

Contents Overview

User's Guide	9
Introducing the NWA1121-NI	11
Introducing the Web Configurator	19
Dashboard	25
Tutorial	29
Technical Reference	47
Monitor	49
Wireless LAN	55
LAN	94
VLAN	98
System	101
Log Settings	115
Maintenance	119
Troubleshooting	129

Table of Contents

Contents Overview	3
Table of Contents	5
 Part I: User's Guide	 9
 Chapter 1	
Introducing the NWA1121-NI.....	11
1.1 Introducing the NWA1121-NI	11
1.2 Wireless Modes	11
1.2.1 MBSSID	12
1.2.2 Wireless Client	13
1.2.3 Root AP	14
1.2.4 Repeater	14
1.3 Ways to Manage the NWA1121-NI	15
1.4 Configuring Your NWA1121-NI's Security Features	16
1.4.1 Control Access to Your Device	16
1.4.2 Wireless Security	16
1.5 Good Habits for Managing the NWA1121-NI	16
1.6 Hardware Connections	17
1.7 LED	17
 Chapter 2	
Introducing the Web Configurator	19
2.1 Accessing the Web Configurator	19
2.2 Resetting the NWA1121-NI	20
2.2.1 Methods of Restoring Factory-Defaults	21
2.3 Navigating the Web Configurator	22
2.3.1 Title Bar	22
2.3.2 Navigation Panel	23
2.3.3 Main Window	24
 Chapter 3	
Dashboard	25
3.1 The Dashboard Screen	25
 Chapter 4	
Tutorial	29

4.1 How to Configure the Wireless LAN	29
4.1.1 Choosing the Wireless Mode	29
4.1.2 Further Reading	29
4.2 How to Configure Multiple Wireless Networks	29
4.2.1 Configure the SSID Profiles	31
4.2.2 Configure the Standard Network	33
4.2.3 Configure the VoIP Network	34
4.2.4 Configure the Guest Network	36
4.2.5 Testing the Wireless Networks	38
4.3 NWA1121-NI Setup in AP and Wireless Client Modes	38
4.3.1 Scenario	38
4.3.2 Configuring the NWA1121-NI in MBSSID or Root AP Mode	39
4.3.3 Configuring the NWA1121-NI in Wireless Client Mode	42
4.3.4 MAC Filter Setup	44
4.3.5 Testing the Connection and Troubleshooting	45

Part II: Technical Reference..... 47

Chapter 5 Monitor..... 49

5.1 Overview	49
5.2 What You Can Do	49
5.3 View Logs	49
5.4 Statistics	50
5.5 Association List	51
5.6 Channel Usage	52

Chapter 6 Wireless LAN..... 55

6.1 Overview	55
6.2 What You Can Do in this Chapter	55
6.3 What You Need To Know	56
6.4 Wireless Settings Screen	60
6.4.1 Root AP Mode	61
6.4.2 Repeater Mode	64
6.4.3 Wireless Client Mode	67
6.4.4 MBSSID Mode	69
6.5 SSID Screen	72
6.5.1 Configuring SSID	73
6.6 Wireless Security Screen	74
6.6.1 Security: WEP	76

6.6.2 Security: 802.1x Only	77
6.6.3 Security: 802.1x Static WEP	79
6.6.4 Security: WPA, WPA2, WPA2-MIX	83
6.6.5 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX	86
6.7 RADIUS Screen	87
6.8 MAC Filter Screen	89
6.9 Technical Reference	91
6.9.1 Additional Wireless Terms	91
6.9.2 WMM QoS	92
6.9.3 Security Mode Guideline	93
Chapter 7	
LAN	94
7.1 Overview	94
7.2 What You Can Do in this Chapter	94
7.3 What You Need to Know	94
7.4 LAN IP Screen	96
Chapter 8	
VLAN	98
8.1 Overview	98
8.1.1 What You Can Do in This Chapter	98
8.2 What You Need to Know	98
8.3 VLAN Screen	99
Chapter 9	
System	101
9.1 Overview	101
9.2 What You Can Do in this Chapter	101
9.3 What You Need To Know	102
9.4 WWW Screen	104
9.5 Certificates Screen	105
9.6 Telnet Screen	106
9.7 SNMP Screen	107
9.8 FTP Screen	110
9.9 Technical Reference	111
9.9.1 MIB	111
9.9.2 Supported MIBs	111
9.9.3 SNMP Traps	112
9.9.4 Private-Public Certificates	113
9.9.5 Certification Authorities	113
9.9.6 Checking the Fingerprint of a Certificate on Your Computer	113

Chapter 10	
Log Settings	115
10.1 Overview	115
10.2 What You Can Do in this Chapter	115
10.3 What You Need To Know	116
10.4 Log Settings Screen	116
Chapter 11	
Maintenance	119
11.1 Overview	119
11.2 What You Can Do in this Chapter	119
11.3 What You Need To Know	120
11.4 General Screen	120
11.5 Password Screen	121
11.6 Time Screen	122
11.7 Firmware Upgrade Screen	123
11.8 Configuration File Screen	124
11.8.1 Backup Configuration	124
11.8.2 Restore Configuration	125
11.8.3 Back to Factory Defaults	126
11.9 Restart Screen	126
Chapter 12	
Troubleshooting.....	129
12.1 Power, Hardware Connections, and LEDs	129
12.2 NWA1121-NI Access and Login	130
12.3 Internet Access	131
Appendix A Setting Up Your Computer's IP Address	133
Appendix B Pop-up Windows, JavaScript and Java Permissions	161
Appendix C IP Addresses and Subnetting.....	173
Appendix D Wireless LANs.....	181
Appendix E Legal Information.....	195
Index	203

PART I

User's Guide

Introducing the NWA1121-NI

This chapter introduces the main applications and features of the NWA1121-NI. It also discusses the ways you can manage your NWA1121-NI.

1.1 Introducing the NWA1121-NI

Your NWA1121-NI is an IPv6 wireless AP (Access Point) that can function in several wireless modes. It extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

The NWA1121-NI controls network access with MAC address filtering and RADIUS server authentication. It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access (WPA), WPA2 and WEP data encryption. Its Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

Your NWA1121-NI is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance.

See the Quick Start Guide for instructions on how to make hardware connections.

1.2 Wireless Modes

The NWA1121-NI can be configured to use the following WLAN operating modes:

OPERATING MODE	NUMBER OF SUPPORTED SSID	UNIVERSAL REPEATER FUNCTION	AP FUNCTION
MBSSID	8	No	Yes
Client	1	No	No
Root AP	5	Yes	Yes
Repeater	1	Yes	Yes

- 1 ~~MBSSID~~
- 2 ~~Client~~
- 3 ~~Root AP~~
- 4 ~~Repeater~~

Applications for each operating mode are shown below.

1.2.1 MBSSID

A Basic Service Set (BSS) is the set of devices forming a single wireless network (usually an access point and one or more wireless clients). The Service Set Identifier (SSID) is the name of a BSS. In Multiple BSS (MBSSID) mode, the NWA1121-NI provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile.

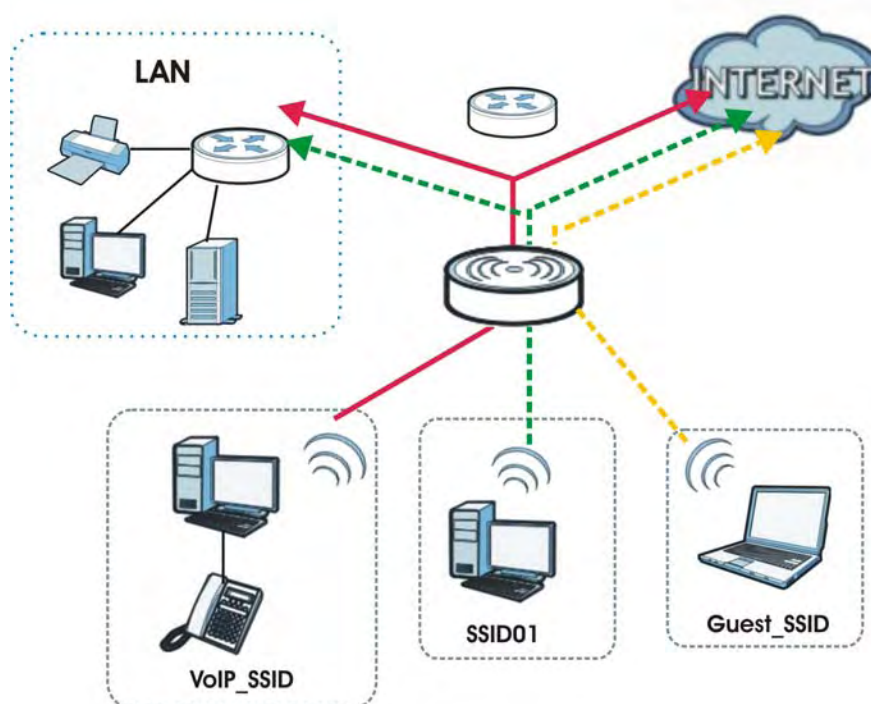
You can configure **up to eight multiple** SSID profiles, **and have all of them active at any one time**.

You can assign different wireless and security settings to each SSID profile. This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs.

To the wireless clients in the network, each SSID appears to be a different access point. As in any wireless network, clients can associate only with the SSIDs for which they have the correct security settings.

For example, you might want to set up a wireless network in your office where Internet telephony (VoIP) users have priority. You also want a regular wireless network for standard users, as well as a 'guest' wireless network for visitors. In the following figure, **VoIP_SSID** users have QoS priority, **SSID01** is the wireless network for standard users, and **Guest_SSID** is the wireless network for guest users. In this example, the guest user is forbidden access to the wired Land Area Network (LAN) behind the AP and can access only the Internet.

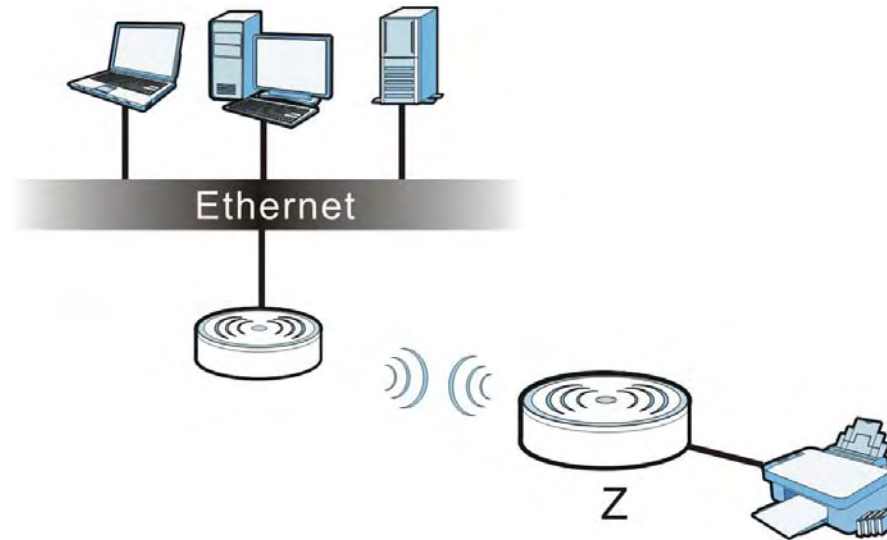
Figure 1 Multiple BSSs



1.2.2 Wireless Client

The NWA1121-NI can be used as a wireless client to communicate with an existing network. In the figure below, the printer can receive requests from the wired computer clients **A** and **B** via the NWA1121-NI in Client mode (**Z**).

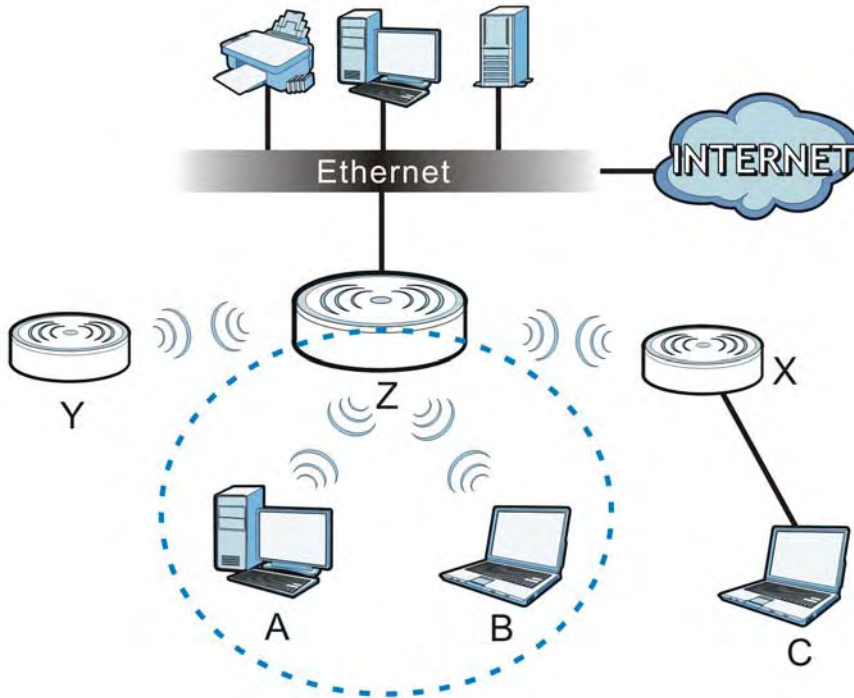
Figure 2 Wireless Client Application



1.2.3 Root AP

In Root AP mode, the NWA1121-NI (**Z**) can act as the root AP in a wireless network and also **allow repeaters (X and Y) to extend the range of its wireless network** at the same time. In the figure below, both clients **A, B** and **C** can access the wired network through the root AP.

Figure 3 Root AP Application



On the NWA1121-NI in Root AP mode, you can have **up to four** multiple SSIDs active for regular wireless connections and one SSID for the connection with a repeater (universal repeater SSID). Wireless clients can use either SSID to associate with the NWA1121-NI in Root AP mode. A repeater must use the universal repeater SSID to connect to the NWA1121-NI in Root AP mode.

When the NWA1121-NI is in Root AP mode, **universal repeater security** between the NWA1121-NI and other repeater is independent of the security **between the wireless clients and the AP or repeater**. If you do not enable **universal repeater** security, traffic between APs is not encrypted. When **universal repeater** security is enabled, **both APs and repeaters** must use the same pre-shared key. See [Section 6.6 on page 74](#) for more details.

Unless specified, the term “security settings” refers to the traffic between the wireless clients and the AP. **At the time of writing, universal repeater security is compatible with the NWA1121-NI only.**

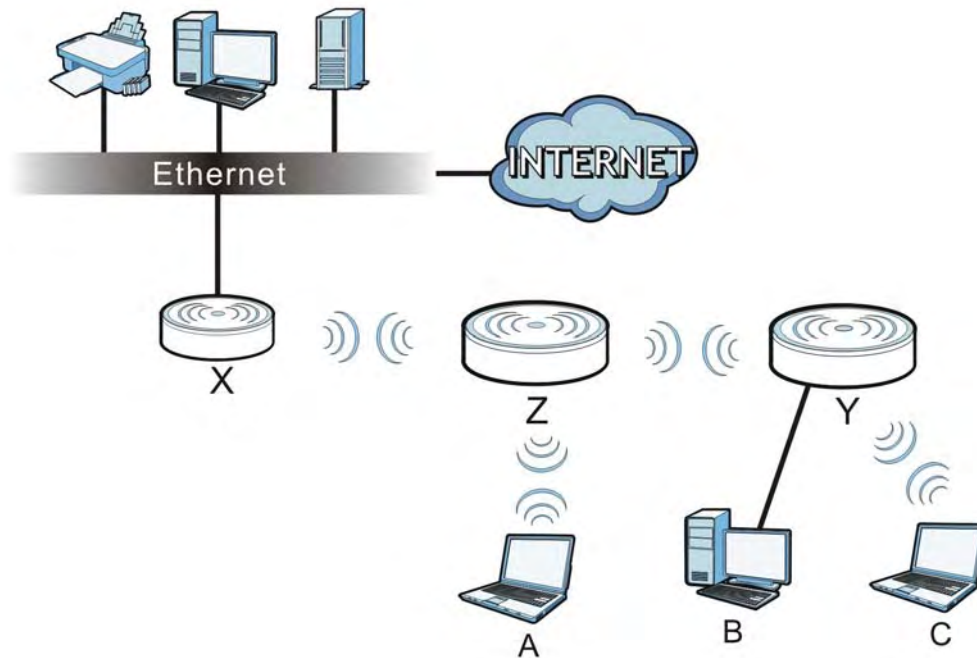
1.2.4 Repeater

The NWA can act as a wireless network repeater **to extend a root AP's wireless network range, and also establish wireless connections with wireless clients.**

Using Repeater mode, your NWA1121-NI can extend the range of the WLAN. In the figure below, the NWA1121-NI in Repeater mode (**Z**) has a wireless connection to the NWA1121-NI in Root AP mode (**X**) which is connected to a wired network and also has a wireless connection to another NWA1121-NI in Repeater mode (**Y**) at the same time. **Z** and **Y** act as repeaters that forward traffic

between associated wireless clients and the wired LAN. Clients **A**, **B** and **C** access the AP and the wired network behind the AP through repeaters **Z** and **Y**.

Figure 4 Repeater Application



When the NWA1121-NI is in Repeater mode, universal repeater security between the NWA1121-NI and other repeater is independent of the security between the wireless clients and the AP or repeater. If you do not enable universal repeater security, traffic between APs is not encrypted. When universal repeater security is enabled, both APs and repeaters must use the same pre-shared key. See [Section 6.6 on page 74](#) for more details.

Once the security settings of peer sides match one another, the connection between devices is made.

At the time of writing, universal repeater security is compatible with the NWA1121-NI only.

1.3 Ways to Manage the NWA1121-NI

Use any of the following methods to manage the NWA1121-NI.

- Web Configurator. This is recommended for everyday management of the NWA1121-NI using a (supported) web browser.
- ~~Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.~~
- FTP (File Transfer Protocol) for firmware upgrades.
- SNMP (Simple Network Management Protocol). The device can be monitored by an SNMP manager.

1.4 Configuring Your NWA1121-NI's Security Features

Your NWA1121-NI comes with a variety of security features. This section summarizes these features and provides links to sections in the User's Guide to configure security settings on your NWA1121-NI. Follow the suggestions below to improve security on your NWA1121-NI and network.

1.4.1 Control Access to Your Device

Ensure only people with permission can access your NWA1121-NI.

- Control physical access by locating devices in secure areas, such as locked rooms. Most NWA1121-NIs have a reset button. If an unauthorized person has access to the reset button, they can then reset the device's password to its default password, log in and reconfigure its settings.
- Change any default passwords on the NWA1121-NI, such as the password used for accessing the NWA1121-NI's web configurator (if it has a web configurator). Use a password with a combination of letters and numbers and change your password regularly. Write down the password and put it in a safe place.
- ~~Avoid setting a long timeout period before the NWA1121-NI's web configurator automatically times out. A short timeout reduces the risk of unauthorized person accessing the web configurator while it is left idle.~~
- See [Section 11.5 on page 121](#) for instructions on changing your password ~~and setting the timeout period.~~
- Configure remote management to control who can manage your NWA1121-NI. See [Chapter 9 on page 101](#) for more information. If you enable remote management, ensure you have enabled remote management only on the IP addresses, services or interfaces you intended and that other remote management settings are disabled.

1.4.2 Wireless Security

Wireless devices are especially vulnerable to attack. ~~If your NWA1121-NI has a wireless function,~~ take the following measures to improve wireless security.

- Enable wireless security on your NWA1121-NI. Choose the most secure encryption method that all devices on your network support. See [Section 6.6 on page 74](#) for directions on configuring encryption. If you have a RADIUS server, enable IEEE 802.1x or WPA(2) user identification on your network so users must log in. This method is more common in business environments.
- Hide your wireless network name (SSID). The SSID can be regularly broadcast and unauthorized users may use this information to access your network. See [Section 6.5 on page 72](#) for directions on using the web configurator to hide the SSID.
- Enable the MAC filter to allow only trusted users to access your wireless network or deny unwanted users access based on their MAC address. See [Section 6.8 on page 89](#) for directions on configuring the MAC filter.

1.5 Good Habits for Managing the NWA1121-NI

Do the following things regularly to make the NWA1121-NI more secure and to manage it more effectively.

1.6 Hardware Connections

See your Quick Start Guide for information on making hardware connections.

1.7 LED

Figure 5 LED

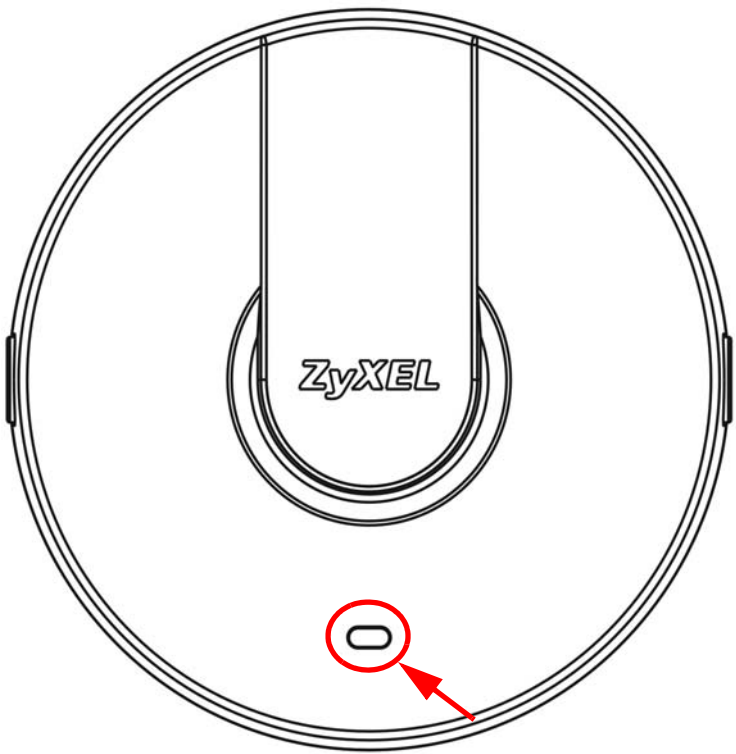


Table 1 LED

COLOR	STATUS	DESCRIPTION
Amber	On	There is system error and the NWA1121-NI cannot boot up, or the NWA1121-NI doesn't have an Ethernet connection with the LAN.
	Flashing	The NWA1121-NI is starting up.
	Off	The NWA1121-NI is receiving power and ready for use.
Green	Blinking	The WLAN is active, and transmitting or receiving data.
	Off	The WLAN is not active.

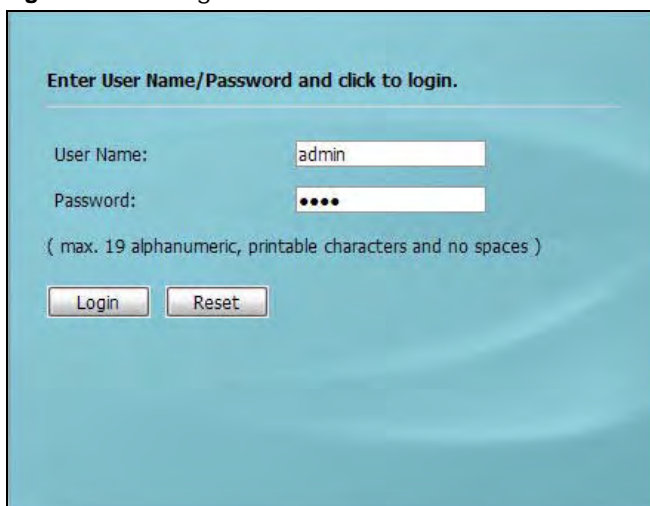
Introducing the Web Configurator

This chapter describes how to access the NWA1121-NI's web configurator and provides an overview of its screens.

2.1 Accessing the Web Configurator

- 1 Make sure your hardware is properly connected and prepare your computer or computer network to connect to the NWA1121-NI (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.2" as the URL (default). The login screen appears.

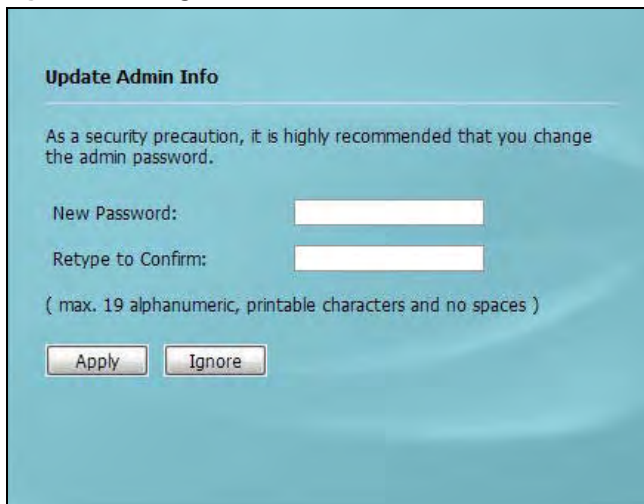
Figure 6 The Login Screen



- 4 Type "admin" as the (default) username and "1234" as the (default) password. Click **Login**.
- 5 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) then click **Apply**. Alternatively, click **Ignore**.

Note: If you do not change the password, the following screen appears every time you login.

Figure 7 Change Password Screen



You should now see the **Dashboard** screen. See [Chapter 2 on page 19](#) for details about the **Dashboard** screen.

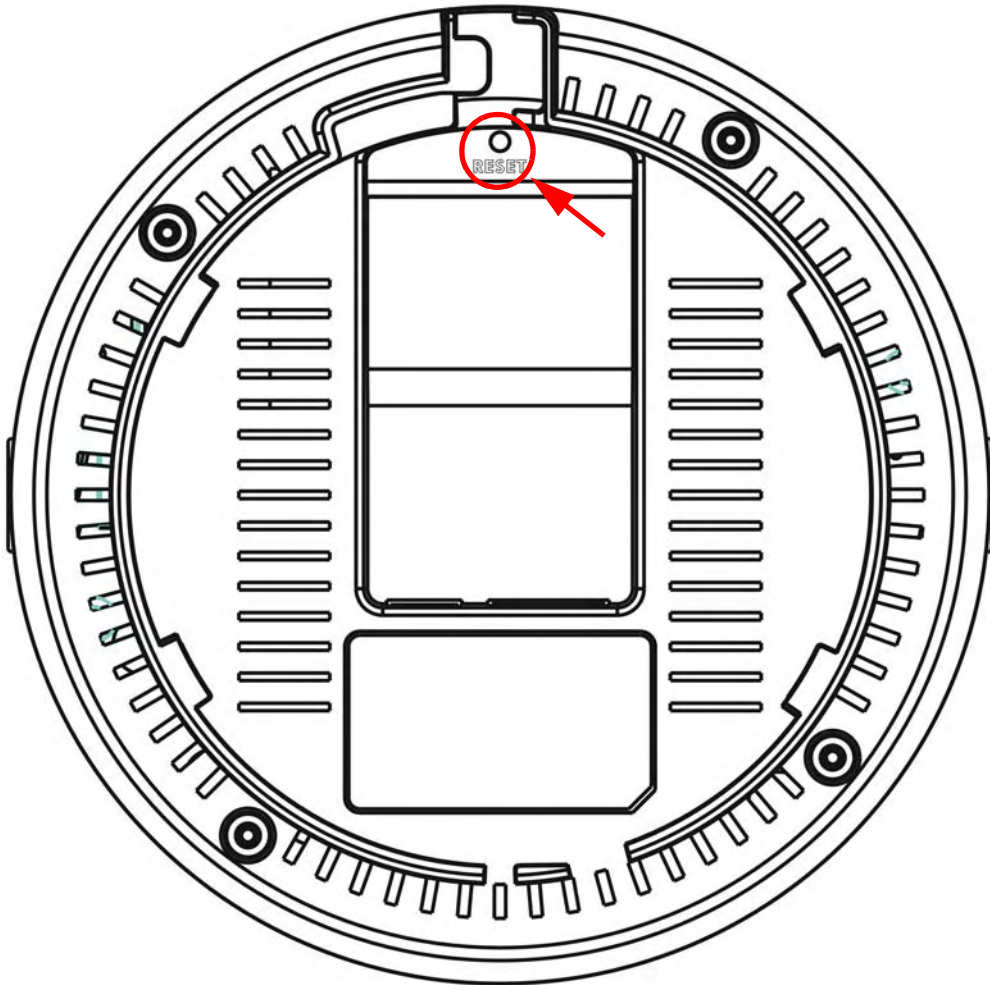
Note: ~~For security reasons, the NWA1121-NI automatically logs you out if you do not use the web configurator for five minutes (default). Simply log back into the NWA1121-NI if this happens.~~

2.2 Resetting the NWA1121-NI

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the rear panel of the NWA1121-NI. This replaces the current configuration file with the

factory-default configuration file. This means that you will lose all the settings you previously configured. The password will be reset to "1234".

Figure 8 The RESET Button



2.2.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in two ways:

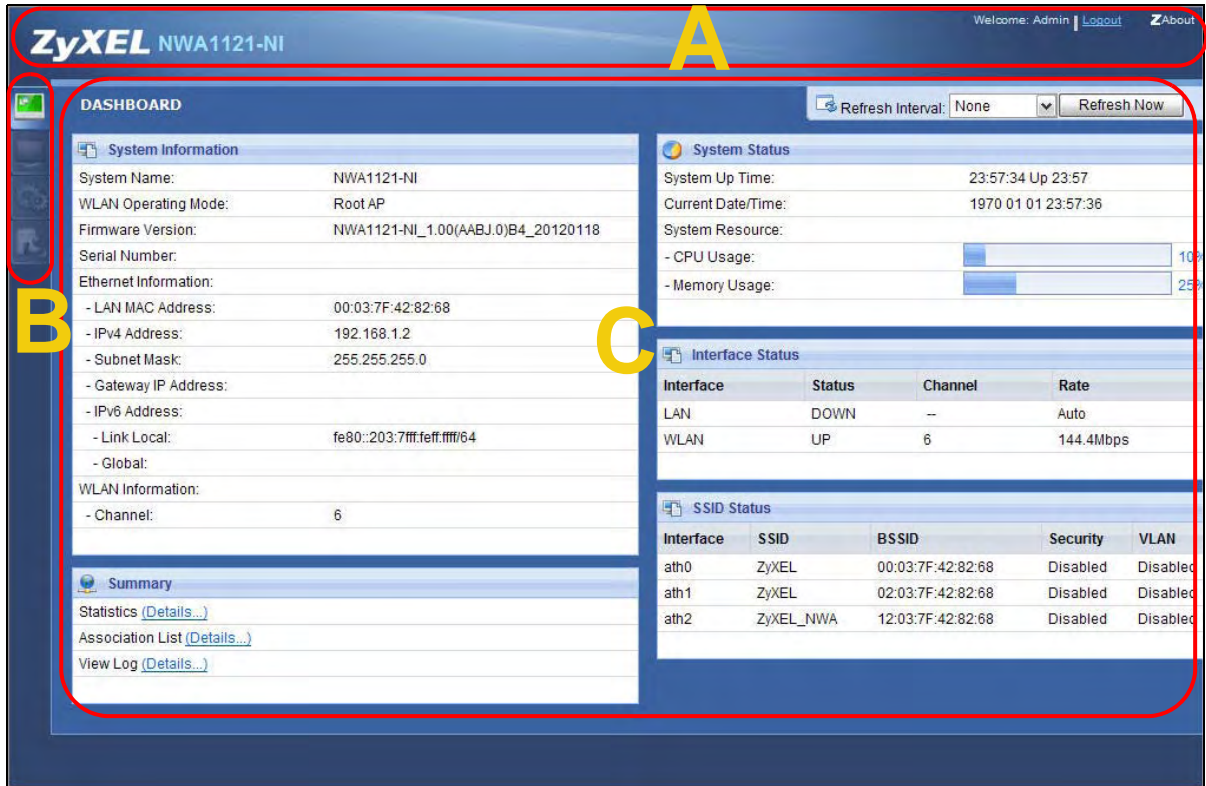
Use the **RESET** button to upload the default configuration file. Hold this button in **for about 3 seconds (the light will begin to blink)**. Use this method for cases when the password or IP address of the NWA1121-NI is not known.

Use the web configurator to restore defaults (refer to [Section 11.8 on page 124](#)).

2.3 Navigating the Web Configurator

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

Figure 9 Status Screen of the Web Configurator



As illustrated above, the Web Configurator screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window

2.3.1 Title Bar

Click **Logout** at any time to exit the Web Configurator.

Click **ZAbout** to open the about window, which provides information of the boot module and driver versions.

2.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure NWA1121-NI features. The following tables describe each menu item.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Dashboard		This screen shows the NWA1121-NI's general device and network status information. Use this screen to access the statistics and client list.
Monitor		
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Statistics		Use this screen to view port status, packet specific statistics, the "system up time" and so on.
Association List		Use this screen to view the wireless stations that are currently associated to the NWA1121-NI.
Channel Usage		Use this screen to know whether a channel is used by another wireless network or not.
Configuration		
Network		
Wireless LAN	Wireless Settings	Use this screen to configure the wireless LAN settings and NWA1121-NI's operation mode.
	SSID	Use this screen to configure up to eight SSID profiles for your NWA1121-NI.
	Security	Use this screen to configure wireless security profiles on the NWA1121-NI.
	RADIUS	Use this screen to configure up to four RADIUS profiles.
	MAC Filter	Use this screen to configure MAC filtering profiles.
LAN		Use this screen to configure the NWA1121-NI's LAN IP address.
VLAN		Use this screen to configure the NWA1121-NI's VLAN settings.
System	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NWA1121-NI.
	Certificates	Use this screen to import or remove a certificate from the NWA1121-NI.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NWA1121-NI.
	SNMP	Use this screen to configure the NWA1121-NI for SNMP management.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the NWA1121-NI.
Log Settings		Use this screen to change your log settings.
Maintenance		
General		Use this screen to configure your device's name.
Password		Use this screen to configure your device's password.
Time		Use this screen to change your NWA1121-NI's time and date.
Firmware Upgrade		Use this screen to upload firmware to your device.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Configuration File		Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Restart		Use this screen to reboot the NWA1121-NI without turning the power off.

2.3.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Dashboard

The **Dashboard** screens display when you log into the NWA1121-NI, or click **Dashboard** in the navigation menu.

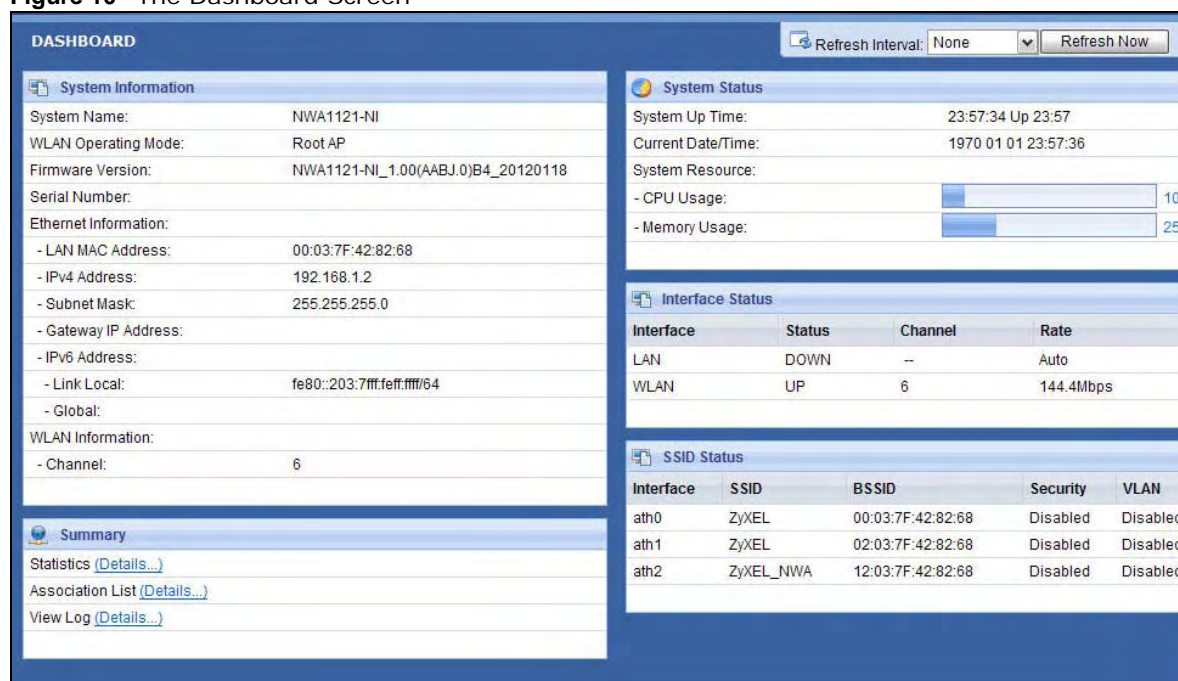
Use the **Dashboard** screen to look at the current status of the device, system resources, and interfaces. The **Dashboard** screens also provide detailed information about system statistics, associated wireless clients, and logs.

3.1 The Dashboard Screen

Use this screen to get a quick view of system, Ethernet, WLAN and other information regarding your NWA1121-NI.

Click **Dashboard**. The following screen displays.

Figure 10 The Dashboard Screen



The following table describes the labels in this screen.

Table 3 The Dashboard Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the NWA1121-NI to update this screen.
Refresh Now	Click this to update this screen immediately.
System Information	
System Name	This field displays the NWA1121-NI system name. It is used for identification. You can change this in the Maintenance > General screen's System Name field.
WLAN Operating Mode	This field displays the current operating mode of the first wireless module (RootAP , Repeater , Client , or MBSSID). You can change the operating mode in the Configuration > Wireless LAN > Wireless Settings screen.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in Maintenance > Firmware Upgrade .
Serial Number	This field displays the serial number of the NWA1121-NI.
Ethernet Information	
LAN MAC Address	This displays the MAC (Media Access Control) address of the NWA1121-NI on the LAN. Every network device has a unique MAC address which identifies it across the network.
IPv4 Address	This field displays the current IPv4 address of the NWA1121-NI on the network.
Subnet Mask	Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.
Gateway IP Address	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN port. The gateway helps forward packets to their destinations.
IPv6 Address	This field displays the current IPv6 address(es) of the NWA1121-NI on the network.
Link Local	This is the IPv6 link-local address that the NWA1121-NI generates automatically.
Global	This is the NWA1121-NI's IPv6 global address that you specify manually in the Configuration > LAN screen.
WLAN Information	
SSID	This field displays the SSID (Service Set Identifier). This is available only when the WLAN operation mode is Client .
Channel	The channel or frequency used by the NWA1121-NI to send and receive information.
Status	This shows the current status of the wireless LAN. This is available only when the WLAN operation mode is Client .
Security Mode	This displays the security mode the NWA1121-NI is using. This is available only when the WLAN operation mode is Client.
Summary	
Statistics	Click this link to view port status and packet specific statistics. See Section 5.4 on page 50 .
Association List	Click this to see a list of wireless clients currently associated to each of the NWA1121-NI's wireless modules. See Section 5.5 on page 51 .
View Log	Click this to see a list of logs produced by the NWA1121-NI. See Section 5.3 on page 49 .
System Status	
System Up Time	This field displays the elapsed time since the NWA1121-NI was turned on.

Table 3 The Dashboard Screen (continued)

LABEL	DESCRIPTION
Current Date/Time	This field displays the date and time configured on the NWA1121-NI. You can change this in the Maintenance > Time screen.
System Resource	
CPU Usage	This field displays what percentage of the NWA1121-NI's processing ability is currently being used. The higher the CPU usage, the more likely the NWA1121-NI is to slow down.
Memory Usage	This field displays what percentage of the NWA1121-NI's volatile memory is currently in use. The higher the memory usage, the more likely the NWA1121-NI is to slow down. Some memory is required just to start the NWA1121-NI and to run the web configurator.
Interface Status	
Interface	This column displays each interface of the NWA1121-NI.
Status	This field indicates whether or not the NWA1121-NI is using the interface. For each interface, this field displays Up when the NWA1121-NI is using the interface and Down when the NWA1121-NI is not using the interface.
Channel	This shows the channel number which the NWA1121-NI is currently using over the wireless LAN.
Rate	For the LAN port this displays the port speed and duplex setting. For the WLAN interface, it displays the downstream and upstream transmission rate or N/A if the interface is not in use.
SSID Status	This section is not available when the WLAN operation mode is Client .
Interface	This column displays each of the NWA1121-NI's wireless interfaces.
SSID	This field displays the SSID(s) currently used by each wireless module.
BSSID	This field displays the MAC address of the wireless module.
Security	This field displays the type of wireless security used by each SSID.
VLAN	This field displays the VLAN ID of each SSID in use, or Disabled if the SSID does not use VLAN.

Tutorial

This chapter first provides an overview of how to configure the wireless LAN on your NWA1121-NI, and then gives step-by-step guidelines showing how to configure your NWA1121-NI for some example scenarios.

4.1 How to Configure the Wireless LAN

This section illustrates how to choose which wireless operating mode to use on the NWA1121-NI and how to set up the wireless LAN in each wireless mode. See [Section 4.1.2 on page 29](#) for links to more information on each step.

4.1.1 Choosing the Wireless Mode

- Use **MBSSID** (Multiple Basic Service Set Identifier) operating mode if you want to use the NWA1121-NI as an access point with some groups of users having different security or QoS settings from other groups of users. See [Section 1.2.1 on page 12](#) for details.
- Use **Client** operating mode if you want to use the NWA1121-NI to access a wireless network. See [Section 1.2.2 on page 13](#) for details.
- Use **Root AP** operating mode if you want to allow wireless clients to access your wired network through the NWA1121-NI and also have repeaters communicate with the NWA1121-NI to expand wireless coverage. See [Section 1.2.3 on page 14](#) for details.
- Use **Repeater** operating mode if you want to use the NWA1121-NI to communicate with the root AP or other repeaters. See [Section 1.2.4 on page 14](#) for details.

4.1.2 Further Reading

Use these links to find more information on the steps:

- Choosing **802.11 Mode**: see [Section 6.4 on page 60](#).
- Choosing a wireless **Channel ID**: see [Section 6.4 on page 60](#).
- Choosing a **Security** mode: see [Section 6.6 on page 74](#).
- Configuring an external **RADIUS** server: see [Section 6.7 on page 87](#).
- Configuring **MAC Filtering**: see [Section 6.8 on page 89](#).

4.2 How to Configure Multiple Wireless Networks

In this example, you have been using your NWA1121-NI as an access point for your office network. Now your network is expanding and you want to make use of the MBSSID feature (see [Section](#)

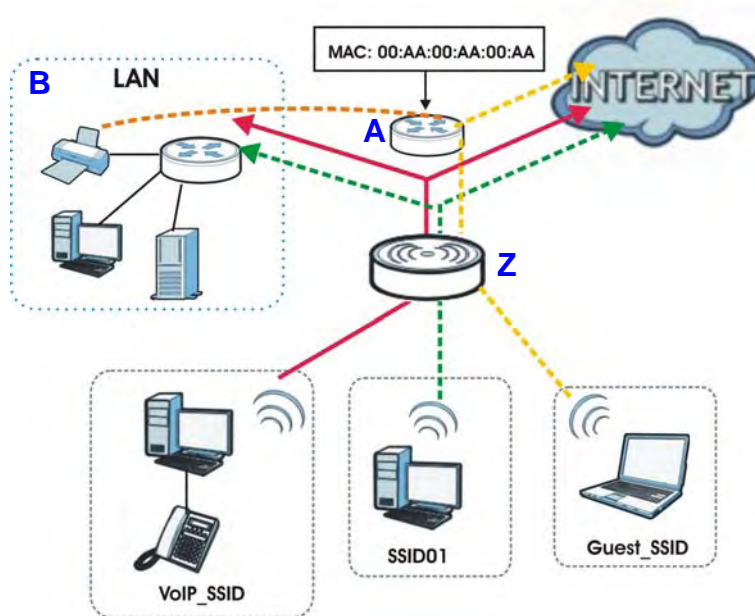
6.4.4 on page 69) to provide multiple wireless networks. Each wireless network will cater to a different type of user.

You want to make three wireless networks: one standard office wireless network with all the same settings you already have, another wireless network with high priority QoS settings for Voice over IP (VoIP) users, and a guest network that allows visitors to access only the Internet and the network printer.

To do this, you will take the following steps:

- 1 Edit the SSID profiles.
- 2 Change the operating mode from **Root AP** to **MBSSID** and reactivate the standard network.
- 3 Configure different security modes for the networks.
- 4 Configure a wireless network for standard office use.
- 5 Configure a wireless network for VoIP users.
- 6 Configure a wireless network for guests to your office.

The following figure shows the multiple networks you want to set up. Your NWA1121-NI is marked **Z**, the main network router is marked **A**, and your network printer is marked **B**.



The standard network (**SSID01**) has access to all resources. The VoIP network (**VoIP_SSID**) has access to all resources and a high QoS priority. The guest network (**Guest_SSID**) has access to the Internet and the network printer only, and a low QoS priority.

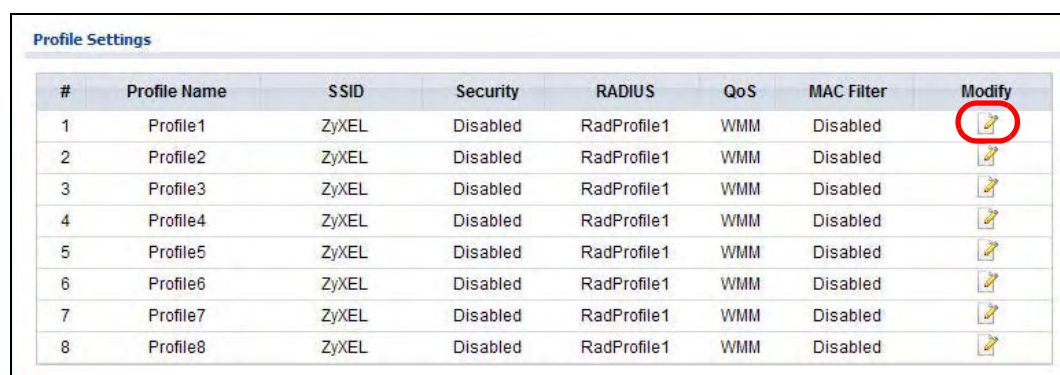
To configure these settings, you need to know the Media Access Control (MAC) addresses of the devices you want to allow users of the guest network to access. The following table shows the addresses used in this example.









Table 4 Tutorial: Example Information

Network router (A) MAC address	00:AA:00:AA:00:AA
Network printer (B) MAC address	AA:00:AA:00:AA:00

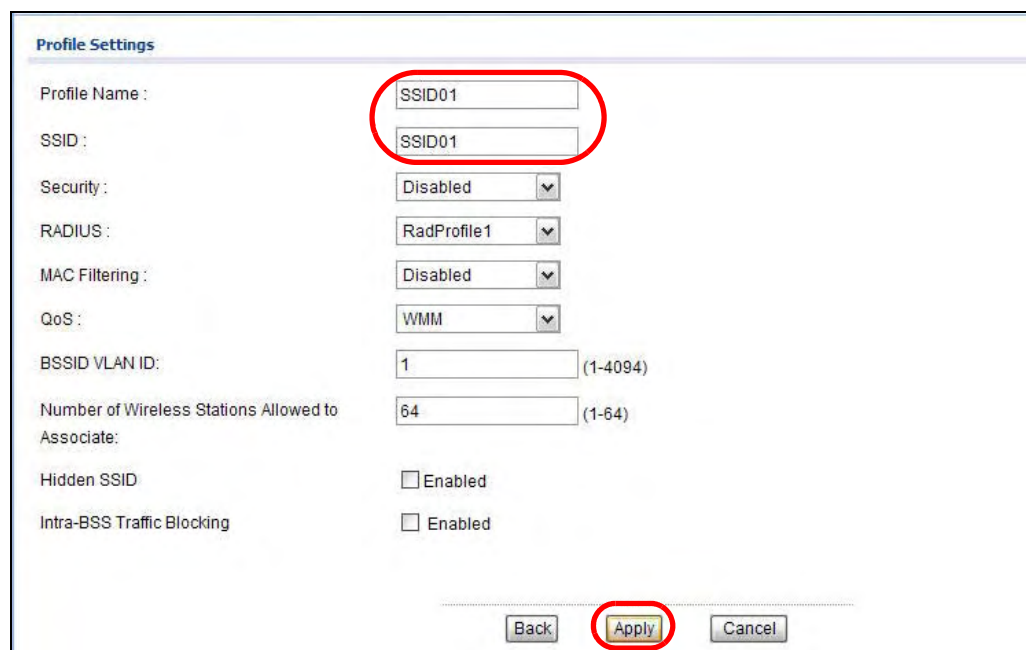
4.2.1 Configure the SSID Profiles

- 1 Log in to the NWA1121-NI (see [Section 2.1 on page 19](#)). Click **Wireless LAN > SSID**. The **SSID** screen appears.
- 2 Click the **Edit** icon next to the **Profile1**.



#	Profile Name	SSID	Security	RADIUS	QoS	MAC Filter	Modify
1	Profile1	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
2	Profile2	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
3	Profile3	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
4	Profile4	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
5	Profile5	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
6	Profile6	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
7	Profile7	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
8	Profile8	ZyXEL	Disabled	RadProfile1	WMM	Disabled	

- 3 Rename the **Profile Name** and **SSID** as **SSID01**. Click **Apply**.



Profile Settings

Profile Name :

SSID :

Security :

RADIUS :

MAC Filtering :

QoS :

BSSID VLAN ID: (1-4094)

Number of Wireless Stations Allowed to Associate: (1-64)

Hidden SSID ☐ Enabled

Intra-BSS Traffic Blocking ☐ Enabled

- 4 Repeat Step 2 and 3 to change **Profile2** and **Profile3** to **VoIP_SSID** and **Guest_SSID**.

4.2.1.1 MBSSID

- 1 Go to **Wireless LAN > Wireless Settings**. Select **MBSSID** from the **Operation Mode** drop-down list box.
- 2 **SSID01** is the standard network, so select **SSID01** as the first profile. It is always active.
- 3 Select **VoIP_SSID** as the second profile, and **Guest_SSID** as the third profile. Select the corresponding **Active** check-boxes.
- 4 Click **Apply** to save your settings. Now the three SSIDs are activated.

The screenshot shows the 'Wireless Settings' page with the 'SSID' tab selected. The 'Basic Settings' section includes:

- Wireless LAN Interface: ☒ Enabled
- Operation Mode: MBSSID (highlighted with a red circle)
- Wireless Mode: 802.11b/g/n
- Channel: 6
- Channel Width: 20MHZ

The 'Select SSID Profile' section contains a table with two columns of settings:

#	Active	Profile	#	Active	Profile
1	<input checked="" type="checkbox"/>	SSID01	2	<input type="checkbox"/>	SSID01
3	<input checked="" type="checkbox"/>	VoIP_SSID	4	<input type="checkbox"/>	SSID01
5	<input checked="" type="checkbox"/>	Guest_SSID	6	<input type="checkbox"/>	SSID01
7	<input type="checkbox"/>	SSID01	8	<input type="checkbox"/>	SSID01

The 'Advanced Settings' section includes:









- Beacon Interval: 100 (25-1000 ms)
- DTIM Interval: 1 (1-15)
- Output Power: Full
- Preamble Type: Dynamic
- RTS/CTS Threshold: 2346 (1-2346)
- Extension Channel Protection Mode: None
- A-MPDU Aggregation: ☒ Enabled
- Short GI: ☒ Enabled

At the bottom, the 'MCS Rate' section shows a table with checkboxes for rates 0 through 15. The 'Apply' button is highlighted with a red circle.

4.2.2 Configure the Standard Network

- 1 Click **Wireless LAN > SSID**. Click the **Edit** icon next to **SSID01**.

Profile Settings

#	Profile Name	SSID	Security	RADIUS	QoS	MAC Filter	Modify
1	SSID01	SSID01	Disabled	RadProfile1	WMM	Disabled	
2	VoIP_SSID	VoIP_SSID	Disabled	RadProfile1	WMM	Disabled	
3	Guest_SSID	Guest_SSID	Disabled	RadProfile1	WMM	Disabled	
4	Profile4	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
5	Profile5	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
6	Profile6	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
7	Profile7	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
8	Profile8	ZyXEL	Disabled	RadProfile1	WMM	Disabled	

- 2 Select **SecProfile1** as **SSID01**'s security profile. Select the **Hidden SSID** checkbox as you want only authorized company employees to use this network, so there is no need to broadcast the SSID to wireless clients scanning the area.

Also, the clients on **SSID01** might need to access other clients on the same wireless network. Do not select the **Intra-BSS Traffic blocking** check-box.

Click **Apply**.

Profile Settings

Profile Name :

SSID :

Security :

RADIUS :

MAC Filtering :

QoS :

BSSID VLAN ID: (1-4094)

Number of Wireless Stations Allowed to Associate: (1-64)









Hidden SSID ☒ Enabled

Intra-BSS Traffic Blocking ☐ Enabled

Back **Apply** Cancel

- 3 Next, click **Wireless LAN > Security**. Click the **Edit** icon next to **SecProfile1**.

Security Profiles

#	Profile Name	Security Mode	Modify
1	SecProfile1	None	
2	SecProfile2	None	
3	SecProfile3	None	
4	SecProfile4	None	
5	SecProfile5	None	
6	SecProfile6	None	
7	SecProfile7	None	
8	SecProfile8	None	

- 4 Since **SSID01** is the standard network that has access to all resources, assign a more secure security mode. Select **WPA2-PSK-MIX** as the **Security Mode**, and enter the **Pre-Shared Key**. In this example, use **ThisisSSID01PreSharedKey**. Click **Apply**.

Security Settings

Profile Name:

Security Mode:









Pre-Shared Key: (8-63 ASCII Characters)

- 5 You have finished configuring the standard network, **SSID01**.

4.2.3 Configure the VoIP Network

- 1 Go to **Wireless LAN > SSID**. Click the **Edit** icon next to **VoIP_SSID**.

Profile Settings

#	Profile Name	SSID	Security	RADIUS	QoS	MAC Filter	Modify
1	SSID01	SSID01	Disabled	RadProfile1	WMM	Disabled	
2	VoIP_SSID	VoIP_SSID	Disabled	RadProfile1	WMM	Disabled	
3	Guest_SSID	Guest_SSID	Disabled	RadProfile1	WMM	Disabled	
4	Profile4	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
5	Profile5	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
6	Profile6	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
7	Profile7	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
8	Profile8	ZyXEL	Disabled	RadProfile1	WMM	Disabled	

- 2 Select **SecProfile2** as the **Security Profile** for the VoIP network. Select the **Hidden SSID** checkbox.

- 3 Select **WMM_VOICE** in the **QoS** field to give VoIP the highest priority in the wireless network. Click **Apply**.

Profile Settings

Profile Name : VoIP_SSID

SSID : VoIP_SSID

Security : SecProfile2

RADIUS : RadProfile1

MAC Filtering : Disabled

QoS : WMM_VOICE

BSSID VLAN ID: 1 (1-4094)

Number of Wireless Stations Allowed to Associate: 64 (1-64)









Hidden SSID ☒ Enabled

Intra-BSS Traffic Blocking ☐ Enabled

Back **Apply** Cancel

- 4 Next, click **Wireless LAN > Security**. Click the **Edit** icon next to **SecProfile2**.

Security Profiles

#	Profile Name	Security Mode	Modify
1	SecProfile1	WPA2-PSK-MIX	
2	SecProfile2	None	
3	SecProfile3	None	
4	SecProfile4	None	
5	SecProfile5	None	
6	SecProfile6	None	
7	SecProfile7	None	
8	SecProfile8	None	

- 5 Select **WPA2-PSK** as the **Security Mode**, and enter the **Pre-Shared Key**. In this example, use **ThisisVoIPPreSharedKey**. Click **Apply**.

Security Settings

Profile Name:

Security Mode:

Pre-Shared Key: (8-63 ASCII Characters)

- 6 Your VoIP wireless network is now ready to use. Any traffic using the **VoIP_SSID** profile will be given the highest priority across the wireless network.

4.2.4 Configure the Guest Network

When you are setting up the wireless network for guests to your office, your primary concern is to keep your network secure while allowing access to certain resources (such as a network printer, or the Internet). For this reason, the pre-configured **Guest_SSID** profile has intra-BSS traffic blocking enabled by default. "Intra-BSS traffic blocking" means that the client cannot access other clients on the same wireless network.

- 1 Click **Wireless LAN > SSID**. Click the **Edit** icon next to **Guest_SSID**.

Profile Settings

#	Profile Name	SSID	Security	RADIUS	QoS	MAC Filter	Modify
1	SSID01	SSID01	Disabled	RadProfile1	WMM	Disabled	
2	VoIP_SSID	VoIP_SSID	Disabled	RadProfile1	WMM	Disabled	
3	Guest_SSID	Guest_SSID	Disabled	RadProfile1	WMM	Disabled	
4	Profile4	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
5	Profile5	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
6	Profile6	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
7	Profile7	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
8	Profile8	ZyXEL	Disabled	RadProfile1	WMM	Disabled	

- 2 Select **SecProfile3** in the **Security** field. Do not select the **Hidden SSID** check-box so the guests can easily find the wireless network.
- 3 Select **WMM_BESTEFFORT** in the **QoS** field to give the guest a lower QoS priority.

- 4 Select the check-box of **Intra-BSS Traffic blocking Enabled**. Click **Apply**.

Profile Settings

Profile Name : Guest_SSID

SSID : Guest_SSID

Security : SecProfile3

RADIUS : RadProfile1

MAC Filtering : Disabled

QoS : WMM_BESTEFFC

BSSID VLAN ID: 1 (1-4094)

Number of Wireless Stations Allowed to Associate: 64 (1-64)









Hidden SSID ☐ Enabled

Intra-BSS Traffic Blocking ☒ Enabled

Back Apply Cancel

- 5 Next, click **Wireless LAN > Security**. Click the **Edit** icon next to **SecProfile3**.

Security Profiles

#	Profile Name	Security Mode	Modify
1	SecProfile1	WPA2-PSK-MIX	
2	SecProfile2	WPA2-PSK	
3	SecProfile3	None	
4	SecProfile4	None	
5	SecProfile5	None	
6	SecProfile6	None	
7	SecProfile7	None	
8	SecProfile8	None	

- 6 Select **WPA-PSK** in the **Security Mode** field. WPA-PSK provides strong security that is supported by most wireless clients. Even though your **Guest_SSID** clients do not have access to sensitive information on the network, you should not leave the network without security. An attacker could still cause damage to the network or intercept unsecured communications or use your Internet access for illegal activities.

- 7 Enter the PSK you want to use in your network in the **Pre Shared Key** field. In this example, the PSK is **ThisismyGuestWPApre-sharedkey**. Click **Apply**.

- 8 Your guest wireless network is now ready to use.

4.2.5 Testing the Wireless Networks

To make sure that the three networks are correctly configured, do the following.

- On a computer with a wireless client, scan for access points. You should see the **Guest_SSID** network, but not the **SSID01** and **VoIP_SSID** networks. If you can see the **SSID01** and **VoIP_SSID** networks, go to its **SSID Edit** screen and make sure to select the **Hidden SSID** check-box and click **Apply**.
- Try to access each network using the correct security settings, and then using incorrect security settings, such as the WPA-PSK for another active network. If the behavior is different from expected (for example, if you can access the **SSID01** or **VoIP_SSID** wireless network using the security settings for the **Guest_SSID** wireless network) check that the SSID profile is set to use the correct security profile, and that the settings of the security profile are correct.

4.3 NWA1121-NI Setup in AP and Wireless Client Modes

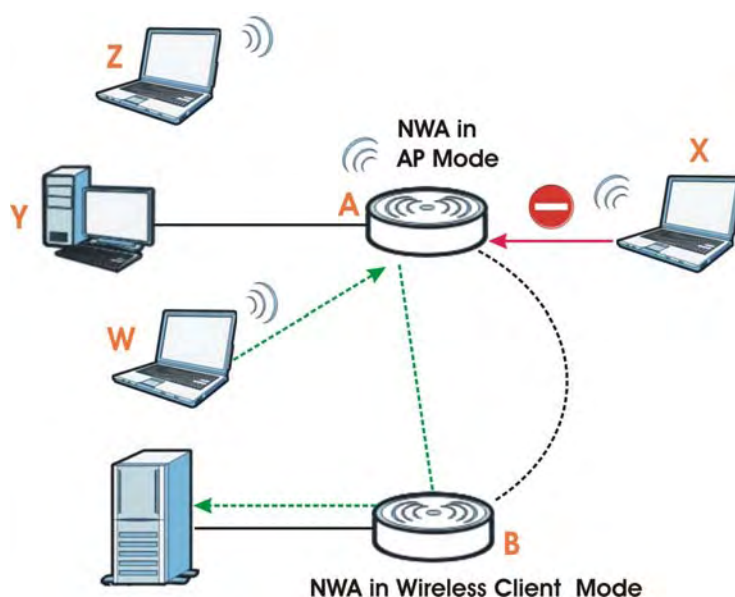
This example shows you how to restrict wireless access to your NWA1121-NI.

4.3.1 Scenario

In the figure below, there are two NWA1121-NIs (**A** and **B**) in the network. **A is in MBSSID or root AP mode while station B is in wireless client mode**. Station **B** is connected to a File Transfer Protocol (FTP) server. You want only specified wireless clients to be able to access station **B**. You also want

to allow wireless traffic between **B** and wireless clients connected to **A** (**W**, **Y** and **Z**). Other wireless devices (**X**) must not be able to connect to the FTP server.

Figure 11 FTP Server Connected to a Wireless Client



4.3.2 Configuring the NWA1121-NI in MBSSID or Root AP Mode

Before setting up the NWA1121-NI as a wireless client (**B**), you need to make sure there is an access point to connect to. Use the Ethernet port on NWA1121-NI (**A**) to configure it via a wired connection.

Log into the Web Configurator on NWA1121-NI (A) and go to the **Wireless LAN > Wireless Settings** screen.

Basic Settings

Wireless LAN Interface : ☒ Enabled

Operation Mode : Root AP

Wireless Mode : 802.11b/g/n

Channel : 6

Channel Width : 20MHz

Select SSID Profile :

#	Active	Profile	#	Active	Profile
1	<input checked="" type="checkbox"/>	Profile1	2	<input type="checkbox"/>	Profile1
3	<input type="checkbox"/>	Profile1	4	<input type="checkbox"/>	Profile1

Universal Repeater Settings

Local MAC Address : 00:03:7F:42:82:68

Universal Repeater SSID Profile : Profile1

Advanced Settings

Beacon Interval : 100 (25-1000 ms)

DTIM Interval : 1 (1-15)

Output Power : Full

Preamble Type : Dynamic

RTS/CTS Threshold : 2346 (1-2346)

Extension Channel Protection Mode : None

A-MPDU Aggregation : ☒ Enabled

Short GI : ☒ Enabled









MCS Rate	Auto	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Cancel

- 1 Set the **Operation Mode** to **Root AP**.
- 2 Select the **Wireless Mode**. In this example, select **802.11b/g/n**.
- 3 Select **Profile1** as the **SSID Profile**.
- 4 Choose the **Channel** you want NWA1121-NI (A) to use.
- 5 Click **Apply**.

- 6 Go to **Wireless LAN > SSID**. Click the **Edit** icon next to **Profile1**.

Profile Settings

#	Profile Name	SSID	Security	RADIUS	QoS	MAC Filter	Modify
1	Profile1	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
2	Profile2	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
3	Profile3	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
4	Profile4	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
5	Profile5	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
6	Profile6	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
7	Profile7	ZyXEL	Disabled	RadProfile1	WMM	Disabled	
8	Profile8	ZyXEL	Disabled	RadProfile1	WMM	Disabled	

- 7 Change the **SSID** to **AP-A**.
- 8 Select **SecProfile1** in the **Security** field.
- 9 Select the check-box for **Intra-BSS Traffic blocking Enabled** so the client cannot access other clients on the same wireless network.
- 10 Click **Apply**.

Profile Settings

Profile Name :

SSID :

Security :

RADIUS :

MAC Filtering :

QoS :

BSSID VLAN ID: (1-4094)







Number of Wireless Stations Allowed to Associate: (1-64)

Hidden SSID ☐ Enabled

Intra-BSS Traffic Blocking ☒ Enabled

Back Apply Cancel

- 11 Go to **Wireless LAN > Security**. Click the **Edit** icon next to **SecProfile1**.

Security Profiles			
#	Profile Name	Security Mode	Modify
1	SecProfile1	None	
2	SecProfile2	None	
3	SecProfile3	None	
4	SecProfile4	None	
5	SecProfile5	None	
6	SecProfile6	None	
7	SecProfile7	None	
8	SecProfile8	None	

- 12 Configure **WPA-PSK** as the **Security Mode** and enter **ThisIsMyPreSharedKey** in the **Pre-Shared Key** field.
- 13 Click **Apply** to finish configuration for NWA1121-NI (A).

Security Settings	
Profile Name:	SecProfile1
Security Mode:	WPA-PSK
Pre-Shared Key	ThisIsMyPreSharedKey (8-63 ASCII Characters)
<div> <input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>	

4.3.3 Configuring the NWA1121-NI in Wireless Client Mode

The NWA1121-NI (B) should have a wired connection before it can be set to wireless client operating mode. Connect your NWA1121-NI to the FTP server. Login to NWA1121-NI (B)'s Web Configurator and go to the **Wireless LAN > Wireless Settings** screen. Follow these steps to configure station B.

- 1 Select **Client** as **Operation Mode**. Click **Apply**.

Basic Settings

Wireless LAN Interface : ☒ Enabled

Operation Mode : Client Site Survey

SSID Profile : Profile1

Channel : 6

Channel Width : 20MHZ

Advanced Settings

Output Power : Full

Preamble Type : Dynamic

RTS/CTS Threshold : 2346 (1-2346)

Extension Channel Protection Mode : None

A-MPDU Aggregation : ☒ Enabled

Short GI : ☒ Enabled

Apply Cancel

- 2 Click on the **Site Survey** button. A window should pop up which contains a list of all available wireless devices within your NWA1121-NI's range.
- 3 Find and select **NWA1121-NI (A)'s SSID: AP-A**.

Site Survey

Select	SSID	Channel	MAC Address	Wireless Mode	Signal Strength	Security
<input type="radio"/>	ZyXEL_MIS_WPA	1	50:67:F0:37:A0:85	802.11b/g/n	87%	WPA2
<input type="radio"/>	ZT01053-I	1	00:13:49:00:00:06	802.11b/g/n	33%	WPA2-PSK
<input type="radio"/>	AP-A	1	22:00:AA:79:78:47	802.11b/g/n	90%	WPA-PSK
<input type="radio"/>	NWA1121-NI-85898	1	CC:5D:4E:66:3B:3D	802.11b/g/n	70%	WPA2-PSK
<input type="radio"/>	linux-jc	1	C8:3A:35:C0:00:F5	802.11b/g	33%	WPA-PSK
<input type="radio"/>	ZT01053	5	40:4A:03:49:6E:0C	802.11b/g/n	50%	WPA2-PSK
<input type="radio"/>	Home_3160-N	6	40:4A:03:79:ED:4D	802.11b/g/n	80%	WPA2-PSK
<input type="radio"/>	w8021xwpa	6	50:67:F0:37:9F:72	802.11b/g	16%	WPA

Refresh

- Go to **Wireless LAN > Security** to configure the NWA1121-NI to use the same security mode and Pre-Shared Key as **NWA1121-NI (A): WPA-PSK/ThisisMyPreSharedKey**. Click **Apply**.

Figure 12

Security Settings

Profile Name: SecProfile1

Security Mode: WPA-PSK

Pre-Shared Key: ThisisMyPreSharedKey (8-63 ASCII Characters)

Back Apply Cancel

4.3.4 MAC Filter Setup

One way to ensure that only specified wireless clients can access the FTP server is by enabling MAC filtering on NWA1121-NI (B) (See [Section 6.8 on page 89](#) for more information on MAC Filter).

- Go to **Wireless LAN > MAC Filter**. Click the **Edit** icon next to **MacProfile1**.

#	Profile Name	Filter Action	Modify
1	MacProfile1	Disabled	
2	MacProfile2	Disabled	
3	MacProfile3	Disabled	
4	MacProfile4	Disabled	
5	MacProfile5	Disabled	
6	MacProfile6	Disabled	
7	MacProfile7	Disabled	
8	MacProfile8	Disabled	

- Select **Allow** in the **Access Control Mode** field. Enter the MAC addresses of the wireless clients (**W**, **Y** and **Z**) you want to associate with the NWA1121-NI. Click **Apply**.

MAC Filter

MAC Filter Settings

Profile Name: MacProfile1

Access Control Mode: Allow

#	MAC Address	#	MAC Address
1		2	
3		4	

Now, only the authorized wireless clients (**W**, **Y** and **Z**) can access the FTP server.

4.3.5 Testing the Connection and Troubleshooting

This section discusses how you can check if you have correctly configured your network setup as described in this tutorial.

- Try accessing the FTP server from wireless clients **W**, **Y** or **Z**. Test if you can send or retrieve a file. If you cannot establish a connection with the FTP server, do the following steps.

- 1 Make sure **W**, **Y** and **Z** use the same wireless security settings as **A** and can access **A**.
 - 2 Make sure **B** uses the same wireless and wireless security settings as **A** and can access **A**.
 - 3 Make sure intra-BSS traffic is enabled on **A**.
 - Try accessing the FTP server from **X**. If you are able to access the FTP server, do the following.
- 1 Make sure MAC filtering is enabled.
 - 2 Make sure **X**'s MAC address is not entered in the list of allowed devices.

PART II

Technical Reference

The appendices provide general information. Some details may not apply to your NWA1121-NI.

Monitor

5.1 Overview

This chapter discusses read-only information related to the device state of the NWA1121-NI.

Note: To access the **Monitor** screens, you can also click the links in the Summary table of the **Dashboard** screen to view the **wireless packets** sent/received as well as the status of clients connected to the NWA1121-NI.

5.2 What You Can Do

- Use the **Logs** screen to see the logs for the categories that you selected in the **Configuration > Log Settings** screen (see [Section 5.3 on page 49](#)). You can view logs in this page. **Once the log entries are all used, the log will wrap around and the old logs will be deleted.**
- use the **Statistics** screen to **view 802.11 mode, channel number, wireless packet specific statistics and so on** (see [Section 5.4 on page 50](#)).
- Use the **Association List** screen to view the **wireless devices** that are currently associated to the NWA1121-NI (see [Section 5.5 on page 51](#)).
- Use the **Channel Usage** screen to view whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap (see [Section 5.6 on page 52](#)).

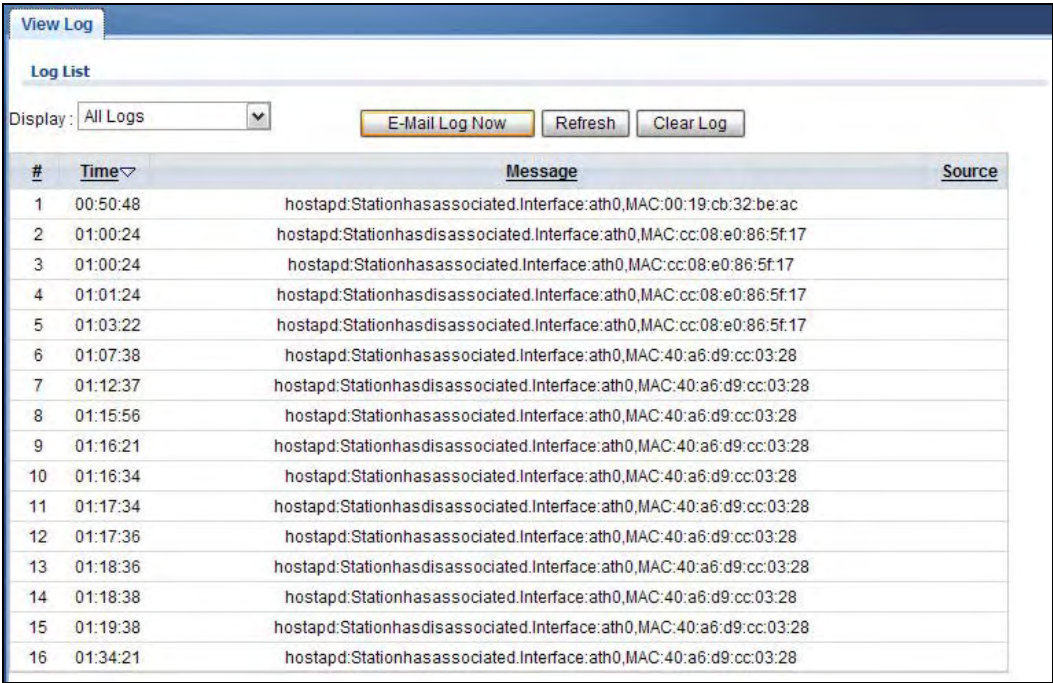
5.3 View Logs

Use the **Logs** screen to see the logged messages for the NWA1121-NI.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills.

Click **Monitor > Logs**.

Figure 13 Logs



The following table describes the labels in this screen.

Table 5 Logs

LABEL	DESCRIPTION
Display	Select a category of logs to view. Select All Log to view logs from all of the log categories that you selected in the Configuration > Log Settings screen.
E-Mail Log Now	Click E-Mail Log Now to send the log screen to the e-mail address specified in the Log Settings page (make sure that you have first filled in the E-mail Log Settings fields in Configuration > Log Settings).
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
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.

5.4 Statistics

Use this screen to view read-only information, including 802.11 Mode, Channel ID, Retry Count and FCS Error Count. Also provided is the "poll interval". The **Poll Interval** field is configurable and is used for refreshing the screen.

Click **Monitor > Statistics**. The following screen pops up.

Figure 14 Statistics

The screenshot shows a web interface titled "Statistics". Below the title is a "View Status" section containing a table with the following data:

Description	802.11 Mode	Channel ID	RX Pkts	TX Pkts	Retry Count	FCS Error Count
WLAN1	802.11ng	6	7288510	936751	0	0

Below the table, there is a "Poll Interval(s)" field set to "5", a range "(1-65534) sec", a "Set Interval" button, and a "Stop" button.

The following table describes the labels in this screen.

Table 6 Statistics

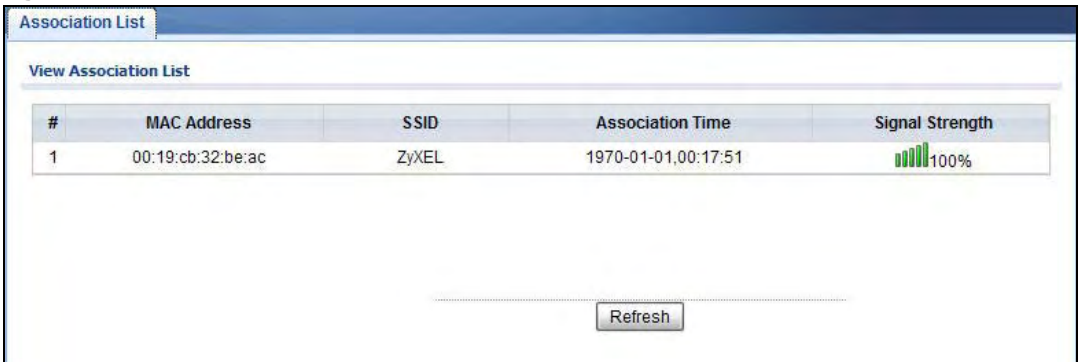
LABEL	DESCRIPTION
Description	This is the wireless interface on the NWA1121-NI.
802.11 Mode	This field shows which 802.11 mode the NWA1121-NI is using.
Channel ID	This shows the channel number which the NWA1121-NI is currently using over the wireless LAN.
RX Pkts	This is the number of received packets on this port.
TX Pkts	This is the number of transmitted packets on this port.
Retry Count	This is the total number of retries for transmitted packets (TX).
FCS Error Count	This is the ratio percentage showing the total number of checksum error of received packets (RX) over total RX.
Poll Interval	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.

5.5 Association List

View the wireless devices that are currently associated with the NWA1121-NI in the **Association List** screen. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Click **Monitor** > **Association List** to display the screen as shown next.

Figure 15 Association List



The following table describes the labels in this screen.

Table 7 Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless device.
MAC Address	This field displays the MAC address of an associated wireless device.
SSID	This field displays the SSID to which the wireless device is associated.
Association Time	This field displays the time a wireless device first associated with the NWA1121-NI's wireless network.
Signal Strength	This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection.
Refresh	Click Refresh to reload the list.
















5.6 Channel Usage

Use this screen to know whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.

Click **Monitor** > **Channel Usage** to display the screen shown next.

Wait a moment while the NWA1121-NI compiles the information.

Figure 16 Channel Usage

Channel Usage						
Site Survey						
SSID	Channel	MAC Address	Wireless Mode	Signal Strength	Security	
ZyXEL_NAS_Aslan	6	00:02:CF:9C:63:F0	802.11b/g	 73%	WPA2-PSK	
ZyXEL_MIS_WPA	6	06:19:CB:8A:34:D0	802.11b/g	 22%	WPA2	
HCILab	9	00:17:9A:50:24:9F	802.11b/g	 77%	WPA2-PSK	
ZyXEL_4CWHW7	6	00:13:49:FA:54:B4	802.11b/g	 46%	WPA2-PSK	
ZyXEL_MT01991	6	C8:6C:87:80:D2:6C	802.11b/g	 26%	WPA2-PSK	
kkap	6	04:46:65:74:C8:F9	802.11b/g	 9%	WPA2-PSK	
SecureWirelessNetwork	6	00:19:CB:00:00:00	802.11b/g	 16%	WPA2-PSK	
	6	68:92:34:09:9E:C1	802.11b/g	 9%	WPA-PSK	
5200-TUN24G-IN-PSK	6	22:4A:03:05:82:3B	802.11b/g	 16%	WPA2-PSK	
5200-TUN24G-OUT-WPA2	6	02:4A:03:05:82:3B	802.11b/g	 16%	WPA2	
5200-TUN24G-IN-WPA2	6	40:4A:03:05:82:3B	802.11b/g	 16%	WPA2	
TN_private_H77E9W	7	00:13:49:12:84:60	802.11b/g	 1%	WPA-PSK	
ZyXEL_MIS_WPA	11	40:4A:03:69:D9:F5	802.11b/g	 43%	WPA2	
ZyXEL_MIS_WPA	1	50:67:F0:37:A0:25	802.11b/g	 87%	WPA2	
ZyXEL_GUEST	36	62:67:F0:37:A0:26	802.11a	 5%	WEP	
<div>Refresh</div>						

The following table describes the labels in this screen.

Table 8 Channel Usage

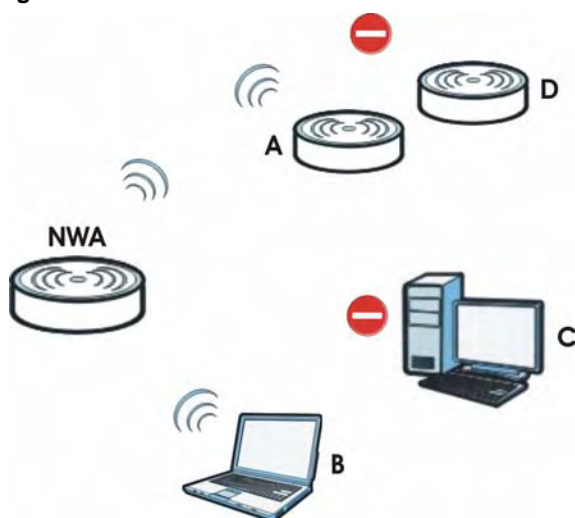
LABEL	DESCRIPTION
SSID	This is the Service Set IDentification (SSID) name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the chapter on wireless configuration for more information on basic service sets (BSS) and extended service sets (ESS).
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.
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.
Wireless Mode	This is the IEEE 802.1x standard used by the wireless network.
Signal Strength	This field displays the strength of the AP's signal. If you must choose a channel that is currently in use, choose one with low signal strength for minimum interference.
Security	This is the wireless security method used by the wireless network to protect wireless communication between wireless stations, access points and the wired network.
Refresh	Click Refresh to reload the screen.

Wireless LAN

6.1 Overview

This chapter discusses the steps to configure the Wireless Settings screen on the NWA1121-NI. It also introduces the wireless LAN (WLAN) and some basic scenarios.

Figure 17 Wireless Mode



In the figure above, the NWA1121-NI allows access to another bridge device (**A**) and a notebook computer (**B**) upon verifying their settings and credentials. It denies access to other devices (**C** and **D**) with configurations that do not match those specified in your NWA1121-NI.

6.2 What You Can Do in this Chapter

- Use the **Wireless Settings** screen to configure the NWA1121-NI's operation mode (see [Section 6.4 on page 60](#)).
- Use the **SSID** screen to configure up to eight SSID profiles for your NWA1121-NI (see [Section 6.5 on page 72](#)).
- Use the **Security** screen to choose the wireless security mode for your NWA1121-NI (see [Section 6.6 on page 74](#)).
- Use the **RADIUS** screen if you want to authenticate wireless users using a RADIUS Server and/or accounting server (see [Section 6.7 on page 87](#)).
- Use the **MAC Filter** screen to specify which wireless station is allowed or denied access to the NWA1121-NI (see [Section 6.8 on page 89](#)).

6.3 What You Need To Know

BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS.

ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

Operating Mode

The NWA1121-NI can run in four operating modes as follows:

- **Root AP.** The NWA1121-NI is a wireless access point that allows wireless communication to other devices in the network.
- **Repeater.** The NWA1121-NI acts as a **wireless repeater and increase a root AP's wireless coverage area.**
- **Client.** The NWA1121-NI acts as a wireless client to access a wireless network.
- **MBSSID.** The Multiple Basic Service Set Identifier (MBSSID) mode allows you to use one access point to provide several BSSs simultaneously.

Refer to [Chapter 1 on page 11](#) for illustrations of these wireless applications.

SSID

The SSID (Service Set Identifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. **In other words, it is the name of the wireless network that clients use to connect to it.**

Normally, the NWA1121-NI acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the NWA1121-NI does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference.

Wireless Mode

The IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. Your NWA1121-NI can support **802.11b/g**, **802.11n** and **802.11b/g/n**.

MBSSID

Traditionally, you needed to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there was also the possibility of channel interference. The NWA1121-NI's MBSSID (Multiple Basic Service Set Identifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying levels of privilege to different SSIDs.

Wireless stations can use different BSSIDs to associate with the same AP.

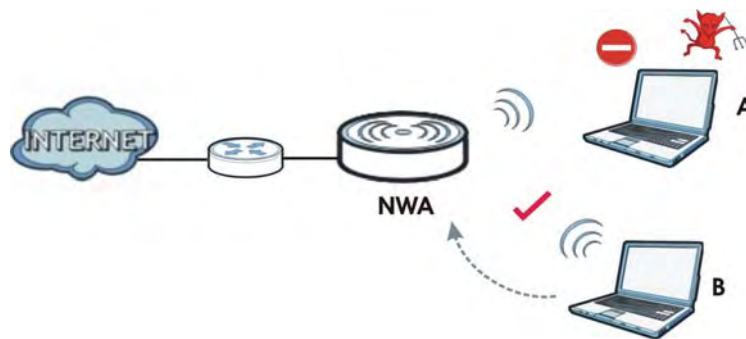
The following are some notes on multiple BSS.

- A maximum of four BSSs are allowed on one AP simultaneously.
- You must use different WEP keys for different BSSs. If two stations have different BSSIDs (they are in different BSSs), but have the same WEP keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

Wireless Security

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

Figure 18 Securing the Wireless Network



In the figure above, the NWA1121-NI checks the identity of devices before giving them access to the network. In this scenario, Computer **A** is denied access to the network, while Computer **B** is granted connectivity.

The NWA1121-NI secure communications via data encryption, wireless client authentication and MAC address filtering. It can also hide its identity in the network.

User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

The following table shows the relative effectiveness of wireless security methods: .

Table 9 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
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

The available security modes in your NWA1121-NI are as follows:

- **None.** No data encryption.
- **WEP.** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.
- **802.1x-Only.** This is a standard that extends the features of IEEE 802.11 to support extended authentication. It provides additional accounting and control features. This option does not support data encryption.
- **802.1x-Static WEP.** This provides 802.1x-Only authentication with a static 64bit or 128bit WEP key and an authentication server.
- **WPA.** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard.
- **WPA2.** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
- **WPA2-MIX.** This commands the NWA1121-NI to use either WPA2 or WPA depending on which security mode the wireless client uses.
- **WPA2-PSK.** This adds a pre-shared key on top of WPA2 standard.
- **WPA2-PSK-MIX.** This commands the NWA1121-NI to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.

Note: To guarantee 802.11n wireless speed, please only use WPA2 or WPA2-PSK security mode. Other security modes may degrade the wireless speed performance to 802.11g.

Passphrase

A passphrase functions like a password. In WEP security mode, it is further converted by the NWA1121-NI into a complicated string that is referred to as the “key”. This key is requested from all devices wishing to connect to a wireless network.

PSK

The Pre-Shared Key (PSK) is a password shared by a wireless access point and a client during a previous secure connection. The key can then be used to establish a connection between the two parties.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message. Encryption is the process of converting data into unreadable text. This secures information in network communications. The intended recipient of the data can “unlock” it with a pre-assigned key, making the information readable only to him. The NWA1121-NI when used as a wireless client employs Temporal Key Integrity Protocol (TKIP) data encryption.

EAP

Extensible Authentication Protocol (EAP) is a protocol used by a wireless client, an access point and an authentication server to negotiate a connection.

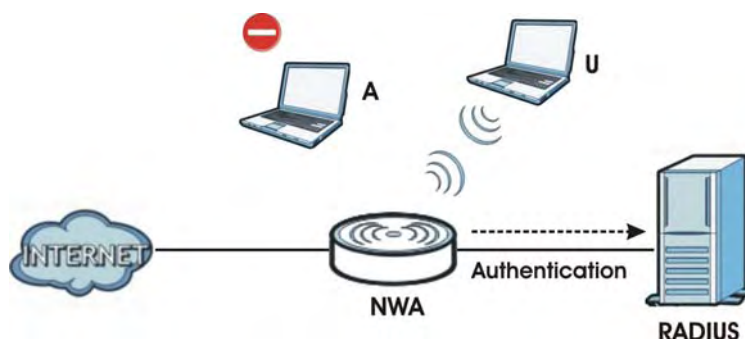
The EAP methods employed by the NWA1121-NI when in Wireless Client operating mode are Transport Layer Security (TLS), Protected Extensible Authentication Protocol (PEAP), Lightweight Extensible Authentication Protocol (LEAP) and Tunneled Transport Layer Security (TTLS). The authentication protocol may either be Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) or Generic Token Card (GTC).

Further information on these terms can be found in [Appendix D on page 181](#).

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a protocol that can be used to manage user access to large networks. It is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server.

Figure 19 RADIUS Server Setup



In the figure above, wireless clients **A** and **B** are trying to access the Internet via the NWA1121-NI. The NWA1121-NI in turn queries the RADIUS server if the identity of clients A and U are allowed access to the Internet. In this scenario, only client **U**'s identity is verified by the RADIUS server and allowed access to the Internet.

The RADIUS server handles the following tasks:

- **Authentication** which determines the identity of the users.
- **Authorization** which determines the network services available to authenticated users once they are connected to the network.
- **Accounting** which keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

You should know the IP addresses, ports and share secrets of the external RADIUS server and/or the external RADIUS accounting server you want to use with your NWA1121-NI. You can configure a primary and backup RADIUS and RADIUS accounting server for your NWA1121-NI.

6.4 Wireless Settings Screen

Use this screen to choose the operating mode for your NWA1121-NI. Click **Network > Wireless LAN > Wireless Settings**. The screen varies depending upon the operating mode you select.

6.4.1 Root AP Mode

Use this screen to use your NWA1121-NI as an access point. Select **Root AP** as the **Operation Mode**. The following screen displays.

Figure 20 Wireless LAN > Wireless Settings: Root AP

Wireless Settings

SSID

Security

RADIUS

MAC Filter

Basic Settings

Wireless LAN Interface :

☒ Enabled

Operation Mode :

Root AP

Wireless Mode :

802.11b/g/n

Channel :

6

Channel Width :

20MHZ

Select SSID Profile :

#	Active	Profile	#	Active	Profile
1	<input checked="" type="checkbox"/>	Profile1	2	<input type="checkbox"/>	Profile1
3	<input checked="" type="checkbox"/>	Profile2	4	<input type="checkbox"/>	Profile1

Universal Repeater Settings

Local MAC Address :

00:03:7F:42:82:68

Universal Repeater SSID Profile :

Profile2

Advanced Settings

Beacon Interval :

100

(25-1000 ms)

DTIM Interval :

1

(1-15)

Output Power :

Full

Preamble Type :

Dynamic

RTS/CTS Threshold :

2346

(1-2346)

Extension Channel Protection Mode :

None

A-MPDU Aggregation :

☒ Enabled

Short GI :

☒ Enabled

MCS Rate	Auto	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

Cancel

The following table describes the general wireless LAN labels in this screen.

Table 10 Wireless LAN > Wireless Settings: Root AP

LABEL	DESCRIPTION
Basic Settings	
Wireless LAN Interface	Select the check box to turn on the wireless LAN on the NWA1121-NI.
Operation Mode	Select Root AP from the drop-down list.
Wireless Mode	<p>Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of your NWA1121-NI might be reduced.</p> <p>Select 802.11b/g/n to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of the NWA1121-NI might be reduced.</p> <p>Select 802.11n to allow only IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI.</p>
Channel	Select the operating frequency/channel depending on your particular region from the drop-down list box.
Channel Width	<p>This field displays only when you select 802.11n or 802.11b/g/n in the Wireless Mode field.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. However, not all devices support 40MHz channels.</p> <p>Select the channel bandwidth you want to use for your wireless network.</p> <p>It is recommended that you select 20/40MHz. This allows the NWA1121-NI to adjust the channel bandwidth depending on network conditions.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>
Select SSID Profile	<p>The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. You can have up to four SSIDs active at the same time.</p> <p>Note: If you are configuring the NWA1121-NI from a computer connected to the wireless LAN and you change the NWA1121-NI's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the NWA1121-NI's new settings.</p>
#	This is the index number of each SSID profile.
Active	Select the check box to enable an SSID profile. Otherwise, clear the check box.
Profile	Select an SSID Profile from the drop-down list box.
Universal Repeater Settings	
<p>The Universal repeater function allows the NWA1121-NI in root AP or repeater mode to set up a wireless connection between it and another NWA1121-NI in root AP or repeater mode.</p> <p>Note: Universal repeater security is independent of the security settings between the NWA1121-NI and any wireless clients.</p>	
Local MAC Address	Local MAC Address is the MAC address of your NWA1121-NI.
Universal Repeater SSID Profile	<p>Select the SSID profile you want to use for universal repeater connections.</p> <p>Note: You can only configure None, WPA-PSK or WPA2-PSK security mode for the SSID used by a universal repeater connection.</p>

Table 10 Wireless LAN > Wireless Settings: Root AP (continued)

LABEL	DESCRIPTION
Advanced Settings	
Beacon Interval	When a wireless network device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in lowpower mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network.
Output Power	Set the output power of the NWA1121-NI in this field. If there is a high density of APs in an area, decrease the output power of the NWA1121-NI to reduce interference with other APs. Select one of the following Full (Full Power), 50% , 25% , or 12.5% . See the product specifications for more information on your NWA1121-NI's output power.
Preamble Type	Select Dynamic to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble. Select Long if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.
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 its smallest value (1) turns on the RTS/CTS handshake.
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.
Extension Channel Protection Mode	You can use CTS to self or RTS-CTS protection mechanism to reduce conflicts with other wireless networks or hidden wireless clients. The throughput of RTS-CTS is much lower than CTS to self . Using this mode may decrease your wireless performance.
A-MPDU Aggregation	This field is available only when 802.11 b/g/n is selected as the Wireless Mode. Select to enable A-MPDU aggregation. Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.
Short GI	This field is available only when 802.11 b/g/n is selected as the Wireless Mode. Select Enabled to use Short GI (Guard Interval). The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the GI increases data transfer rates but also increases interference. Increasing the GI reduces data transfer rates but also reduces interference.
MCS Rate	The MCS Rate table is available only when 802.11 b/g/n is selected in the Wireless Mode field. IEEE 802.11n supports many different data rates which are called MCS rates. MCS stands for Modulation and Coding Scheme. This is an 802.11n feature that increases the wireless network performance in terms of throughput. For each MCS Rate (0-15), select either Enabled to have the NWA1121-NI use the data rate. Clear the Enabled check box if you do not want the NWA1121-NI to use the data rate. Turn on the Auto option to have the NWA1121-NI set the data rates automatically to optimize the throughput. Note: You can set the NWA1121-NI to use up to four MCS rates at a time.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.4.2 Repeater Mode

Use this screen to have the NWA1121-NI act as a **wireless repeater**. You need to know the MAC address of the peer device, which also must be in **Repeater** or **Root AP mode**.

Figure 21 Wireless LAN > Wireless Settings: Repeater

Wireless Settings

SSID

Security

RADIUS

MAC Filter

Basic Settings

Wireless LAN Interface :

☒ Enabled

Operation Mode :

Repeater

Wireless Mode :

802.11b/g/n

Channel :

6

Channel Width :

20MHZ

Universal Repeater Settings

Local MAC Address :

00:03:7F:42:82:68

Universal Repeater SSID Profile :

Profile2

Root MAC Address :

00:A0:c5:01:23:45

Advanced Settings

Beacon Interval :

100

(25-1000 ms)

DTIM Interval :

1

(1-15)

Output Power :

Full

Preamble Type :

Dynamic

RTS/CTS Threshold :

2346

(1-2346)

Extension Channel Protection Mode :

None

A-MPDU Aggregation :

☒ Enabled

Short GI :

☒ Enabled

MCS Rate

Auto

0

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

Enabled

☒

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☒

☐

☐

☐

Apply

Cancel

The following table describes the bridge labels in this screen.

Table 11 Wireless LAN > Wireless Settings: Repeater

LABEL	DESCRIPTION
Basic Settings	
Wireless LAN Interface	Select the check box to turn on the wireless LAN on the NWA1121-NI.
Operation Mode	Select Repeater from the drop-down list.

Table 11 Wireless LAN > Wireless Settings: Repeater (continued)

LABEL	DESCRIPTION
Wireless Mode	<p>Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of your NWA1121-NI might be reduced.</p> <p>Select 802.11b/g/n to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of the NWA1121-NI might be reduced.</p> <p>Select 802.11n to allow only IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI.</p>
Channel	Select the operating frequency/channel depending on your particular region from the drop-down list box.
Channel Width	<p>This field displays only when you select 802.11n or 802.11b/g/n in the Wireless Mode field.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. However, not all devices support 40MHz channels.</p> <p>Select the channel bandwidth you want to use for your wireless network.</p> <p>It is recommended that you select 20/40MHz. This allows the NWA1121-NI to adjust the channel bandwidth depending on network conditions.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>
<p>Universal Repeater Settings</p> <p>The Universal repeater function allows the NWA1121-NI in root AP or repeater mode to set up a wireless connection between it and another NWA1121-NI in root AP or repeater mode.</p> <p>Note: Universal repeater security is independent of the security settings between the NWA1121-NI and any wireless clients.</p>	
Local MAC Address	Local MAC Address is the MAC address of your NWA1121-NI.
Universal Repeater SSID Profile	<p>Select the SSID profile you want to use for universal repeater connections with an AP or repeater or regular wireless connections with wireless clients.</p> <p>Note: You can only configure None, WPA-PSK or WPA2-PSK security mode for the SSID used by a universal repeater connection.</p>
Root MAC Address	Specify the peer device's MAC address. The peer device can be a NWA1121-NI in either root AP mode or repeater mode.
Advanced Settings	
Beacon Interval	When a wirelessly network device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in lowpower mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network.
Output Power	Set the output power of the NWA1121-NI in this field. If there is a high density of APs in an area, decrease the output power of the NWA1121-NI to reduce interference with other APs. Select one of the following Full (Full Power), 50% , 25% or 12.5% . See the product specifications for more information on your NWA1121-NI's output power.

Table 11 Wireless LAN > Wireless Settings: Repeater (continued)

LABEL	DESCRIPTION
Preamble Type	<p>Select Dynamic to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.</p> <p>Select Long if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.</p>
RTS/CTS Threshold	<p>(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 its smallest value (1) turns on the RTS/CTS handshake.</p>
Fragmentation	<p>The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.</p>
Extension Channel Protection Mode	<p>You can use CTS to self or RTS-CTS protection mechanism to reduce conflicts with other wireless networks or hidden wireless clients. The throughput of RTS-CTS is much lower than CTS to self. Using this mode may decrease your wireless performance.</p>
A-MPDU Aggregation	<p>This field is available only when 802.11 b/g/n is selected as the Wireless Mode.</p> <p>Select to enable A-MPDU aggregation.</p> <p>Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.</p>
Short GI	<p>This field is available only when 802.11 b/g/n is selected as the Wireless Mode. Select Enabled to use Short GI (Guard Interval). The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the GI increases data transfer rates but also increases interference. Increasing the GI reduces data transfer rates but also reduces interference.</p>
MCS Rate	<p>The MCS Rate table is available only when 802.11 b/g/n is selected in the Wireless Mode field.</p> <p>IEEE 802.11n supports many different data rates which are called MCS rates. MCS stands for Modulation and Coding Scheme. This is an 802.11n feature that increases the wireless network performance in terms of throughput.</p> <p>For each MCS Rate (0-15), select either Enabled to have the NWA1121-NI use the data rate.</p> <p>Clear the Enabled check box if you do not want the NWA1121-NI to use the data rate.</p> <p>Turn on the Auto option to have the NWA1121-NI set the data rates automatically to optimize the throughput.</p> <p>Note: You can set the NWA1121-NI to use up to four MCS rates at a time.</p>
Apply	<p>Click Apply to save your changes.</p>
Cancel	<p>Click Cancel to begin configuring this screen afresh.</p>

6.4.3 Wireless Client Mode

Use this screen to turn your NWA1121-NI into a wireless client. Select **Client** as the **Operation Mode**. The following screen displays.

Figure 22 Wireless LAN > Wireless Settings: Wireless Client

The screenshot shows the 'Wireless Settings' configuration page for a wireless client. It is divided into two main sections: 'Basic Settings' and 'Advanced Settings'. In the 'Basic Settings' section, the 'Wireless LAN Interface' is checked and set to 'Enabled'. The 'Operation Mode' is set to 'Client', and there is a 'Site Survey' button next to it. The 'SSID Profile' is set to 'Profile1', the 'Channel' is set to '6', and the 'Channel Width' is set to '20MHZ'. In the 'Advanced Settings' section, 'Output Power' is set to 'Full', 'Preamble Type' is set to 'Dynamic', 'RTS/CTS Threshold' is set to '2346' (with a range of '1-2346' indicated), 'Extension Channel Protection Mode' is set to 'None', 'A-MPDU Aggregation' is checked and set to 'Enabled', and 'Short GI' is checked and set to 'Enabled'. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

The following table describes the general wireless LAN labels in this screen.

Table 12 Wireless LAN > Wireless Settings: Wireless Client

LABEL	DESCRIPTION
Basic Settings	
Wireless LAN Interface	Select the check box to turn on the wireless LAN on the NWA1121-NI.
Operation Mode	Select Client in this field.
Site Survey	Click this to view a list of available wireless access points within the range. Select the AP you want to use. Note: After selecting Client as the Operation Mode in the Basic Settings section, you must click Apply to be able to select from the AP list.

Table 12 Wireless LAN > Wireless Settings: Wireless Client (continued)

LABEL	DESCRIPTION
SSID Profile	<p>The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID.</p> <p>In this field, select the SSID profile of the AP you want to use. Click Apply.</p> <p>The SSID used in the selected SSID profile automatically changes to be the one you select in the Site Survey screen.</p> <p>Set the security configuration for this operating mode in the Wireless LAN > Security screen. Check the Dashboard screen to check if the settings you set show in the WLAN information.</p> <p>Note: If you are configuring the NWA1121-NI from a computer connected to the wireless LAN and you change the NWA1121-NI's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the NWA1121-NI's new settings.</p>
Channel	This shows the operating frequency/channel in use. This field is read-only when you select Client as your operation mode.
Channel Width	<p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. However, not all devices support 40MHz channels.</p> <p>Select the channel bandwidth you want to use for your wireless network.</p> <p>It is recommended that you select 20/40MHz. This allows the NWA1121-NI to adjust the channel bandwidth depending on network conditions.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the AP do not support channel bonding.</p>
Advanced Settings	
Output Power	Set the output power of the NWA1121-NI in this field. If there is a high density of APs in an area, decrease the output power of the NWA1121-NI to reduce interference with other APs. Select one of the following Full (Full Power), 50% , 25% or 12.5% . See the product specifications for more information on your NWA1121-NI's output power.
Preamble Type	<p>Select Dynamic to have the NWA1121-NI automatically use short preamble when the wireless network your NWA1121-NI is connected to supports it, otherwise the NWA1121-NI uses long preamble.</p> <p>Select Long preamble if you are unsure what preamble mode the wireless device your NWA1121-NI is connected to supports, and to provide more reliable communications in busy wireless networks.</p>
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 its smallest value (1) turns on the RTS/CTS handshake.
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.
Extension channel protection mode	You can use CTS to self or RTS-CTS protection mechanism to reduce conflicts with other wireless networks or hidden wireless clients. The throughput of RTS-CTS is much lower than CTS to self . Using this mode may decrease your wireless performance.
A-MPDU Aggregation	<p>Select to enable A-MPDU aggregation.</p> <p>Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.</p>

Table 12 Wireless LAN > Wireless Settings: Wireless Client (continued)

LABEL	DESCRIPTION
Short GI	Select Enabled to use Short GI (Guard Interval). The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the GI increases data transfer rates but also increases interference. Increasing the GI reduces data transfer rates but also reduces interference.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.4.4 MBSSID Mode

Use this screen to have the NWA1121-NI function in MBSSID mode. Select **MBSSID** as the **Operation Mode**. The following screen displays.

Figure 23 Wireless LAN > Wireless Settings: MBSSID

Wireless Settings | SSID | Security | RADIUS | MAC Filter

Basic Settings

Wireless LAN Interface : ☒ Enabled

Operation Mode : MBSSID

Wireless Mode : 802.11b/g/n

Channel : 6

Channel Width : 20MHZ

Select SSID Profile :

#	Active	Profile	#	Active	Profile
1	<input checked="" type="checkbox"/>	Profile1	2	<input type="checkbox"/>	Profile1
3	<input checked="" type="checkbox"/>	Profile2	4	<input type="checkbox"/>	Profile1
5	<input type="checkbox"/>	Profile1	6	<input type="checkbox"/>	Profile1
7	<input type="checkbox"/>	Profile1	8	<input type="checkbox"/>	Profile1

Advanced Settings

Beacon Interval : 100 (25-1000 ms)

DTIM Interval : 1 (1-15)

Output Power : Full

Preamble Type : Dynamic

RTS/CTS Threshold : 2346 (1-2346)

Extension Channel Protection Mode : None

A-MPDU Aggregation : ☒ Enabled

Short GI : ☒ Enabled

MCS Rate	Auto	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Enabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Cancel

The following table describes the labels in this screen.

Table 13 Wireless LAN > Wireless Settings: MBSSID

LABEL	DESCRIPTION
Basic Settings	
Wireless LAN Interface	Select the check box to turn on the wireless LAN on the NWA1121-NI.
Operation Mode	Select MBSSID from the drop-down list.
Wireless Mode	<p>Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of your NWA1121-NI might be reduced.</p> <p>Select 802.11b/g/n to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI. The transmission rate of the NWA1121-NI might be reduced.</p> <p>Select 802.11n to allow only IEEE802.11n compliant WLAN devices to associate with the NWA1121-NI.</p>
Channel	Select the operating frequency/channel depending on your particular region from the drop-down list box.
Channel Width	<p>This field displays only when you select 802.11n or 802.11b/g/n in the Wireless Mode field.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. However, not all devices support 40MHz channels.</p> <p>Select the channel bandwidth you want to use for your wireless network.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>
Select SSID Profile	<p>The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. You can have up to eight SSIDs active at the same time.</p> <p>Note: If you are configuring the NWA1121-NI from a computer connected to the wireless LAN and you change the NWA1121-NI's SSID or security settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the NWA1121-NI's new settings.</p>
#	This is the index number of each SSID profile.
Active	Select the check box to enable an SSID profile. Otherwise, clear the check box.
Profile	Select an SSID Profile from the drop-down list box.
Advanced Settings	
Beacon Interval	When a wireless network device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in lowpower mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network.
Output Power	Set the output power of the NWA1121-NI in this field. If there is a high density of APs in an area, decrease the output power of the NWA1121-NI to reduce interference with other APs. Select one of the following Full (Full Power), 50% , 25% or 12.5% . See the product specifications for more information on your NWA1121-NI's output power.

Table 13 Wireless LAN > Wireless Settings: MBSSID (continued)

LABEL	DESCRIPTION
Preamble Type	<p>Select Dynamic to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.</p> <p>Select Long if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.</p>
RTS/CTS Threshold	<p>(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 its smallest value (1) turns on the RTS/CTS handshake.</p>
Extension Channel Protection Mode	<p>You can use CTS to self or RTS-CTS protection mechanism to reduce conflicts with other wireless networks or hidden wireless clients. The throughput of RTS-CTS is much lower than CTS to self. Using this mode may decrease your wireless performance.</p>
A-MPDU Aggregation	<p>This field is available only when 802.11 b/g/n is selected as the Wireless Mode.</p> <p>Select to enable A-MPDU aggregation.</p> <p>Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.</p>
Short GI	<p>This field is available only when 802.11 b/g/n is selected as the Wireless Mode. Select Enabled to use Short GI (Guard Interval). The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the GI increases data transfer rates but also increases interference. Increasing the GI reduces data transfer rates but also reduces interference.</p>
MCS Rate	<p>The MCS Rate table is available only when 802.11 b/g/n is selected in the Wireless Mode field.</p> <p>IEEE 802.11n supports many different data rates which are called MCS rates. MCS stands for Modulation and Coding Scheme. This is an 802.11n feature that increases the wireless network performance in terms of throughput.</p> <p>For each MCS Rate (0-15), select either Enabled to have the NWA1121-NI use the data rate.</p> <p>Clear the Enabled check box if you do not want the NWA1121-NI to use the data rate.</p> <p>Turn on the Auto option to have the NWA1121-NI set the data rates automatically to optimize the throughput.</p> <p>Note: You can set the NWA1121-NI to use up to four MCS rates at a time.</p>
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.5 SSID Screen

Use this screen to **view and modify the settings of the SSID profiles on the NWA1121-NI**. Click **Wireless LAN > SSID** to display the screen as shown.

Figure 24 Wireless LAN > SSID

Wireless Settings









SSID

Security

RADIUS

MAC Filter

Profile Settings

#	Profile Name	SSID	Security	RADIUS	QoS	MAC Filter	Modify
1	Profile1	ZyXEL_NWA	Disabled	RadProfile1	None	Disabled	
2	Profile2	ZyXEL	SecProfile2	RadProfile1	None	Disabled	
3	Profile3	ZyXEL	Disabled	RadProfile1	None	Disabled	
4	Profile4	ZyXEL	Disabled	RadProfile1	None	Disabled	
5	Profile5	ZyXEL	Disabled	RadProfile1	None	Disabled	
6	Profile6	ZyXEL	Disabled	RadProfile1	None	Disabled	
7	Profile7	ZyXEL	Disabled	RadProfile1	None	Disabled	
8	Profile8	ZyXEL	Disabled	RadProfile1	None	Disabled	

The following table describes the labels in this screen.

Figure 25 Wireless LAN > SSID

LABEL	DESCRIPTION
Profile Settings	
#	This field displays the index number of each SSID profile.
Profile Name	This field displays the identification name of each SSID profile on the NWA1121-NI.
SSID	This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates which security profile is currently associated with each SSID profile. See Section 6.6 on page 74 for more information.
RADIUS	This field displays which RADIUS profile is currently associated with each SSID profile, if you have a RADIUS server configured.
QoS	This field displays the Quality of Service setting for this profile or NONE if QoS is not configured on a profile.
MAC Filter	This field displays which MAC filter profile is currently associated with each SSID profile, or Disable if MAC filtering is not configured on an SSID profile.
Modify	Click Edit to go to the SSID configuration screen where you can modify settings in an SSID profile.

6.5.1 Configuring SSID

Use this screen to configure an SSID profile. In the **Wireless LAN > SSID** screen, click **Edit** next to the SSID profile you want to configure to display the following screen.

Figure 26 SSID: Edit

The screenshot shows the 'SSID: Edit' configuration window. It has a title bar with 'SSID' and a 'Profile Settings' section. The settings are as follows:

- Profile Name: Profile1
- SSID: ZyXEL
- Security: Disabled (dropdown)
- RADIUS: RadProfile1 (dropdown)
- MAC Filtering: Disabled (dropdown)
- QoS: None (dropdown)
- BSSID VLAN ID: 1 (range 1-4094)
- Number of Wireless Stations Allowed to Associate: 64 (range 1-64)
- Hidden SSID: ☐ Enabled
- Intra-BSS Traffic Blocking: ☐ Enabled

At the bottom are three buttons: Back, Apply, and Cancel.

The following table describes the labels in this screen.

Table 14 SSID: Edit

LABEL	DESCRIPTION
Profile Name	This is the name that identifying this profile.
SSID	When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	Select a security profile to use with this SSID profile. See Section 6.6 on page 74 for more information. If you do not want this profile to use wireless security, select Disabled .
RADIUS	Select a RADIUS profile from the drop-down list box, if you have a RADIUS server configured. If you do not need to use RADIUS authentication, ignore this field. See Section 6.7 on page 87 for more information.
MAC Filtering	Select a MAC filter profile from the drop-down list box. If you do not want to use MAC filtering on this profile, select Disabled .
QoS	<p>Select the Quality of Service priority for this BSS's traffic.</p> <ul style="list-style-type: none"> If you select WMM from the QoS list, the priority of a data packet depends on the packet's IEEE 802.1q or DSCP header. If a packet has no WMM value assigned to it, it is assigned the default priority. If you select WMM_VOICE, WMM_VIDEO, WMM_BESTEFFORT or WMM_BACKGROUND, the NWA1121-NI applies that QoS setting to all of that SSID's traffic. If you select None, the NWA1121-NI applies no priority to traffic on this SSID. <p>Note: When you configure an SSID profile's QoS settings, the NWA1121-NI applies the same QoS setting to all of the profile's traffic.</p>

Table 14 SSID: Edit (continued)

LABEL	DESCRIPTION
BSSID VLAN ID	Enter a VLAN ID for the SSID profile. Packets coming from the WLAN using this SSID profile are tagged with the VLAN ID number by the NWA1121-NI.
Number of Wireless Stations Allowed to Associate	Use this field to set a maximum number of wireless stations that may connect to the device.
Hidden SSID	If you do not select the checkbox, the NWA1121-NI broadcasts this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, if you select the checkbox, the NWA1121-NI hides this SSID (a wireless client scanning for an AP will not find this SSID).
Intra-BSS Traffic Blocking	Select the check box to prevent wireless clients in this profile's BSS from communicating with one another.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.6 Wireless Security Screen

Use this screen to choose the security mode for your NWA1121-NI.

Click **Wireless LAN > Security**. Select the profile that you want to configure and click **Edit**.

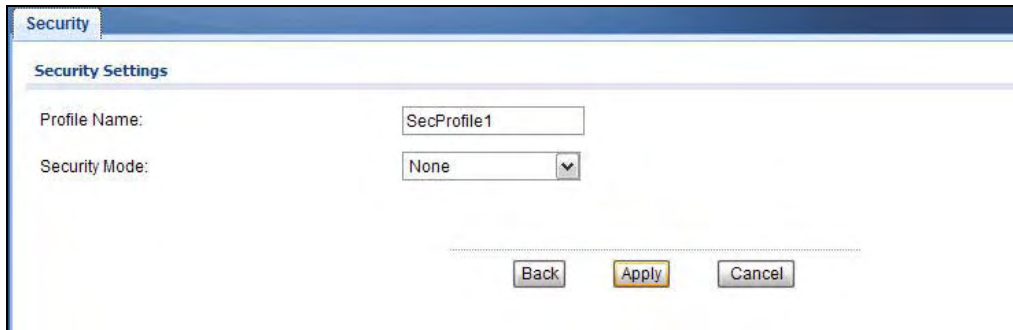
Figure 27 Wireless > Security

The screenshot shows the 'Wireless Settings' interface with the 'Security' tab selected. Below the tabs, there is a section titled 'Security Profiles' containing a table with 8 rows. Each row represents a security profile with columns for an index number, the profile name, the security mode, and a 'Modify' button (represented by a pencil icon).

#	Profile Name	Security Mode	Modify
1	SecProfile1	None	
2	SecProfile2	WPA-PSK	
3	SecProfile3	None	
4	SecProfile4	None	
5	SecProfile5	None	
6	SecProfile6	None	
7	SecProfile7	None	
8	SecProfile8	None	

The **Security Settings** screen varies depending upon the security mode you select.

Figure 28 Security: None



The screenshot shows a web-based configuration interface. At the top, there is a blue header bar with the word "Security" in white. Below this, the title "Security Settings" is displayed in a smaller font. The main area contains two labels: "Profile Name:" followed by a text input field containing "SecProfile1", and "Security Mode:" followed by a dropdown menu currently showing "None". At the bottom of the form, there are three buttons: "Back", "Apply" (which is highlighted with a yellow border), and "Cancel".

Note that some screens display differently depending on the operating mode selected in the **Wireless LAN > Wireless Settings** screen.

Note: You must enable the same wireless security settings on the NWA1121-NI and on all wireless clients that you want to associate with it.

6.6.1 Security: WEP

Use this screen to use WEP as the security mode for your NWA1121-NI. Select **WEP** in the **Security Mode** field to display the following screen.

Figure 29 Security: WEP

The screenshot shows the 'Security Settings' window. At the top, there's a 'Security' tab. Below it, the 'Security Settings' section contains several fields: 'Profile Name' with the value 'SecProfile1', 'Security Mode' set to 'WEP', 'Authentication Type' set to 'Open', and 'Data Encryption' set to '128-bit WEP'. A 'Passphrase' field is followed by a 'Generate' button and a note: '(max. 16 alphanumeric, printable characters)'. Below this is a 'Note' box stating: 'Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key.' Underneath the note are four radio buttons labeled 'Key 1:', 'Key 2:', 'Key 3:', and 'Key 4:', each with a corresponding text input field. Another 'Note' box follows, providing instructions: '64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)' and '128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)'. At the bottom of the window are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the labels in this screen.

Table 15 Security: WEP

LABEL	DESCRIPTION
Profile Name	This is the name that identifying this profile.
Security Mode	Choose WEP in this field.
Authentication Type	Select Open or Shared from the drop-down list box.
Data Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.
Passphrase	Enter the passphrase or string of text used for automatic WEP key generation on wireless client adapters.
Generate	Click this to get the keys from the Passphrase you entered.

Table 15 Security: WEP (continued)

LABEL	DESCRIPTION
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the NWA1121-NI and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be activated at any one time.</p>
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.6.2 Security: 802.1x Only

This screen varies depending on the **operating mode** you select in the **Wireless LAN > Wireless Settings** screen.

6.6.2.1 Access Point

Use this screen to use 802.1x-Only security mode for your NWA1121-NI that is in **root AP, MBSSID or repeater operating mode**. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

Figure 30 Security: 802.1x Only for Access Point

The screenshot shows a web-based configuration interface for the NWA1121-NI. The title bar is 'Security'. Below it is a section 'Security Settings' with two fields: 'Profile Name' set to 'SecProfile1' and 'Security Mode' set to '802.1X-Only'. Below this is a section 'Rekey Options' with two fields: 'Reauthentication Time' set to '300' seconds (max. 100-3600) and 'Enable Group-Key Update' set to 'Every 100' seconds (max. 100-3600). At the bottom are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the labels in this screen.

Table 16 Security: 802.1x Only for Access Point

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose 802.1x-Only in this field.
Rekey Options	

Table 16 Security: 802.1x Only for Access Point (continued)

LABEL	DESCRIPTION
Reauthentication Time	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 100 and 3600 seconds. Alternatively, enter "0" to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Enable Group-Key Update	Select this option to have the NWA1121-NI automatically disconnect a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. Enter a time interval between 100 and 3600 seconds.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.6.2.2 Wireless Client

Use this screen to use 802.1x-Only security mode for your NWA1121-NI that is in wireless client operating mode. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

Figure 31 Security: 802.1x Only for Wireless Client

The screenshot shows a web-based configuration interface for a wireless client. The main title is 'Security'. Under 'Security Settings', the 'Profile Name' is set to 'SecProfile1' and the 'Security Mode' is set to '802.1X-Only'. The 'IEEE802.1X Authentication' section shows 'Eap Type' set to 'TLS'. The 'User Information' section has an empty 'Login Name' field. The 'Certificate' section has empty fields for 'User Certificate' and 'Password'. At the bottom of the form, there are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the labels in this screen.

Table 17 Security: 802.1x Only for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.

Table 17 Security: 802.1x Only for Wireless Client (continued)

LABEL	DESCRIPTION
Security Mode	Choose the same security mode used by the AP.
IEEE802.1x Authentication	
Eap Type	The options on the left refer to EAP methods. You can choose either TLS , LEAP , PEAP or TTLS . If you select TTLS or PEAP , the options on the right refer to authentication protocols. You can choose between PAP , CHAP , MSCHAP , MSCHAPv2 and/or GTC .
User Information	
Username Login Name	Supply the user name of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Certificate	
User Certificate	If you select TLS , enter the name of the certificate used to to verify the identity of clients.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.6.3 Security: 802.1x Static WEP

This screen varies depending on the **operating mode** you select in the **Wireless LAN > Wireless Settings** screen.

6.6.3.1 Access Point

Use this screen to use 802.1x static WEP security mode for your NWA1121-NI that is in **root AP**, **MBSSID** or **repeater operating mode**. Select **802.1X-Static WEP** in the **Security Mode** field to display the following screen.

Figure 32 Security: 802.1X-Static WEP for Access Point

Security

Security Settings

Profile Name:

Security Mode:

Data Encryption:

Passphrase: (max. 16 alphanumeric, printable characters)

Note:
Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key.

☒ Key 1:

☐ Key 2:

☐ Key 3:

☐ Key 4:

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)

Rekey Options

Reauthentication Time: Seconds (max. 100-3600)

Enable Group-Key Update: ☐ Every Seconds (max. 100-3600)

The following table describes the labels in this screen.

Table 18 Security: 802.1X-Static WEP for Access Point

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose 802.1X-Static WEP in this field.
Data Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.
Passphrase	Enter the passphrase or string of text used for automatic WEP key generation on wireless client adapters.
Generate	Click this to get the keys from the Passphrase you entered.

Table 18 Security: 802.1X-Static WEP for Access Point (continued)

LABEL	DESCRIPTION
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the NWA1121-NI and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be activated at any one time.</p>
Rekey Options	
Reauthentication Time	<p>Specify how often wireless stations have to resend user names and passwords in order to stay connected.</p> <p>Enter a time interval between 100 and 3600 seconds. Alternatively, enter "0" to turn reauthentication off.</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Enable Group-Key Update	<p>Select this option to have the NWA1121-NI automatically disconnect a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.</p> <p>Enter a time interval between 100 and 3600 seconds.</p>
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.6.3.2 Wireless Client

Use this screen to use 802.1x-Only security mode for your NWA1121-NI that is in wireless client operating mode. Select **802.1X-Static WEP** in the **Security Mode** field to display the following screen.

Figure 33 Security: 802.1X-Static WEP for Wireless Client

Security

Security Settings

Profile Name:

SecProfile1

Security Mode:

802.1X-Static WEP

Data Encryption:

128-bit WEP

Passphrase:

Generate

(max. 16 alphanumeric, printable characters)

Note:

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key.

☒ Key 1:

☐ Key 2:

☐ Key 3:

☐ Key 4:

Note:

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)

IEEE802.1X Authentication

Eap Type :

TLS

User Information

Login Name:

Certificate

User Certificate:

Password :

Back

Apply

Cancel

The following table describes the labels in this screen.

Table 19 Security: 802.1X-Static WEP for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose the same security mode used by the AP.

Table 19 Security: 802.1X-Static WEP for Wireless Client (continued)

LABEL	DESCRIPTION
Data Encryption	Select 64-bit WEP or 128-bit WEP to enable data encryption.
Passphrase	Enter the passphrase or string of text used for automatic WEP key generation.
Generate	Click this to get the keys from the Passphrase you entered.
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the NWA1121-NI and the AP must use the same WEP key for data transmission.</p> <p>If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be activated at any one time.</p>
IEEE802.1x Authentication	
Eap Type	<p>The options on the left refer to EAP methods. You can choose either TLS, LEAP, PEAP or TTLS.</p> <p>If you select TTLS or PEAP, the options on the right refer to authentication protocols. You can choose between PAP, CHAP, MSCHAP, MSCHAPv2 and/or GTC.</p>
User Information	
Username Login Name	Supply the user name of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Certificate	
User Certificate	If you select TLS , enter the name of the certificate used to to verify the identity of clients.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.6.4 Security: WPA, WPA2, WPA2-MIX

This screen varies depending on the **operating mode** you select in the **Wireless LAN > Wireless Settings** screen.

6.6.4.1 Access Point

Use this screen to employ WPA or WPA2 as the security mode for your NWA1121-NI that is in **root AP, MBSSID or repeater operating mode**. Select **WPA**, **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 34 Security: WPA/WPA2 for Access Point

Security

Security Settings

Profile Name:

SecProfile1

Security Mode:

WPA2-MIX

Rekey Options

Reauthentication Time

300

Seconds (max. 100-3600)

Enable Group-Key Update

☐ Every 100

Seconds (max. 100-3600)

Back

Apply

Cancel

The following table describes the labels in this screen.

Table 20 Security: WPA/WPA2 for Access Point

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose WPA , WPA2 or WPA-MIX in this field.
Rekey Options	
Reauthentication Time	<p>Specify how often wireless stations have to resend user names and passwords in order to stay connected.</p> <p>Enter a time interval between 100 and 3600 seconds. Alternatively, enter "0" to turn reauthentication off.</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Enable Group-Key Update	<p>Select this option to have the NWA1121-NI automatically disconnect a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.</p> <p>Enter a time interval between 100 and 3600 seconds.</p>
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.6.4.2 Wireless Client

Use this screen to employ WPA or WPA2 as the security mode for your NWA1121-NI that is in wireless client operating mode. Select **WPA or WPA2** in the **Security Mode** field to display the following screen.

Figure 35 Security: WPA for Wireless Client

Security

Security Settings

Profile Name:

SecProfile1

Security Mode:

WPA2

Data Encryption:

AES

IEEE802.1X Authentication

Eap Type :

TLS

User Information

Login Name:

Certificate

User Certificate:

Password :

Back

Apply

Cancel

The following table describes the labels in this screen.

Table 21 Security: WPA/WPA2 for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose the same security mode used by the AP.
Data Encryption	This shows the encryption method used by the NWA1121-NI.
IEEE802.1x Authentication	
Eap Type	The options on the left refer to EAP methods. You can choose either TLS , LEAP , PEAP or TTLS . If you select TTLS or PEAP , the options on the right refer to authentication protocols. You can choose between PAP , CHAP , MSCHAP , MSCHAPv2 and/or GTC .
User Information	
Username	Supply the user name of the account created in the RADIUS server.
Login Name	
Password	Supply the password of the account created in the RADIUS server.
Certificate	
User Certificate	If you select TLS , enter the name of the certificate used to to verify the identity of clients.

Table 21 Security: WPA/WPA2 for Wireless Client (continued)

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.6.5 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Use this screen to employ WPA-PSK, WPA2-PSK or WPA2-PSK-MIX as the security mode of your NWA1121-NI. Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in the **Security Mode** field to display the following screen.

Figure 36 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

The following table describes the labels not previously discussed





Table 22 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Profile Name	This is the name that identifying this profile.
Security Mode	Choose WPA-PSK , WPA2-PSK or WPA2-PSK-MIX 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).
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.7 RADIUS Screen

Use this screen to set up your NWA1121-NI's RADIUS server settings. Click **Wireless LAN > RADIUS**. The screen appears as shown.

Figure 37 Wireless LAN > RADIUS

Wireless Settings SSID Security RADIUS MAC Filter						
RADIUS Profiles						
#	Profile Name	Primary Server Status	Primary Server Accounting	Backup Server Status	Backup Server Accounting	Modify
1	RadProfile1	Active	Inactive	Inactive	Inactive	
2	RadProfile2	Inactive	Inactive	Inactive	Inactive	
3	RadProfile3	Inactive	Inactive	Inactive	Inactive	
4	RadProfile4	Inactive	Inactive	Inactive	Inactive	

Select a profile you want to configure and click **Edit**.

Figure 38 Wireless LAN > RADIUS

RADIUS

RADIUS Profile

Profile Name :

RadProfile1

RADIUS Server Settings

Primary RADIUS Server :

☒ Enabled

Primary Server IP Address :

0.0.0.0

Primary Server Port :

1812

Primary Share Secret :

password

Backup RADIUS Server :

☐ Enabled

Backup Server IP Address :

Backup Server Port :

Backup Share Secret :

Accounting Server Settings

Primary Accounting Server :

☐ Enabled

Primary Server IP Address :

Primary Server Port :

Primary Share Secret :

Backup Accounting Server :

☐ Enabled

Backup Server IP Address :

Backup Server Port :

Backup Share Secret :

Back

Apply

Cancel

The following table describes the labels in this screen.

Table 23 Wireless LAN > RADIUS

LABEL	DESCRIPTION
Profile Name	This is the name that identifying this RADIUS profile.
Primary RADIUS Server	Select the check box to enable user authentication through an external authentication server.
Primary Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Primary Server Port	Enter the port number of the RADIUS server to be used for authentication.
Primary Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the NWA1121-NI. The key must be the same on the external authentication server and your NWA1121-NI. The key is not sent over the network.
Backup RADIUS Server	<p>If the NWA1121-NI cannot communicate with the primary RADIUS server, you can have the NWA1121-NI use a backup RADIUS server. Make sure the check box is selected if you want to use the backup server.</p> <p>The NWA1121-NI will attempt to communicate three times before using the backup server. Requests can be issued from the client interface to use the backup server. The length of time for each authentication is decided by the wireless client or based on the configuration of the Reauthentication Time field in the Wireless LAN > Security screen.</p>
Backup Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Backup Server Port	Enter the port number of the RADIUS server to be used for authentication.
Backup Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the NWA1121-NI. The key must be the same on the external authentication server and your NWA1121-NI. The key is not sent over the network.
Primary Accounting Server	Select the check box to enable user accounting through an external authentication server.
Primary Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Primary Server Port	Enter the port number of the external accounting server.
Primary Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the NWA1121-NI. The key must be the same on the external accounting server and your NWA1121-NI. The key is not sent over the network.
Backup Accounting Server	<p>If the NWA1121-NI cannot communicate with the primary accounting server, you can have the NWA1121-NI use a backup accounting server. Make sure the check box is selected if you want to use the backup server.</p> <p>The NWA1121-NI will attempt to communicate three times before using the backup server.</p>
Backup Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Backup Server Port	Enter the port number of the external accounting server.
Backup Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the NWA1121-NI. The key must be the same on the external accounting and your NWA1121-NI. The key is not sent over the network.
Back	Click Back to return to the previous screen.

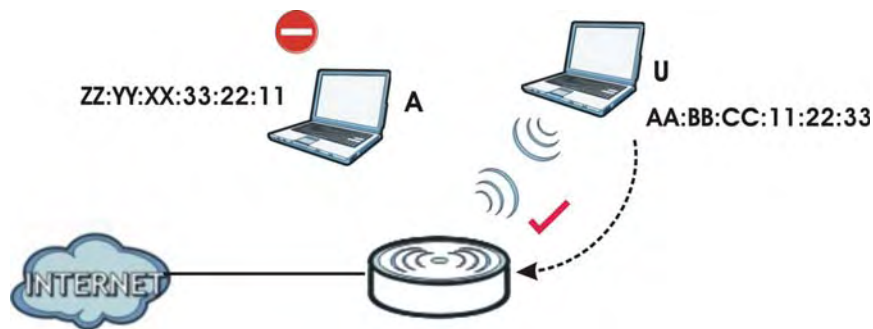
Table 23 Wireless LAN > RADIUS (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.8 MAC Filter Screen

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 each device to configure MAC filtering on the NWA1121-NI.









The MAC filter function allows you to configure the NWA1121-NI to grant access to the NWA1121-NI from other wireless devices (Allow Association) or exclude devices from accessing the NWA1121-NI (Deny Association).

Figure 39 MAC Filtering

In the figure above, wireless client **U** is able to connect to the Internet because its MAC address is in the allowed association list specified in the NWA1121-NI. The MAC address of client **A** is either denied association or is not in the list of allowed wireless clients specified in the NWA1121-NI.

Use this screen to enable MAC address filtering in your NWA1121-NI. You can specify MAC addresses to either allow or deny association with your NWA1121-NI. Click **Wireless LAN > MAC Filter**. The screen displays as shown.

Figure 40 Wireless LAN > MAC Filter

Wireless Settings SSID Security RADIUS MAC Filter			
MAC Filter Profiles			
#	Profile Name	Filter Action	Modify
1	MacProfile1	Disabled	
2	MacProfile2	Disabled	
3	MacProfile3	Disabled	
4	MacProfile4	Disabled	
5	MacProfile5	Disabled	
6	MacProfile6	Disabled	
7	MacProfile7	Disabled	
8	MacProfile8	Disabled	

Select a profile you want to configure and click **Edit**.

Figure 41 MAC Filter: Edit

MAC Filter

MAC Filter Settings

Profile Name : MacProfile1

Access Control Mode: Disabled

#	MAC Address	#	MAC Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
		16	
		18	
		20	
		22	
		24	
		26	
		28	
		30	
		32	
		34	
		36	
		38	
		40	
		42	
		44	
		46	
		48	
		50	
		52	
		54	
		56	
		58	
		60	
		62	
		64	
		66	
		68	
		70	
		72	
		74	
		76	
		78	
		80	
		82	
		84	
		86	
		88	
		90	
		92	
		94	
		96	
		98	
		100	
		102	
		104	
		106	
		108	
		110	
		112	
		114	
		116	
		118	
		120	
		122	
		124	
127		128	

Back Apply Cancel

The following table describes the labels in this screen.

Table 24 Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Profile Name	This is the name that identifying this profile.
Access Control Mode	Select Disabled if you do not want to use this feature. Select Allow to permit access to the NWA1121-NI. MAC addresses not listed will be denied access to the NWA1121-NI. Select Deny to block access to the NWA1121-NI. MAC addresses not listed will be allowed to access the NWA1121-NI.
#	This is the index number of the MAC address listed.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station to be allowed or denied access to the NWA1121-NI.
Back	Click Back to return to the previous screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

6.9 Technical Reference

This section provides technical background information about the topics covered in this chapter. Refer to [Appendix D on page 181](#) for further readings on Wireless LAN.

6.9.1 Additional Wireless Terms

Table 25 Additional Wireless Terms

TERM	DESCRIPTION
Intra-BSS Traffic	This describes direct communication (not through the NWA1121-NI) between two wireless devices within a wireless network. You might disable this kind of communication to enhance security within your wireless network.
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the NWA1121-NI. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the NWA1121-NI.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the NWA1121-NI does, it cannot communicate with the NWA1121-NI.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

TERM	DESCRIPTION
Roaming	If you have two or more NWA1121-NIs (or other wireless access points) on your wireless network, you can enable this option so that wireless devices can change locations without having to log in again. This is useful for devices, such as notebooks, that move around a lot.
Antenna	An antenna couples Radio Frequency (RF) signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air. Positioning the antennas properly increases the range and coverage area of a wireless LAN.

6.9.2 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual and applications. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The NWA1121-NI uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q or DSCP information in each packet's header. The NWA1121-NI automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency and jitter (variations in delay).

6.9.2.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the NWA1121-NI uses.

Table 26 WMM QoS Priorities

Priority Level	description
voice (WMM_VOICE)	Typically used for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality.
video (WMM_VIDEO)	Typically used for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.
best effort (WMM_BESTEFFORT)	Typically used for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
background (WMM_BACKGROUND)	This is typically used for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements.

6.9.3 Security Mode Guideline

The following is a general guideline in choosing the security mode for your NWA1121-NI.

- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.
- Use WPA(2) security if you have WPA(2)-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.
- If you don't have WPA(2)-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security. You can manually enter 64-bit or 128-bit WEP keys.

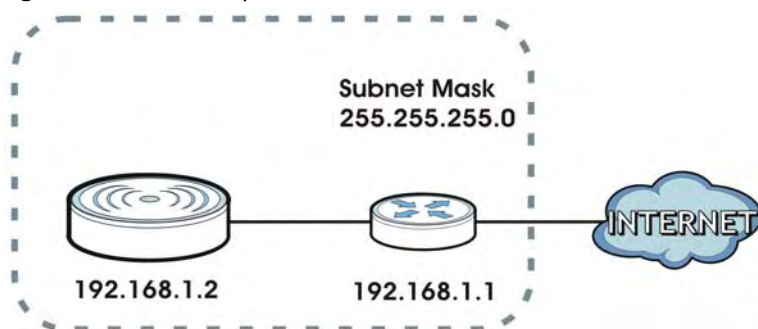
More information on Wireless Security can be found in [Appendix D on page 181](#).

7.1 Overview

This chapter describes how you can configure the IP address of your NWA1121-NI.

The Internet Protocol (IP) address identifies a device on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Figure 42 IPv4 Setup



The figure above illustrates one possible setup of your NWA1121-NI. The gateway IPv4 address is 192.168.1.1 and the IPv4 address of the NWA1121-NI is 192.168.1.2 (default). The gateway and the device must belong in the same subnet mask to be able to communicate with each other.

7.2 What You Can Do in this Chapter

Use the **LAN IP** screen to configure the IP address of your NWA1121-NI (see [Section 7.4 on page 96](#)).

7.3 What You Need to Know

The Ethernet parameters of the NWA1121-NI 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)

IPv6

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address 2001:0db8:1a2b:0015:0000:0000:1a2f:0000.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So 2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as 2001:db8:1a2b:15:0:0:1a2f:0.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So 2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as 2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015, 2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

2001:db8:1a2b:15::1a2f:0/32

means that the first 32 bits (2001:db8) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 27 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

7.4 LAN IP Screen

Use this screen to configure the IP address for your NWA1121-NI. Click **Network > LAN** to display the following screen.

Figure 43 LAN IP

The following table describes the labels in this screen.

Table 28 LAN IP

LABEL	DESCRIPTION
IPv4 Address Assignment	
Obtain IP Address Automatically	Select this option if your NWA1121-NI is using a dynamically assigned IPv4 address from a DHCP server each time. Note: You must know the IP address assigned to the NWA1121-NI (by the DHCP server) to access the NWA1121-NI again.
Use Fixed IP Address	Select this option if your NWA1121-NI is using a static IPv4 address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your NWA1121-NI in dotted decimal notation. Note: If you change the NWA1121-NI's IP address, you must use the new IP address if you want to access the web configurator again.
Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IPv4 address of the gateway. The gateway is an immediate neighbor of your NWA1121-NI that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NWA1121-NI; over the WAN, the gateway must be the IP address of one of the remote nodes.

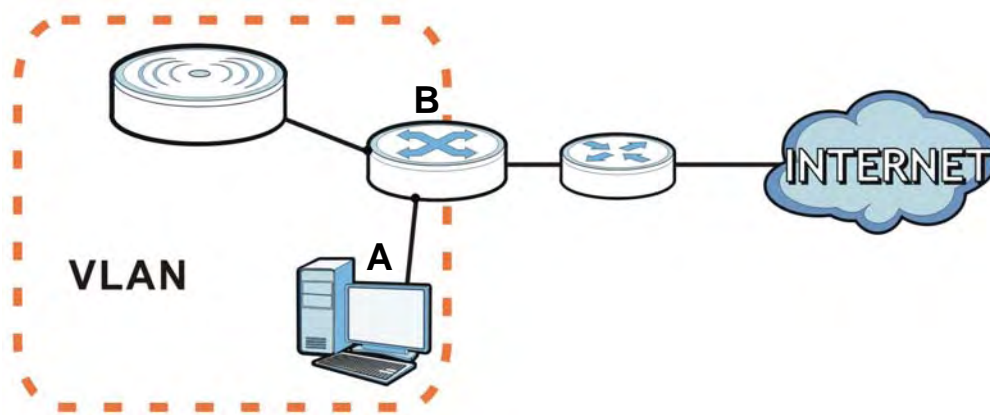
Table 28 LAN IP (continued)

LABEL	DESCRIPTION
IPv6 Address Assignment	
Enable Stateful Address Auto-configuration	Select this to turn on IPv6 stateful autoconfiguration to have the NWA1121-NI obtain an IPv6 global address from a DHCPv6 server in your network.
IPv6 Address/Prefix Length	Enter your IPv6 address and prefix manually.
System DNS Servers	
Primary DNS Server	Enter the IPv4 address of the first DNS (Domain Name Service) server, if provided.
Secondary DNS Server	Enter the IPv4 address of the second DNS (Domain Name Service) server address, if provided.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

8.1 Overview

This chapter discusses how to configure the NWA1121-NI's VLAN settings.

Figure 44 Management VLAN Setup



In the figure above, to access and manage the NWA1121-NI from computer **A**, the NWA1121-NI and switch **B**'s ports to which computer **A** and the NWA1121-NI are connected should be in the same VLAN.

8.1.1 What You Can Do in This Chapter

The **VLAN** screens let you set up the NWA1121-NI's management VLAN (Section 8.3 on page 99).

8.2 What You Need to Know

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

8.3 VLAN Screen

Use this screen to set up the VLAN for managing the NWA1121-NI. Click **Network > VLAN** to display the screen as shown.

Figure 45 Network > VLAN

The following table describes the labels in this screen.

Figure 46 Network > VLAN

LABEL	DESCRIPTION
802.1Q VLAN	Select this to enable VLAN tagging on the NWA1121-NI.
Management VLAN	Select this to enable VLAN management. Only traffic tagged with the management VLAN ID can access the NWA1121-NI. At least one device in your network must belong to the VLAN specified below in order to manage the NWA1121-NI.
Management VLAN ID	Enter a number from 1 to 4094 to define the NWA1121-NI's management VLAN group.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh.

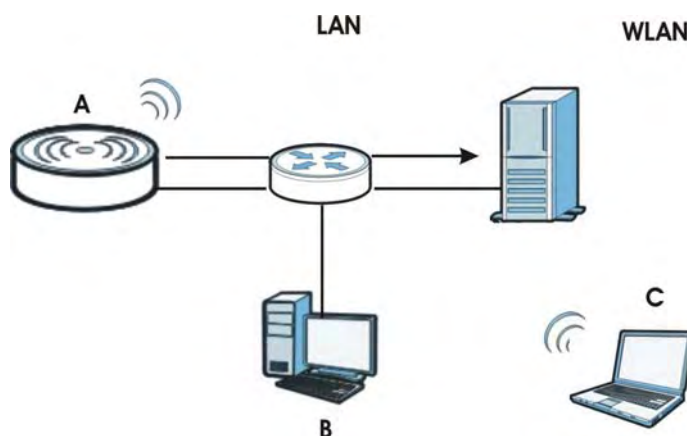
9.1 Overview

This chapter shows you how to enable remote management of your NWA1121-NI. It provides information on determining which services or protocols can access which of the NWA1121-NI's interfaces.

Remote Management allows a user to administrate the device over the network. You can manage your NWA1121-NI from a remote location via the following interfaces:

- WLAN
- LAN
- Both WLAN and LAN
- Neither (Disable)

Figure 47 Remote Management Example



In the figure above, the NWA1121-NI (A) is being managed by a desktop computer (B) connected via LAN (Land Area Network). It is also being accessed by a notebook (C) connected via WLAN (Wireless LAN).

9.2 What You Can Do in this Chapter

- Use the **WWW** screen to configure through which interface(s) and from which IP address(es) you can use the Web Browser to manage the NWA1121-NI (see [Section 9.4 on page 104](#)).
- Use the **Certificates** screen to delete and import certificates (seen [Section 9.5 on page 105](#)).

- Use the **Telnet** screen to configure through which interface(s) and from which IP address(es) you can use Telnet to manage the NWA1121-NI. A Telnet connection is prioritized by the NWA1121-NI over other remote management sessions (see [Section 9.6 on page 106](#)).
- Use the **SNMP** screen to configure through which interface(s) and from which IP address(es) a network systems manager can access the NWA1121-NI (see [Section 9.7 on page 107](#)).
- Use the **FTP** screen to configure through which interface(s) and from which IP address(es) you can use File Transfer Protocol (FTP) to manage the NWA1121-NI. You can use FTP to upload the latest firmware for example (see [Section 9.8 on page 110](#)).

9.3 What You Need To Know

WWW

The World Wide Web allows you to access files hosted in a remote server. For example, you can view text files (usually referred to as 'pages') using your web browser via HyperText Transfer Protocol (HTTP).

Telnet

Telnet is short for Telecommunications Network, which is a client-side protocol that enables you to access a device over the network.

FTP

File Transfer Protocol (FTP) allows you to upload or download a file or several files to and from a remote location using a client or the command console.

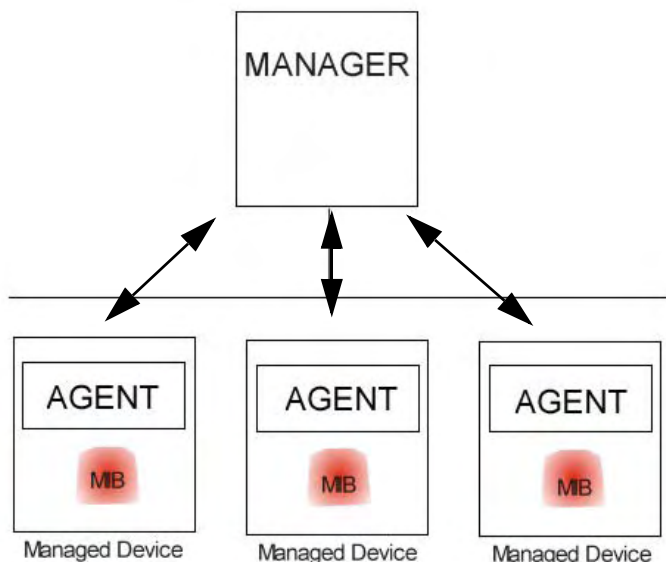
SNMP

Simple Network Management Protocol (SNMP) is a member of the TCP/IP protocol suite used for exchanging management information between network devices.

Your NWA1121-NI supports SNMP agent functionality, which allows a manager station to manage and monitor the NWA1121-NI through the network. [The NWA1121-NI supports SNMP version one \(SNMPv1\), version two \(SNMPv2c\) and version three \(SNMPv3\).](#)

The next figure illustrates an SNMP management operation.

Figure 48 SNMP Management Mode



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the NWA1121-NI). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

SNMP allows a manager and agents to communicate for the purpose of accessing information such as packets received, node port status, etc.

SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

Remote Management Limitations

Remote management over LAN or WLAN will not work when:

- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the NWA1121-NI will disconnect the session immediately.

- You may only have one remote management session running at one time. The NWA1121-NI automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows:

- 1 Telnet
- 2 HTTP

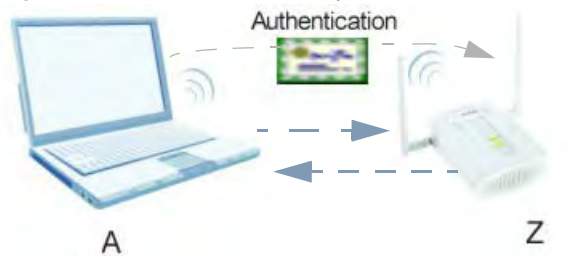
System Timeout

~~There is a default system management idle timeout of five minutes (three hundred seconds). The NWA1121-NI automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **SYSTEM** screen.~~

Certificate

A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Figure 49 Certificates Example



In the figure above, the NWA1121-NI (Z) checks the identity of the notebook (A) using a certificate before granting access to the network.

The certification authority certificate that you can import to your NWA1121-NI should be in PFX PKCS#12 file format. This format referred to as the Personal Information Exchange Syntax Standard is comprised of a private key-public certificate pair that is further encrypted with a password. Before you import a certificate into the NWA1121-NI, you should verify that you have the correct certificate.

Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

9.4 WWW Screen

Use this screen to configure your NWA1121-NI via the World Wide Web (**WWW**) using a Web browser. This lets you specify which IP addresses or computers are able to communicate with and access the NWA1121-NI.

To change your NWA1121-NI's **WWW** settings, click **System** > **WWW**. The following screen shows.

Figure 50 System > WWW

The screenshot shows the 'WWW' configuration page. At the top, there are tabs: 'WWW', 'Certificates', 'Telnet', 'SNMP', and 'FTP'. The 'WWW' tab is selected. Below the tabs, the page is titled 'www'. There are five main configuration sections: 'HTTP Port' with a text box containing '80'; 'HTTPS Port' with a text box containing '443'; 'Server Access' with a dropdown menu showing 'Disable'; 'Secured Client IP Address' with radio buttons for 'All' (selected) and 'Selected' (with a text box containing '0.0.0.0'); and 'Secured Client MAC Address' with radio buttons for 'All' (selected) and 'Selected' (with a text box containing '00:00:00:00:00:00'). At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 29 System > WWW

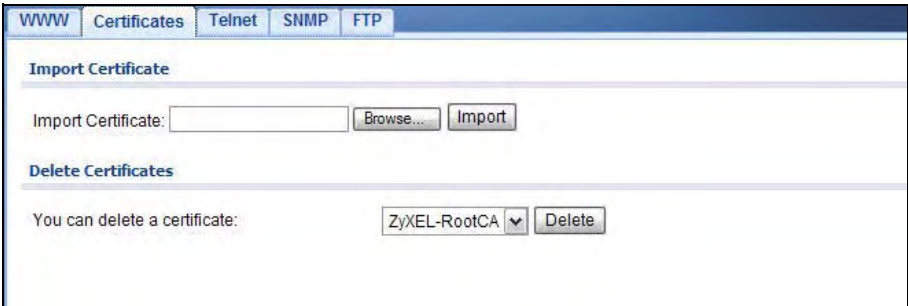
LABEL	DESCRIPTION
WWW	
HTTP Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
HTTPS Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the NWA1121-NI, for example 8443, then you must notify people who need to access the NWA1121-NI web configurator to use "https://NWA1121-NI IP Address:8443" as the URL.
Server Access	Select the interface(s) through which a computer may access the NWA1121-NI using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NWA1121-NI using this service. Select All to allow any computer to access the NWA1121-NI using this service. Choose Selected to just allow the computer with the IP address that you specify to access the NWA1121-NI using this service.
Secured Client MAC Address	Select All to allow any computer to access the NWA1121-NI using this service. Choose Selected to just allow the computer with the MAC address that you specify to access the NWA1121-NI using this service.
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

9.5 Certificates Screen

Use this screen to delete or import certificates.

Click **System > Certificates**. The following screen shows.

Figure 51 System > Certificates



The following table describes the labels in this screen.

Table 30 System > Certificates

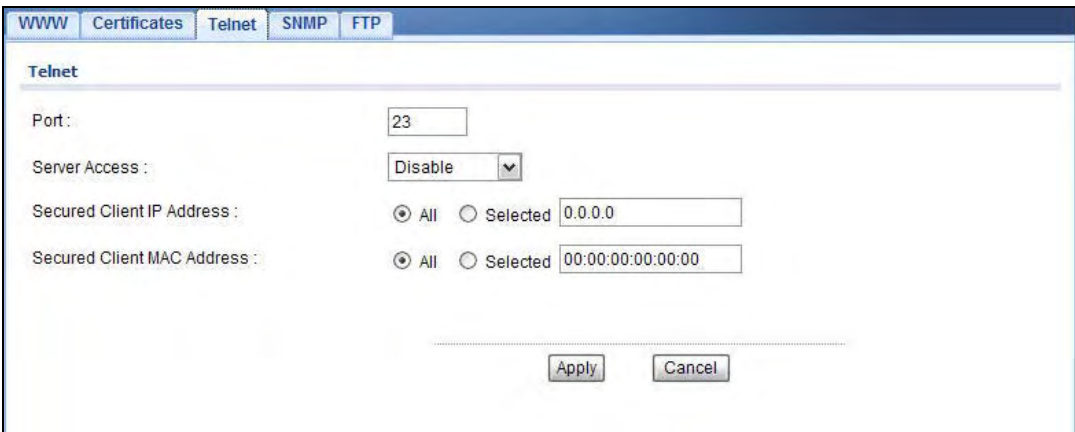
LABEL	DESCRIPTION
Import Certificate	
Import Certificate	Enter the location of a previously-saved certificate to upload to the NWA1121-NI. Alternatively, click the Browse button to locate a list.
Browse	Click this button to locate a previously-saved certificate to upload to the NWA1121-NI.
Import	Click this button to upload the previously-saved certificate displayed in the Import Certificate field to the NWA1121-NI.
Delete Certificate	
You can delete a certificate	Select the certificate from the list that you want to delete.
Delete	Click this to delete the selected certificate.

9.6 Telnet Screen

Use this screen to configure your NWA1121-NI for remote Telnet access. **You can use Telnet to access the NWA1121-NI's Command Line Interface (CLI).**

Click **System > Telnet**. The following screen displays.

Figure 52 System > Telnet



The following table describes the labels in this screen.

Table 31 System > Telnet

LABEL	DESCRIPTION
TELNET	
Port	You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NWA1121-NI using Telnet.
Secured Client IP Address	<p>A secured client is a “trusted” computer that is allowed to communicate with the NWA1121-NI using this service.</p> <p>Select All to allow any computer to access the NWA1121-NI using this service.</p> <p>Choose Selected to just allow the computer with the IP address that you specify to access the NWA1121-NI using this service.</p>
Secured Client MAC Address	<p>Select All to allow any computer to access the NWA1121-NI using this service.</p> <p>Choose Selected to just allow the computer with the MAC address that you specify to access the NWA1121-NI using this service.</p>
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

9.7 SNMP Screen

Use this screen to have a manager station administrate your NWA1121-NI over the network and configure SNMP accounts on the SNMP v3 manager. An SNMP administrator/user is an SNMP

manager. To change your NWA1121-NI's SNMP settings, click **System > SNMP**. The following screen displays.

Figure 53 System > SNMP

SNMP

Port : 161

Server Access : Disable

Secured Client IP Address : ☒ All ☐ Selected 0.0.0.0

Secured Client MAC Address : ☒ All ☐ Selected 00:00:00:00:00:00

SNMP Configuration

Protocol Version: V3

Get Community : public

Set Community : private

Trap Community : private

Trap Destination : 192.168.1.10

SNMPv3 Admin Settings

SNMPv3 Admin: ☒ Enabled

User Name: SNMPv3Admin

Password: (8 - 32 alphanumeric, printable characters and no spaces)

Confirm Password:

Access Type: Read/Write

Authentication Protocol: SHA

Privacy Protocol: DES

SNMPv3 User Settings

SNMPv3 User: ☒ Enabled

User Name: SNMPv3User

Password: (8 - 32 alphanumeric, printable characters and no spaces)

Confirm Password:

Access Type: Read Only

Authentication Protocol: MD5

Privacy Protocol: None

Apply Cancel

The following table describes the labels in this screen.

Table 32 System > SNMP

LABEL	DESCRIPTION
SNMP	
Port	You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

Table 32 System > SNMP (continued)

LABEL	DESCRIPTION
Server Access	Select the interface(s) through which a computer may access the NWA1121-NI using Telnet.
Secured Client IP Address	<p>A secured client is a “trusted” computer that is allowed to communicate with the NWA1121-NI using this service.</p> <p>Select All to allow any computer to access the NWA1121-NI using this service.</p> <p>Choose Selected to just allow the computer with the IP address that you specify to access the NWA1121-NI using this service.</p>
Secured Client MAC Address	<p>Select All to allow any computer to access the NWA1121-NI using this service.</p> <p>Choose Selected to just allow the computer with the MAC address that you specify to access the NWA1121-NI using this service.</p>
SNMP Configuration	
Protocol Version	<p>Select the SNMP version for the NWA1121-NI, which you allow the SNMP manager to use to access the NWA1121-NI.</p> <p>The SNMP version on the NWA1121-NI must match the version on the SNMP manager.</p> <p>Note: SNMP version 2c is backwards compatible with SNMP version 1.</p>
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
SNMPv3 Admin Settings	
SNMPv3 Admin	Select the check box to enable the SNMP administrator account for authentication with SNMP managers using SNMP v3.
User Name	Specify the user name of the SNMP administrator account.
Password	Enter the password for SNMP administrator authentication.
Confirm Password	Retype the password for confirmation.
Access type	<p>Specify the SNMP administrator's access rights to MIBs.</p> <p>Read/Write - The SNMP administrator has read and write rights, meaning that the user can create and edit the MIBs on the NWA1121-NI.</p> <p>Read Only - The SNMP administrator has read rights only, meaning the user can collect information from the NWA1121-NI.</p>
Authentication Protocol	<p>Select an authentication algorithm used for SNMP communication with the SNMP administrator.</p> <p>MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.</p>
Privacy Protocol	<p>Specify the encryption method used for SNMP communication with the SNMP administrator.</p> <p>DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.</p> <p>AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.</p>

Table 32 System > SNMP (continued)

LABEL	DESCRIPTION
SNMPv3 User Settings	
SNMPv3 User	Select the check box to enable the SNMP user account for authentication with SNMP managers using SNMP v3.
User Name	Specify the user name of the SNMP user account.
Password	Enter the password for SNMP user authentication.
Confirm Password	Retype the password for confirmation.
Access Type	Specify the SNMP user's access rights to MIBs. Read Only - The SNMP user has read rights only, meaning the user can collect information from the NWA1121-NI. Read/Write - The SNMP user has read and write rights, meaning that the user can create and edit the MIBs on the NWA1121-NI.
Authentication Protocol	Select an authentication algorithm used for SNMP communication with the SNMP user. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5 , but is slower.
Privacy Protocol	Specify the encryption method used for SNMP communication with the SNMP user. DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

9.8 FTP Screen

Use this screen to upload and download the NWA1121-NI's firmware using FTP. To use this feature, your computer must have an FTP client.

To change your NWA1121-NI's FTP settings, click **System** > **FTP**. The following screen displays.

Figure 54 System > FTP

The following table describes the labels in this screen.

Table 33 System > FTP

LABEL	DESCRIPTION
FTP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NWA1121-NI using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NWA1121-NI using this service. Select All to allow any computer to access the NWA1121-NI using this service. Choose Selected to just allow the computer with the IP address that you specify to access the NWA1121-NI using this service.
Secured Client MAC Address	Select All to allow any computer to access the NWA1121-NI using this service. Choose Selected to just allow the computer with the MAC address that you specify to access the NWA1121-NI using this service.
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

9.9 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

9.9.1 MIB

Managed devices in an SMNP managed network contain object variables or managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

9.9.2 Supported MIBs

The NWA1121-NI supports MIB II that is defined in RFC-1213 and RFC-1215 as well as the proprietary ZyXEL private MIB. The purpose of the MIBs is to let administrators collect statistical data and monitor status and performance.

9.9.3 ~~SNMP Traps~~

~~SNMP traps are messages sent by the agents of each managed device to the SNMP manager. These messages inform the administrator of events in data networks handled by the device. The NWA1121-NI can send the following traps to the SNMP manager.~~

Table 34 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Generic Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent after booting (power on). This trap is defined in RFC-1215.
warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent after booting (software reboot). This trap is defined in RFC-1215.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure (defined in <i>RFC-1215</i>)	1.3.6.1.6.3.1.1.5.5	The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password). Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps.
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.13.0.1	This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.
pwTFTPStatus	1.3.6.1.4.1.890.1.9.2.3.3.1	This trap is sent to indicate the status and result of a TFTP client session that has ended.

~~Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the NWA1121-NI's physical and virtual ports.~~

Table 35 SNMP Interface Index to Physical and Virtual Port Mapping

TYPE	INTERFACE	PORT
Physical	enet0	Wireless LAN adaptor WLAN1
	enet1	Ethernet port (LAN)
	enet2	Wireless LAN adaptor WLAN2
Virtual	enet3 ~ enet9	WLAN1 in MBSSID mode
	enet10 ~ enet16	WLAN2 in MBSSID mode
	enet17 ~ enet21	WLAN1 in WDS mode
	enet22 ~ enet26	WLAN2 in WDS mode

9.9.4 Private-Public Certificates

When using public-key cryptology for authentication, 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.

These keys work like a handwritten signature (in fact, certificates are often referred to as “digital signatures”). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key “writes” your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

- 1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
- 2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
- 3 Tim uses his private key to sign the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim’s public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim’s private key).
- 5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny’s public key to verify the message.

9.9.5 Certification Authorities

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 NWA1121-NI to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

9.9.6 Checking the Fingerprint of a Certificate on Your Computer

A certificate’s fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate’s fingerprint to verify that you have the actual certificate.

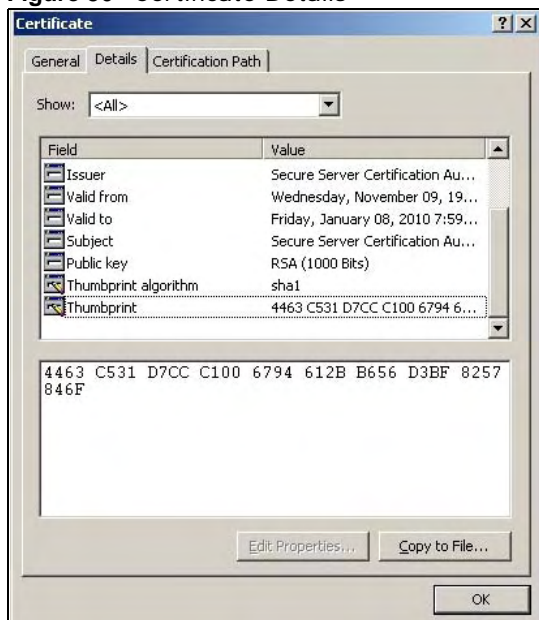
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a “.cer” or “.crt” file name extension.

Figure 55 Certificates on Your Computer



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 56 Certificate Details



- 4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary according to your situation. Possible examples would be over the telephone or through an HTTPS connection.

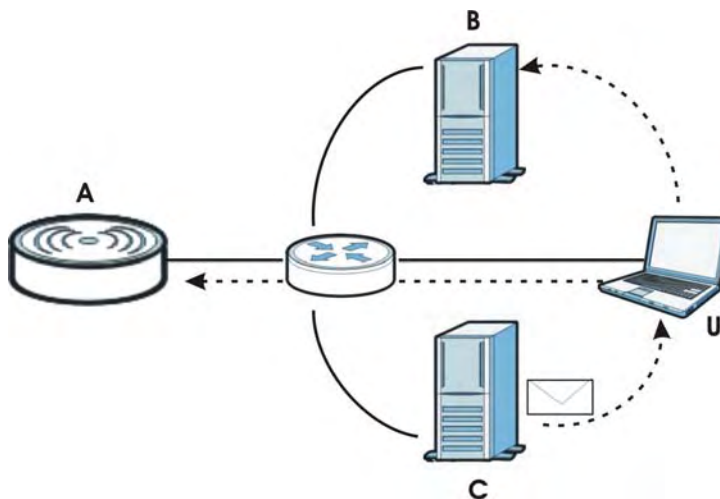
Log Settings

10.1 Overview

This chapter provides information on viewing and generating logs on your NWA1121-NI.

Logs are files that contain recorded network activity over a set period. They are used by administrators to monitor the health of the system(s) they are managing. Logs enable administrators to effectively monitor events, errors, progress, etc. so that when network problems or system failures occur, the cause or origin can be traced. Logs are also essential for auditing and keeping track of changes made by users.

Figure 57 Accessing Logs in the Network



The figure above illustrates three ways to access logs. The user (**U**) can access logs directly from the NWA1121-NI (**A**) via the Web configurator. Logs can also be located in an external log server (**B**). An email server (**C**) can also send harvested logs to the user's email account.

10.2 What You Can Do in this Chapter

Use the **Log Settings** screen to configure where and when the NWA1121-NI will send the logs, and which logs ~~and/or immediate alerts~~ it will send ([Section 10.4 on page 116](#)). Use the **Monitor > Logs** screen to display all logs or logs for a certain category.

10.3 What You Need To Know

Alerts and Logs

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

Receiving Logs via E-mail

If you want to receive logs in your e-mail account, you need to have the necessary details ready, such as the Server Name or Simple Mail Transfer Protocol (SMTP) Address of your e-mail account. Ensure that you have a valid e-mail address.

Enabling Syslog Logging

To enable Syslog Logging, obtain your Syslog server's IP address (or server name).

10.4 Log Settings Screen

Use this screen to configure to where and when the NWA1121-NI is to send the logs and which logs and/or immediate alerts it is to send.

To change your NWA1121-NI's log settings, click **Configuration > Log Settings**. The screen appears as shown.

Figure 58 Log Settings

The following table describes the labels in this screen.

Table 36 Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
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 NWA1121-NI sends.
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.

Table 36 Log Settings (continued)

LABEL	DESCRIPTION
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs. If you use SMTP authentication, the mail receiver should be the owner of the SMTP account.
User Name	If your e-mail account requires SMTP authentication, enter the username here.
Password	Enter the password associated with the above username.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Syslog Logging	Select the check box to enable syslog logging.
Syslog Server IP Address	Enter the IP address of the syslog server that will log the selected categories of logs.
Syslog Port Number	Enter the port number of the syslog server that will log the selected categories of logs.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: <ul style="list-style-type: none">• When Log is Full• Hourly• Daily• Weekly• 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 Category	
System Maintenance	Click this to receive logs related to system maintenance.
System Error	Click this to receive logs related to system errors.
802.1x	Click this to receive logs related to the 802.1x mode.
Wireless	Click this to receive logs related to the wireless function.
Email Log Now	Select the categories of alerts for which you want the NWA1121-NI to immediately send e-mail alerts.
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

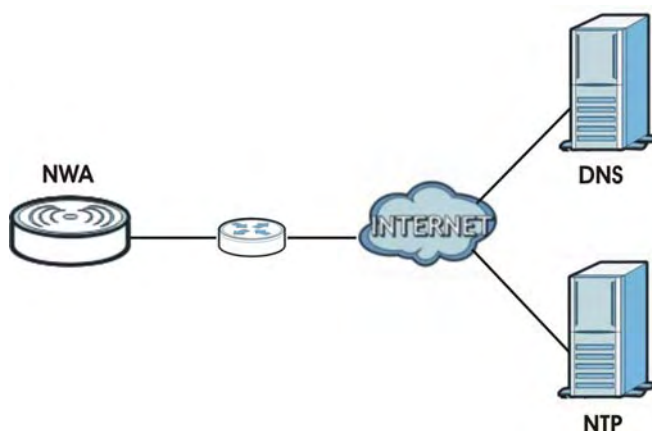
Maintenance

11.1 Overview

This chapter describes the maintenance screens. It discusses how you can upload new firmware, manage configuration and restart your NWA1121-NI without turning it off and on.

This chapter provides information and instructions on how to identify and manage your NWA1121-NI over the network.

Figure 59 NWA1121-NI Setup



In the figure above, the NWA1121-NI connects to a Domain Name Server (DNS) server to avail of a domain name. It also connects to an Network Time Protocol (NTP) server to set the time on the device.

11.2 What You Can Do in this Chapter

- Use the **General** screen to specify the system name (see [Section 11.4 on page 120](#)).
- Use the **Password** screen to manage the password for your NWA1121-NI (see [Section 11.5 on page 121](#)).
- Use the **Time** screen to change your NWA1121-NI's time and date. This screen allows you to configure the NWA1121-NI's time based on your local time zone (see [Section 11.6 on page 122](#)).
- Use the **Firmware Upload** screen to upload the latest firmware for your NWA1121-NI (see [Section 11.7 on page 123](#)).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (see [Section 11.8 on page 124](#)).

- Use **Restart** screen to reboot the NWA1121-NI without turning the power off (see [Section 11.9 on page 126](#)).

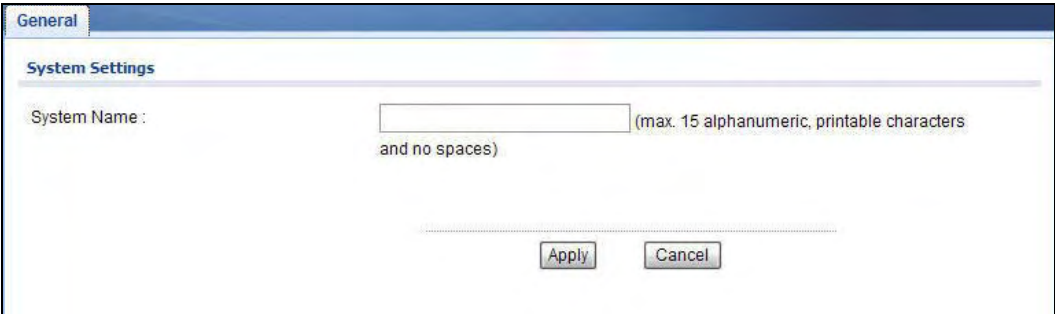
11.3 What You Need To Know

You can find the firmware for your device at www.zyxel.com. It is a file that (usually) uses the system model name with a ".bin" extension, for example "[Model #].bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

11.4 General Screen

Use the **General** screen to identify your NWA1121-NI over the network. Click **Maintenance > General**. The following screen displays.

Figure 60 Maintenance > General



The following table describes the labels in this screen.

Table 37 Maintenance > General

LABEL	DESCRIPTION
System Settings	
System Name	Type a descriptive name to identify the NWA1121-NI in the Ethernet network. This name can be up to 15 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.5 Password Screen

Use this screen to control access to your NWA1121-NI by assigning a password to it. Click **Maintenance > Password**. The following screen displays.

Figure 61 Maintenance > Password

The screenshot shows a web-based 'Password Setup' interface. It features a blue header with the word 'Password'. Below the header, the title 'Password Setup' is displayed. The form includes three text input fields: 'Current Password:', 'New Password:', and 'Retype to Confirm:'. The 'New Password:' field is accompanied by a character count '(1-32 characters)'. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 38 Maintenance > Password

LABEL	DESCRIPTIONS
Current Password	Type in your existing system password.
New Password	Type your new system password. Note that as you type a password, the screen displays a dot (.) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.6 Time Screen

Use this screen to change your NWA1121-NI's time and date, click **Maintenance > Time**. The following screen displays.

Figure 62 Maintenance > Time

Time

Current Time and Date

Current Time :

23

40

34

(hh:mm:ss)

Current Date :

1970

Jan

7

(YY:MM:DD)

Time and Date Setup

NTP Client Update:

☒ Enabled

☒ NTP Server:

ntp1.cs.wisc.edu

☐ Manual IP :

Time Zone Setup

Time Zone :

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Apply

Cancel

The following table describes the labels in this screen.

Table 39 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NWA1121-NI. Each time you reload this page, the NWA1121-NI synchronizes the time with the time server (if configured). When you disable NTP Client Update , you can manually enter the new time in this field and then click Apply .
Current Date	This field displays the last updated date from the time server. When you disable NTP Client Update , you can manually enter the new date in this field and then click Apply .
Time and Date Setup	
NTP Client Update	Select this to have the NWA1121-NI get the time and date from the time server you specified below.
NTP server	Select this option to use the predefined list of Network Time Protocol (NTP) servers. Select an NTP server from the drop-list box.
Manual IP	Select this option to enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Apply	Click Apply to save your changes.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.7 Firmware Upgrade Screen

Use this screen to upload a firmware to your NWA1121-NI. Click **Maintenance > Firmware Upgrade**. Follow the instructions in this section to upload firmware to your NWA1121-NI.

Figure 63 Maintenance > Firmware Upgrade

The following table describes the labels in this screen.

Table 40 Maintenance > Firmware Upgrade

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.

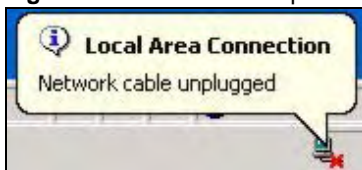
Do not turn off the NWA1121-NI while firmware upload is in progress!

After you see the ~~Firmware Upload in Process~~ screen, wait two minutes before logging into the NWA1121-NI again.

Figure 64 Firmware Upload In Process

The NWA1121-NI automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

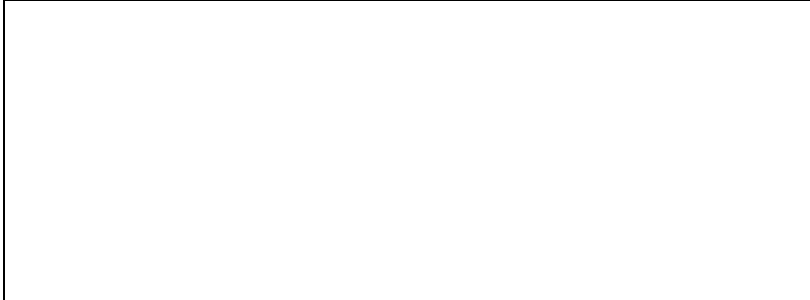
Figure 65 Network Temporarily Disconnected



After the upload was finished, log in again and check your new firmware version in the **Dashboard** screen.

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

Figure 66 ~~Firmware Upload Error~~



11.8 Configuration File Screen

Use this screen to backup, restore and reset the configuration of your NWA1121-NI.

Click **Maintenance > Configuration File**. The screen appears as shown next.

Figure 67 Maintenance > Configuration File

The screenshot shows the 'Configuration File' screen with a blue header. It contains three main sections:

- Backup Configuration:** A section with a 'Backup' button and the instruction: 'Click **Backup** to save the current configuration of your system to your computer.'
- Restore Configuration:** A section with instructions: 'To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.' It includes a 'File Path:' text box, a 'Browse...' button, and an 'Upload' button.
- Back to Factory Defaults:** A section with a 'Reset' button and instructions: 'Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the'
 - Password will be 1234
 - LAN IP address will be 192.168.1.2

11.8.1 Backup Configuration

Backup configuration allows you to back up (save) the NWA1121-NI's current configuration to a file on your computer. Once your NWA1121-NI 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 NWA1121-NI's current configuration to your computer.

11.8.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NWA1121-NI.

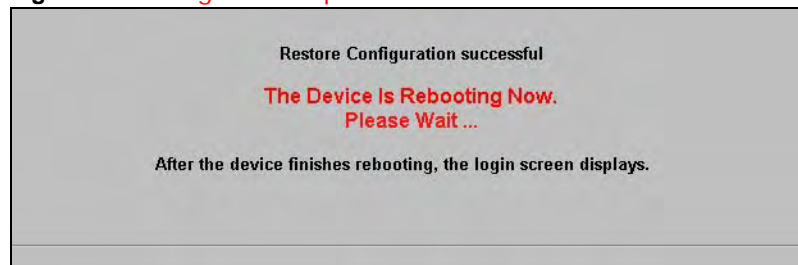
Table 41 Restore Configuration

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.

Do not turn off the NWA1121-NI while configuration file upload is in progress.

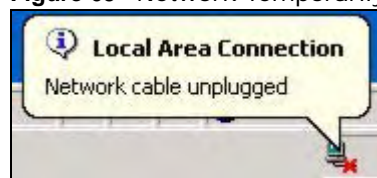
~~After you see a "restore configuration successful" screen~~, you must then wait one minute before logging into the NWA1121-NI again.

Figure 68 ~~Configuration Upload Successful~~



The NWA1121-NI automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

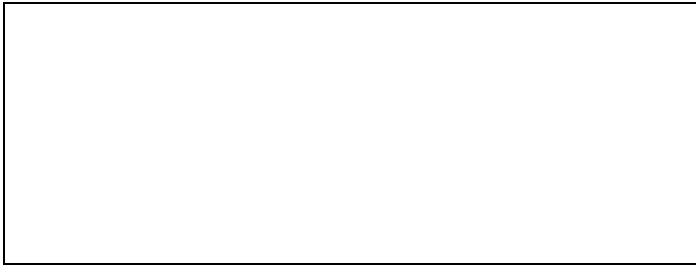
Figure 69 Network Temporarily Disconnected



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 NWA1121-NI IP address (192.168.1.2). See [Appendix A on page 133](#) 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 Backup/Restore screen.~~

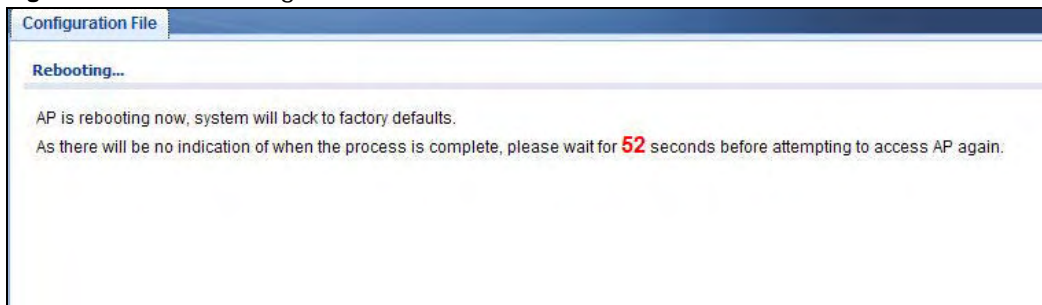
Figure 70 Configuration Upload Error



11.8.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NWA1121-NI to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 71 Reset Message



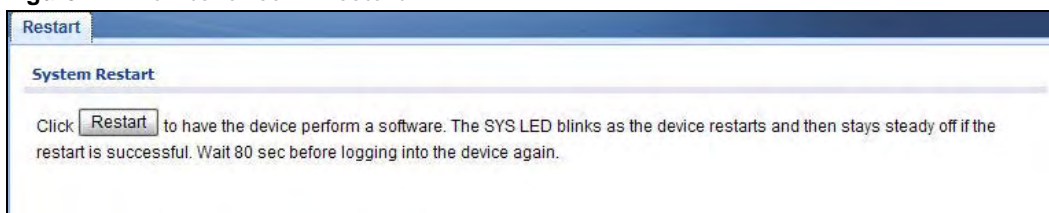
You can also press the **RESET** button to reset your NWA1121-NI to its factory default settings. Refer to [Section 2.2 on page 20](#) for more information.

11.9 Restart Screen

Use this screen to reboot the NWA1121-NI without turning the power off.

Click **Maintenance** > **Restart**. The following screen displays.

Figure 72 Maintenance > Restart



Click **Restart** to have the NWA1121-NI reboot. This does not affect the NWA1121-NI's configuration.

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [NWA1121-NI Access and Login](#)
- [Internet Access](#)

12.1 Power, Hardware Connections, and LEDs

[The NWA1121-NI does not turn on. None of the LEDs turn on.](#)

- 1 Make sure you are using the power adaptor or cord included with the NWA1121-NI.
- 2 Make sure the power adaptor or cord is connected to the NWA1121-NI and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adaptor or cord to the NWA1121-NI.
- 4 If the problem continues, contact the vendor.

[One of the LEDs does not behave as expected.](#)

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.7 on page 17](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the power adaptor to the NWA1121-NI.
- 5 If the problem continues, contact the vendor.

12.2 NWA1121-NI Access and Login

I forgot the IP address for the NWA1121-NI.

- 1 The default IP address is **192.168.1.2**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the NWA1121-NI by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter "**cmd**", and then enter "**ipconfig**". The IP address of the **Default Gateway** might be the IP address of the NWA1121-NI (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 2.2 on page 20](#).

I forgot the password.

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 2.2 on page 20](#).

I cannot see or access the **Login** screen in the web configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is 192.168.1.2.
 - If you changed the IP address ([Section 7.4 on page 96](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the NWA1121-NI](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.7 on page 17](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See [Section 12.1 on page 129](#).
- 4 Make sure your computer is in the same subnet as the NWA1121-NI. (If you know that there are routers between your computer and the NWA1121-NI, skip this step.)
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NWA1121-NI.
- 5 Reset the device to its factory defaults, and try to access the NWA1121-NI with the default IP address. See [Chapter 2 on page 20](#).

- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NWA1121-NI using another service, such as Telnet. If you can access the NWA1121-NI, check the remote management settings to find out why the NWA1121-NI does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a LAN/Ethernet port.

I can see the **Login** screen, but I cannot log in to the NWA1121-NI.

- 1 Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using the Telnet to access the NWA1121-NI. Log out of the NWA1121-NI in the other session, or ask the person who is logged in to log out.
- 3 Disconnect and re-connect the power adaptor or cord to the NWA1121-NI.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 2.2 on page 20](#).

I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

12.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 12.1 on page 129](#).
- 2 Make sure your NWA1121-NI is connected to a networking device that provides Internet access.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings on the wireless client are the same as the settings on the AP.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

- 5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NWA1121-NI), but my Internet connection is not available anymore.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.7 on page 17](#).
- 2 Reboot the NWA1121-NI.
- 3 If the problem continues, contact your ISP or network administrator.

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.7 on page 17](#). If the NWA1121-NI is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal is weak, try moving the NWA1121-NI (in wireless client mode) closer to the AP (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).
- 3 Reboot the NWA1121-NI.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it.

Setting Up Your Computer's IP Address

Note: Your specific NWA1121-NI may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

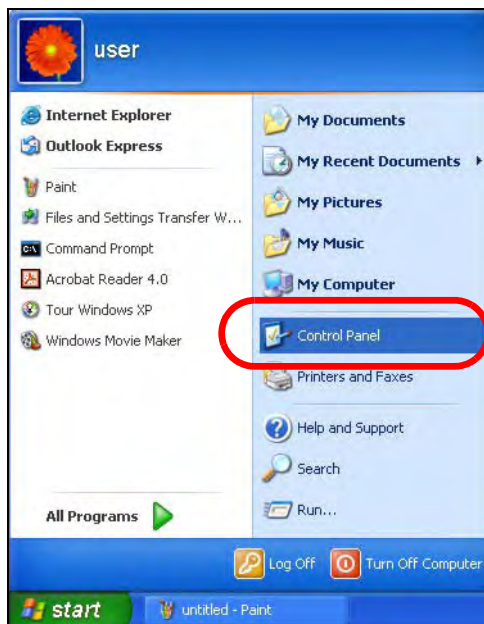
In this appendix, you can set up an IP address for:

- [Windows XP/NT/2000](#) on [page 133](#)
- [Windows Vista](#) on [page 137](#)
- [Windows 7](#) on [page 141](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 145](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 148](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 151](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 155](#)

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

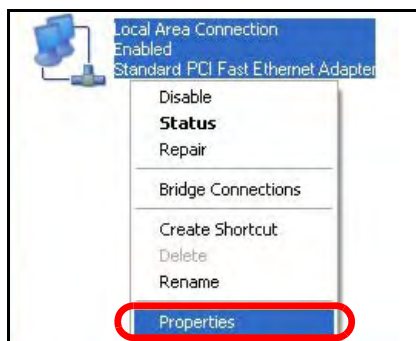
- 1 Click **Start > Control Panel**.



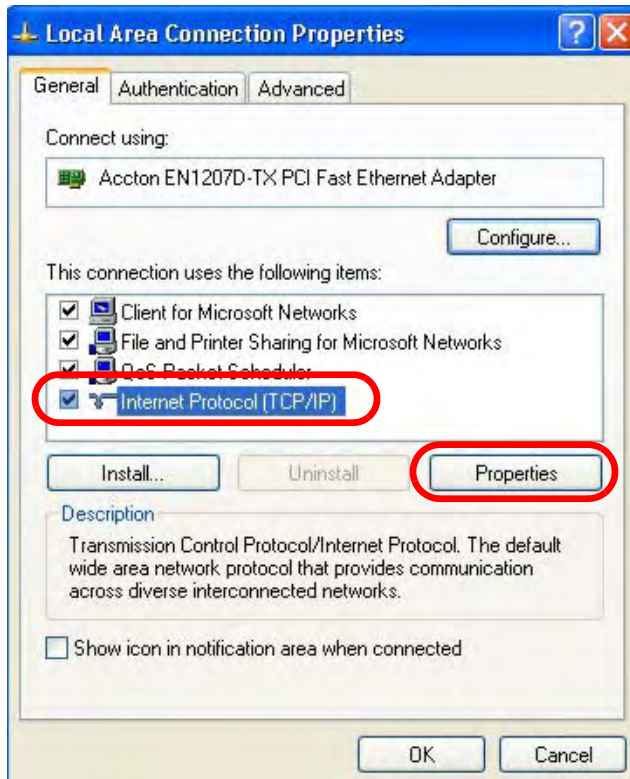
- 2 In the **Control Panel**, click the **Network Connections** icon.



- 3 Right-click **Local Area Connection** and then select **Properties**.



- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



- 5 The **Internet Protocol TCP/IP Properties** window opens.



- 6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided.

- 7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

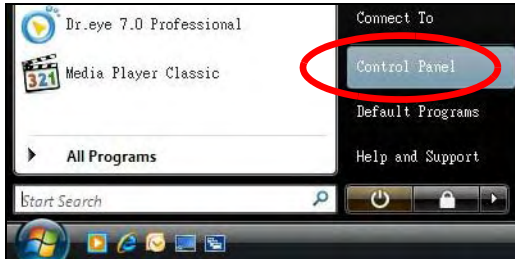
- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

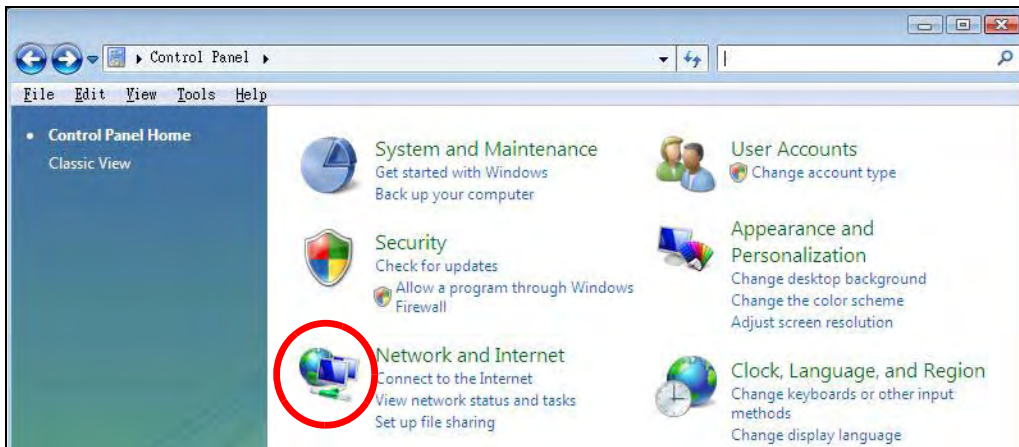
Windows Vista

This section shows screens from Windows Vista Professional.

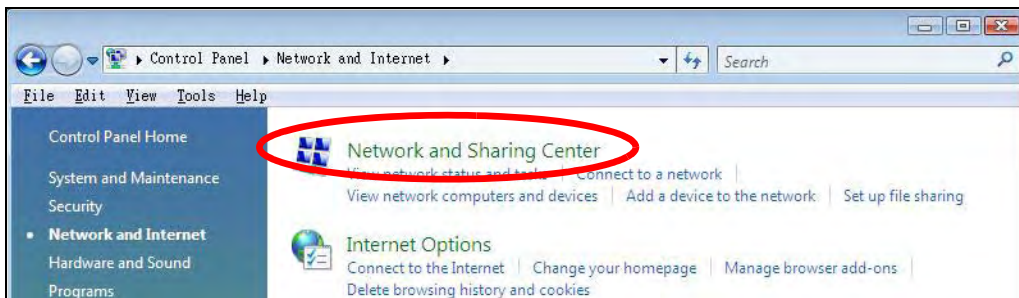
- 1 Click **Start > Control Panel**.



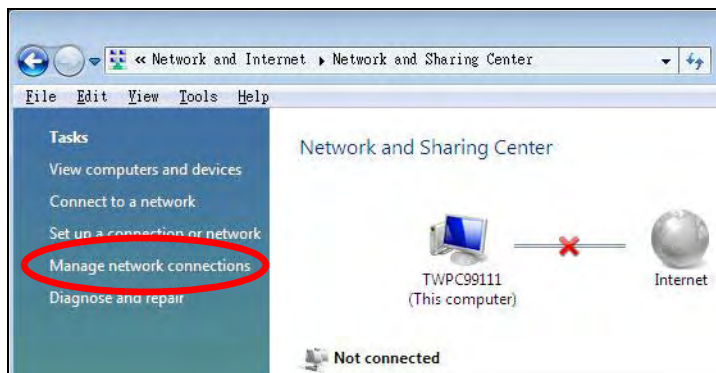
- 2 In the **Control Panel**, click the **Network and Internet** icon.



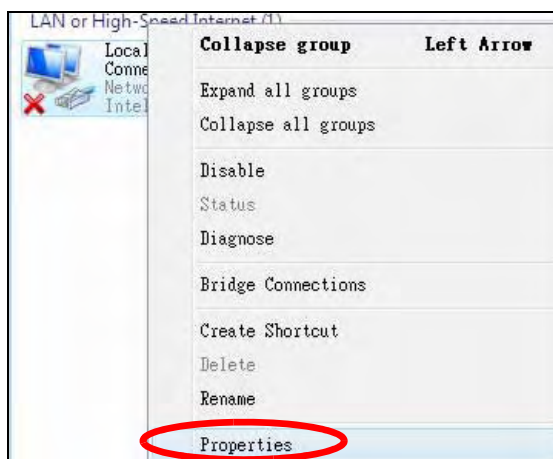
- 3 Click the **Network and Sharing Center** icon.



- 4 Click **Manage network connections**.

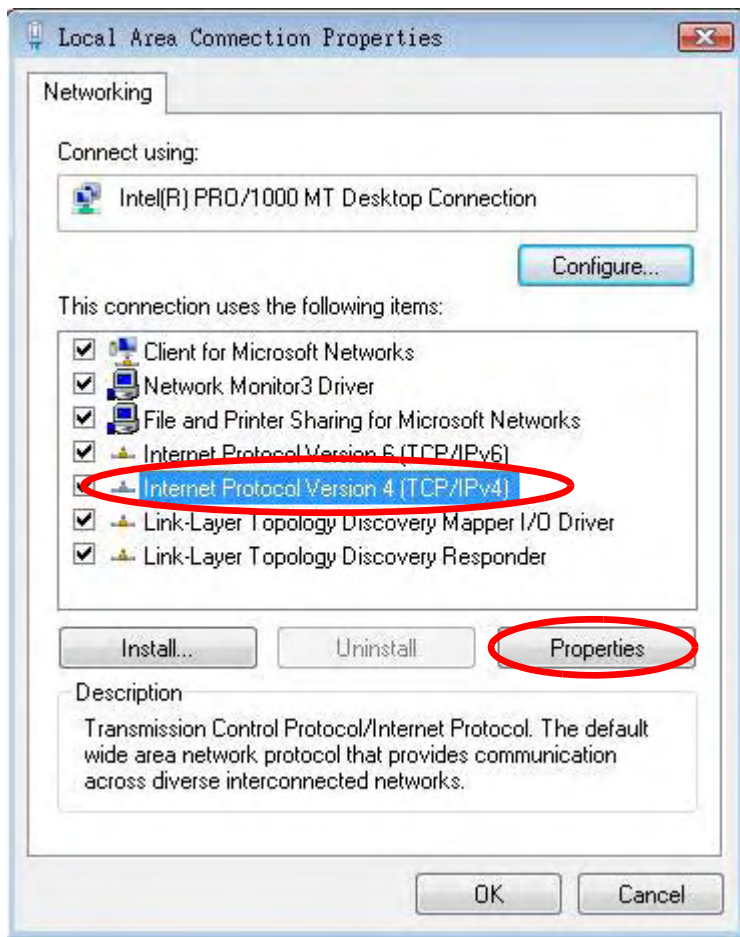


- 5 Right-click **Local Area Connection** and then select **Properties**.

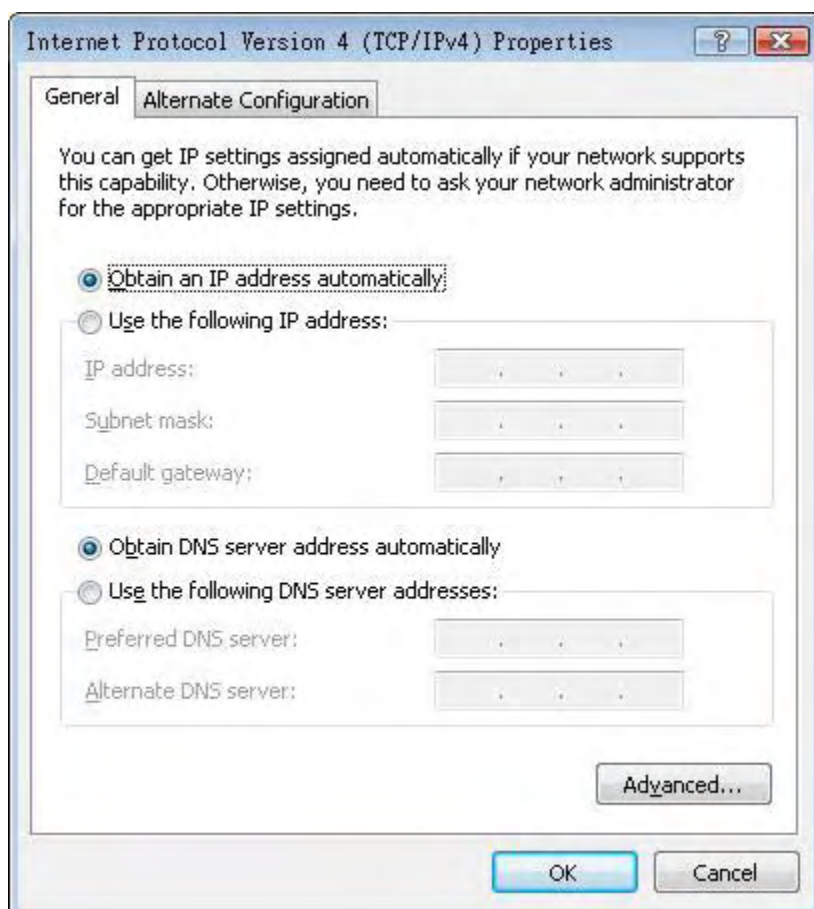


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



- 8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.
- Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced**.
- 9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 10 Click **OK** to close the **Local Area Connection Properties** window.

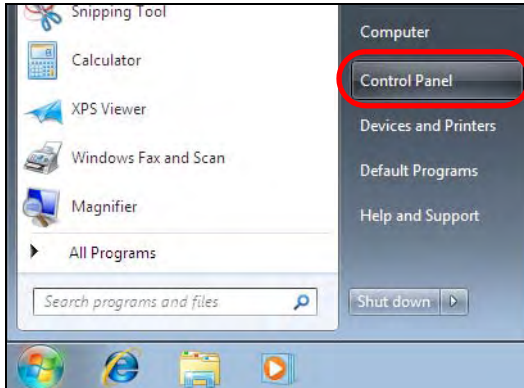
Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].
- You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

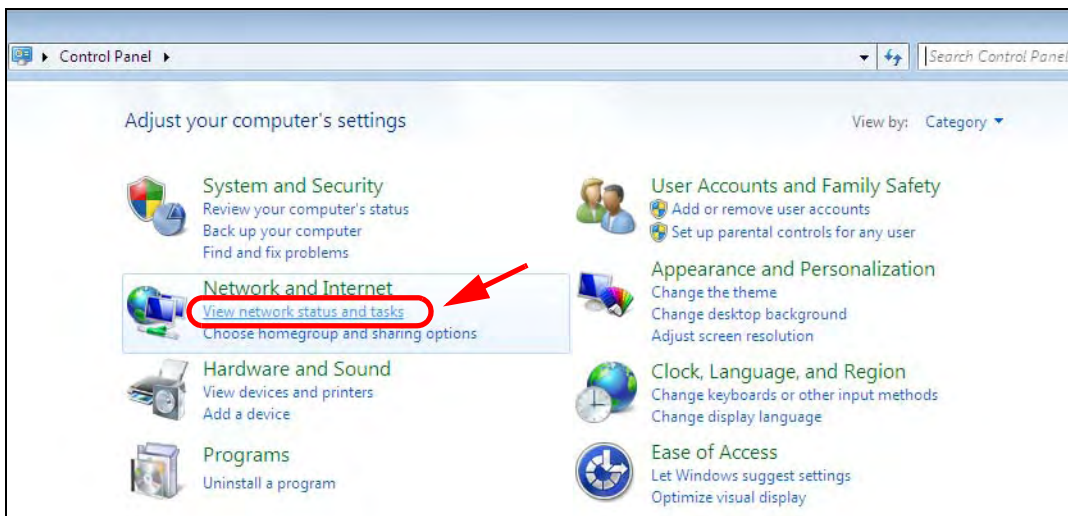
Windows 7

This section shows screens from Windows 7 Enterprise.

- 1 Click **Start > Control Panel**.



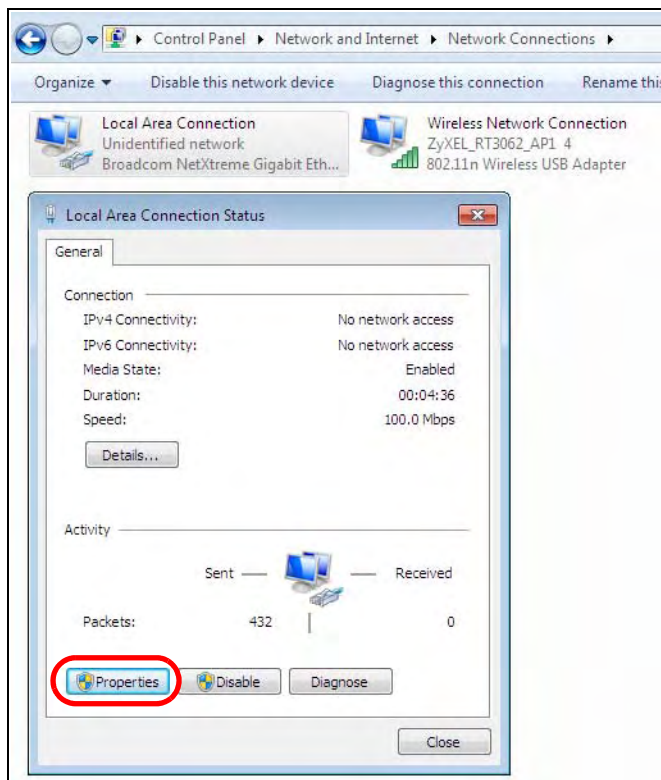
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



- 3 Click **Change adapter settings**.

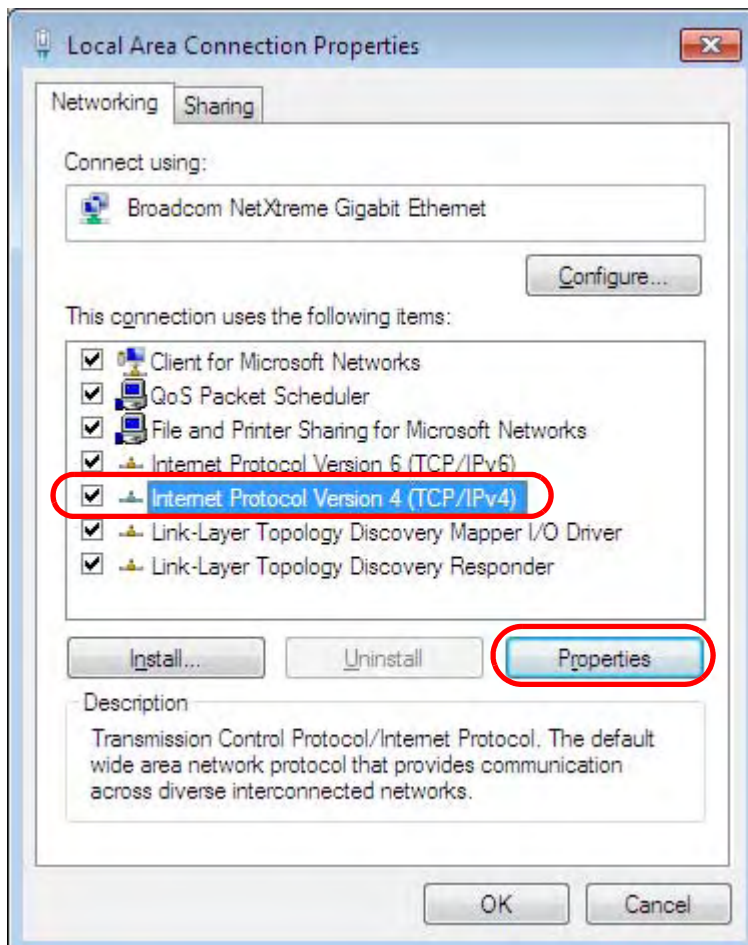


- 4 Double click **Local Area Connection** and then select **Properties**.

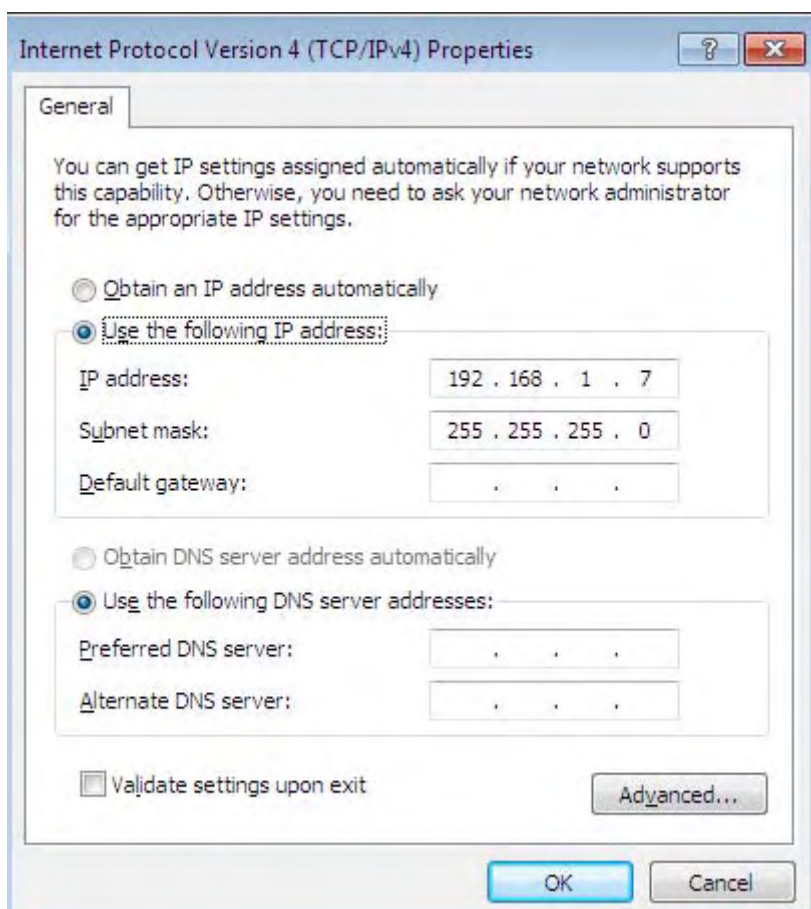


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



- 6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.



- 7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

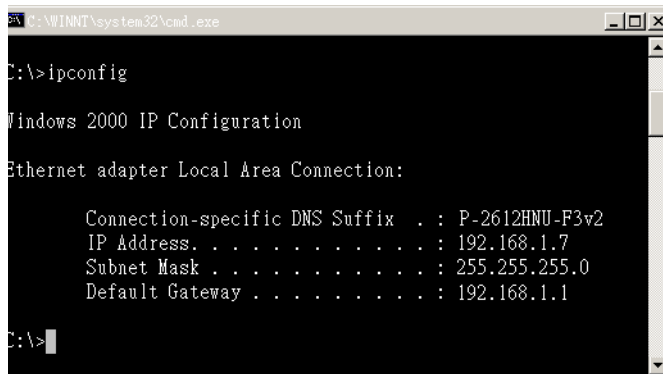
Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server**, if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

- 3 The IP settings are displayed as follows.



```
C:\WINNT\system32\cmd.exe

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

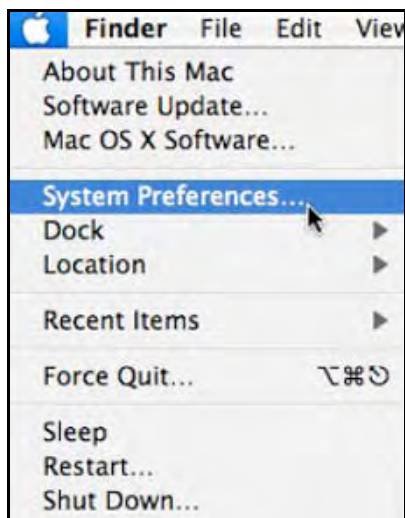
    Connection-specific DNS Suffix  . : P-2612HNU-F3v2
    IP Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>
```

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

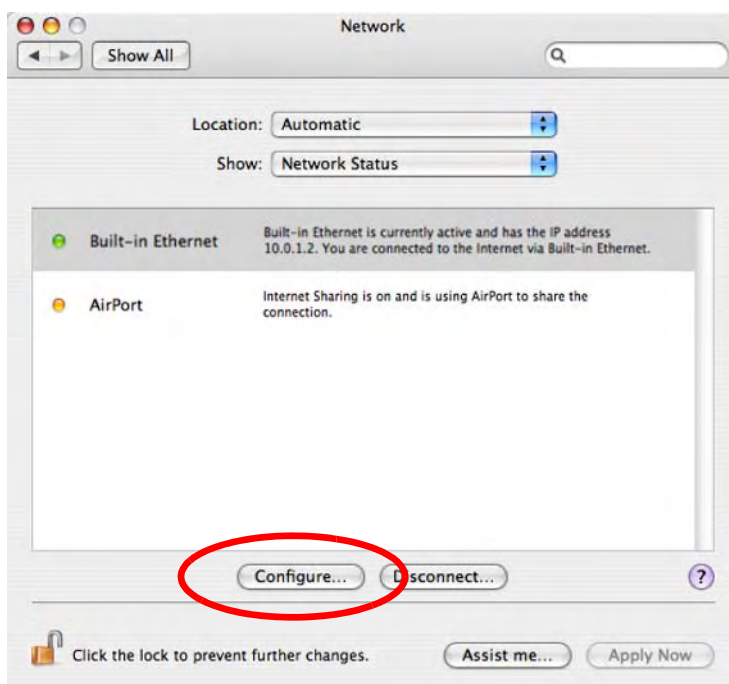
- 1 Click **Apple > System Preferences**.



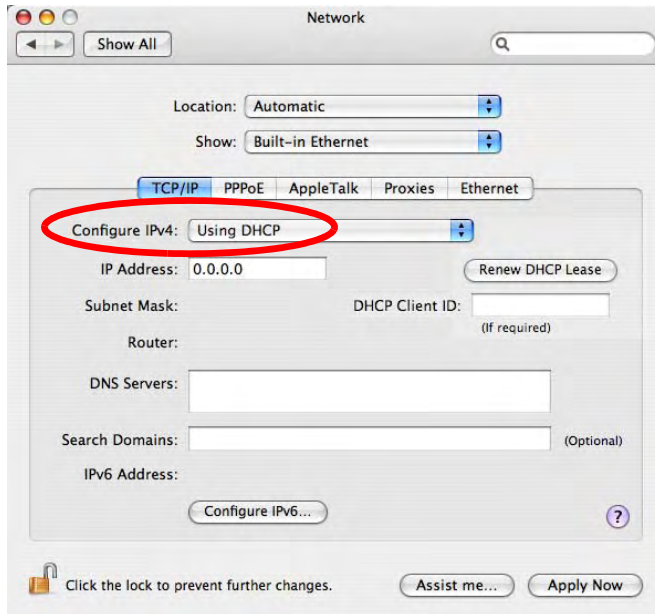
- 2 In the **System Preferences** window, click the **Network** icon.



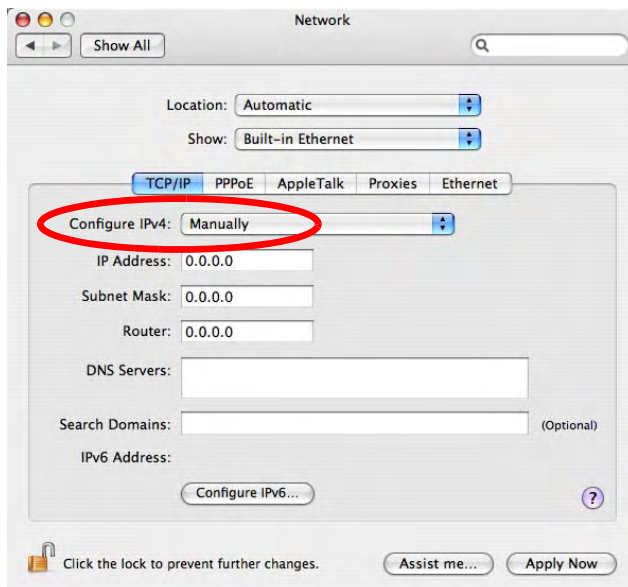
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.



- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



- 5 For statically assigned settings, do the following:
- From the **Configure IPv4** list, select **Manually**.
 - In the **IP Address** field, type your IP address.
 - In the **Subnet Mask** field, type your subnet mask.
 - In the **Router** field, type the IP address of your device.

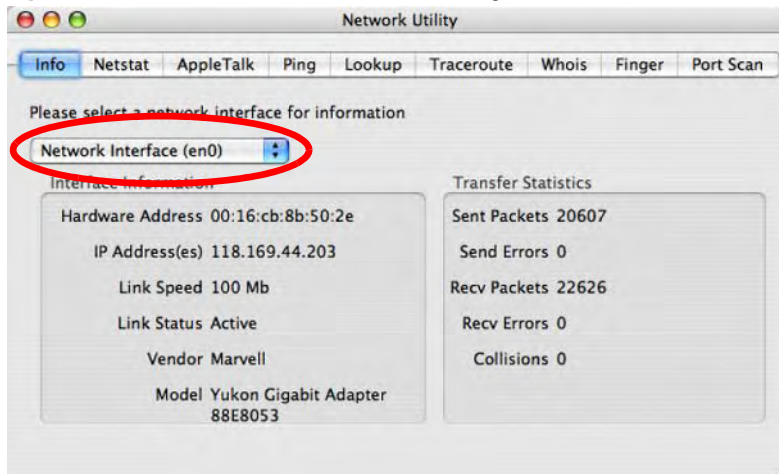


- 6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

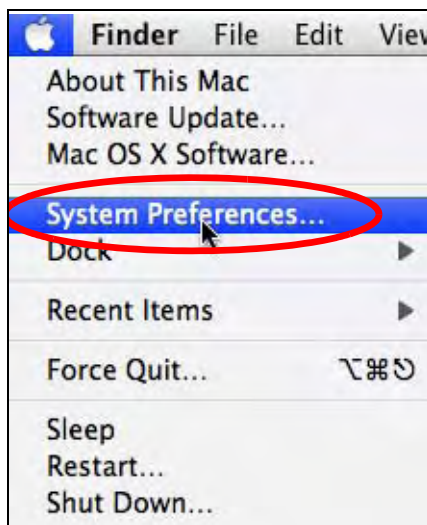
Figure 73 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

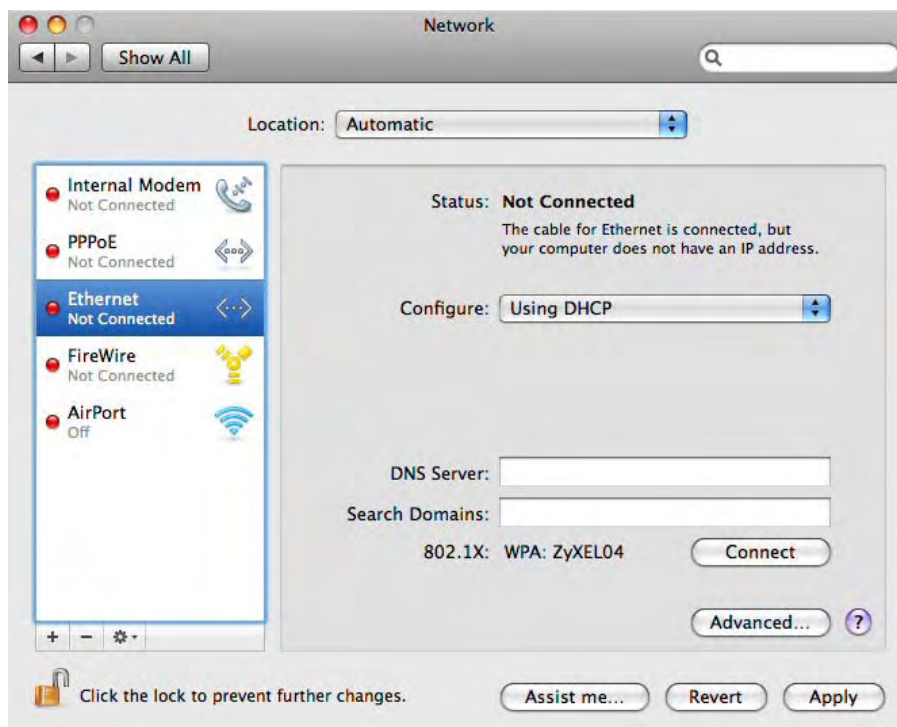
- 1 Click **Apple > System Preferences**.



- 2 In **System Preferences**, click the **Network** icon.

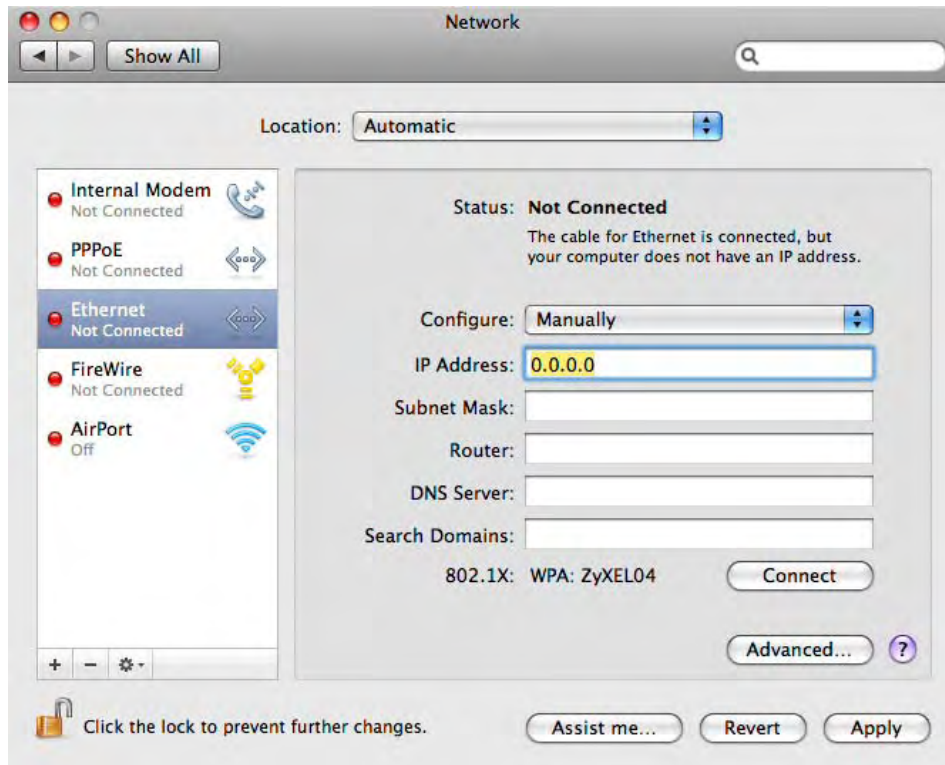


- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



- 4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.
- 5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your NWA1121-NI.

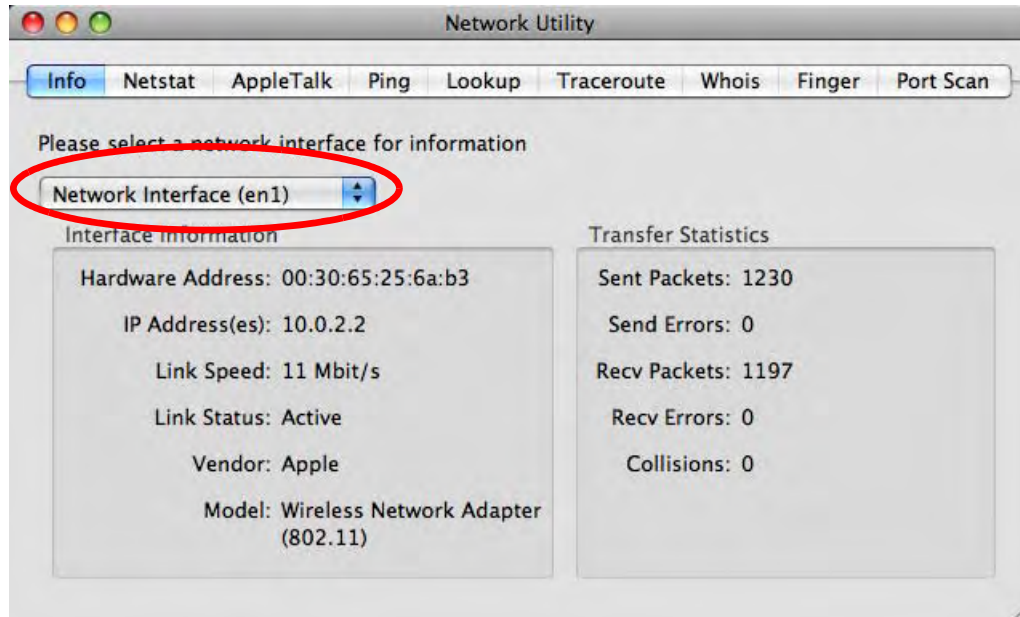


- 6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 74 Mac OS X 10.5: Network Utility



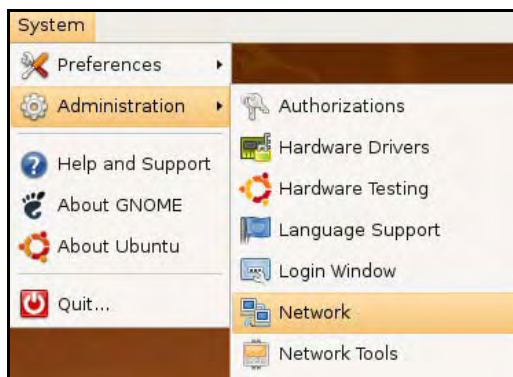
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

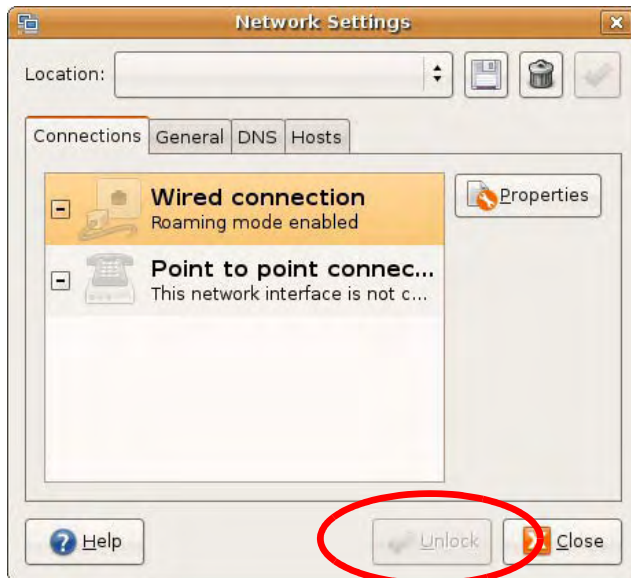
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

- 1 Click **System > Administration > Network**.



- When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



- In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.



- 4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.



- 5 The **Properties** dialog box opens.



- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
 - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

- 7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

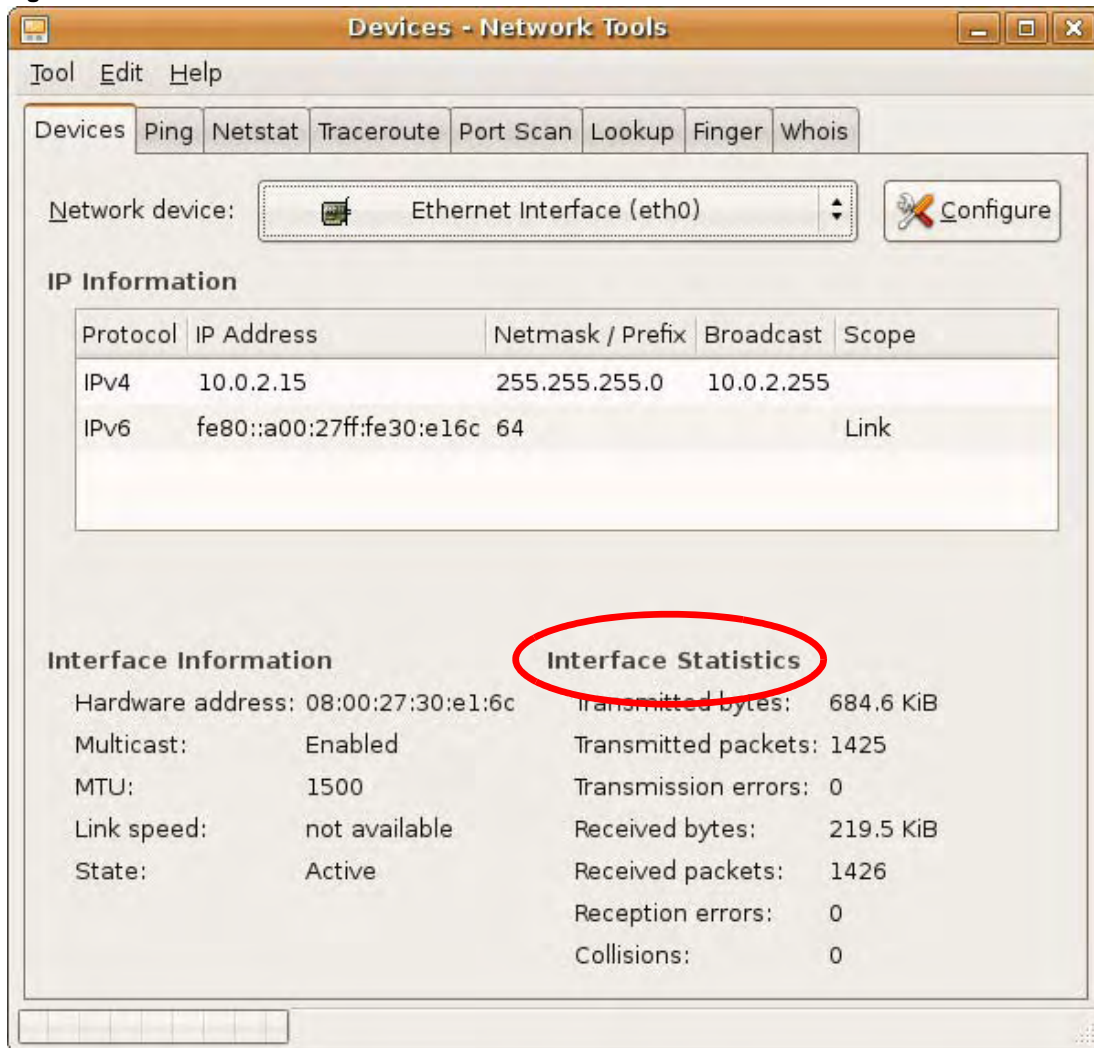


- 8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 75 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

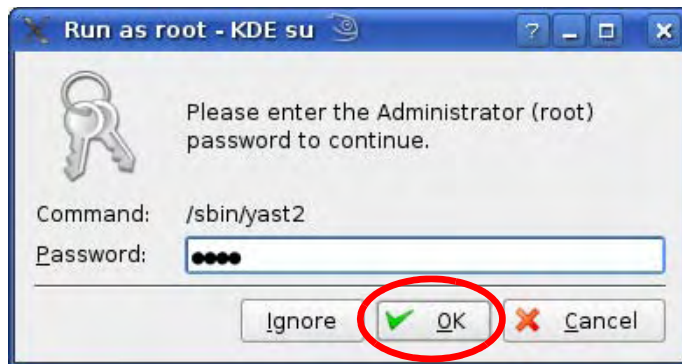
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

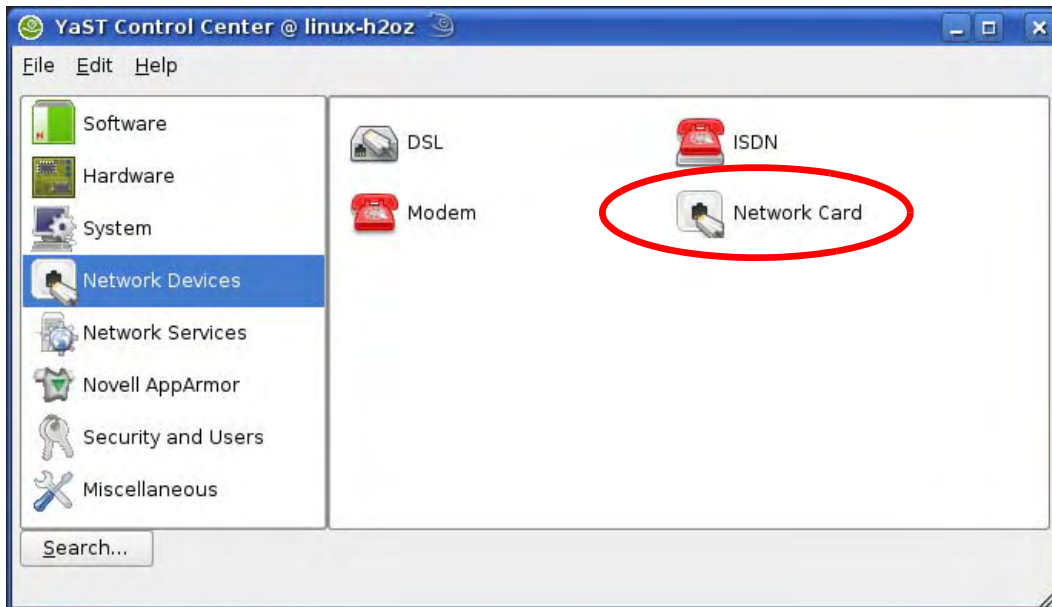
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.



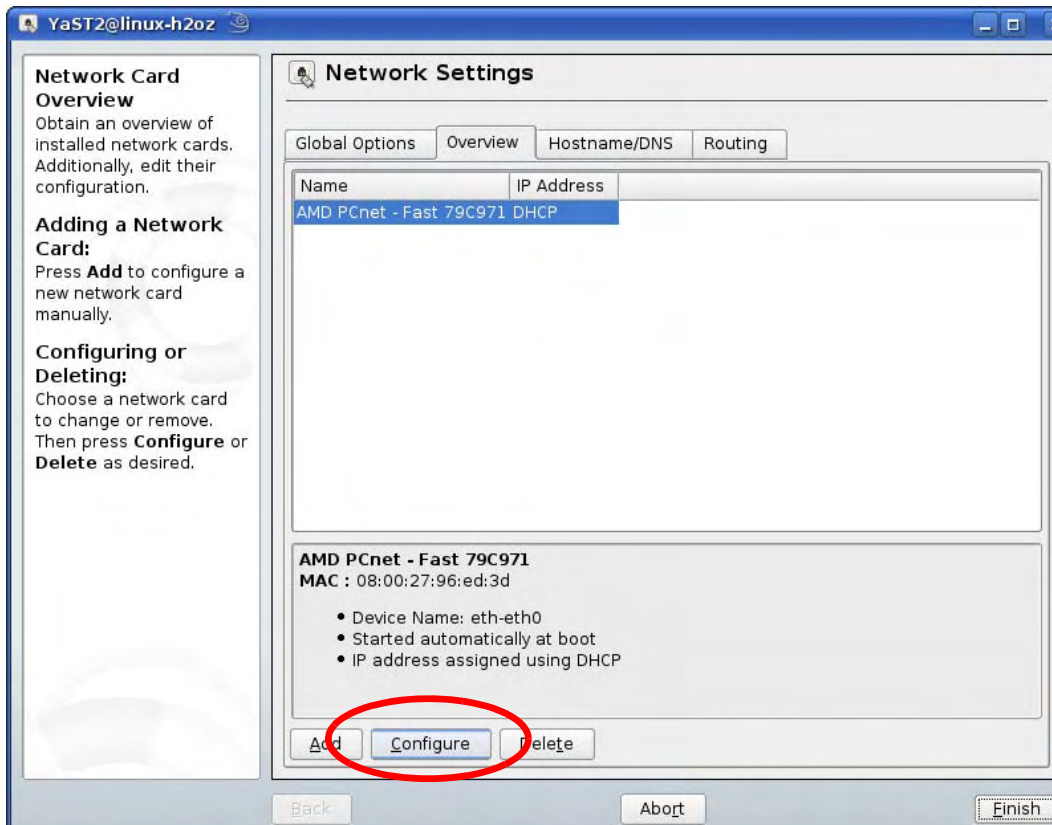
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.



- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

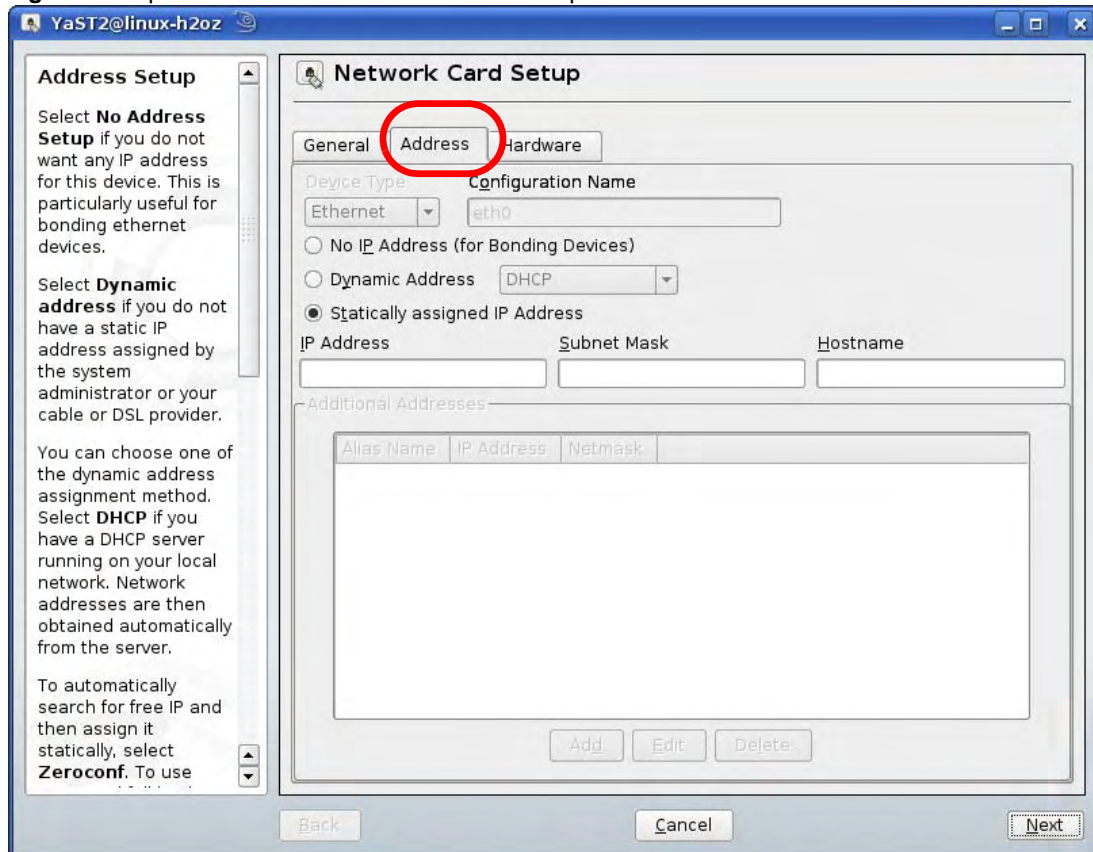


- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



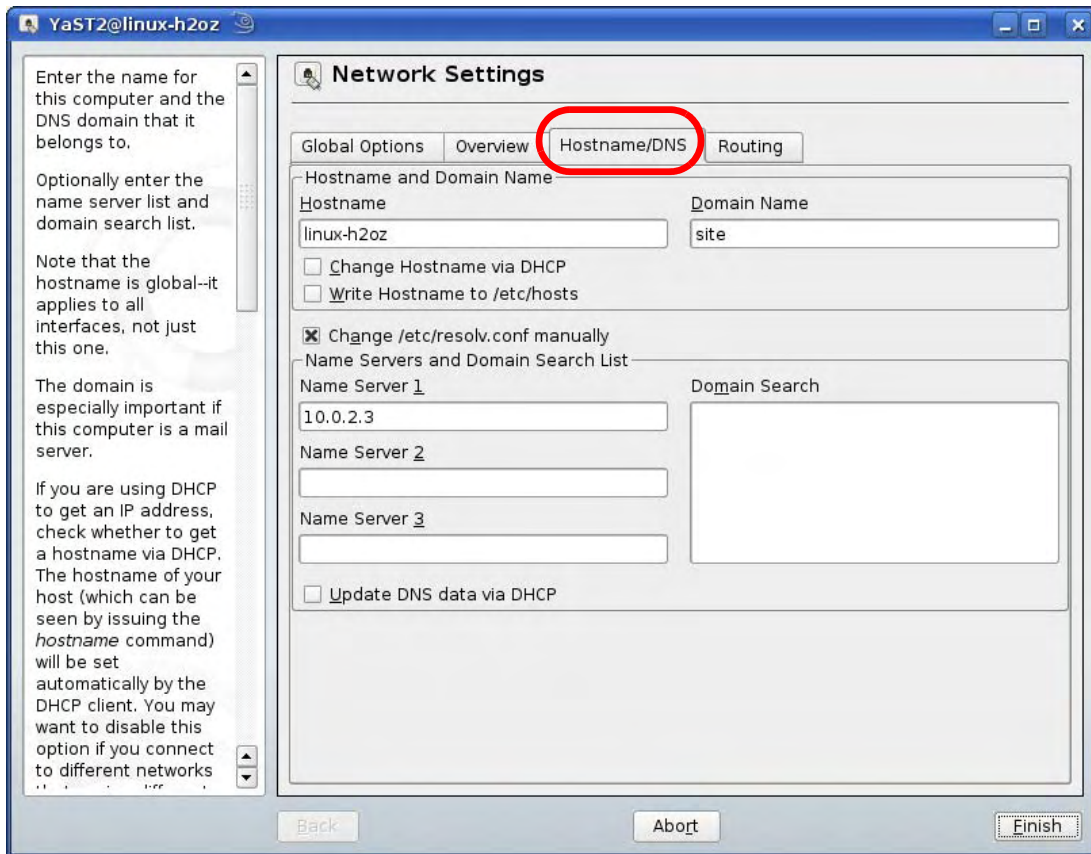
- 5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 76 openSUSE 10.3: Network Card Setup



- 6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.
Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.

- 8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

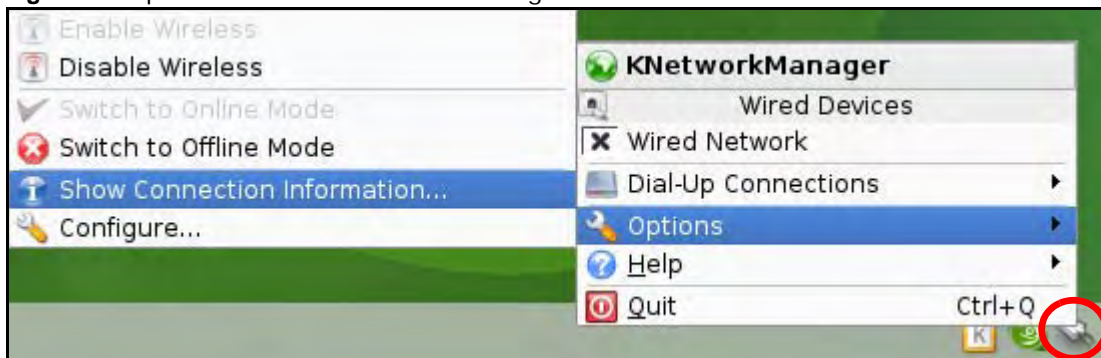


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

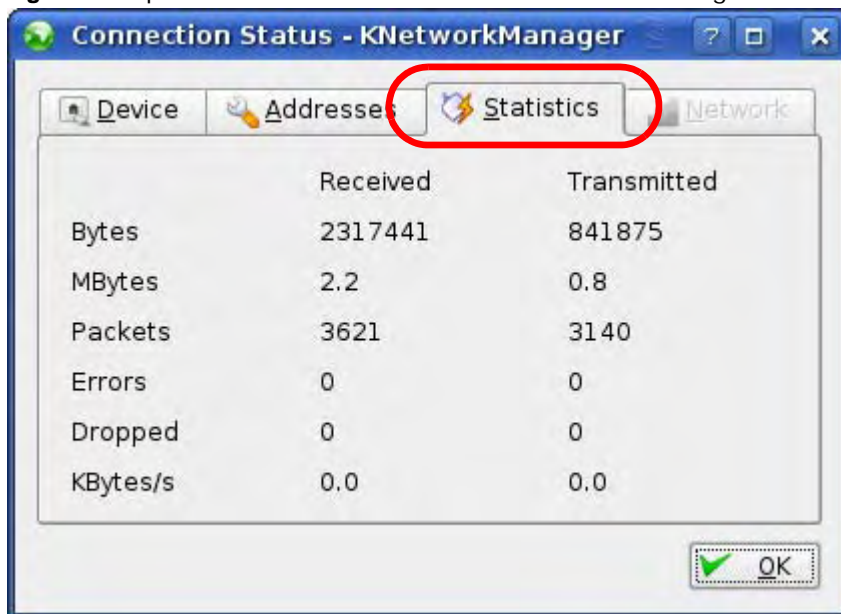
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 77 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics** tab to see if your connection is working properly.

Figure 78 openSUSE: Connection Status - KNetwork Manager



Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

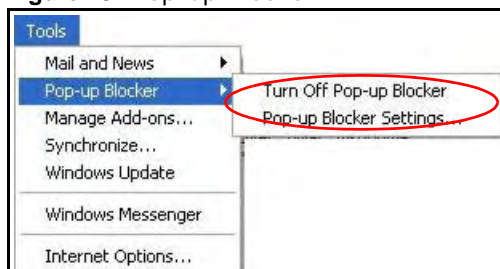
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 79 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.

- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 80 Internet Options: Privacy



- 3 Click **Apply** to save this setting.

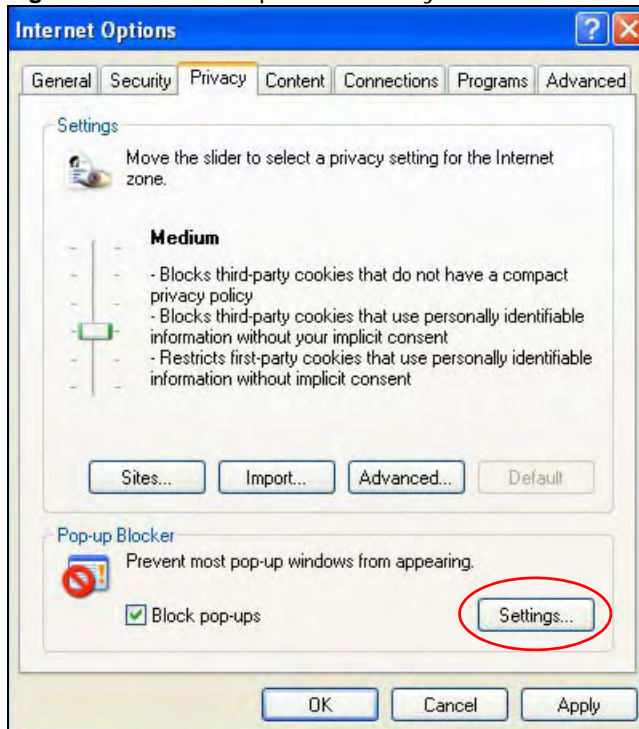
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

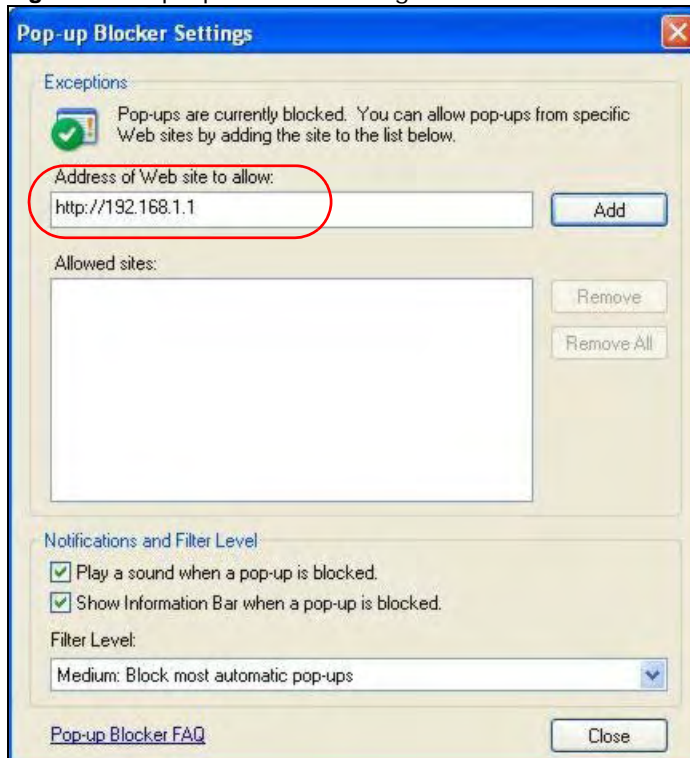
Figure 81 Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

- Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 82 Pop-up Blocker Settings



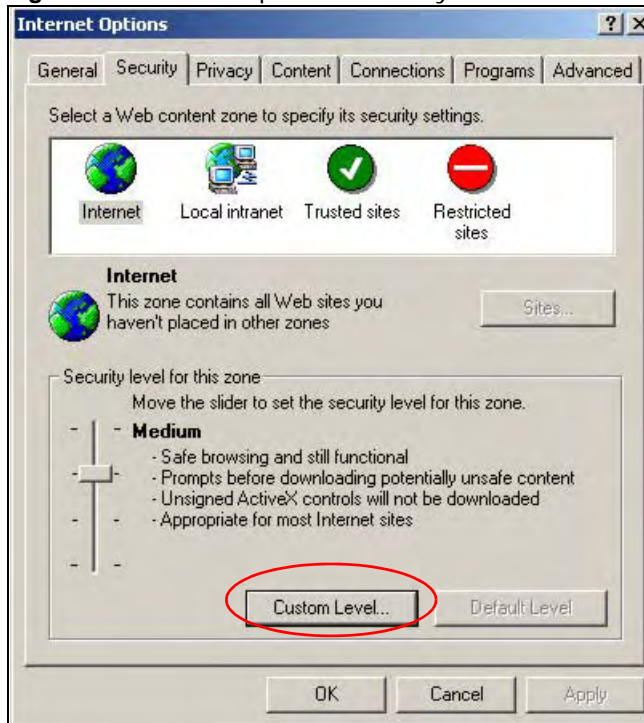
- Click **Close** to return to the **Privacy** screen.
- Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

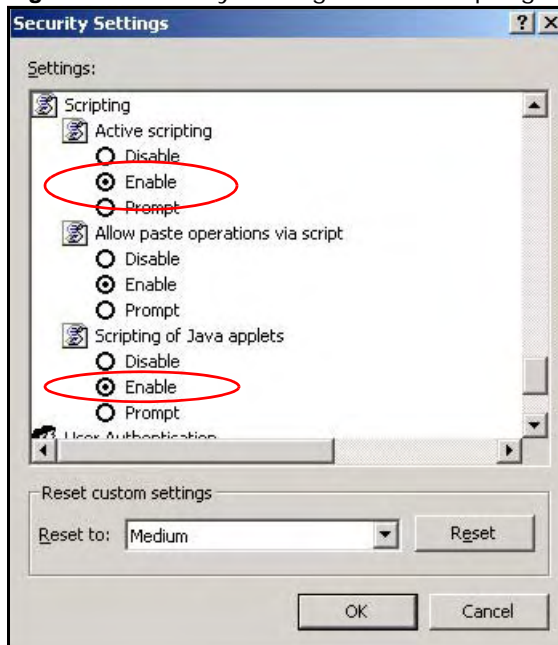
Figure 83 Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

Figure 84 Security Settings - Java Scripting

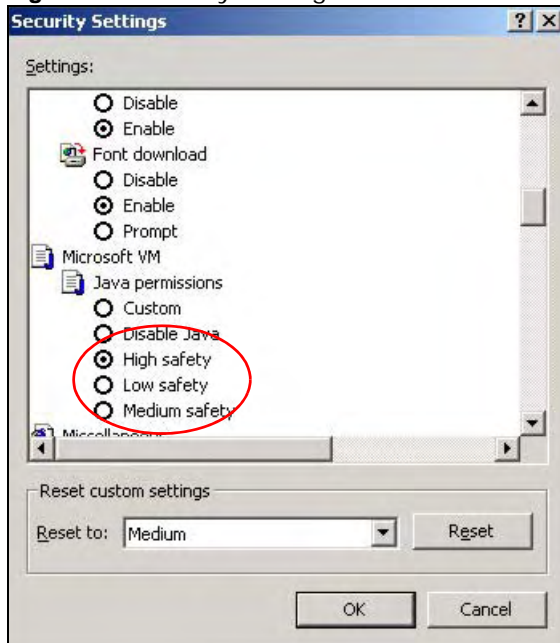


Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

Figure 85 Security Settings - Java

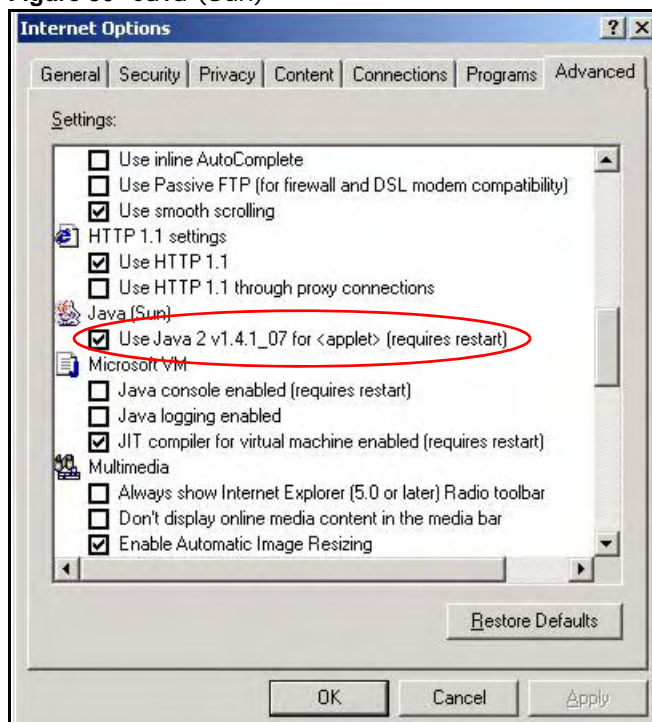


JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

- 3 Click **OK** to close the window.

Figure 86 Java (Sun)

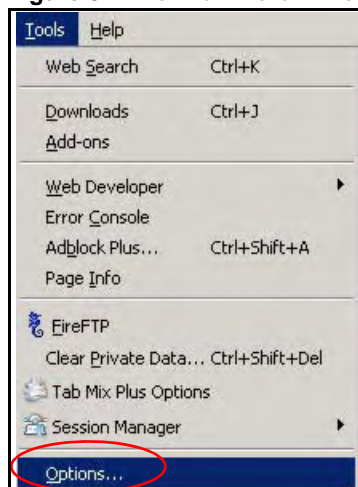


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

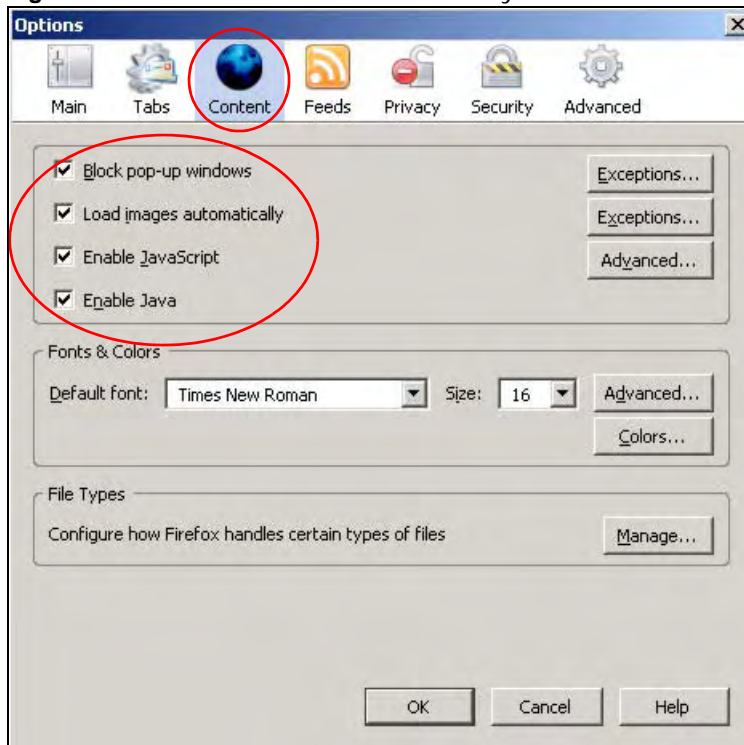
You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 87 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 88 Mozilla Firefox Content Security



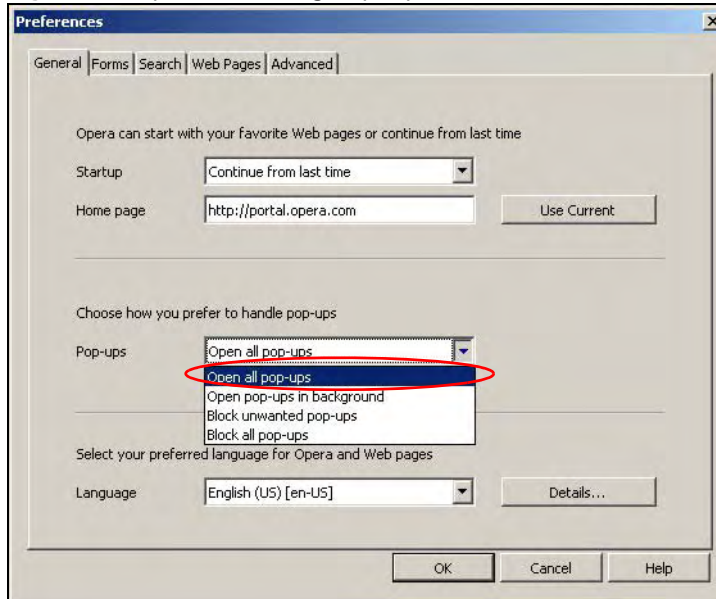
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

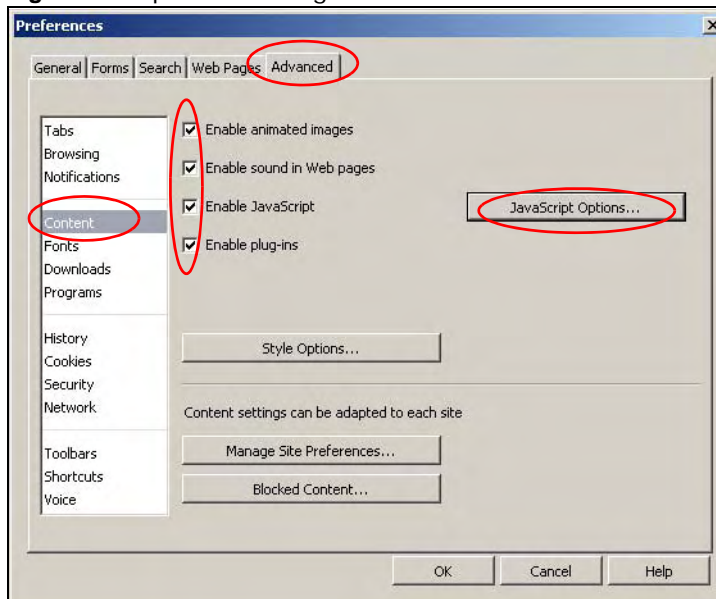
Figure 89 Opera: Allowing Pop-Ups



Enabling Java

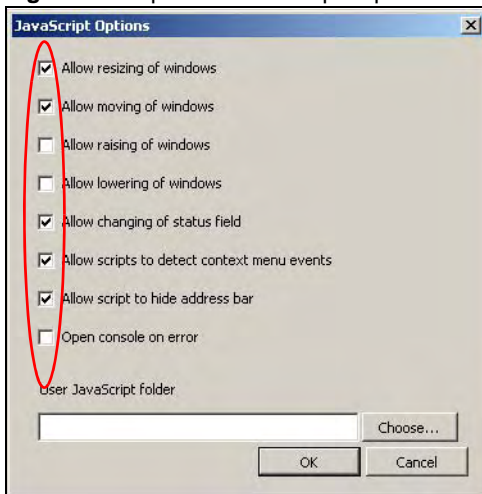
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 90 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 91 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

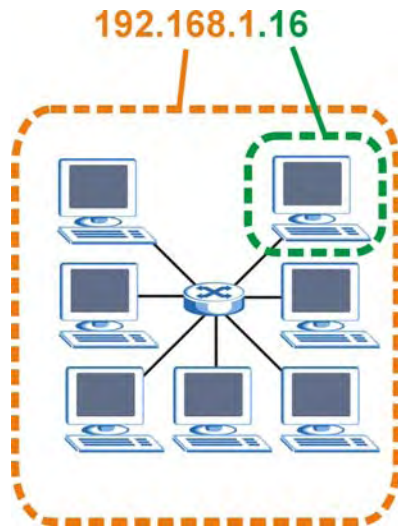
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 92 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 42 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 43 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 44 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 45 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

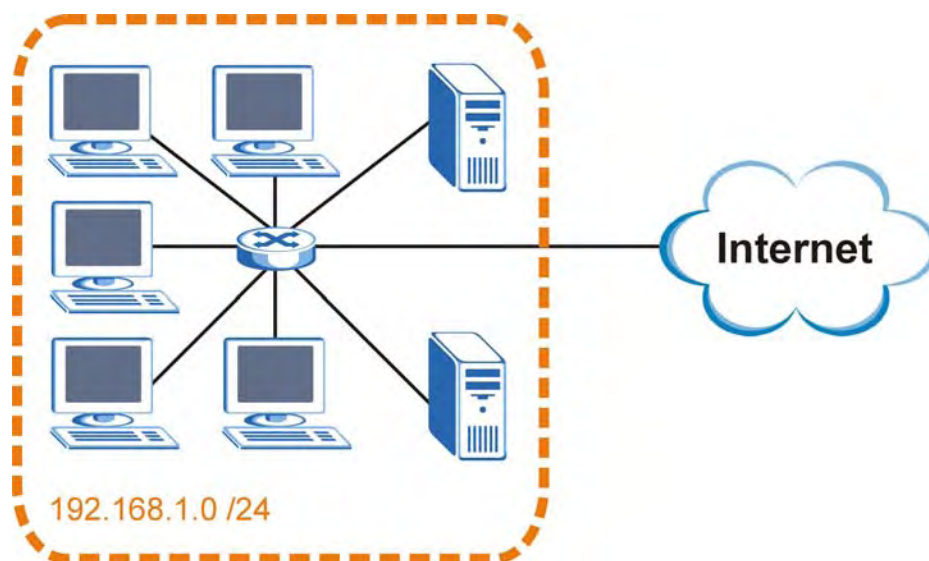
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 93 Subnetting Example: Before Subnetting

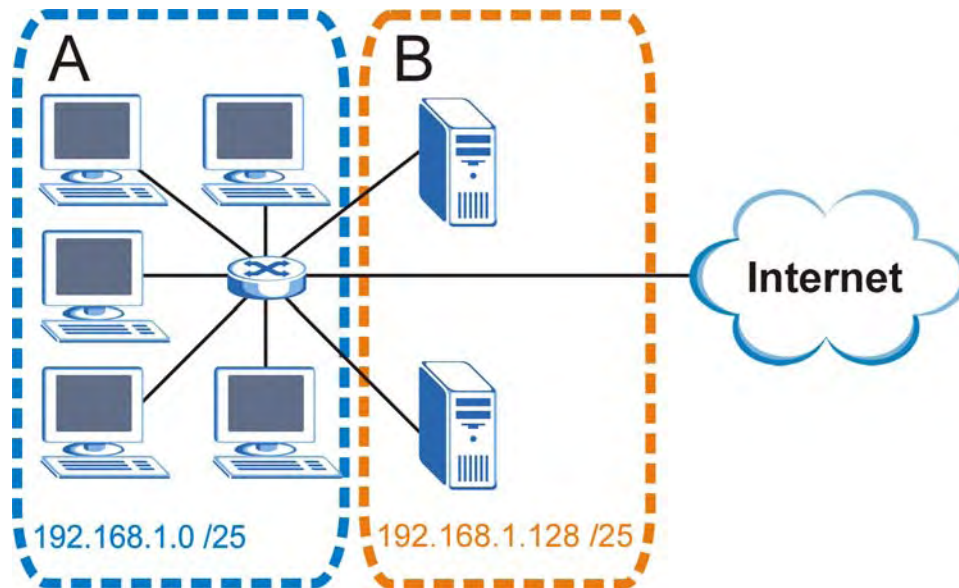


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 94 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 46 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000

Table 46 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 47 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 48 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 49 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 50 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 51 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 52 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14

Table 52 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

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. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. 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. You must also enable Network Address Translation (NAT) on the NWA1121-NI.

Once you have decided on the network number, pick an IP address for your NWA1121-NI that is easy to remember (for instance, 192.168.1.1) 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 NWA1121-NI 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 NWA1121-NI unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) 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:

- 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 it can be assigned from 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.

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*.

Wireless LANs

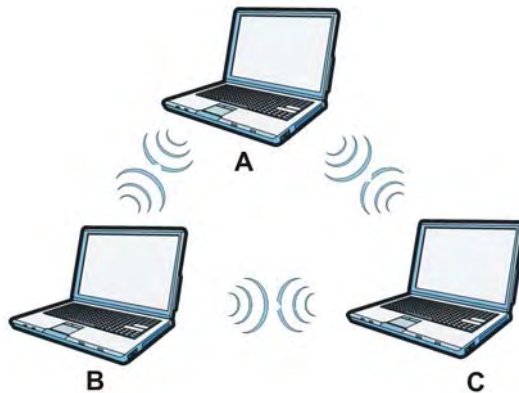
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 95 Peer-to-Peer Communication in an Ad-hoc Network



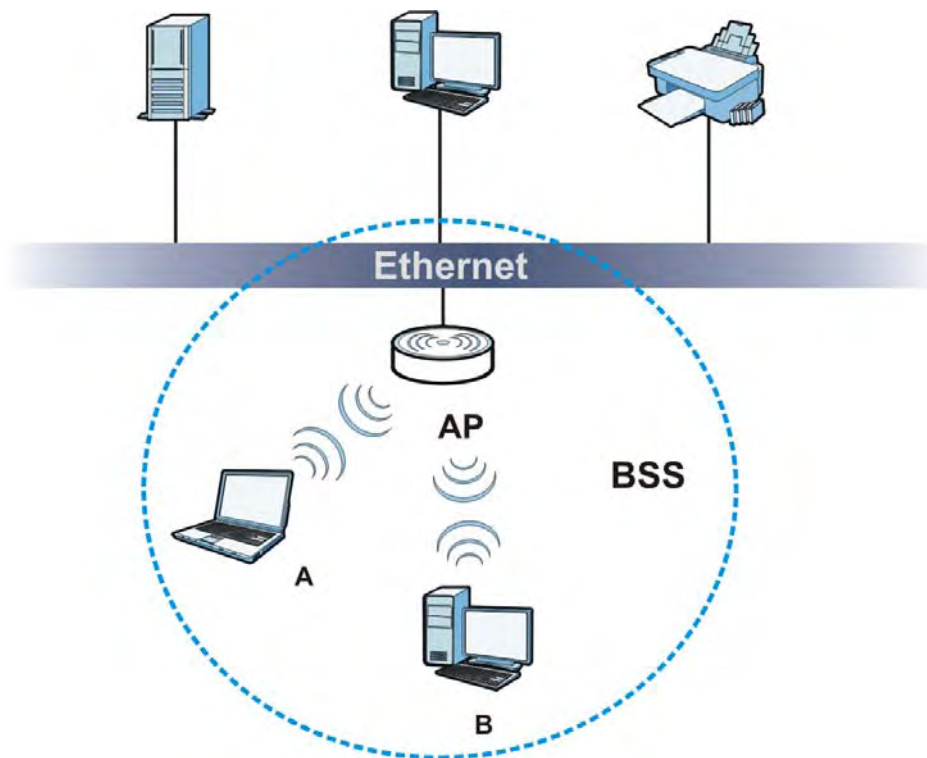
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is

disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 96 Basic Service Set



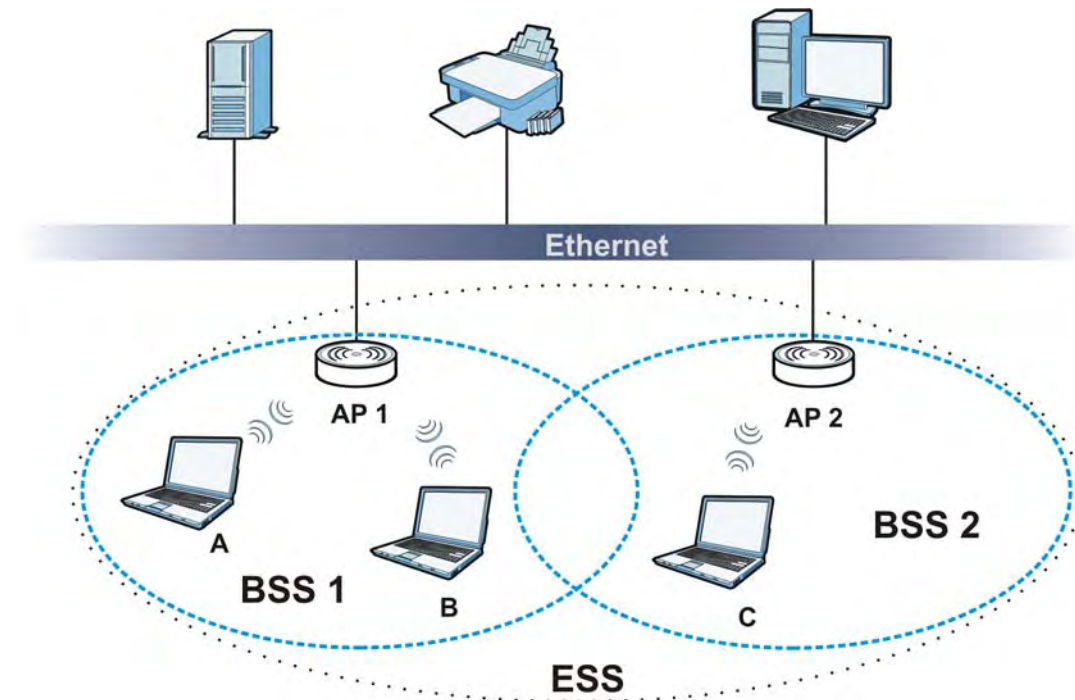
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 97 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

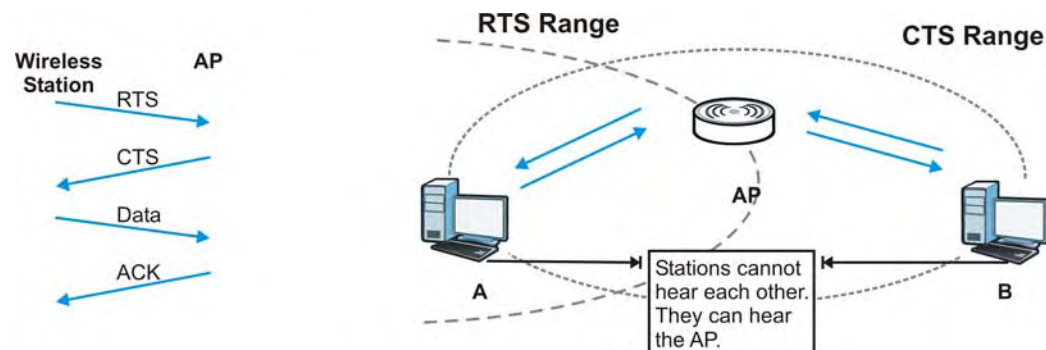
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they

cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 98 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NWA1121-NI uses long preamble.

Note: The wireless devices **MUST** use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. 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:

Table 53 IEEE 802.11g

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

Wireless Security Overview

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

Wireless security methods available on the NWA1121-NI are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NWA1121-NI identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NWA1121-NI.

Table 54 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
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the NWA1121-NI and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**
Sent by an access point requesting authentication.
- **Access-Reject**
Sent by a RADIUS server rejecting access.
- **Access-Accept**
Sent by a RADIUS server allowing access.
- **Access-Challenge**
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**
Sent by the access point requesting accounting.
- **Accounting-Response**
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 55 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm

called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

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 PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevents all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go through the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

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.

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.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) 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 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 99 WPA(2) with RADIUS Application Example



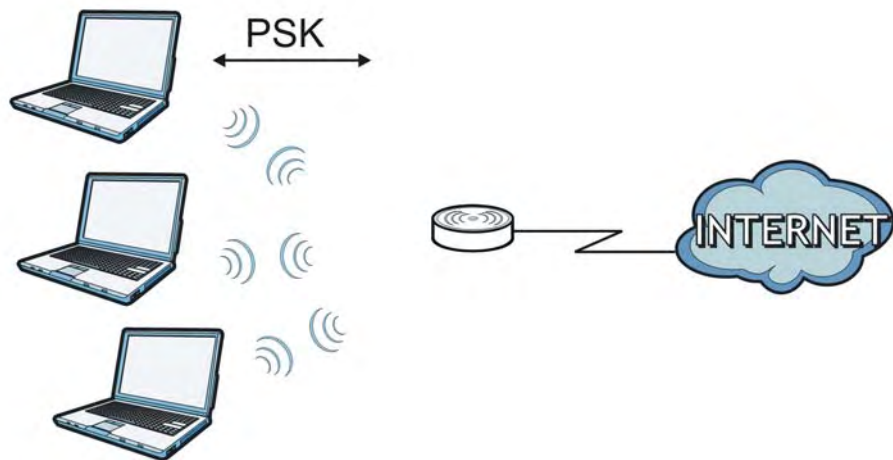
WPA(2)-PSK Application Example

A WPA(2)-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 or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 100 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 56 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz or 5GHz is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the NWA1121-NI is subject to the terms and conditions of any related service providers. Use with products that have NAT, and/or 3G.

Do not use the NWA1121-NI for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws, and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature. Use for products that have a download service.

Make sure all data and programs on the NWA1121-NI are also stored elsewhere. ZyXEL is not responsible for any loss of or damage to any data, programs, or storage media resulting from the use, misuse, or disuse of this or any other ZyXEL product. Use for storage/backup devices.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The 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.

This device 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 residential installation. This device 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. However, there is no guarantee that interference will not occur in a particular installation.

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

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

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.



FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 802.11g or 802.11n (20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n (40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement (For all products)

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- 1) this device may not cause interference and
- 2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IMPORTANT NOTE

Device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems; users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

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

This device is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

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.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erkläre ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΖΥΧΕΛ ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrustings in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.

[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/EC.



National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Ausnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "Overview of Regulatory Requirements for Wireless LANs":

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP) ¹ (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check <http://www.arcep.fr/> for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez <http://www.arcep.fr/> pour de plus amples détails.

R&TTE 1999/5/EC		
WLAN 2.4 – 2.4835 GHz		
IEEE 802.11 b/g/n		
Location	Frequency Range(GHz)	Power (EIRP)
Indoor (No restrictions)	2.4 – 2.4835	100mW (20dBm)
Outdoor	2.4 – 2.454	100mW (20dBm)
	2.454 – 2.4835	10mW (10dBm)

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check <http://www.sviluppoeconomico.gov.it/> for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <http://www.sviluppoeconomico.gov.it/> per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <http://www.esd.lv> for more details.

2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <http://www.esd.lv>.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Index

Numbers

802.1x-Only [58](#)
 802.1x-Static128 [58](#)
 802.1x-Static64 [58](#)

A

access privileges [12](#)
 Accounting Server [88](#)
 Advanced Encryption Standard
 See AES.
 AES [189](#)
 Alerts [116](#)
 Alternative subnet mask notation [176](#)
 Antenna [92](#)
 antenna
 directional [193](#)
 gain [193](#)
 omni-directional [193](#)
 AP (access point) [183](#)
 Applications
 Access Point [14](#)
 AP + Bridge [14](#)
 applications
 MBSSID [12](#)
 Repeater [14](#)
 ATC [73](#)
 ATC+WMM [73](#)

B

Basic Service Set [56](#)
 see BSS
 Basic Service Set, See BSS [181](#)
 beacon [56](#)
 Beacon Interval [63, 65, 70](#)

BSS [12, 56, 181](#)

C

CA [188](#)
 Certificate
 authentication [104](#)
 file format [104](#)
 Certificate Authority
 See CA.
 Certificates
 Fingerprint [113](#)
 MD5 [113](#)
 public key [104](#)
 SHA1 [113](#)
 Certification Authority [113](#)
 certifications [195](#)
 notices [197](#)
 viewing [198](#)
 Channel [56](#)
 channel [183](#)
 interference [183](#)
 command interface [15](#)
 Controlling network access, Ways of [11](#)
 copyright [195](#)
 CTS (Clear to Send) [184](#)

D

disclaimer [195](#)
 Distribution System [56](#)
 DNS [97, 119](#)
 Domain Name Server (DNS) [119](#)
 DS [56](#)
 DTIM Interval [63, 65, 70](#)
 dynamic WEP key exchange [188](#)

E

EAP [59](#)
EAP Authentication [187](#)
Encryption [59, 76, 80, 83, 85](#)
encryption [14, 189](#)
ESS [56, 182](#)
Ethernet device [89](#)
Extended Service Set [56](#)
Extended Service Set, See ESS [182](#)
Extensible Authentication Protocol [59](#)

F

Factory Defaults [126](#)
 restoring [21](#)
FCC interference statement [195](#)
Firmware [120](#)
Fragmentation [63, 66, 68, 71](#)
Fragmentation threshold [91](#)
fragmentation threshold [184](#)
FTP [103](#)
 restrictions [103](#)

G

Generic Token Card [59](#)
GTC [59](#)

H

hidden node [183](#)

I

IANA [180](#)
IBSS [181](#)
IEEE 802.11g [185](#)
IEEE 802.1x [57](#)

Import Certificate [106](#)
Independent Basic Service Set
 See IBSS [181](#)
initialization vector (IV) [190](#)
Internet Assigned Numbers Authority
 See IANA
Internet Protocol version 6, see IPv6
Internet telephony [12](#)
IP Address [94](#)
 Gateway IP address [94](#)
IP Screen [94](#)
 DHCP [96](#)
IPv6 [95](#)
 addressing [95](#)
 global address [95](#)
 link-local address [95](#)
 Neighbor Discovery Protocol [95](#)
 ping [95](#)
 prefix [95](#)
 prefix length [95](#)

K

key [59, 77, 81, 83](#)

L

LEAP [59](#)
LEDs [17, 129](#)
 Blinking [17](#)
 Flashing [17](#)
 Off [17](#)
Lightweight Extensible Authentication Protocol [59](#)
Log [49](#)
Log Screens [115](#)
Logs
 accessing logs [115](#)
 receiving logs via e-mail [116](#)
Logs Screen
 Mail Server [117](#)
 Mail Subject [117](#)
 Send Log to [117](#)
 Syslog [118](#)
Logs, Uses of [115](#)

M

- MAC Filter
 - Allow Association [89](#)
 - Deny Association [89](#)
- Maintenance [119](#)
 - Association List [120](#)
 - Backup [124](#)
 - Restore [125](#)
- Management Information Base (MIB) [111](#)
- managing the device
 - using Telnet. See command interface.
 - using the command interface. See command interface.
- MBSSID [12](#)
- Media Access Control [89](#)
- Message Integrity Check (MIC) [189](#)
- message relay [60](#)
- Microsoft Challenge Handshake Authentication Protocol Version 2 [59](#)
- MSCHAPv2 [59](#)
- MSDU [63, 66, 71](#)

N

- NAT [180](#)
- Network Time Protocol (NTP) [119](#)
- NTP [119](#)

O

- Operating Mode [56](#)
- Output Power Management [63, 65, 68, 70](#)

P

- Pairwise Master Key (PMK) [190, 191](#)
- Passphrase [59](#)
- Password [130](#)
- PEAP [59](#)
- Personal Information Exchange Syntax Standard [104](#)

- PFX PKCS#12 [104](#)
- Preamble [91](#)
- preamble mode [185](#)
- Preamble Type [63, 66, 68, 71](#)
- Pre-Shared Key [59](#)
- priorities [92](#)
- product registration [198](#)
- Protected Extensible Authentication Protocol [59](#)
- PSK [59, 190](#)

Q

- QoS [73](#)

R

- Radio Frequency [92](#)
- RADIUS [59, 186](#)
 - Accounting [60](#)
 - Authentication [60](#)
 - Authorization [60](#)
 - message types [187](#)
 - messages [187](#)
 - shared secret key [187](#)
- RADIUS Screen
 - Accounting Server [88](#)
 - Accounting Server IP Address [88](#)
- RADIUS server [58](#)
 - Backup [88](#)
 - Primary [88](#)
- Rates Configuration [63, 66, 68, 71](#)
- registration
 - product [198](#)
- Remote Authentication Dial In User Service [59](#)
- remote management [16](#)
- remote management limitations [102](#)
- Roaming [92](#)
- RootAP [14](#)
- RTS (Request To Send) [184](#)
 - threshold [183, 184](#)
- RTS/CTS Threshold [63, 66, 68, 71, 91](#)

S

Security Mode, Choosing the [93](#)

Security Modes

- 802.1x-Static64 [58](#)
- IEEE 802.1x-Only [58](#)
- IEEE 802.1x-Static128 [58](#)
- IEEE 802.1x-Static64 [58](#)
- None [58](#)
- WEP [58](#)
- WPA [58](#)
- WPA2 [58](#)
- WPA2-MIX [58](#)
- WPA2-PSK [58](#)

Service Set Identifier [56](#)

Service Set Identifier

- see SSID

Simple Mail Transfer Protocol [116](#)

SMTP [116, 118](#)

SNMP

- MIBs [111](#)
- traps [112](#)

Spanning Tree Protocol [91](#)

SSID [12, 56](#)

SSID profile

- pre-configured [12](#)

SSID profiles [12](#)

Status Screens [25](#)

- 802.11 Mode [50](#)
- Channel ID [50](#)
- Ethernet [25](#)
- FCS Error Count [50](#)
- Firmware Version [26](#)
- Interface Status [27](#)
- Poll Interval [50](#)
- Retry Count [50](#)
- Statistics [51](#)
- system statistics [25](#)
- WLAN [25](#)

Subnet [173](#)

Subnet Mask [94, 174](#)

subnetting [176](#)

Syslog Logging [116](#)

System Screens

- General [120](#)
- Password [121](#)
- Time

Time and Date Setup [122](#)

Time Zone [122](#)

system timeout [104](#)

T

telnet [106](#)

Temporal Key Integrity Protocol [59](#)

Temporal Key Integrity Protocol (TKIP) [189](#)

TFTP restrictions [103](#)

Thumbprint Algorithm [114](#)

timeout [16](#)

TKIP [59](#)

TLS [59](#)

trademarks [195](#)

Transport Layer Security [59](#)

Troubleshooting [129](#)

- connection is slow or intermittent [132](#)
- DHCP [130](#)
- factory defaults [131](#)
- firmware [131](#)
- Internet [131](#)
- LAN/ETHERNET port [131](#)
- QoS [132](#)
- Web Configurator [130](#)

TTLS [59](#)

Tunneled Transport Layer Security [59](#)

Tutorial [29](#)

U

User Authentication [58](#)

V

Virtual Local Area Network [98](#)

VLAN [98](#)

- introduction [98](#)

VoIP [12, 73](#)

W

- warranty [198](#)
 - note [198](#)
- WDS [14](#)
- Web Configurator [19](#)
 - password [19](#)
- WEP [58](#)
- WEP key encrypting [93](#)
- Wi-Fi Multimedia QoS [92](#)
- Wi-Fi Protected Access [58, 189](#)
- Wired Equivalent Privacy [58](#)
- Wireless Client [42](#)
- wireless client WPA supplicants [190](#)
- Wireless Distribution System (WDS) [14](#)
- Wireless Mode [57](#)
- Wireless Mode, Choosing the
 - Access Point [29](#)
 - Bridge [29](#)
 - Wireless Client [29](#)
- Wireless Security [16](#)
 - how to improve [16](#)
 - Levels [58](#)
- wireless security [12, 185](#)
- Wireless Security Screen
 - 802.1x Only [77](#)
 - Access Point [77, 80](#)
 - Wireless Client [78, 82](#)
 - 802.1x Static 64-bit, 802.1x Static 128-bit [79](#)
 - WEP [76](#)
 - WPA [83](#)
 - Access Point [84](#)
 - Wireless Client [85](#)
 - WPA-PSK, WPA2-PSK, WPA2-PSK-MIX [86](#)
- Wireless Settings Screen [55](#)
 - Access Point Mode [61](#)
 - Antenna [92](#)
 - AP + Bridge Mode [67](#)
 - Bridge Mode [64](#)
 - BSS [56](#)
 - Channel [56](#)
 - ESS [56](#)
 - Fragmentation Threshold [91](#)
 - Intra-BSS Traffic [91](#)
 - Operating Mode [56](#)
 - Preamble [91](#)
 - Roaming [92](#)
 - RTS/CTS Threshold [91](#)
 - SSID [56](#)
 - Wireless Client Mode [67](#)
 - Wireless Mode [57](#)
 - WMM QoS [91](#)
- WLAN
 - interference [183](#)
 - security parameters [192](#)
- WMM [73](#)
- WMM QoS [91](#)
- WPA [58, 189](#)
 - key caching [190](#)
 - pre-authentication [190](#)
 - user authentication [190](#)
 - vs WPA-PSK [190](#)
 - wireless client supplicant [190](#)
 - with RADIUS application example [191](#)
- WPA2 [58, 189](#)
 - user authentication [190](#)
 - vs WPA2-PSK [190](#)
 - wireless client supplicant [190](#)
 - with RADIUS application example [191](#)
- WPA2-MIX [58](#)
- WPA2-Pre-Shared Key [189](#)
- WPA2-PSK [189, 190](#)
 - application example [191](#)
- WPA2-PSK-MIX [58](#)
- WPA-PSK [189, 190](#)
 - application example [191](#)

Z

- ZyXEL Device
 - Ethernet parameters [94](#)
 - good habits [16](#)
 - Introduction [11](#)
 - managing [15](#)
 - resetting [20, 126](#)
 - Security Features [16](#)

