

The following table describes the labels in this screen.

Table 37 System Status NOA-3570

LABEL	DESCRIPTION
System Name	This is the **System Name** you enter in the first Internet Access Wizard screen. It is for identification purposes
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.

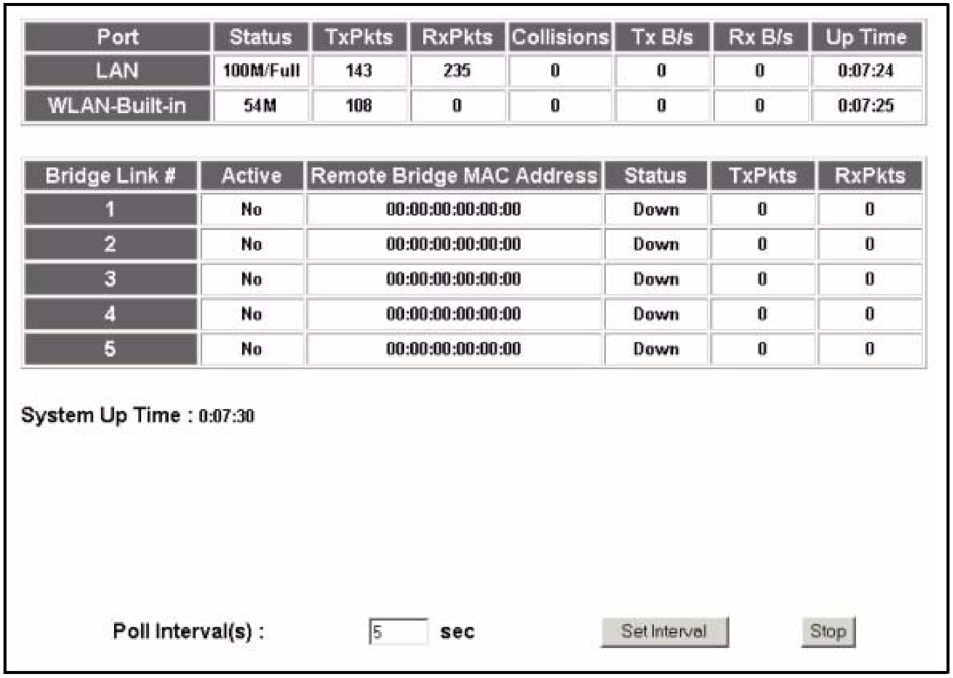
Table 37 System Status NOA-3570

LABEL	DESCRIPTION
IP Address	This is the Ethernet port IP address.
IP Subnet Mask	This is the Ethernet port subnet mask.
DHCP	This is the Ethernet port DHCP role - **Client** or **None**.
Show Statistics	Click **Show Statistics** to see router performance statistics such as number of packets sent and number of packets received for each port.

11.2.1 System Statistics

Read-only information here includes port status, packet specific statistics and bridge link status. Also provided are "system up time" and "poll interval(s)". The **Poll Interval** field is configurable.

Figure 54 System Status: Show Statistics



Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	143	235	0	0	0	0:07:24
WLAN-Built-in	54M	108	0	0	0	0	0:07:25

Bridge Link #	Active	Remote Bridge MAC Address	Status	TxPkts	RxPkts
1	No	00:00:00:00:00:00	Down	0	0
2	No	00:00:00:00:00:00	Down	0	0
3	No	00:00:00:00:00:00	Down	0	0
4	No	00:00:00:00:00:00	Down	0	0
5	No	00:00:00:00:00:00	Down	0	0

System Up Time : 0:07:30

Poll Interval(s) : 5 sec

The following table describes the labels in this screen.

Table 38 System Status: Show Statistics NOA-3570

LABEL	DESCRIPTION
Port	This is the Ethernet port or the built-in wireless card.
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. This shows the transmission speed only for wireless port.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.

Table 38 System Status: Show Statistics NOA-3570

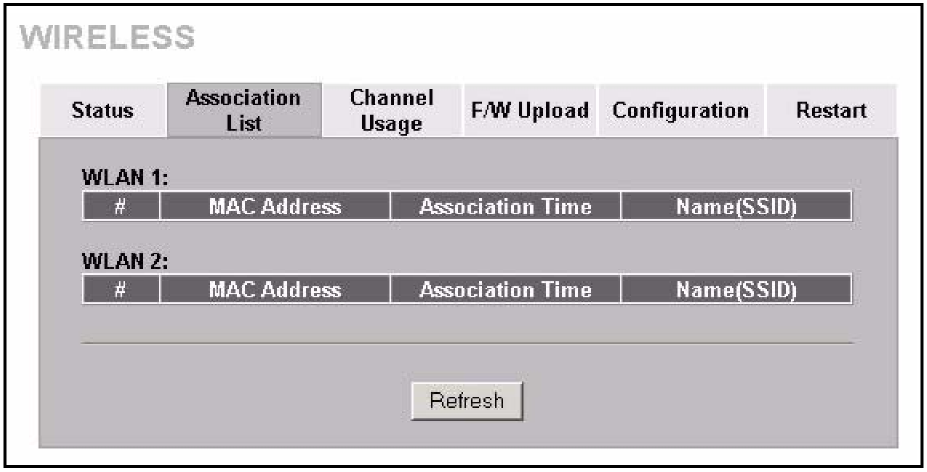
LABEL	DESCRIPTION
Collisions	This is the number of collisions on this port.
Tx B/s	This shows the transmission speed in bytes per second on this port.
Rx B/s	This shows the reception speed in bytes per second on this port.
Up Time	This is total amount of time the line has been up.
Bridge Link #	This is the index number of the bridge connection.
Active	This shows whether the bridge connection is activated or not.
Remote Bridge MAC Address	This is the MAC address of the peer device in bridge mode.
Status	This shows the current status of the bridge connection, which can be **Up** or **Down**.
TxPkts	This is the number of transmitted packets on the wireless bridge.
RxPkts	This is the number of received packets on the wireless bridge.
System Up Time	This is the total time the NOA-3570 has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.
Stop	Click this button to stop refreshing statistics.

11.3 Association List

View the wireless stations that are currently associated to the NOA-3570's WLAN cards in the **Association List** screen.

Click **MAINTENANCE** and then the **Association List** tab to display the screen as shown next.

Figure 55 Association List



WLAN 1:

#	MAC Address	Association Time	Name(SSID)

WLAN 2:

#	MAC Address	Association Time	Name(SSID)

The following table describes the labels in this screen.

Table 39 Association List NOA-3570

LABEL	DESCRIPTION
WLAN 1, 2	This identifies the WLAN adapter to which the list of wireless clients is associated.
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the NOA-3570.
Name (SSID)	This field displays the SS identification name to which the wireless station is associated.
Refresh	Click **Refresh** to reload the screen.

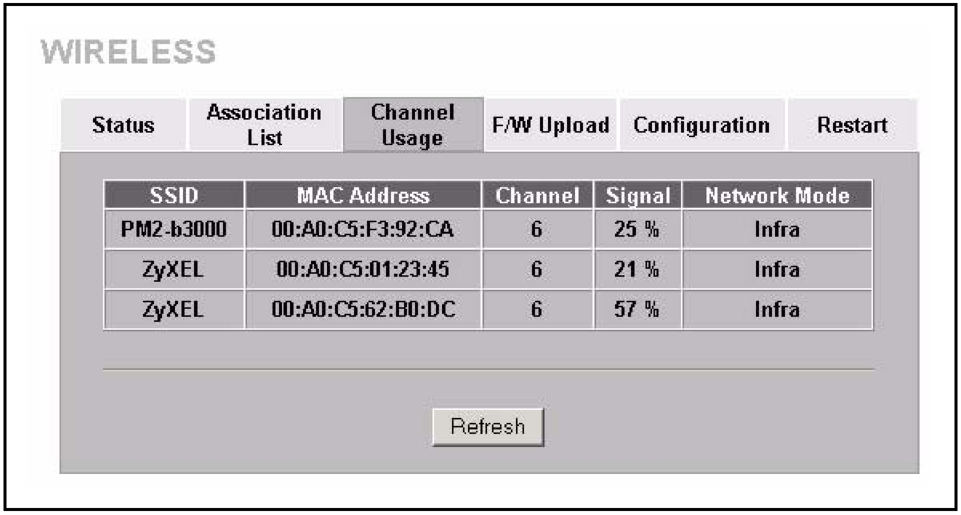
11.4 Channel Usage

The **Channel Usage** screen shows which channels are being used by other wireless networks within the NOA-3570's transmission range. If a channel is being used, select a channel removed from it by five channels to avoid overlap.

Click **MAINTENANCE** and then the **Channel Usage** tab to display the screen shown next.

Wait a moment while the NOA-3570 compiles the information.

Figure 56 Channel Usage



SSID	MAC Address	Channel	Signal	Network Mode
PM2-b3000	00:A0:C5:F3:92:CA	6	25 %	Infra
ZyXEL	00:A0:C5:01:23:45	6	21 %	Infra
ZyXEL	00:A0:C5:62:B0:DC	6	57 %	Infra

The following table describes the labels in this screen.

Table 40 Channel Usage NOA-3570

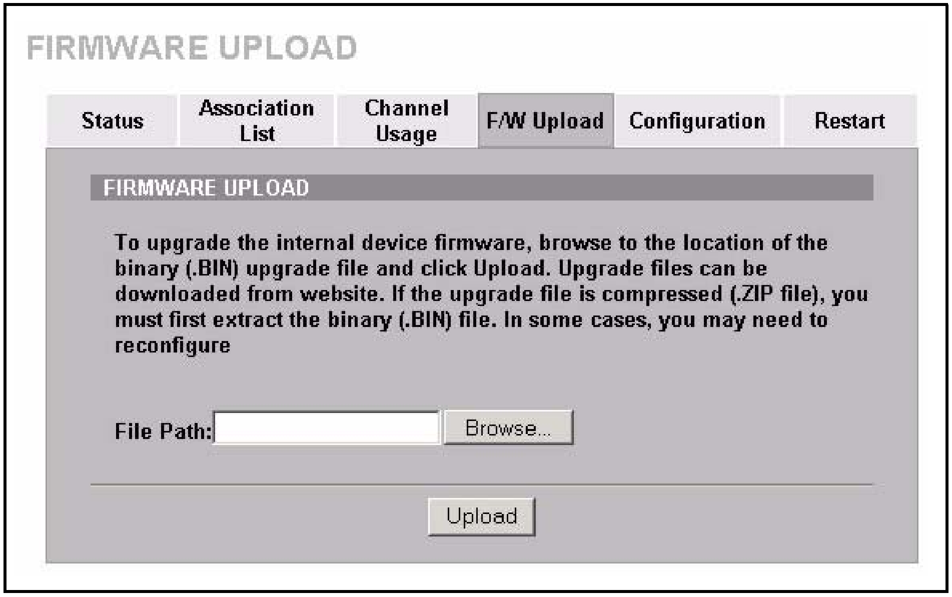
LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See Chapter 5 on page 55 for more information on basic service sets (BSS) and extended service sets (ESS).
MAC Address	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Signal	This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference.
Network Mode	"Network Mode" in this screen refers to your wireless LAN infrastructure and WEP setup (refer to Chapter 5 on page 55). Network modes are: **Infra** (Infrastructure which is the same as an extended service set ESS), **Infra, WEP** (Infrastructure with WEP encryption enabled), **Ad-Hoc** (same as an independent basic service set IBSS), or **Ad-Hoc with WEP**.
Refresh	Click **Refresh** to reload the screen.

11.5 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "NOA-3570.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Chapter 20 on page 169 for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** and then **F/W Upload**. Follow the instructions in this screen to upload firmware to your NOA-3570.

Figure 57 Firmware Upload



FIRMWARE UPLOAD

FIRMWARE UPLOAD

To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure

File Path:

The following table describes the labels in this screen.

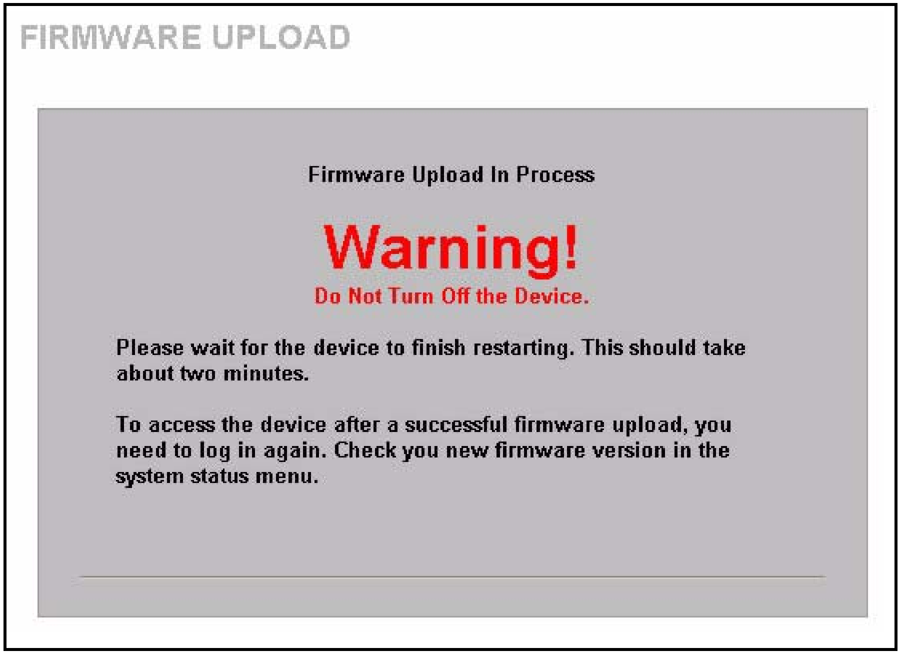
Table 41 Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the NOA-3570 while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the NOA-3570 again.

Figure 58 Firmware Upload In Process



FIRMWARE UPLOAD

Firmware Upload In Process

Warning!

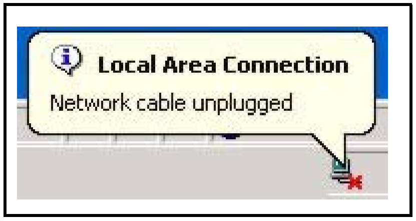
Do Not Turn Off the Device.

Please wait for the device to finish restarting. This should take about two minutes.

To access the device after a successful firmware upload, you need to log in again. Check you new firmware version in the system status menu.

The NOA-3570 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 59 Network Temporarily Disconnected



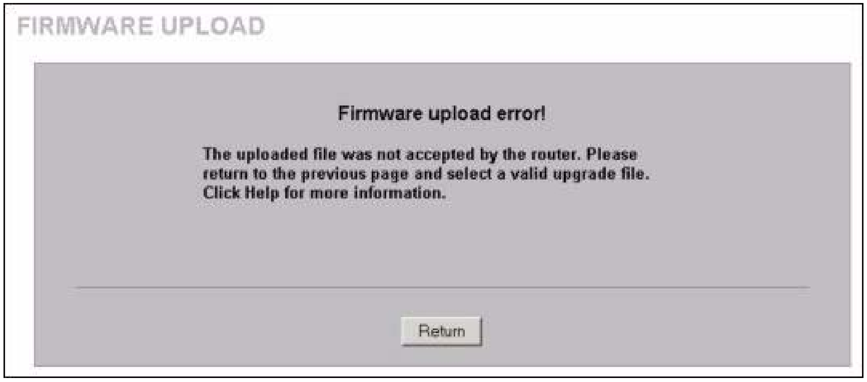
Local Area Connection

Network cable unplugged

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 60 Firmware Upload Error



FIRMWARE UPLOAD

Firmware upload error!

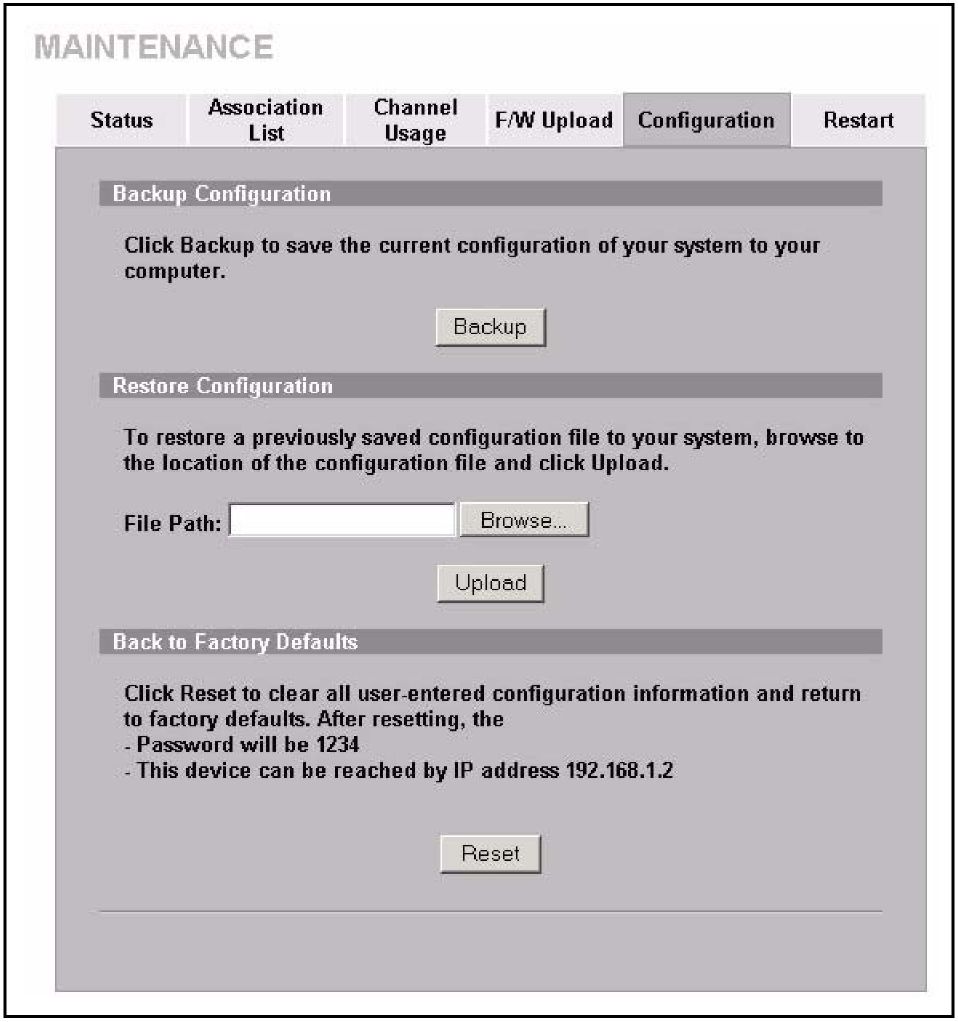
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

11.6 Configuration Screen

See Chapter 20 on page 169 for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to backing up configuration, restoring configuration and restoring factory defaults appears as shown next.

Figure 61 Configuration



Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path:

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- This device can be reached by IP address 192.168.1.2

11.6.1 Backup Configuration

Backup configuration allows you to back up (save) the NOA-3570’s current configuration to a file on your computer. Once your NOA-3570 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the NOA-3570’s current configuration to your computer.

11.6.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NOA-3570.

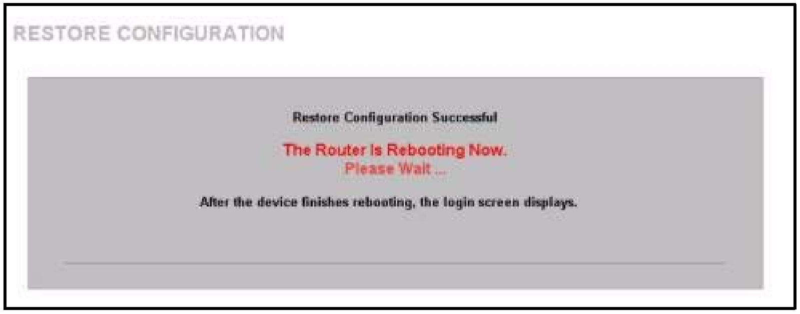
Table 42 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Note: Do not turn off the NOA-3570 while configuration file upload is in progress.

After you see a "restore configuration successful" screen, you must then wait one minute before logging into the NOA-3570 again.

Figure 62 Configuration Upload Successful



RESTORE CONFIGURATION

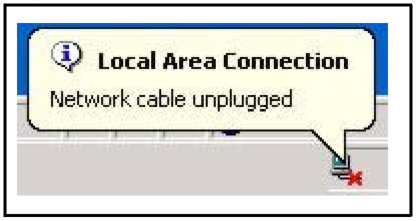
Restore Configuration Successful

The Router Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

The NOA-3570 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 63 Network Temporarily Disconnected

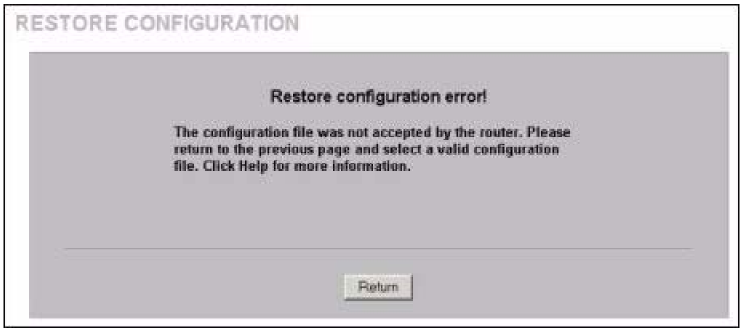


Local Area Connection
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NOA-3570 IP address (192.168.1.2). See Appendix D on page 201 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 64 Configuration Upload Error



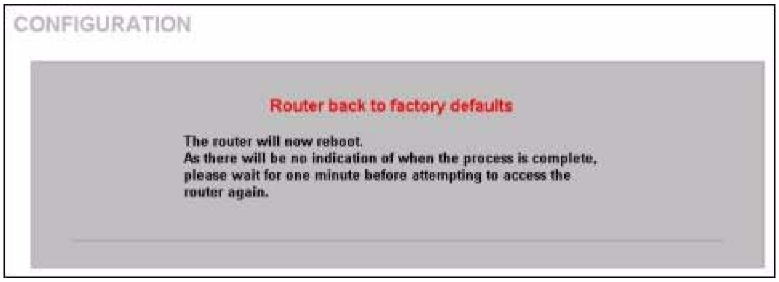
Restore configuration error!

The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.

11.6.3 Back to Factory Defaults

Click the **Reset** button in this section to clear all user-entered configuration information and returns the NOA-3570 to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 65 Reset Warning Message



Router back to factory defaults

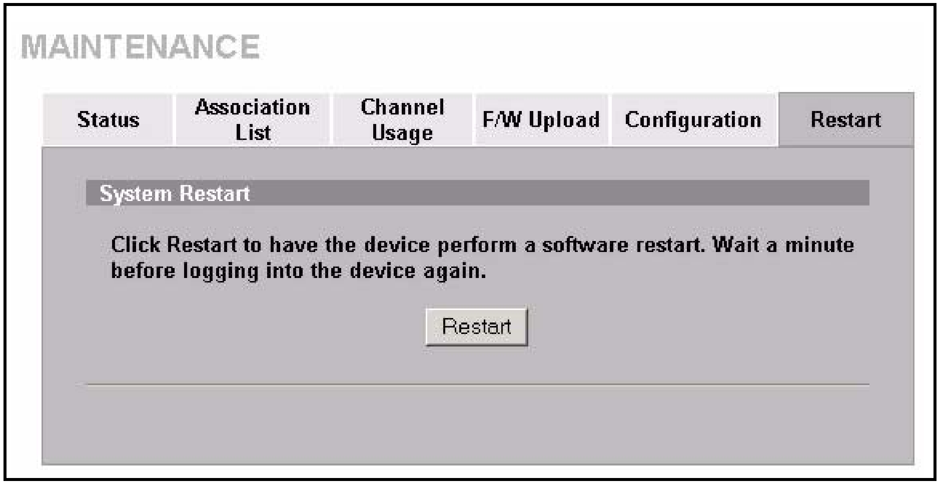
The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

11.7 Restart Screen

System restart allows you to reboot the NOA-3570 without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the NOA-3570 reboot. This does not affect the NOA-3570's configuration.

Figure 66 Restart Screen



Click Restart to have the device perform a software restart. Wait a minute before logging into the device again.