NWA1000 Series

NWA 1100-NH / 1121-NI / 1123-NI / 1123-AC

WLAN PoE Access Points

Version 2.00
Edition 1, 06/2014

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.2
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

Quick Start Guide. The Quick Start Guide shows how to connect the NWA and access the Web Configurator.

Contents Overview

Table of Contents

PART I

User's Guide

1

Introducing the NWA

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

1.1 Introducing the NWA

This User's Guide covers the following models: NWA1100-NH, NWA1121-NI, NWA1123-NI and NWA1123-AC. Your NWA 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.

Table 1 NWA Series Comparison Table

FEATURES	NWA1100-NH	NWA1121-NI	NWA1123-NI	NWA1123-AC
Supported Wireless Standards	IEEE 802.11b IEEE 802.11g IEEE 802.11n	IEEE 802.11b IEEE 802.11g IEEE 802.11n	IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n	IEEE 802.11a IEEE 802.11ac IEEE 802.11b IEEE 802.11g IEEE 802.11n
Supported Frequency Bands	2.4 GHz	2.4 GHz	2.4 GHz 5 GHz	2.4 GHz 5 GHz
Available Security Modes	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX	None WEP WPA2 WPA2-MIX WPA2-PSK WPA2-PSK-MIX
Number of SSID Profiles	8	8	32	32
Layer-2 Isolation	Yes	Yes	Yes	Yes

The NWA 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, WPA2 and WEP data encryption. Its Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

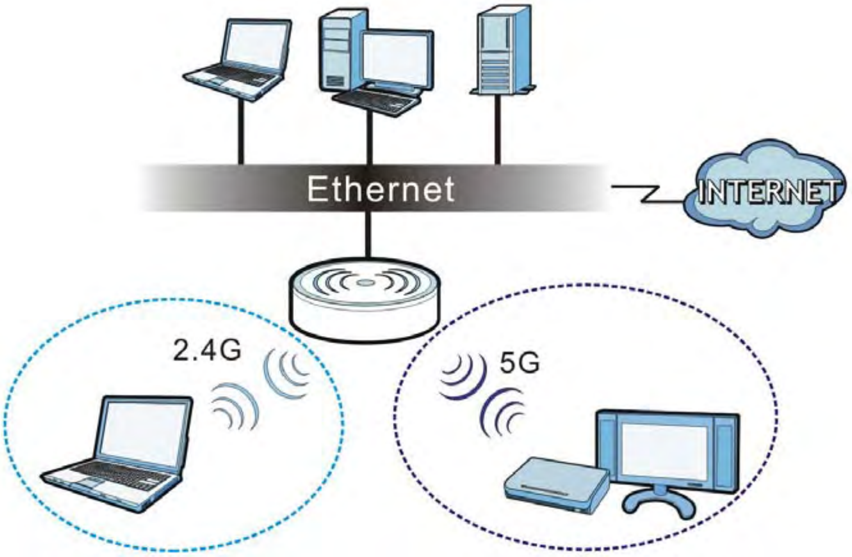
Your NWA is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance.

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

1.1.1 Dual-Band

The NWA1123-NI or NWA1123-AC is a dual-band AP and able to function both 2.4G and 5G networks at the same time. You could use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

Figure 1 Dual-Band Application



1.2 Wireless Modes

The NWA can be configured to use the following WLAN operating modes:

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

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 NWA provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile.

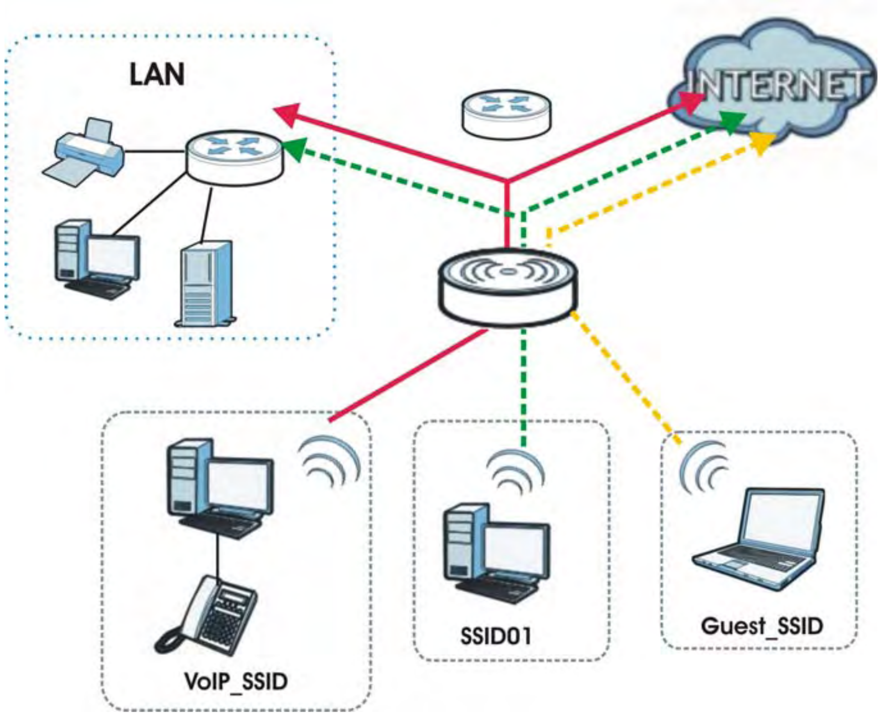
You can configure multiple SSID profiles, and have all of them active at any one time.

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 2 Multiple BSSs



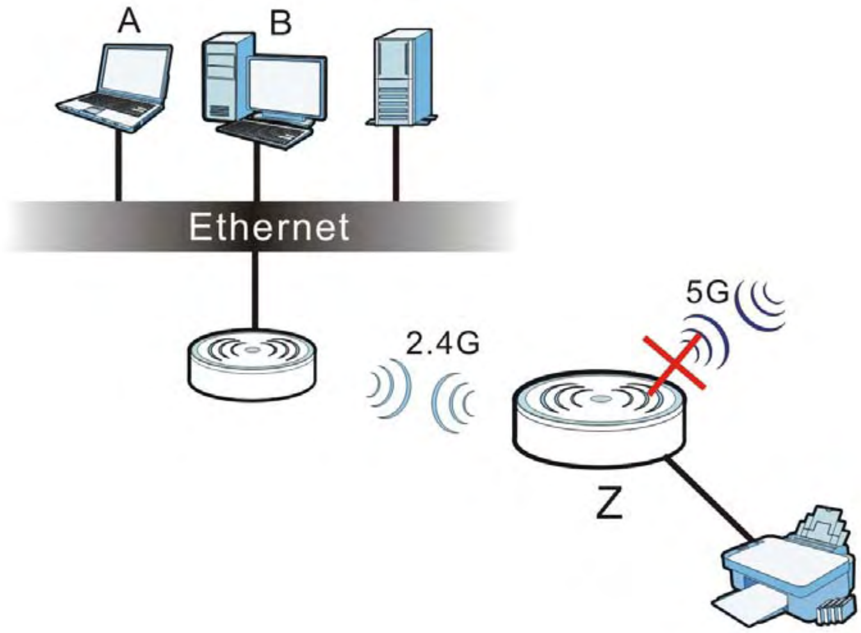
1.2.2 Wireless Client

The NWA can be used as a wireless client to communicate with an existing network.

Note: The NWA1123-NI or NWA1123-AC is a dual-band AP which contains two different types of wireless radios to transmit at 2.4 GHz and 5 GHz bands separately and simultaneously. If one of the NWA1123-NI wireless radio is set to work in client mode, the other radio will be disabled automatically.

In the figure below, the printer can receive requests from the wired computer clients **A** and **B** via the NWA in Client mode (**Z**) using only the 2.4 GHz band.

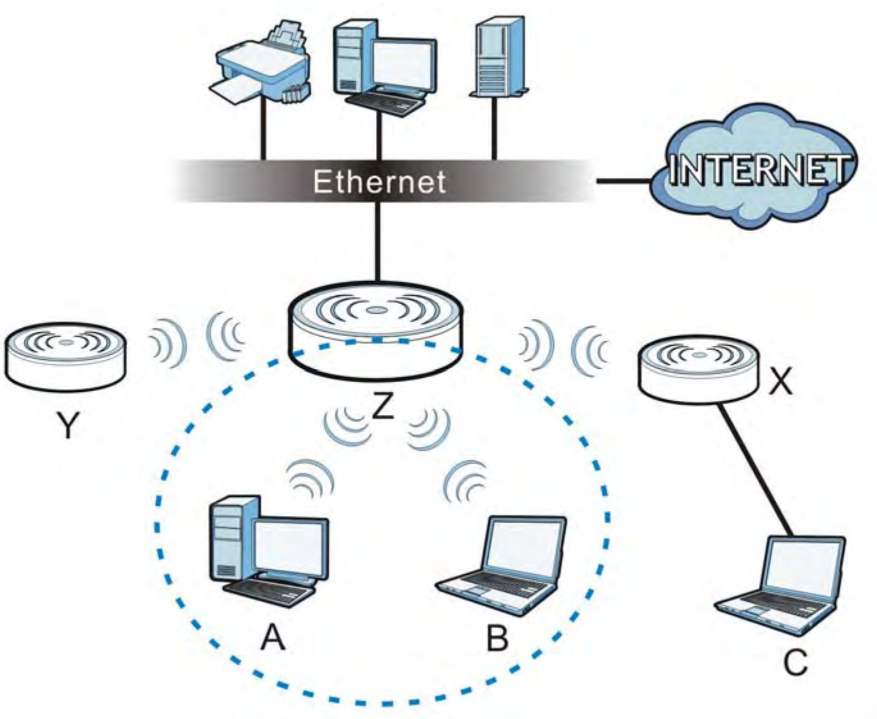
Figure 3 Wireless Client Application



1.2.3 Root AP

In Root AP mode, the NWA (**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 4 Root AP Application



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

When the NWA is in Root AP mode, repeater security between the NWA and other repeater is independent of the security between the wireless clients and the AP or repeater. If you do not enable repeater security, traffic between APs is not encrypted. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 6.6 on page 72 for more details.

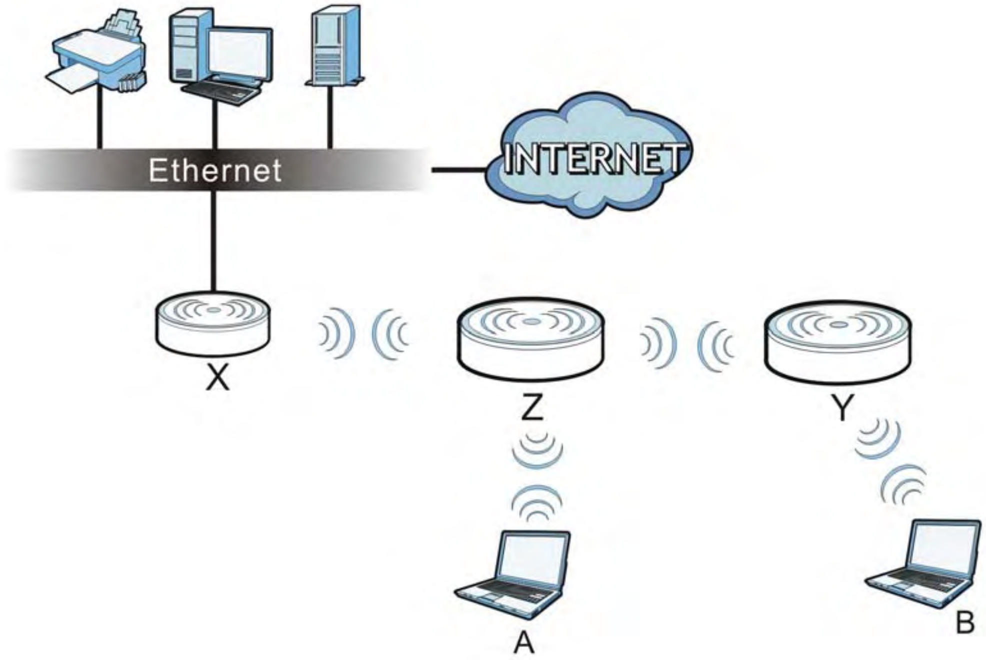
Unless specified, the term “security settings” refers to the traffic between the wireless clients and the AP. At the time of writing, repeater security is compatible with the NWA only.

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 NWA can extend the range of the WLAN. In the figure below, the NWA in Repeater mode (**Z**) has a wireless connection to the NWA in Root AP mode (**X**) which is connected to a wired network and also has a wireless connection to another NWA 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** and **B** access the AP and the wired network behind the AP through repeaters **Z** and **Y**.

Figure 5 Repeater Application



When the NWA is in Repeater mode, repeater security between the NWA and other repeater is independent of the security between the wireless clients and the AP or repeater. If you do not enable repeater security, traffic between APs is not encrypted. When repeater security is enabled, both APs and repeaters must use the same pre-shared key. See Section 6.6 on page 72 for more details.

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

At the time of writing, repeater security is compatible with the NWA only.

1.3 Ways to Manage the NWA

Use any of the following methods to manage the NWA.

- Web Configurator. This is recommended for everyday management of the NWA using a (supported) web browser.
- Telnet to login to the NWA using a virtual terminal connection.
- FTP (File Transfer Protocol) for firmware upgrades and configuration backup and restore.
- SNMP (Simple Network Management Protocol). The device can be monitored by an SNMP manager.

1.4 Configuring Your NWA's Security Features

Your NWA 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 NWA. Follow the suggestions below to improve security on your NWA and network.

1.4.1 Control Access to Your Device

Ensure only people with permission can access your NWA.

- Control physical access by locating devices in secure areas, such as locked rooms. Most NWAs 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 NWA, such as the password used for accessing the NWA'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.
- See Section 10.5 on page 111 for instructions on changing your password.
- Configure remote management to control who can manage your NWA. See Chapter 8 on page 92 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. Take the following measures to improve wireless security.

- Enable wireless security on your NWA. Choose the most secure encryption method that all devices on your network support. See Section 6.6 on page 72 for directions on configuring encryption. If you have a RADIUS server, enable IEEE 802.1x or WPA2 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 70 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 6.9 on page 82 for directions on configuring the MAC filter.

1.5 Good Habits for Managing the NWA

Do the following things regularly to make the NWA more secure and to manage it more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NWA to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NWA. You could simply restore your last configuration.

1.6 Hardware Connections

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

1.7 LED

Figure 6 LED

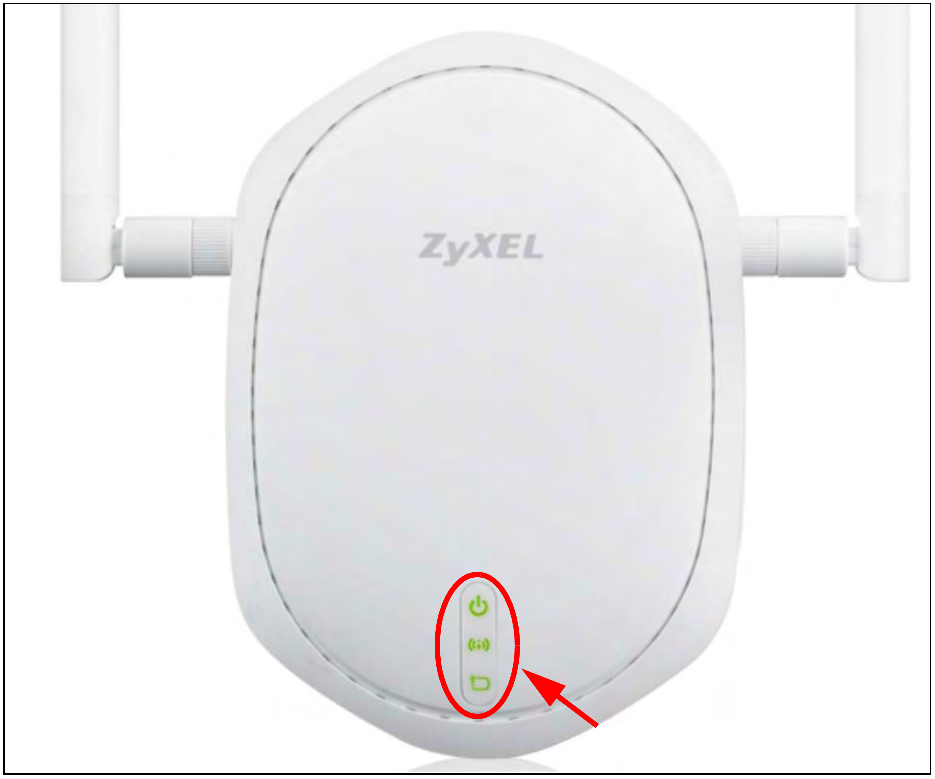


Table 2 LED

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS ⏻	Amber/Red	On	There is system error and the NWA cannot boot up, or the NWA doesn’t have an Ethernet connection with the LAN.
		Blinking	The NWA is starting up.
		Off	The NWA is receiving power and ready for use.
	Green	On	The NWA is receiving power.
		Blinking	The NWA is starting up.
		Off	The NWA is not receiving power.

Table 2 LED (continued)

LED	COLOR	STATUS	DESCRIPTION
WLAN	Green	On	The WLAN is active.
		Blinking	The WLAN is transmitting or receiving data.
		Off	The WLAN is not active.
UPLINK	Green	On	The port is connected.
		Blinking	The NWA is sending/receiving data through the port.
		Off	The port is not connected.

Introducing the Web Configurator

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

2.1 Overview

The NWA Web Configurator allows easy management using an Internet browser.

In order to use the Web Configurator, you must:

- Use Internet Explorer 7.0 and later versions, Mozilla Firefox 9.0 and later versions, Safari 4.0 and later versions, or Google Chrome 10.0 and later versions.
- Allow pop-up windows.
- Enable JavaScript (enabled by default).
- Enable Java permissions (enabled by default).
- Enable cookies.

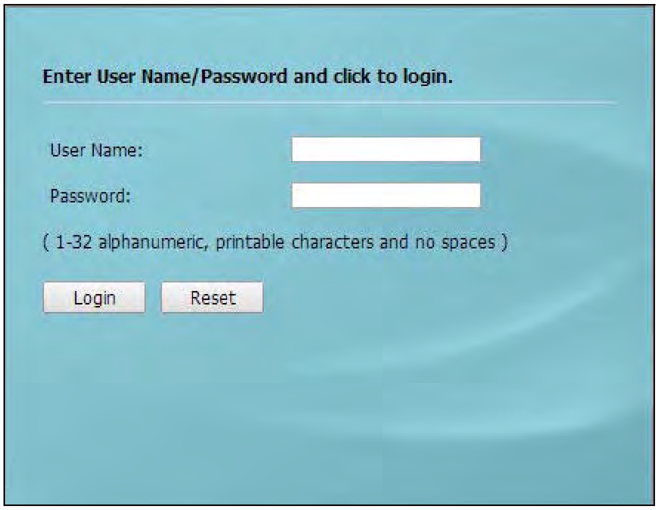
The recommended screen resolution is 1024 x 768 pixels and higher.

2.2 Accessing the Web Configurator

1. Make sure your hardware is properly connected and prepare your computer or computer network to connect to the NWA (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 7 The Login Screen



Enter User Name/Password and click to login.

User Name:

Password:

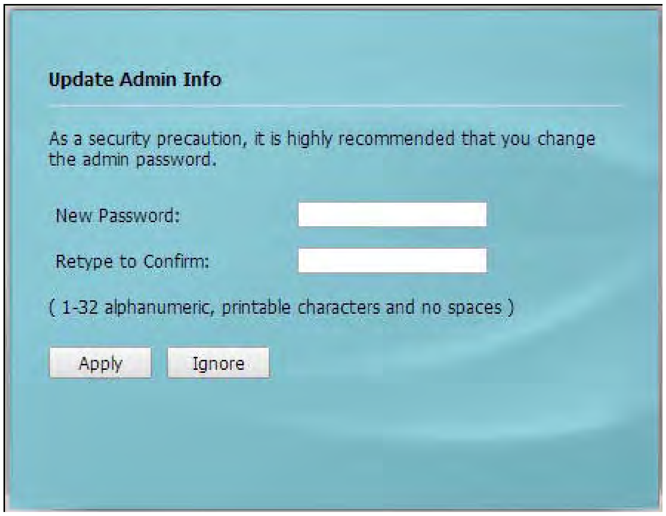
(1-32 alphanumeric, printable characters and no spaces)

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 8 Change Password Screen



Update Admin Info

As a security precaution, it is highly recommended that you change the admin password.

New Password:

Retype to Confirm:

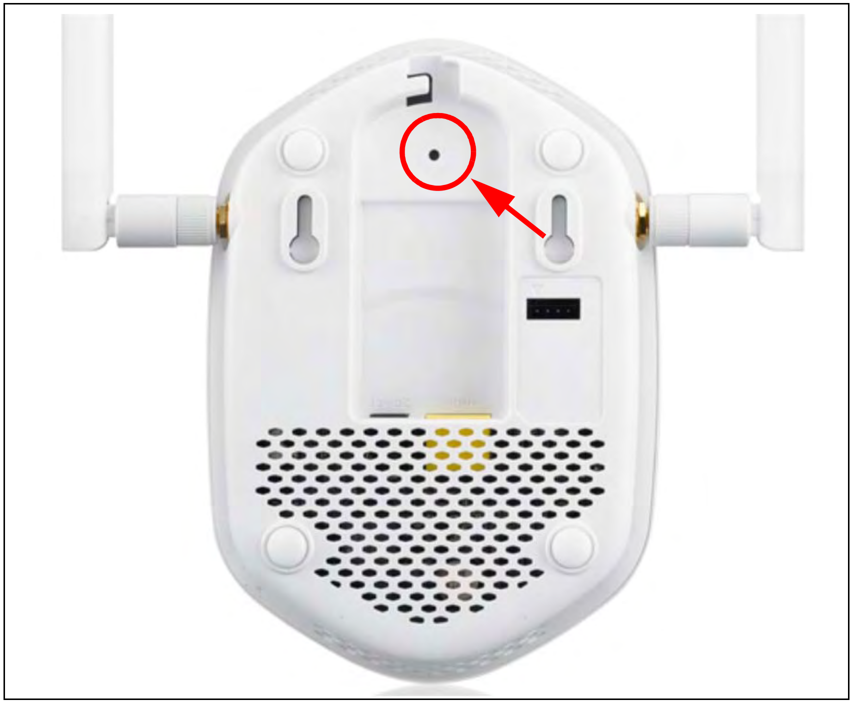
(1-32 alphanumeric, printable characters and no spaces)

You should now see the **Dashboard** screen. See Chapter 2 on page 18 for details about the **Dashboard** screen.

2.3 Resetting the NWA

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 NWA. 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 9 The RESET Button



2.3.1 Methods of Restoring Factory-Defaults

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

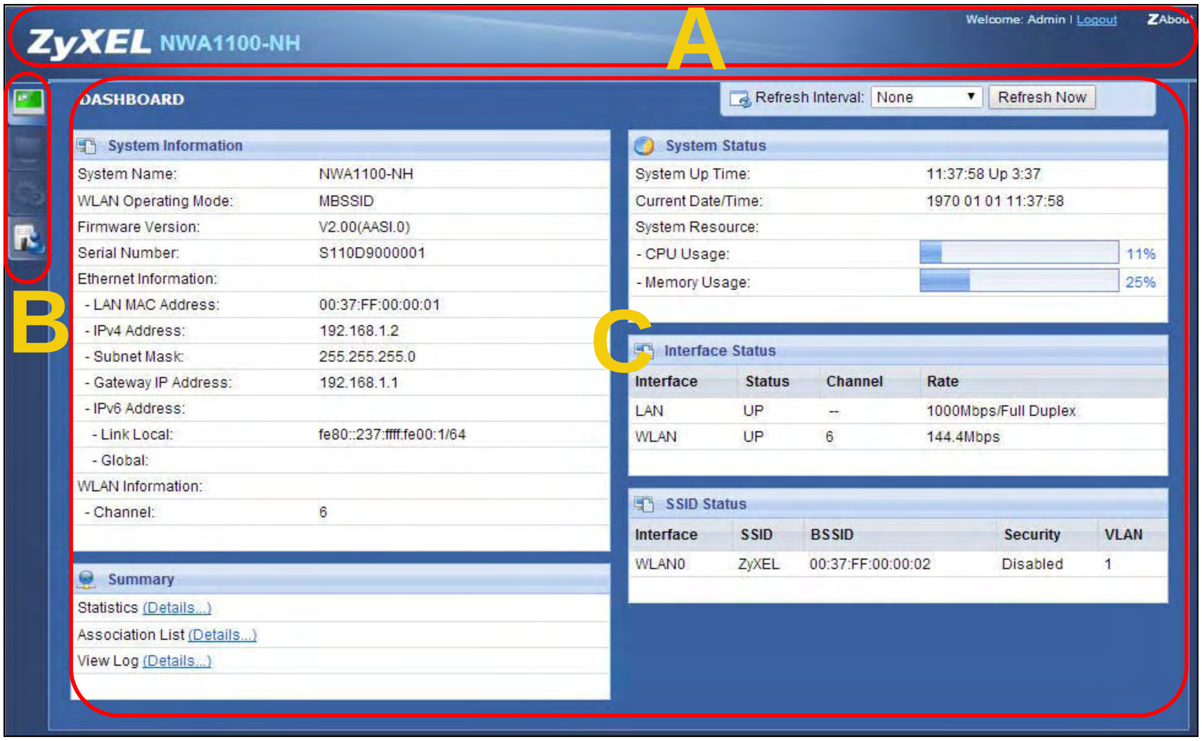
Use the **RESET** button to upload the default configuration file. Hold this button in for about 3 seconds (the light will begin to blink). Use this method for cases when the password or IP address of the NWA is not known.

Use the web configurator to restore defaults (refer to Section 10.8 on page 114).

2.4 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Dashboard** screen. This guide uses the NWA1100-NH screens as an example. The screens may vary slightly for different models.

Figure 10 Status Screen of the Web Configurator



System Information

System Name:	NWA1100-NH
WLAN Operating Mode:	MBSSID
Firmware Version:	V2.00(AASI.0)
Serial Number:	S110D9000001
Ethernet Information:	
- LAN MAC Address:	00:37:FF:00:00:01
- IPv4 Address:	192.168.1.2
- Subnet Mask:	255.255.255.0
- Gateway IP Address:	192.168.1.1
- IPv6 Address:	
- Link Local:	fe80::237:ffff:fe00:1/64
- Global:	
WLAN Information:	
- Channel:	6

Summary

Statistics (Details...)
Association List (Details...)
View Log (Details...)

System Status

System Up Time:	11:37:58 Up 3:37
Current Date/Time:	1970 01 01 11:37:58
System Resource:	
- CPU Usage:	11%
- Memory Usage:	25%

Interface Status

Interface	Status	Channel	Rate
LAN	UP	--	1000Mbps/Full Duplex
WLAN	UP	6	144.4Mbps

SSID Status

Interface	SSID	BSSID	Security	VLAN
WLAN0	ZyXEL	00:37:FF:00:00:02	Disabled	1

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

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

2.4.1 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.

2.4.2 Navigation Panel

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

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Dashboard		This screen shows the NWA’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 NWA.
Channel Usage		Use this screen to know whether a channel is used by another wireless network or not.
Configuration		
Network		
Wireless LAN	Wireless Settings Wireless Settings - 2.4G Wireless Settings - 5G	Use this screen to configure the wireless LAN settings and NWA’s operation mode.
	SSID	Use this screen to configure up to eight SSID profiles for your NWA.
	Security	Use this screen to configure wireless security profiles on the NWA.
	RADIUS	Use this screen to configure up to four RADIUS profiles.
	Layer-2 Isolation	Use this screen to configure the MAC addresses of the devices that you want to allow the associated wireless clients to have access to when layer-2 isolation is enabled
	MAC Filter	Use this screen to configure MAC filtering profiles.
LAN	IP	Use this screen to configure the NWA’s LAN IP address.
System	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NWA.
	Certificates	Use this screen to import or remove a certificate from the NWA.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NWA.
	SNMP	Use this screen to configure the NWA 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 NWA.
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 NWA’s time and date.
Firmware Upgrade		Use this screen to upload firmware to your device.

Table 3 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 NWA without turning the power off.

2.4.3 Main Window

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

3

Dashboard

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

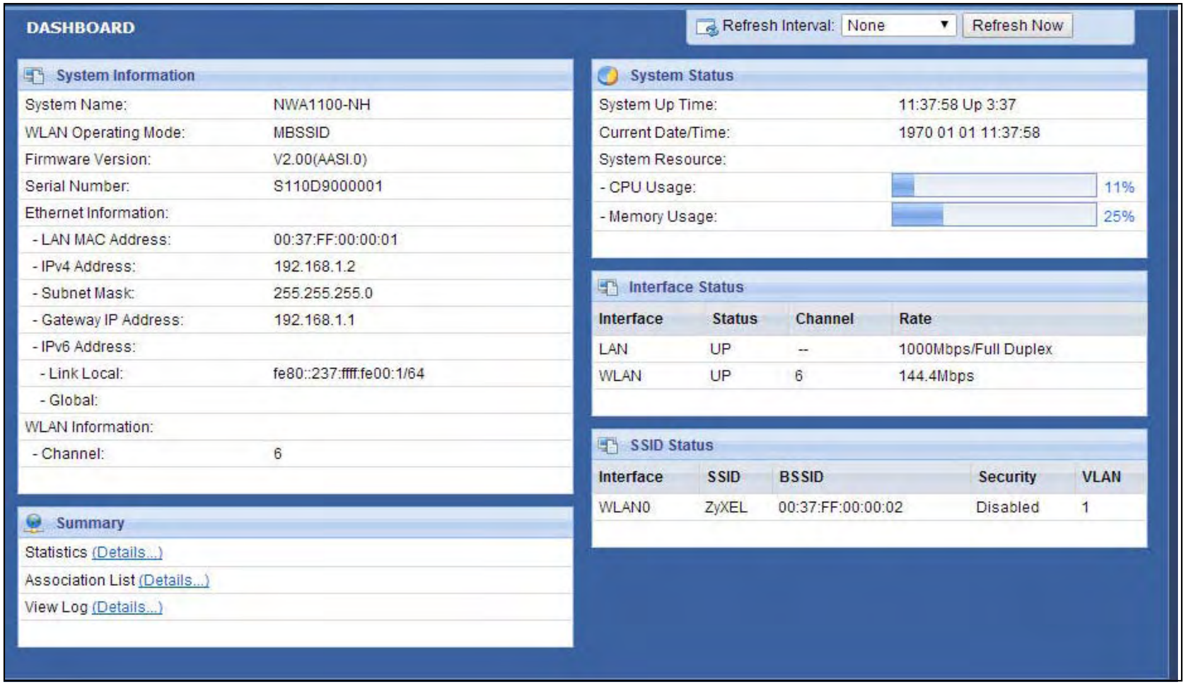
Use the **Dashboard** screen to look at the current status of the device, system resources, and interfaces. The **Dashboard** screens also provide detailed information about system statistics, associated wireless clients, and logs.

3.1 The Dashboard Screen

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

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

Figure 11 The Dashboard Screen (NWA1100-NH)



System Information

System Name:	NWA1100-NH
WLAN Operating Mode:	MBSSID
Firmware Version:	V2.00(AASI.0)
Serial Number:	S110D9000001
Ethernet Information:	
- LAN MAC Address:	00:37:FF:00:00:01
- IPv4 Address:	192.168.1.2
- Subnet Mask:	255.255.255.0
- Gateway IP Address:	192.168.1.1
- IPv6 Address:	
- Link Local:	fe80::237:ffff:fe00:1/64
- Global:	
WLAN Information:	
- Channel:	6

Summary

Statistics (Details...)
Association List (Details...)
View Log (Details...)

System Status

System Up Time:	11:37:58 Up 3:37
Current Date/Time:	1970 01 01 11:37:58
System Resource:	
- CPU Usage:	11%
- Memory Usage:	25%

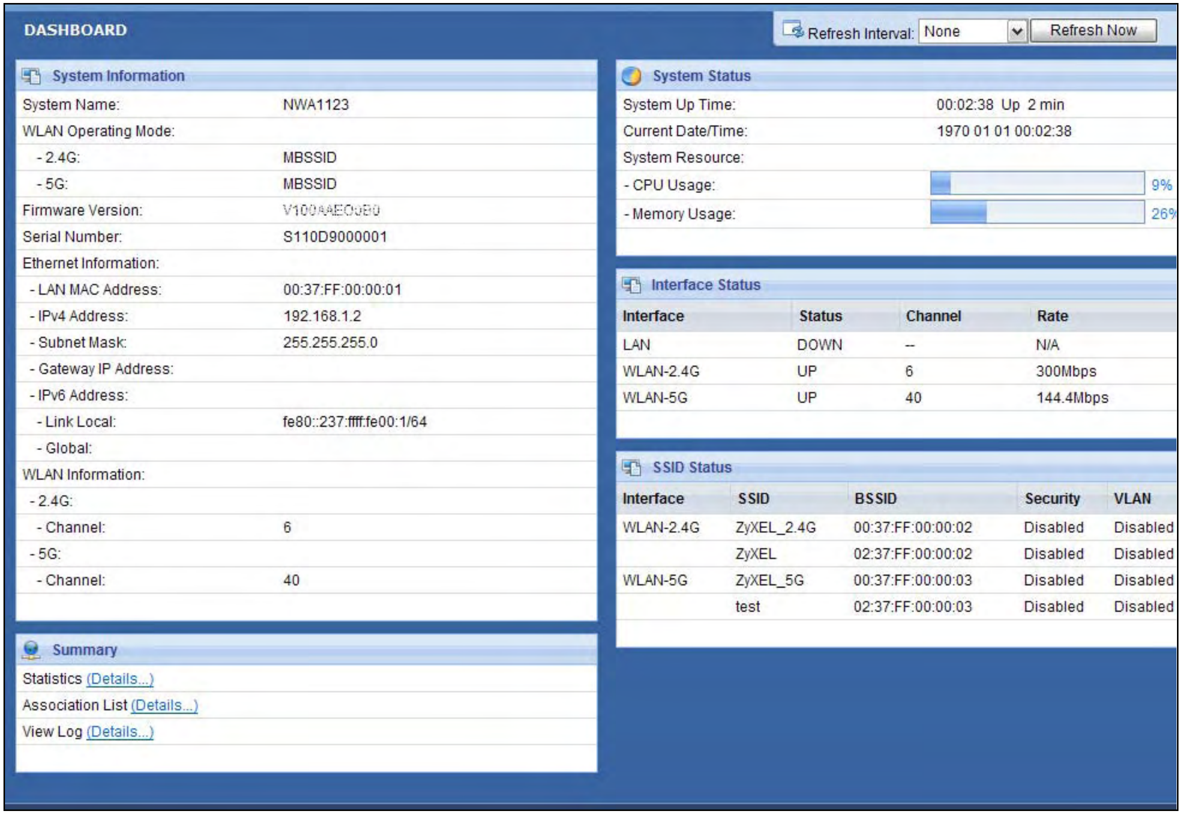
Interface Status

Interface	Status	Channel	Rate
LAN	UP	--	1000Mbps/Full Duplex
WLAN	UP	6	144.4Mbps

SSID Status

Interface	SSID	BSSID	Security	VLAN
WLAN0	ZyXEL	00:37:FF:00:00:02	Disabled	1

Figure 12 The Dashboard Screen (NWA1123-NI or NWA1123-AC)



System Information

System Name:	NWA1123
WLAN Operating Mode:	
- 2.4G:	MBSSID
- 5G:	MBSSID
Firmware Version:	V100AAEO0B0
Serial Number:	S110D9000001
Ethernet Information:	
- LAN MAC Address:	00:37:FF:00:00:01
- IPv4 Address:	192.168.1.2
- Subnet Mask:	255.255.255.0
- Gateway IP Address:	
- IPv6 Address:	
- Link Local:	fe80::237:ffff:fe00:1/64
- Global:	
WLAN Information:	
- 2.4G:	
- Channel:	6
- 5G:	
- Channel:	40

Summary

Statistics (Details...)
Association List (Details...)
View Log (Details...)

System Status

System Up Time:	00:02:38 Up 2 min
Current Date/Time:	1970 01 01 00:02:38
System Resource:	
- CPU Usage:	9%
- Memory Usage:	26%

Interface Status

Interface	Status	Channel	Rate
LAN	DOWN	--	N/A
WLAN-2.4G	UP	6	300Mbps
WLAN-5G	UP	40	144.4Mbps

SSID Status

Interface	SSID	BSSID	Security	VLAN
WLAN-2.4G	ZyXEL_2.4G	00:37:FF:00:00:02	Disabled	Disabled
	ZyXEL	02:37:FF:00:00:02	Disabled	Disabled
WLAN-5G	ZyXEL_5G	00:37:FF:00:00:03	Disabled	Disabled
	test	02:37:FF:00:00:03	Disabled	Disabled

The following table describes the labels in this screen.

Table 4 The Dashboard Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the NWA to update this screen.
Refresh Now	Click this to update this screen immediately.
System Information	
System Name	This field displays the NWA 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 wireless module (**Root AP**, **Repeater**, **Client**, or **MBSSID**). You can change the operating mode in the **Configuration** > **Wireless LAN > Wireless Settings** screen.
2.4G	This field displays the current operating mode of the 2.4G wireless module (**Root AP**, **Repeater**, **Client**, or **MBSSID**). You can change the operating mode in the **Configuration** > **Wireless LAN > Wireless Settings - 2.4G** screen.
5G	This field displays the current operating mode of the 5G wireless module (**Root AP**, **Repeater**, **Client**, or **MBSSID**). You can change the operating mode in the **Configuration** > **Wireless LAN > Wireless Settings - 5G** 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 NWA.
Ethernet Information	
LAN MAC Address	This displays the MAC (Media Access Control) address of the NWA 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 NWA 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 NWA on the network.
Link Local	This is the IPv6 link-local address that the NWA generates automatically.
Global	This is the NWA'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 NWA to send and receive information (in the 2.4G or 5G wireless network).
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 NWA 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 47.
Association List	Click this to see a list of wireless clients currently associated to each of the NWA's wireless modules. See Section 5.5 on page 48.

Table 4 The Dashboard Screen (continued)

LABEL	DESCRIPTION
View Log	Click this to see a list of logs produced by the NWA. See Section 5.3 on page 46.
System Status	
System Up Time	This field displays the elapsed time since the NWA was turned on.
Current Date/Time	This field displays the date and time configured on the NWA. You can change this in the **Maintenance > Time** screen.
System Resource	
CPU Usage	This field displays what percentage of the NWA's processing ability is currently being used. The higher the CPU usage, the more likely the NWA is to slow down.
Memory Usage	This field displays what percentage of the NWA's volatile memory is currently in use. The higher the memory usage, the more likely the NWA is to slow down. Some memory is required just to start the NWA and to run the web configurator.
Interface Status	
Interface	This column displays each interface of the NWA.
Status	This field indicates whether or not the NWA is using the interface. For each interface, this field displays **Up** when the NWA is using the interface and **Down** when the NWA is not using the interface.
Channel	This shows the channel number which the NWA 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 NWA'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.

4

Tutorial

This chapter first provides an overview of how to configure the wireless LAN on your NWA, and then gives step-by-step guidelines showing how to configure your NWA 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 NWA and how to set up the wireless LAN in each wireless mode. See Section 4.1.2 on page 28 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 NWA 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 10 for details.
- Use **Client** operating mode if you want to use the NWA to access a wireless network. See Section 1.2.2 on page 11 for details.
- Use **Root AP** operating mode if you want to allow wireless clients to access your wired network through the NWA and also have repeaters communicate with the NWA to expand wireless coverage. See Section 1.2.3 on page 13 for details.
- Use **Repeater** operating mode if you want to use the NWA to communicate with the root AP or other repeaters. See Section 1.2.4 on page 13 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 56.
- Choosing a wireless **Channel ID**: see Section 6.4 on page 56.
- Choosing a **Security** mode: see Section 6.6 on page 72.
- Configuring an external **RADIUS** server: see Section 6.7 on page 78.
- Configuring **MAC Filtering**: see Section 6.9 on page 82.

4.2 How to Configure Multiple Wireless Networks

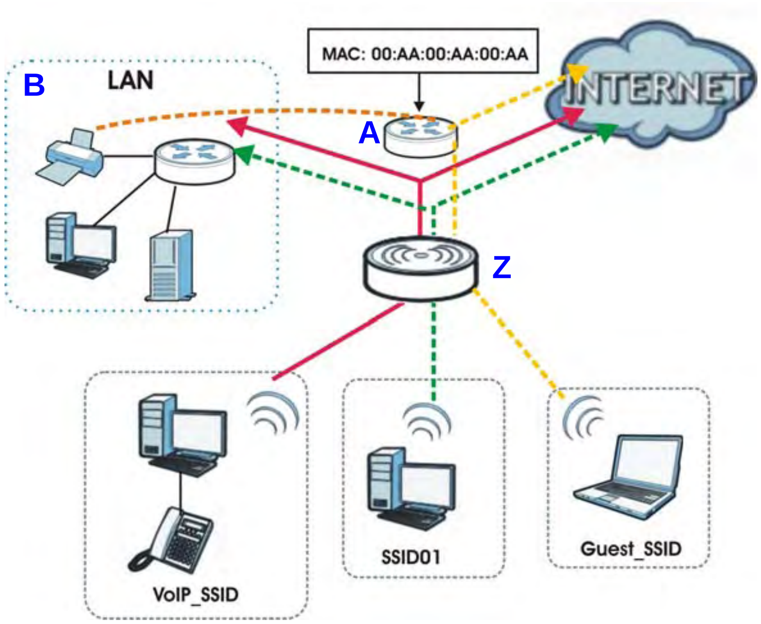
In this example, you have been using your NWA as an access point for your office network. Now your network is expanding and you want to make use of the MBSSID feature (see Section 6.4.4 on page 67) to provide multiple wireless networks. Each wireless network will cater to a different type of user.

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 NWA 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.

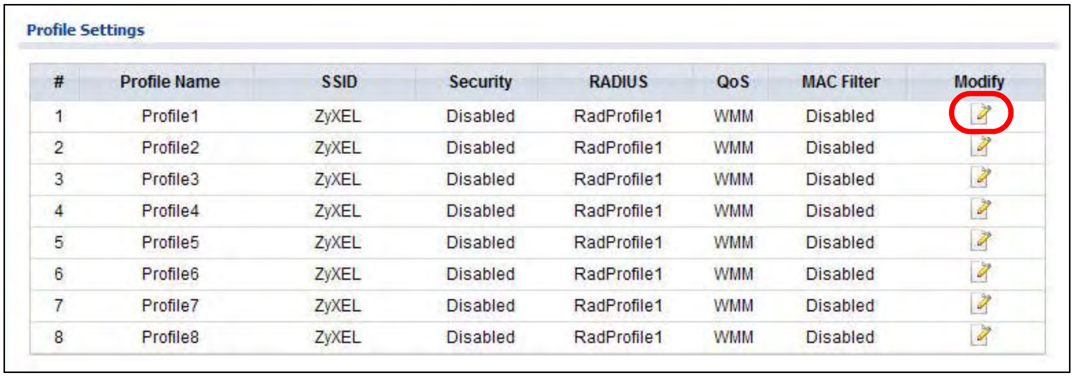
Table 5 Tutorial: Example Information

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 NWA (see Section 2.2 on page 18). Click **Wireless LAN > SSID**. The **SSID** screen appears.

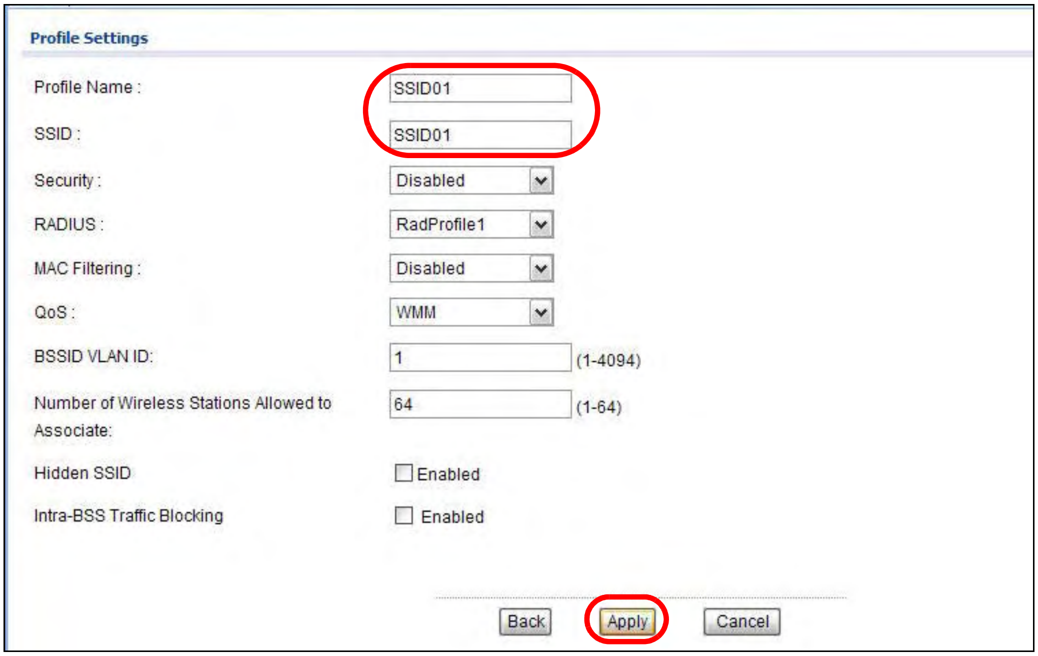
2 Click the **Edit** icon next to the **Profile1**.



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	✎

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



Profile Settings

Profile Name :	SSID01
SSID :	SSID01
Security :	Disabled
RADIUS :	RadProfile1
MAC Filtering :	Disabled
QoS :	WMM
BSSID VLAN ID:	1 (1-4094)
Number of Wireless Stations Allowed to Associate:	64 (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**.

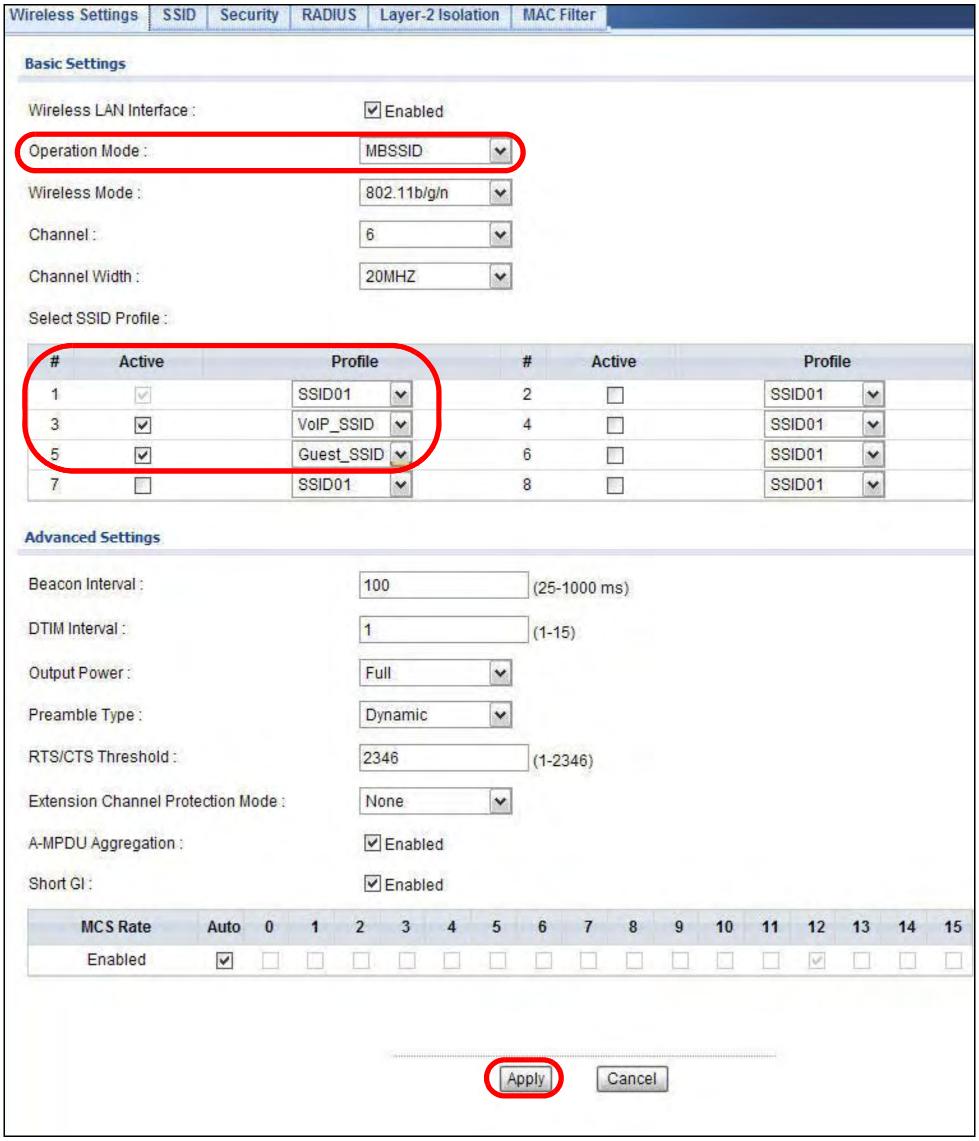
4.2.1.1 MBSSID

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.



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	☑	SSID01	2	□	SSID01
3	☑	VoIP_SSID	4	□	SSID01
5	☑	Guest_SSID	6	□	SSID01
7	□	SSID01	8	□	SSID01

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

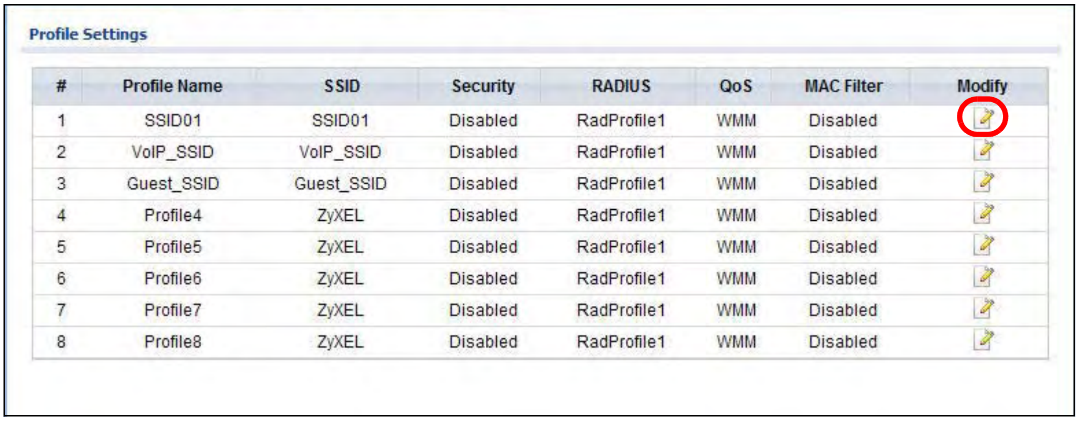
A-MPDU Aggregation : ☑ Enabled

Short GI : ☑ Enabled

MCS Rate	Auto	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Enabled	☑	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□

4.2.2 Configure the Standard Network

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



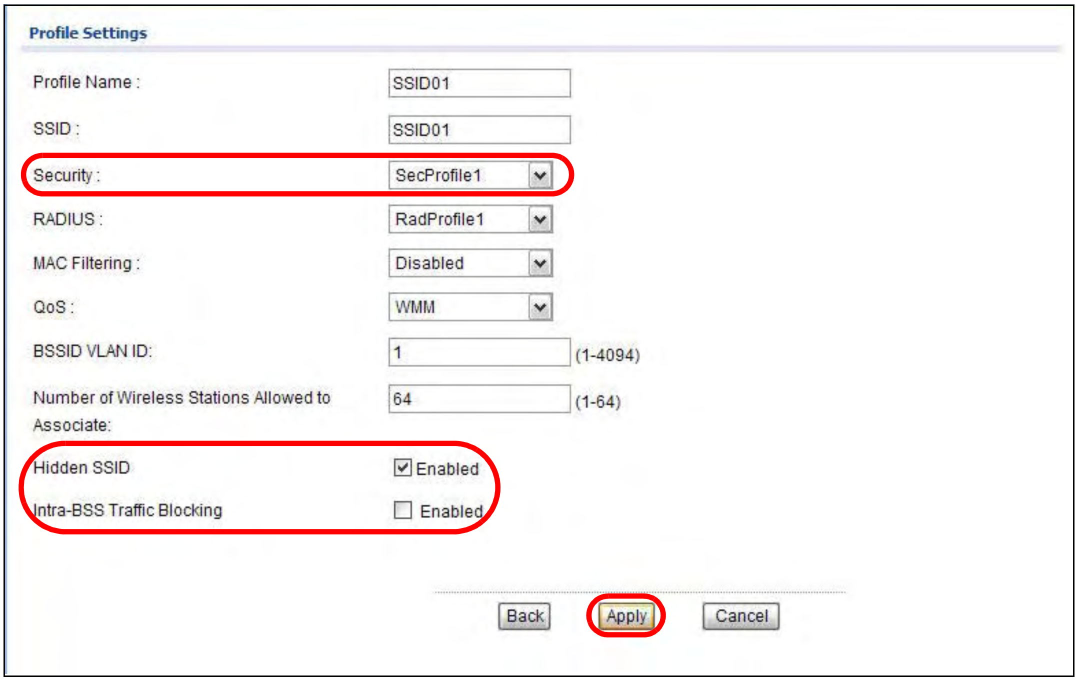
Profile Settings

#	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.

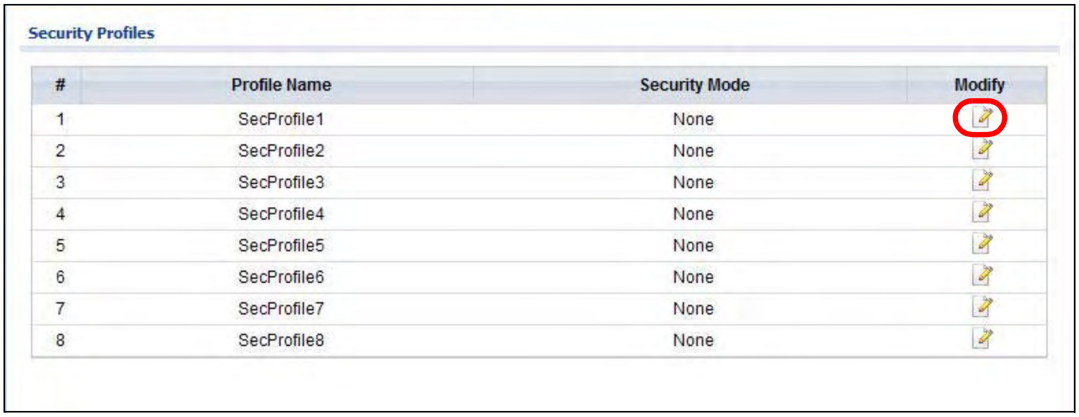
Click **Apply**.



Profile Settings

Profile Name :	SSID01
SSID :	SSID01
Security :	SecProfile1
RADIUS :	RadProfile1
MAC Filtering :	Disabled
QoS :	WMM
BSSID VLAN ID:	1 (1-4094)
Number of Wireless Stations Allowed to Associate:	64 (1-64)
Hidden SSID	☑ Enabled
Intra-BSS Traffic Blocking	□ Enabled

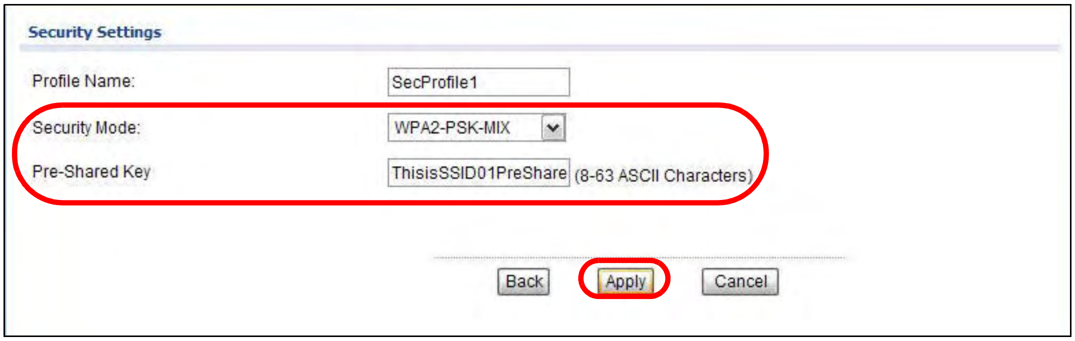
3 Next, click **Wireless LAN > Security**. Click the **Edit** icon next to **SecProfile1**.



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**.



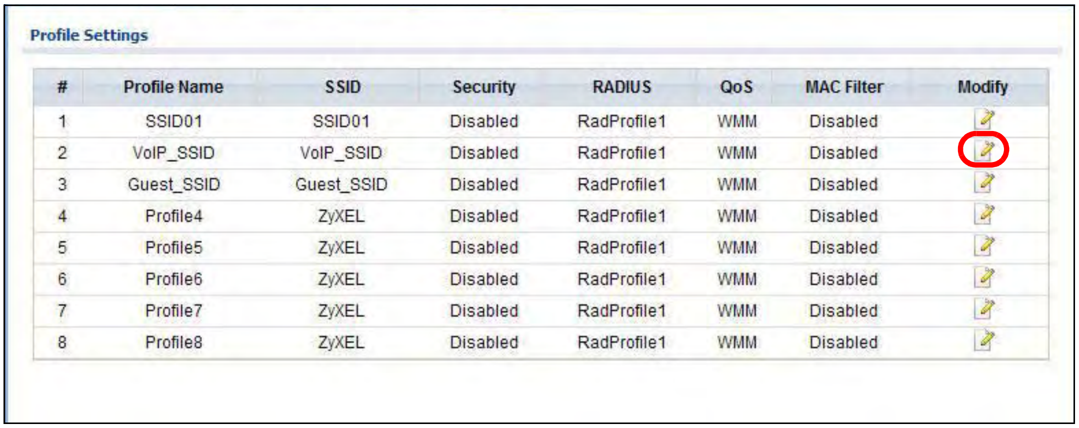
Security Settings

Profile Name:	SecProfile1
Security Mode:	WPA2-PSK-MIX ▾
Pre-Shared Key	ThisisSSID01PreShare (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**.

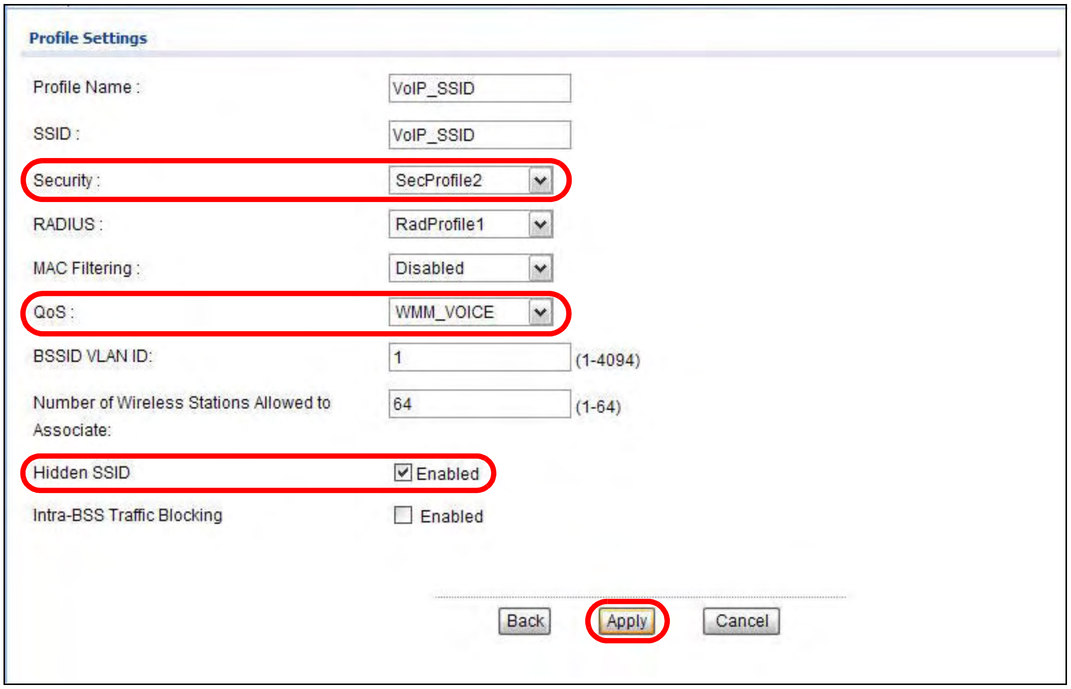


Profile Settings

#	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.

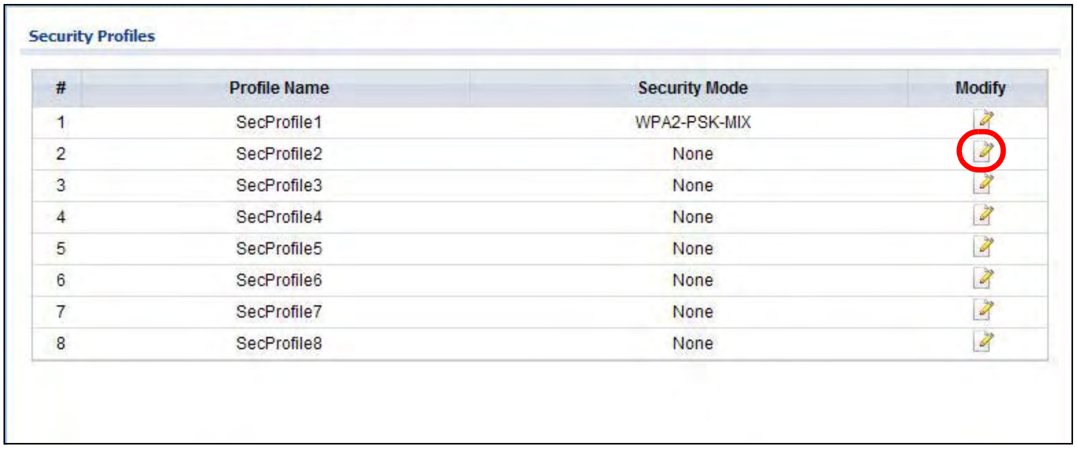
3 Select **WMM_VOICE** in the **QoS** field to give VoIP the highest priority in the wireless network. Click **Apply**.



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

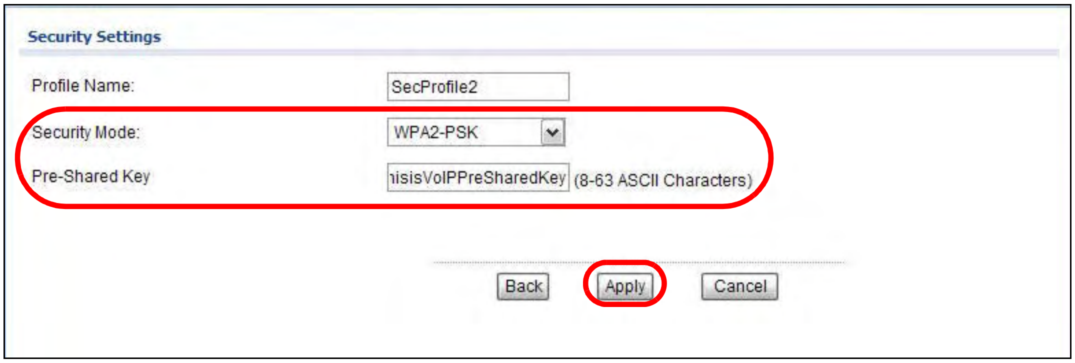
4 Next, click **Wireless LAN > Security**. Click the **Edit** icon next to **SecProfile2**.



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

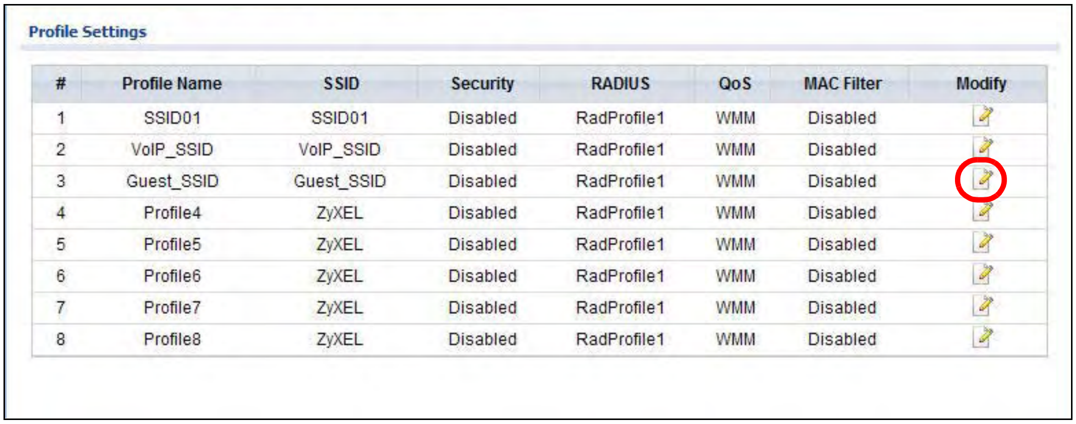
Profile Name:	SecProfile2
Security Mode:	WPA2-PSK
Pre-Shared Key	ıisisVoIPPreSharedKey (8-63 ASCII Characters)

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**.



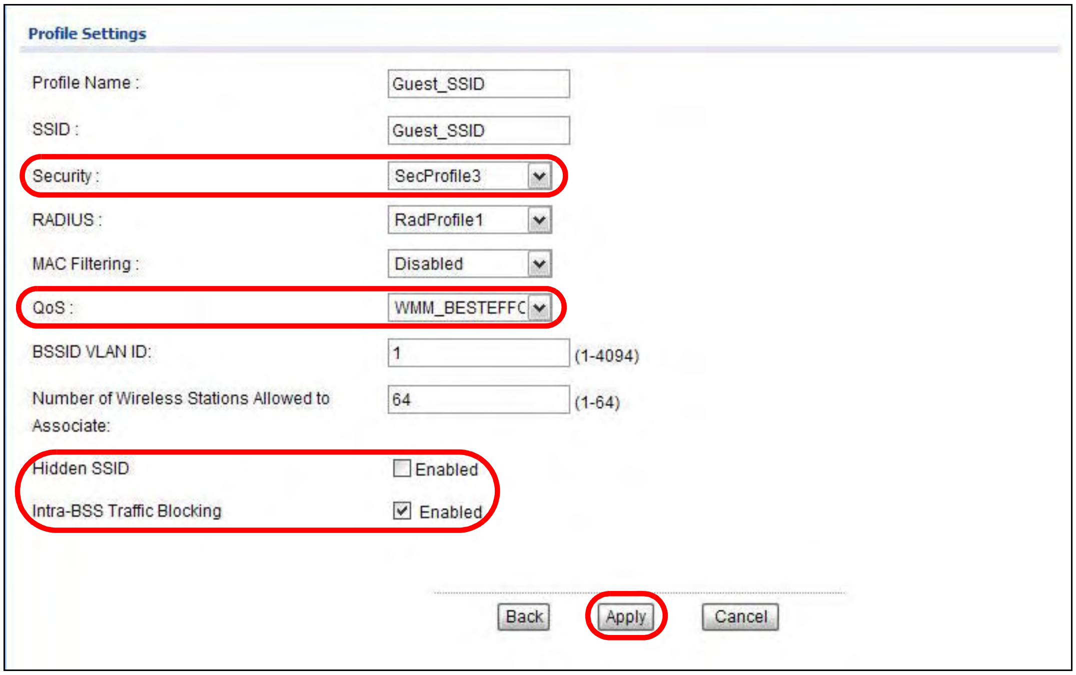
Profile Settings

#	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.

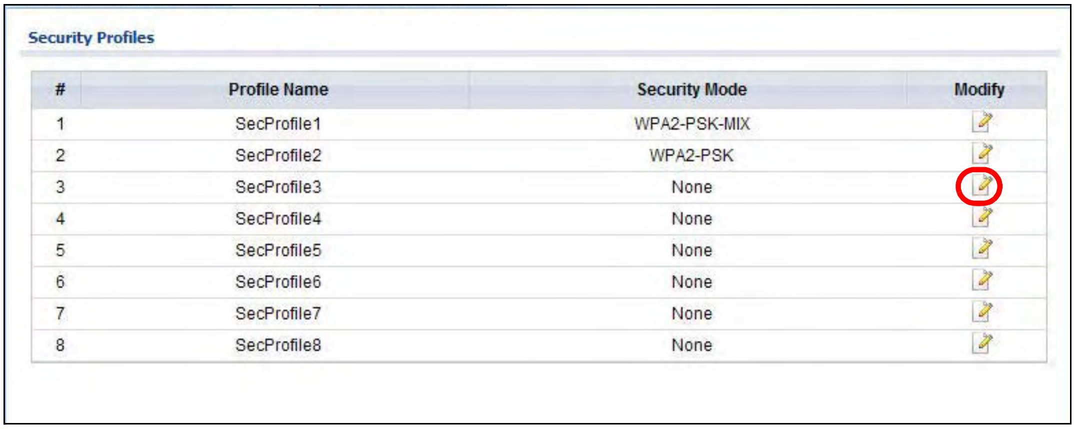
4 Select the check-box of **Intra-BSS Traffic blocking Enabled**. Click **Apply**.



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

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

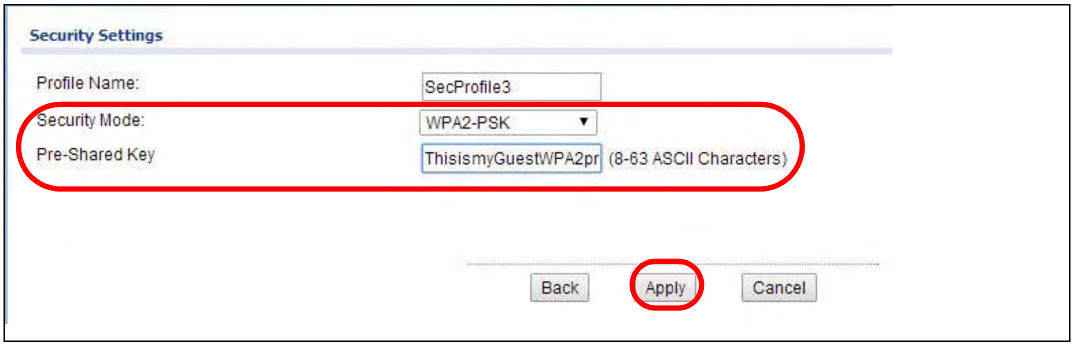


Security Profiles

#	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 **WPA2-PSK** in the **Security Mode** field. WPA2-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 **ThisismyGuestWPA2pre-sharedkey**. Click **Apply**.



Security Settings

Profile Name: SecProfile3

Security Mode: WPA2-PSK

Pre-Shared Key ThisismyGuestWPA2pr (8-63 ASCII Characters)

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 WPA2-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.

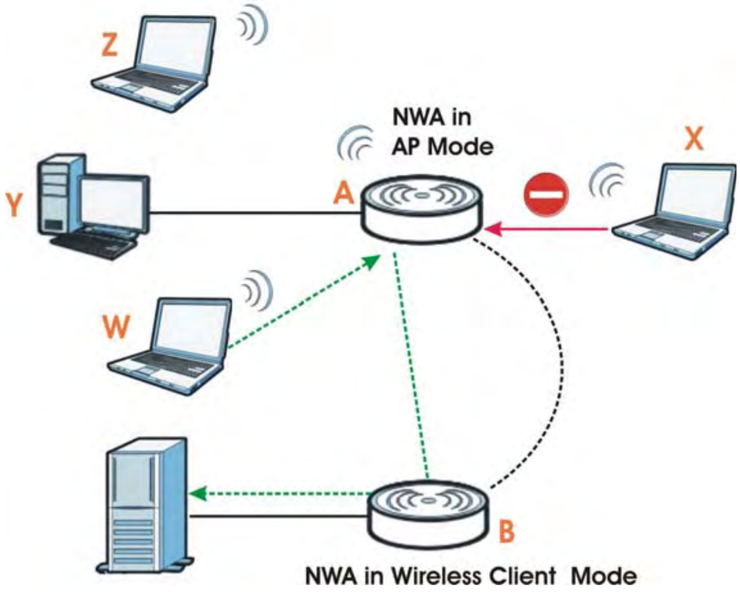
4.3 NWA Setup in AP and Wireless Client Modes

This example shows you how to restrict wireless access to your NWA.

4.3.1 Scenario

In the figure below, there are two NWAs (**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.

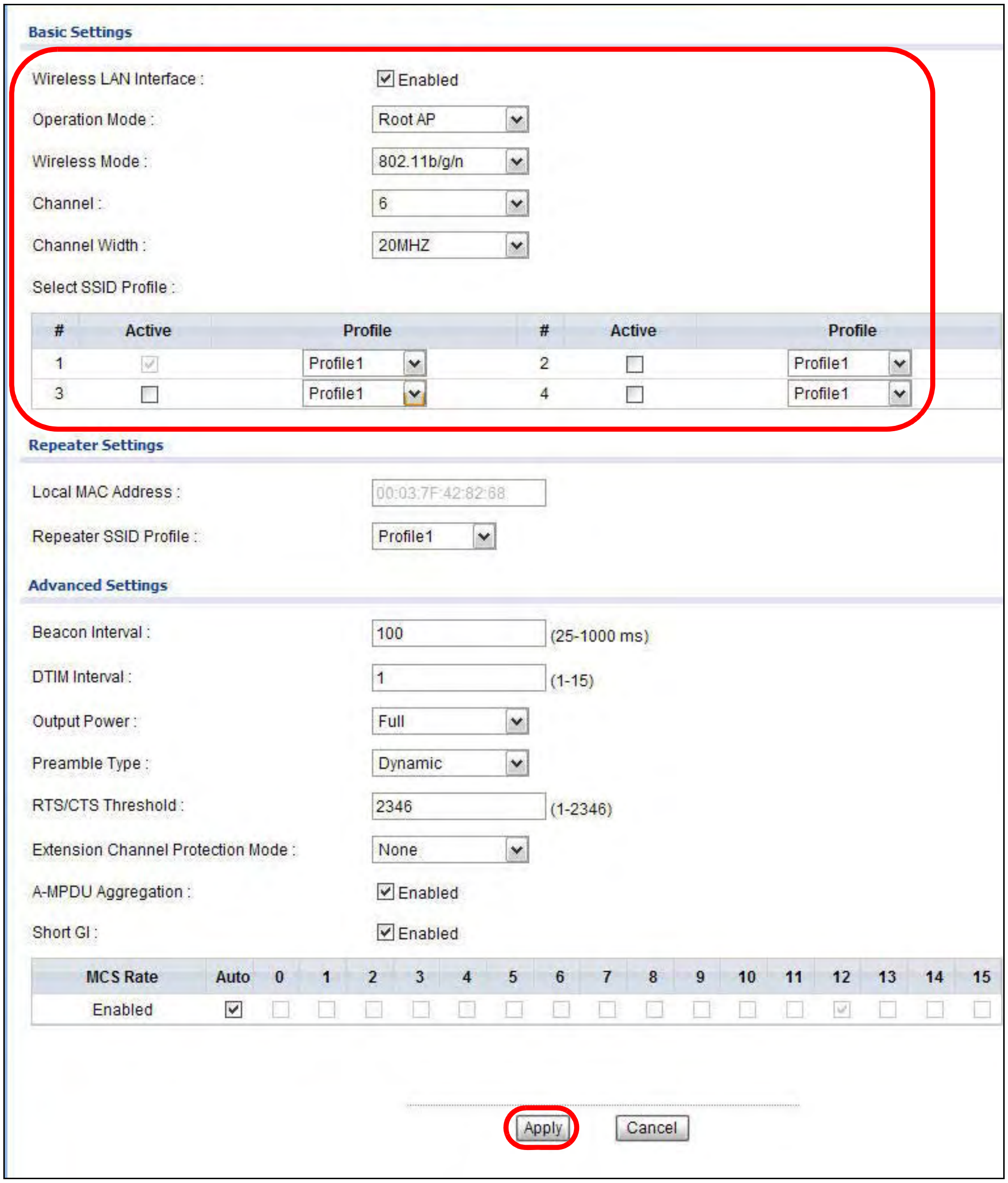
Figure 13 FTP Server Connected to a Wireless Client



4.3.2 Configuring the NWA in MBSSID or Root AP Mode

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

Log into the Web Configurator on NWA (**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	☑	Profile1	2	□	Profile1
3	□	Profile1	4	□	Profile1

Repeater Settings

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

1 Set the **Operation Mode** to **Root AP**.

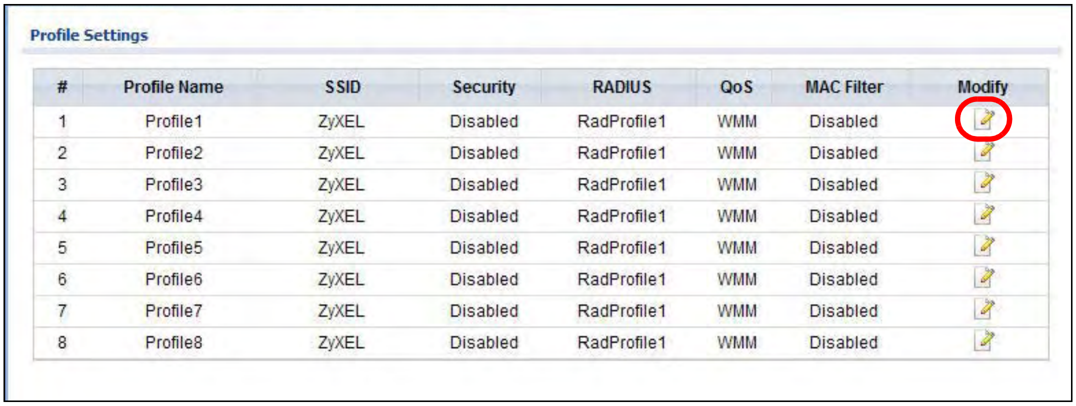
2 Select the **Wireless Mode**. In this example, select **802.11b/g/n**.

3 Select **Profile1** as the **SSID Profile**.

4 Choose the **Channel** you want NWA (**A**) to use.

5 Click **Apply**.

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



Profile Settings

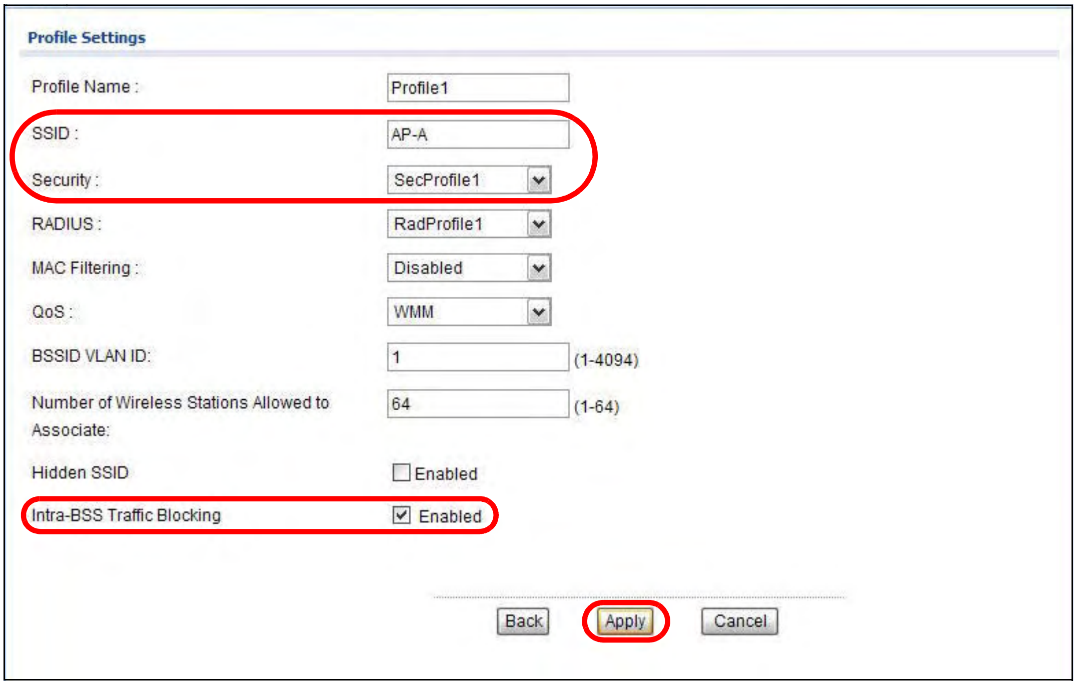
#	Profile Name	SSID	Security	RADIUS	QoS	MAC Filter	Modify
1	Profile1	ZyXEL	Disabled	RadProfile1	WMM	Disabled	✎
2	Profile2	ZyXEL	Disabled	RadProfile1	WMM	Disabled	✎
3	Profile3	ZyXEL	Disabled	RadProfile1	WMM	Disabled	✎
4	Profile4	ZyXEL	Disabled	RadProfile1	WMM	Disabled	✎
5	Profile5	ZyXEL	Disabled	RadProfile1	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.

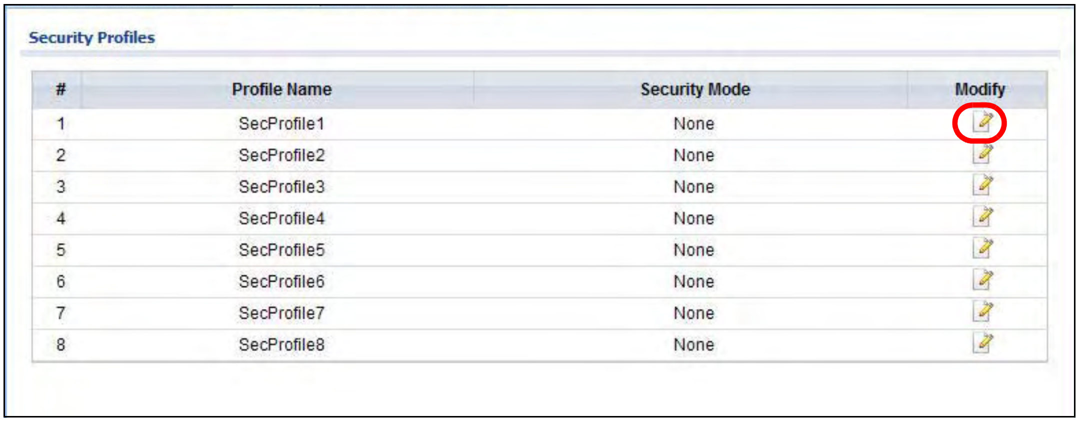
10 Click **Apply**.



Profile Settings

Profile Name :	Profile1
SSID :	AP-A
Security :	SecProfile1
RADIUS :	RadProfile1
MAC Filtering :	Disabled
QoS :	WMM
BSSID VLAN ID:	1 (1-4094)
Number of Wireless Stations Allowed to Associate:	64 (1-64)
Hidden SSID	□ Enabled
Intra-BSS Traffic Blocking	☑ Enabled

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

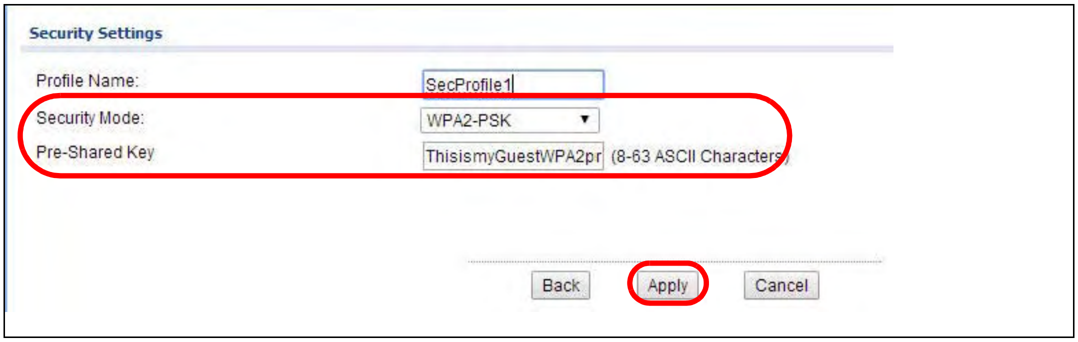


Security Profiles

#	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 **WPA2-PSK** as the **Security Mode** and enter **ThisisMyPreSharedKey** in the **Pre-Shared Key** field.

13 Click **Apply** to finish configuration for NWA (**A**).



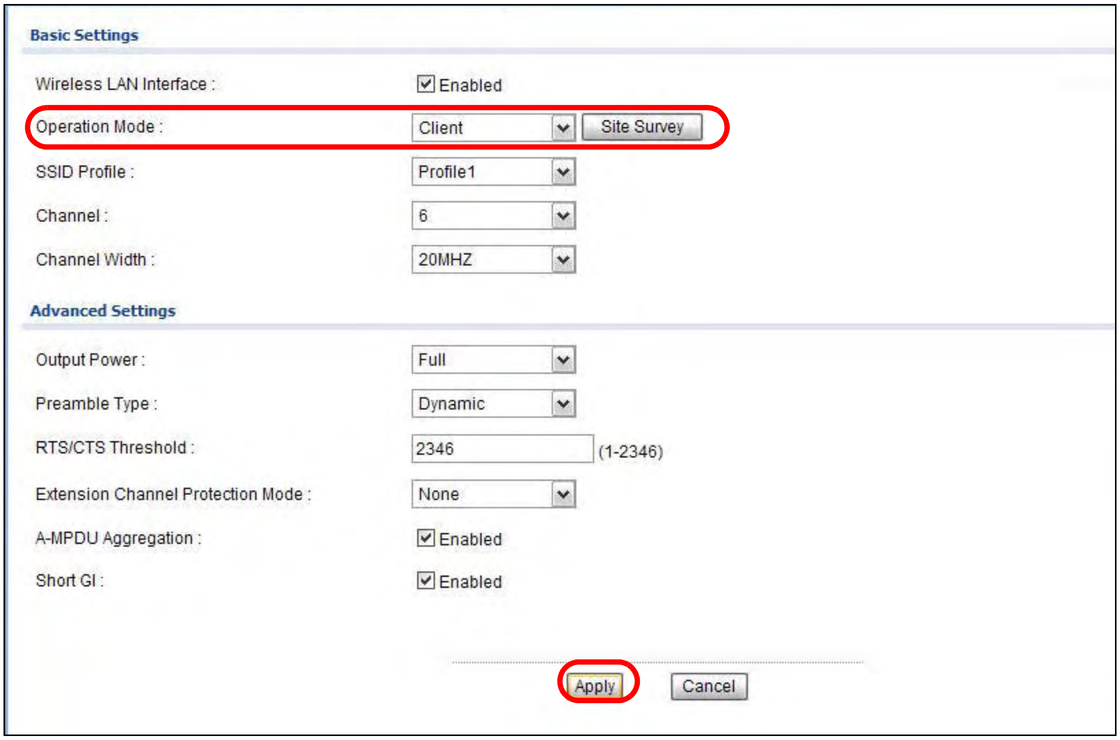
Security Settings

Profile Name:	SecProfile1
Security Mode:	WPA2-PSK ▼
Pre-Shared Key	ThisismyGuestWPA2pr (8-63 ASCII Characters)

4.3.3 Configuring the NWA in Wireless Client Mode

The NWA (**B**) should have a wired connection before it can be set to wireless client operating mode. Connect your NWA to the FTP server. Login to NWA (**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**. Site Survey button appears next to the drop-down list.



Basic Settings

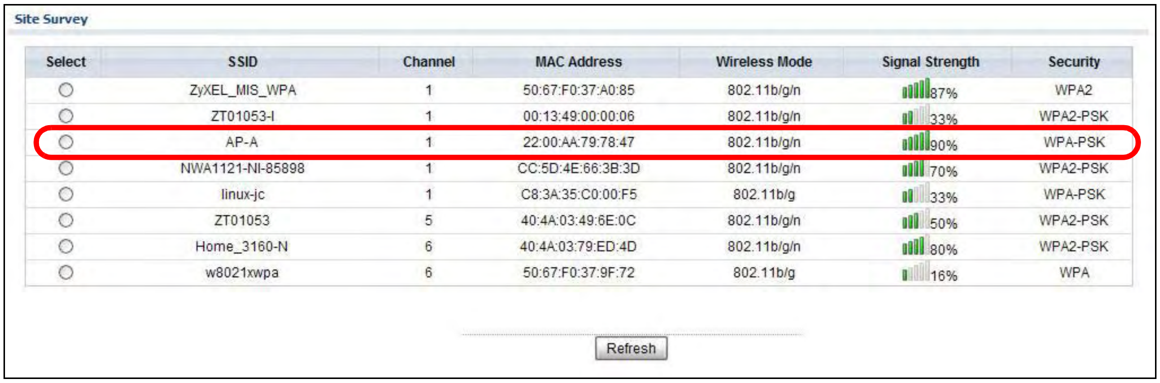
Wireless LAN Interface :	☑ Enabled
Operation Mode :	Client Site Survey
SSID Profile :	Profile1
Channel :	6
Channel Width :	20MHZ

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

2 Click on the **Site Survey** button. A window should pop up which contains a list of all available wireless devices within your NWA's range.

3 Find and select NWA (**A**)'s SSID: **AP-A**.

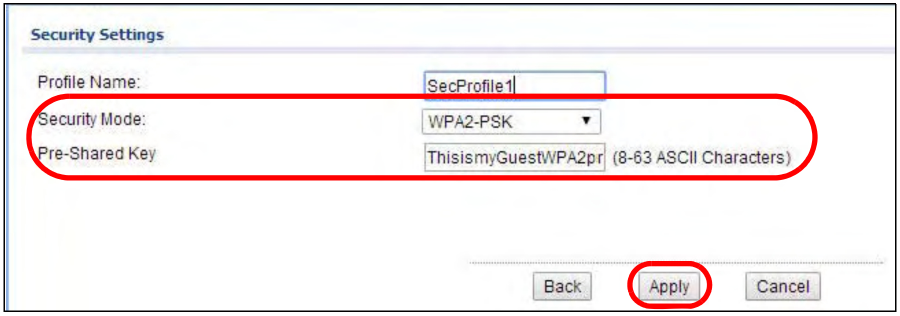


Site Survey

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

4 Go to **Wireless LAN > Security** to configure the NWA to use the same security mode and Pre-Shared Key as NWA (**A**): **WPA2-PSK/ThisisMyPreSharedKey**. Click **Apply**.

Figure 14



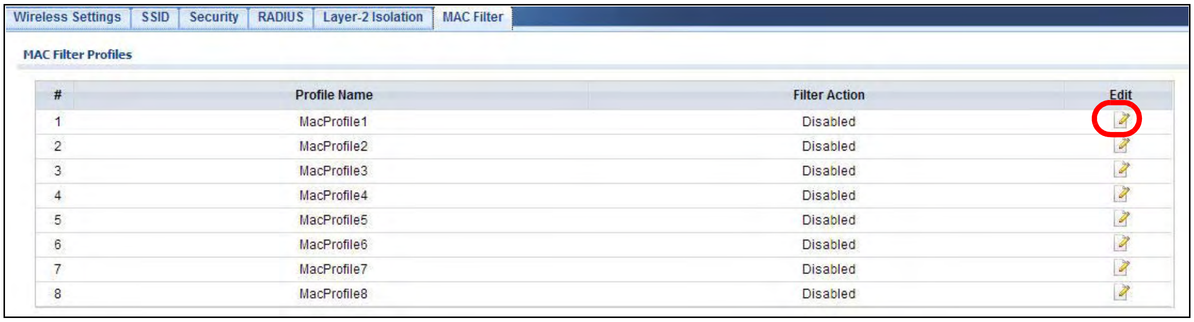
Security Settings

Profile Name:	SecProfile1
Security Mode:	WPA2-PSK ▼
Pre-Shared Key	ThisismyGuestWPA2pr (8-63 ASCII Characters)

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 NWA (**B**) (See Section 6.9 on page 82 for more information on MAC Filter).

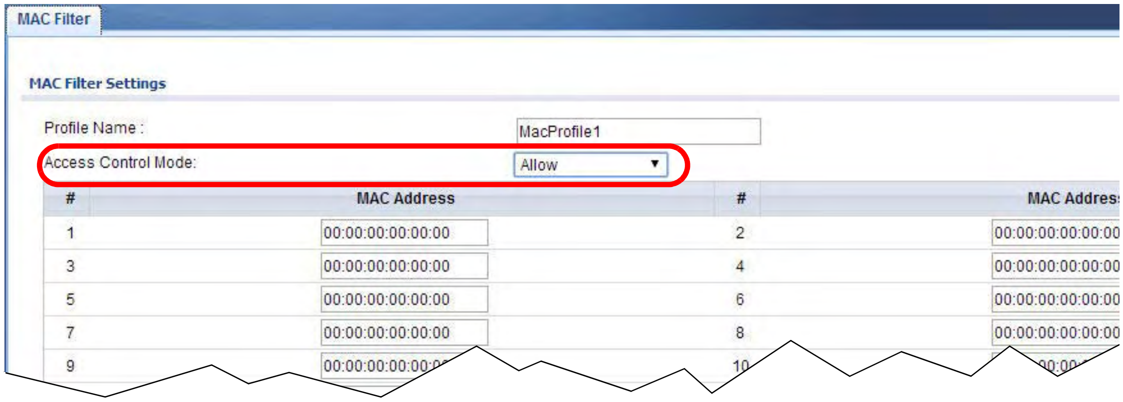
1 Go to **Wireless LAN > MAC Filter**. Click the **Edit** icon next to **MacProfile1**.



MAC Filter Profiles

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

2 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 NWA. Click **Apply**.



MAC Filter Settings

Profile Name :	MacProfile1
Access Control Mode:	Allow ▼

#	MAC Address	#	MAC Addres
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00
9	00:00:00:00:00:0	10	0:00:

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 NWA.

5

Monitor

5.1 Overview

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

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 NWA.

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 46). 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 47).
- Use the **Association List** screen to view the wireless devices that are currently associated to the NWA (see Section 5.5 on page 48).
- 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 49).

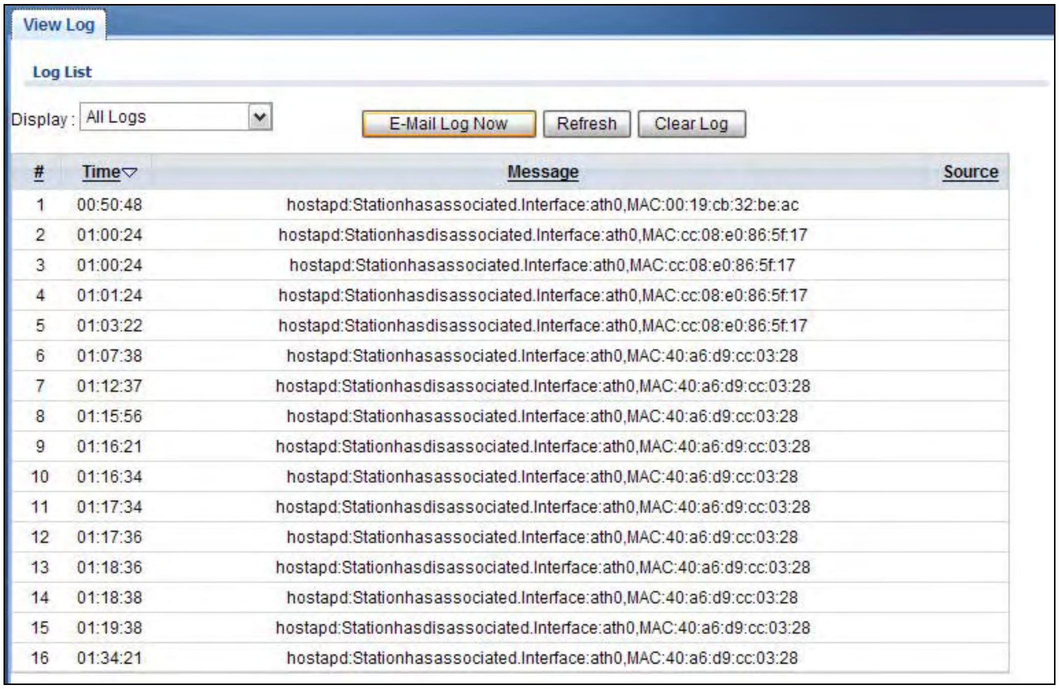
5.3 View Logs

Use the **Logs** screen to see the logged messages for the NWA.

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

Click **Monitor** > **Logs**.

Figure 15 Logs



#	Time▽	Message	Source
1	00:50:48	hostapd:Stationhasassociated.Interface:ath0,MAC:00:19:cb:32:be:ac	
2	01:00:24	hostapd:Stationhasdisassociated.Interface:ath0,MAC:cc:08:e0:86:5f:17	
3	01:00:24	hostapd:Stationhasassociated.Interface:ath0,MAC:cc:08:e0:86:5f:17	
4	01:01:24	hostapd:Stationhasdisassociated.Interface:ath0,MAC:cc:08:e0:86:5f:17	
5	01:03:22	hostapd:Stationhasdisassociated.Interface:ath0,MAC:cc:08:e0:86:5f:17	
6	01:07:38	hostapd:Stationhasassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
7	01:12:37	hostapd:Stationhasdisassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
8	01:15:56	hostapd:Stationhasassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
9	01:16:21	hostapd:Stationhasdisassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
10	01:16:34	hostapd:Stationhasassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
11	01:17:34	hostapd:Stationhasdisassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
12	01:17:36	hostapd:Stationhasassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
13	01:18:36	hostapd:Stationhasdisassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
14	01:18:38	hostapd:Stationhasassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
15	01:19:38	hostapd:Stationhasdisassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	
16	01:34:21	hostapd:Stationhasassociated.Interface:ath0,MAC:40:a6:d9:cc:03:28	

The following table describes the labels in this screen.

Table 6 Logs

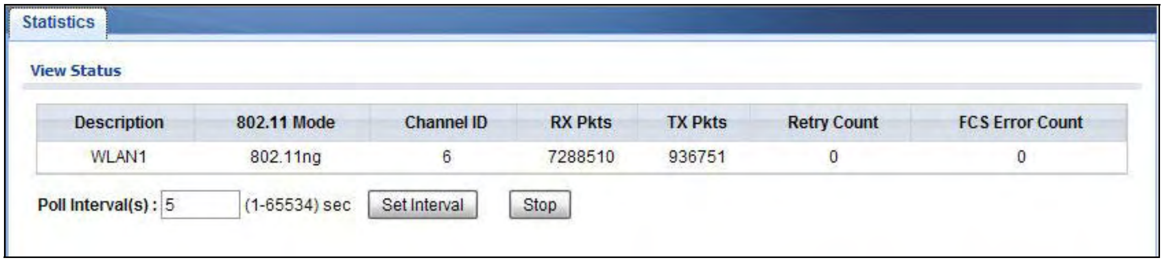
LABEL	DESCRIPTION
Display	Select a category of logs to view. Select **All Log** to view logs from all of the log categories that you selected in the **Configuration** > **Log Settings** screen.
E-Mail Log Now	Click **E-Mail Log Now** to send the log screen to the e-mail address specified in the Log Settings 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 16 Statistics



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

Poll Interval(s) : 5 (1-65534) sec

The following table describes the labels in this screen.

Table 7 Statistics

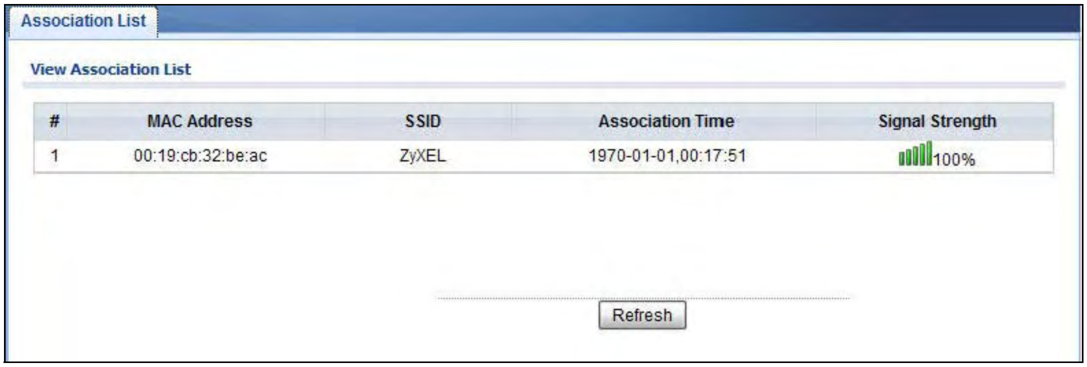
LABEL	DESCRIPTION
Description	This is the wireless interface on the NWA.
802.11 Mode	This field shows which 802.11 mode the NWA is using.
Channel ID	This shows the channel number which the NWA is currently using over the wireless LAN.
RX Pkts	This is the number of received packets on this port.
TX Pkts	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 total number of checksum error of received packets (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 NWA 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 17 Association List



#	MAC Address	SSID	Association Time	Signal Strength
1	00:19:cb:32:be:ac	ZyXEL	1970-01-01,00:17:51	100%

The following table describes the labels in this screen.

Table 8 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 NWA'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.

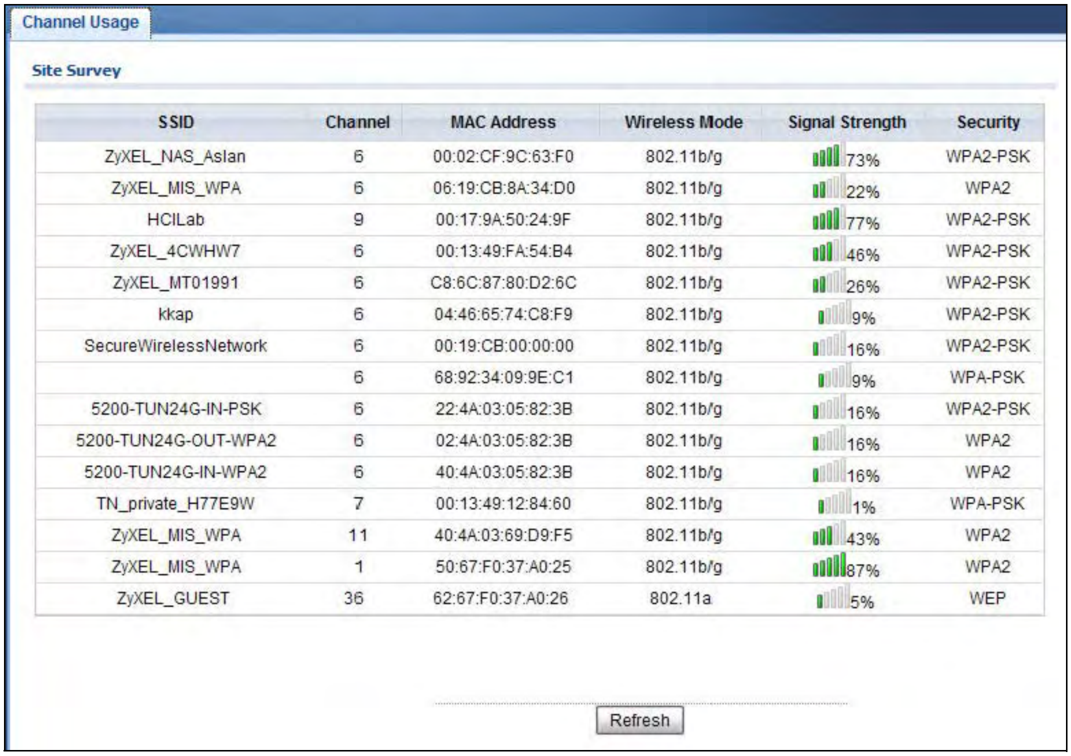
5.6 Channel Usage

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 NWA compiles the information.

Figure 18 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

The following table describes the labels in this screen.

Table 9 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.

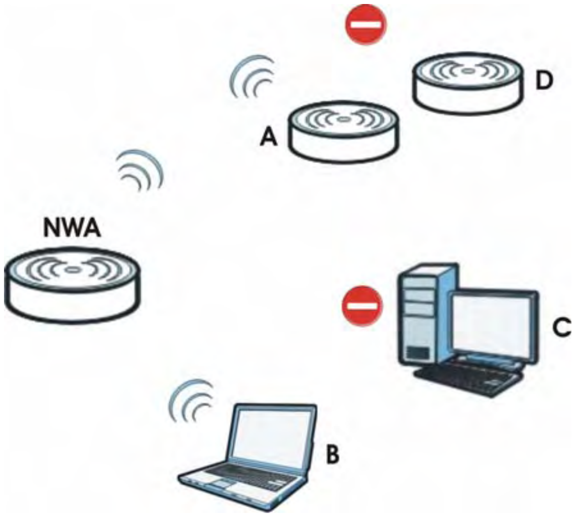
6

Wireless LAN

6.1 Overview

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

Figure 19 Wireless Mode



In the figure above, the NWA 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 NWA.

6.2 What You Can Do in this Chapter

- Use the **Wireless Settings** screen to configure the NWA's operation mode (see Section 6.4 on page 56).
- Use the **SSID** screen to configure up to eight SSID profiles for your NWA (see Section 6.5 on page 70).
- Use the **Security** screen to choose the wireless security mode for your NWA (see Section 6.6 on page 72).
- 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 78).
- Use the **Layer-2 Isolation** screen to configure the MAC addresses of the devices that you want to allow the associated wireless clients to have access to when layer-2 isolation is enabled. (see Section 6.8 on page 80).

- Use the **MAC Filter** screen to specify which wireless station is allowed or denied access to the NWA (see Section 6.9 on page 82).

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 NWA can run in four operating modes as follows:

- **Root AP**. The NWA is a wireless access point that allows wireless communication to other devices in the network.
- **Repeater**. The NWA acts as a wireless repeater and increase a root AP’s wireless coverage area.
- **Client**. The NWA 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 9 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 NWA acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the NWA 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 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.

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 NWA'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.

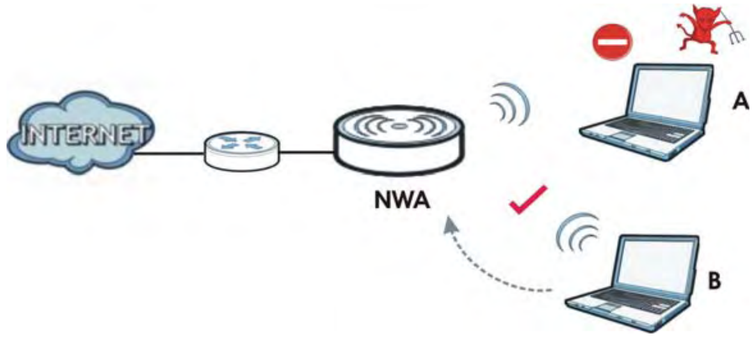
The following are some notes on multiple BSS.

- 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 20 Securing the Wireless Network



In the figure above, the NWA 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 NWA 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 10 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
Most Secure	WPA2

The available security modes in your NWA 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.
- **WPA2.** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management.
- **WPA2-MIX.** This commands the NWA to use either WPA2 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 NWA to use 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 NWA 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 NWA 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.

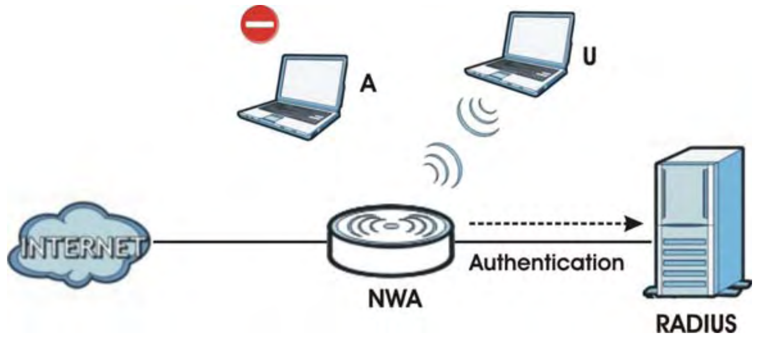
The EAP methods employed by the NWA when in Wireless Client operating mode are Transport Layer Security (TLS), Protected Extensible Authentication Protocol (PEAP), Lightweight Extensible Authentication Protocol (LEAP) and Tunneled Transport Layer Security (TTLS). The authentication protocol may either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

Further information on these terms can be found in Appendix E on page 178.

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 21 RADIUS Server Setup



In the figure above, wireless clients **A** and **B** are trying to access the Internet via the NWA. The NWA 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 NWA. You can configure a primary and backup RADIUS and RADIUS accounting server for your NWA.

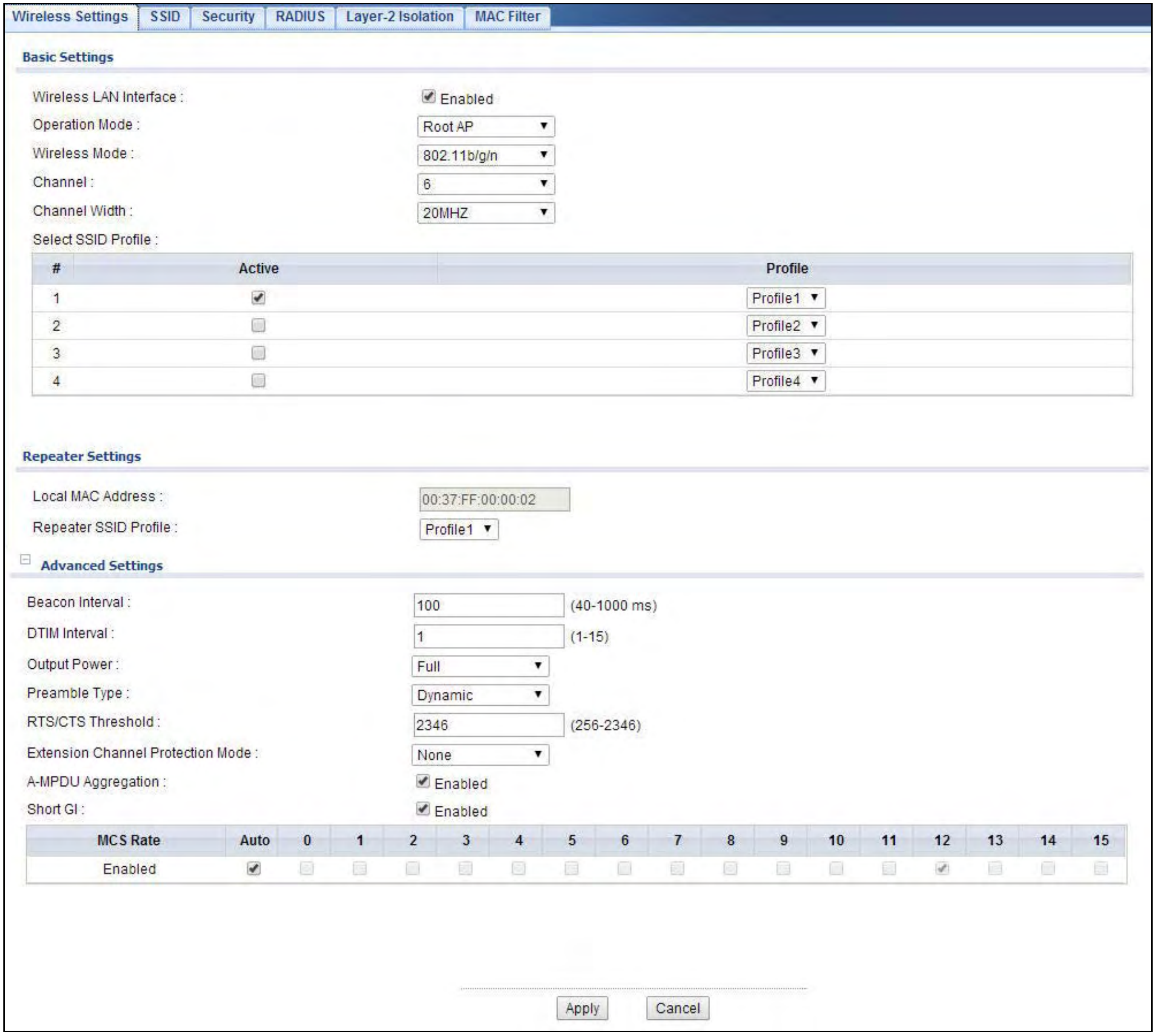
6.4 Wireless Settings Screen

Use this screen to choose the operating mode for your NWA. Click **Network > Wireless LAN > Wireless Settings**, **Network > Wireless LAN > Wireless Settings- 2.4G** or **Network > Wireless LAN > Wireless Settings - 5G**. The screen varies depending upon the operating mode you select.

6.4.1 Root AP Mode

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

Figure 22 Wireless LAN > Wireless Settings: Root AP



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
1	☑	Profile1
2	□	Profile2
3	□	Profile3
4	□	Profile4

Repeater Settings

Local MAC Address : 00:37:FF:00:00:02

Repeater SSID Profile : Profile1

Advanced Settings

Beacon Interval : 100 (40-1000 ms)

DTIM Interval : 1 (1-15)

Output Power : Full

Preamble Type : Dynamic

RTS/CTS Threshold : 2346 (256-2346)

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	☑	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□

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

Table 11 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 NWA.
Operation Mode	Select **Root AP** from the drop-down list.

Table 11 Wireless LAN > Wireless Settings: Root AP (continued)

LABEL	DESCRIPTION
Wireless Mode	If you are in the **Wireless LAN > Wireless Settings** or **Wireless LAN > Wireless Settings- 2.4G** screen, you can select from the following: • **802.11b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced. • **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA. The transmission rate of the NWA might be reduced. • **802.11n** to allow only IEEE802.11n compliant WLAN devices to associate with the NWA. If you are in the **Wireless LAN > Wireless Settings- 5G** screen, you can select from the following: • **802.11a/n** to allow IEEE802.11a and IEEE802.11n compliant WLAN devices to associate with the NWA. • **802.11a** to allow only IEEE802.11a compliant WLAN devices to associate with the NWA. • **802.11n** to allow only IEEE802.11n compliant WLAN devices to associate with the NWA. • **802.11a/n/ac** to allow IEEE802.11a, IEEE802.11n and IEEE802.11ac compliant WLAN devices to associate with the NWA. The transmission rate of the NWA might be reduced.
Channel	Select the operating frequency/channel depending on your particular region from the drop-down list box.
Channel Width	This field displays only when you select **802.11n**, **802.11a/n**, **802.11b/g/n** or **802.11a/n/ac** in the **Wireless Mode** field. 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. Select the channel bandwidth you want to use for your wireless network. It is recommended that you select **20/40MHz**. This allows the NWA to adjust the channel bandwidth depending on network conditions. 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.
Select SSID Profile	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. Note: If you are configuring the NWA from a computer connected to the wireless LAN and you change the NWA'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 NWA's new settings.
#	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.
Repeater Settings The repeater function allows the NWA in root AP or repeater mode to set up a wireless connection between it and another NWA in root AP or repeater mode. Note: Repeater security is independent of the security settings between the NWA and any wireless clients.	
Local MAC Address	**Local MAC Address** is the MAC address of your NWA.

Table 11 Wireless LAN > Wireless Settings: Root AP (continued)

LABEL	DESCRIPTION
Repeater SSID Profile	Select the SSID profile you want to use for repeater connections. Note: You can only configure **None**, or **WPA2-PSK** security mode for the SSID used by a repeater connection.
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 NWA in this field. If there is a high density of APs in an area, decrease the output power of the NWA 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 NWA'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.
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 **802.11n**, **802.11b/g/n**, **802.11a/n** or **802.11a/n/ac** 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 **802.11n**, **802.11b/g/n**, **802.11a/n** or **802.11a/n/ac** 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.

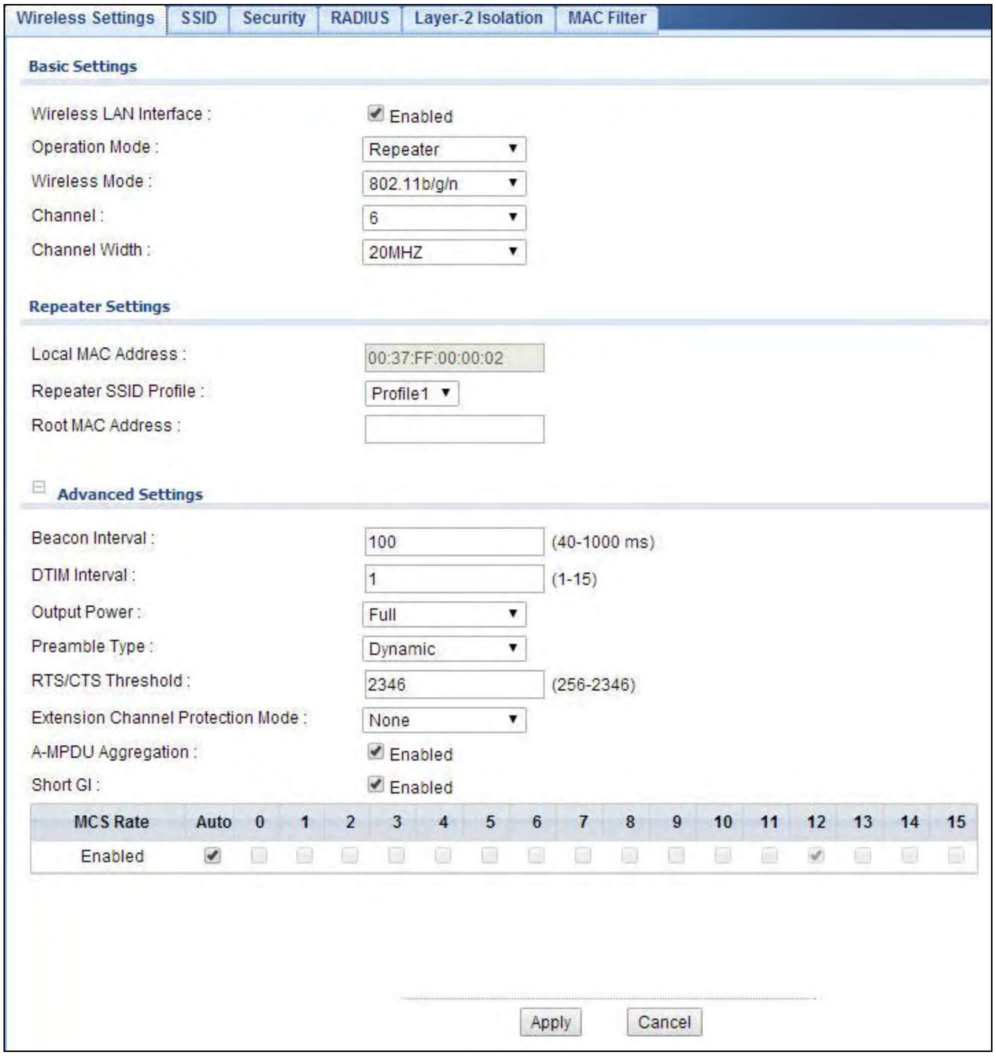
Table 11 Wireless LAN > Wireless Settings: Root AP (continued)

LABEL	DESCRIPTION
MCS Rate	The **MCS Rate** table is available only when **802.11n**, **802.11b/g/n**, **802.11a/n** or **802.11a/n/ac** 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 NWA use the data rate. Clear the **Enabled** check box if you do not want the NWA to use the data rate. Turn on the **Auto** option to have the NWA set the data rates automatically to optimize the throughput. Note: You can set the NWA 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 NWA 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 23 Wireless LAN > Wireless Settings: Repeater



Basic Settings

Wireless LAN Interface : ☑ Enabled

Operation Mode : Repeater

Wireless Mode : 802.11b/g/n

Channel : 6

Channel Width : 20MHZ

Repeater Settings

Local MAC Address : 00:37:FF:00:00:02

Repeater SSID Profile : Profile1

Root MAC Address :

Advanced Settings

Beacon Interval : 100 (40-1000 ms)

DTIM Interval : 1 (1-15)

Output Power : Full

Preamble Type : Dynamic

RTS/CTS Threshold : 2346 (256-2346)

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	☑	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□

The following table describes the bridge labels in this screen.

Table 12 Wireless LAN > Wireless Settings: Repeater

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

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

LABEL	DESCRIPTION
Wireless Mode	If you are in the **Wireless LAN > Wireless Settings** or **Wireless LAN > Wireless Settings- 2.4G** screen, you can select from the following: • **802.11b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced. • **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA. The transmission rate of the NWA might be reduced. • **802.11n** to allow only IEEE802.11n compliant WLAN devices to associate with the NWA. If you are in the **Wireless LAN > Wireless Settings- 5G** screen, you can select from the following: • **802.11a/n** to allow IEEE802.11a and IEEE802.11n compliant WLAN devices to associate with the NWA. • **802.11a** to allow only IEEE802.11a compliant WLAN devices to associate with the NWA. • **802.11n** to allow only IEEE802.11n compliant WLAN devices to associate with the NWA. • **802.11a/n/ac** to allow IEEE802.11a, IEEE802.11n and IEEE802.11ac compliant WLAN devices to associate with the NWA. The transmission rate of the NWA might be reduced.
Channel	Select the operating frequency/channel depending on your particular region from the drop-down list box.
Channel Width	This field displays only when you select **802.11n**, **802.11a/n**, **802.11b/g/n** or **802.11a/n/ac** in the **Wireless Mode** field. 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. Select the channel bandwidth you want to use for your wireless network. It is recommended that you select **20/40MHz**. This allows the NWA to adjust the channel bandwidth depending on network conditions. 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.
Repeater Settings The repeater function allows the NWA in root AP or repeater mode to set up a wireless connection between it and another NWA in root AP or repeater mode. Note: Repeater security is independent of the security settings between the NWA and any wireless clients.	
Local MAC Address	**Local MAC Address** is the MAC address of your NWA.
Repeater SSID Profile	Select the SSID profile you want to use for repeater connections with an AP or repeater or regular wireless connections with wireless clients. Note: You can only configure **None**, or **WPA2-PSK** security mode for the SSID used by a repeater connection.
Root MAC Address	Specify the peer device's MAC address. The peer device can be a NWA 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.

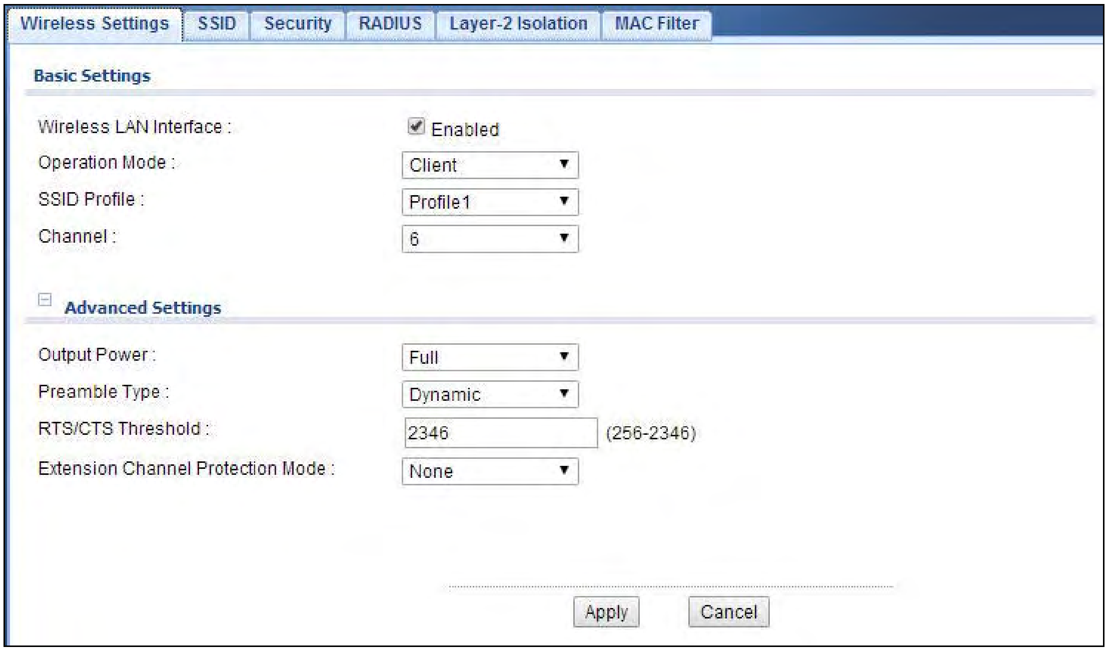
Table 12 Wireless LAN > Wireless Settings: Repeater (continued)

LABEL	DESCRIPTION
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 NWA in this field. If there is a high density of APs in an area, decrease the output power of the NWA 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 NWA'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.
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 **802.11n**, **802.11b/g/n**, **802.11a/n** or **802.11a/n/ac** 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 **802.11n**, **802.11b/g/n**, **802.11a/n** or **802.11a/n/ac** 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 **802.11n**, **802.11b/g/n**, **802.11a/n** or **802.11a/n/ac** 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 NWA use the data rate. Clear the **Enabled** check box if you do not want the NWA to use the data rate. Turn on the **Auto** option to have the NWA set the data rates automatically to optimize the throughput. Note: You can set the NWA 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.

6.4.3 Wireless Client Mode

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

Figure 24 Wireless LAN > Wireless Settings: Wireless Client



Basic Settings

Wireless LAN Interface : ☑ Enabled

Operation Mode : Client

SSID Profile : Profile1

Channel : 6

⊟ Advanced Settings

Output Power : Full

Preamble Type : Dynamic

RTS/CTS Threshold : 2346 (256-2346)

Extension Channel Protection Mode : None

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

Table 13 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 NWA.
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 13 Wireless LAN > Wireless Settings: Wireless Client (continued)

LABEL	DESCRIPTION
SSID Profile	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. In this field, select the SSID profile of the AP you want to use. Click **Apply**. The SSID used in the selected SSID profile automatically changes to be the one you select in the **Site Survey** screen. 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. Note: If you are configuring the NWA from a computer connected to the wireless LAN and you change the NWA'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 NWA's new settings.
Channel	This shows the operating frequency/channel in use. This field is read-only when you select **Client** as your operation mode.
Channel Width	This field is not available in the NWA1123-NI. 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. Select the channel bandwidth you want to use for your wireless network. It is recommended that you select **20/40MHz**. This allows the NWA to adjust the channel bandwidth depending on network conditions. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the AP do not support channel bonding.
Advanced Settings	
Output Power	Set the output power of the NWA in this field. If there is a high density of APs in an area, decrease the output power of the NWA 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 NWA's output power.
Preamble Type	Select **Dynamic** to have the NWA automatically use short preamble when the wireless network your NWA is connected to supports it, otherwise the NWA uses long preamble. Select **Long** preamble if you are unsure what preamble mode the wireless device your NWA is connected to supports, 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.
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 not available in the NWA1100-NH and NWA1123-NI. 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.

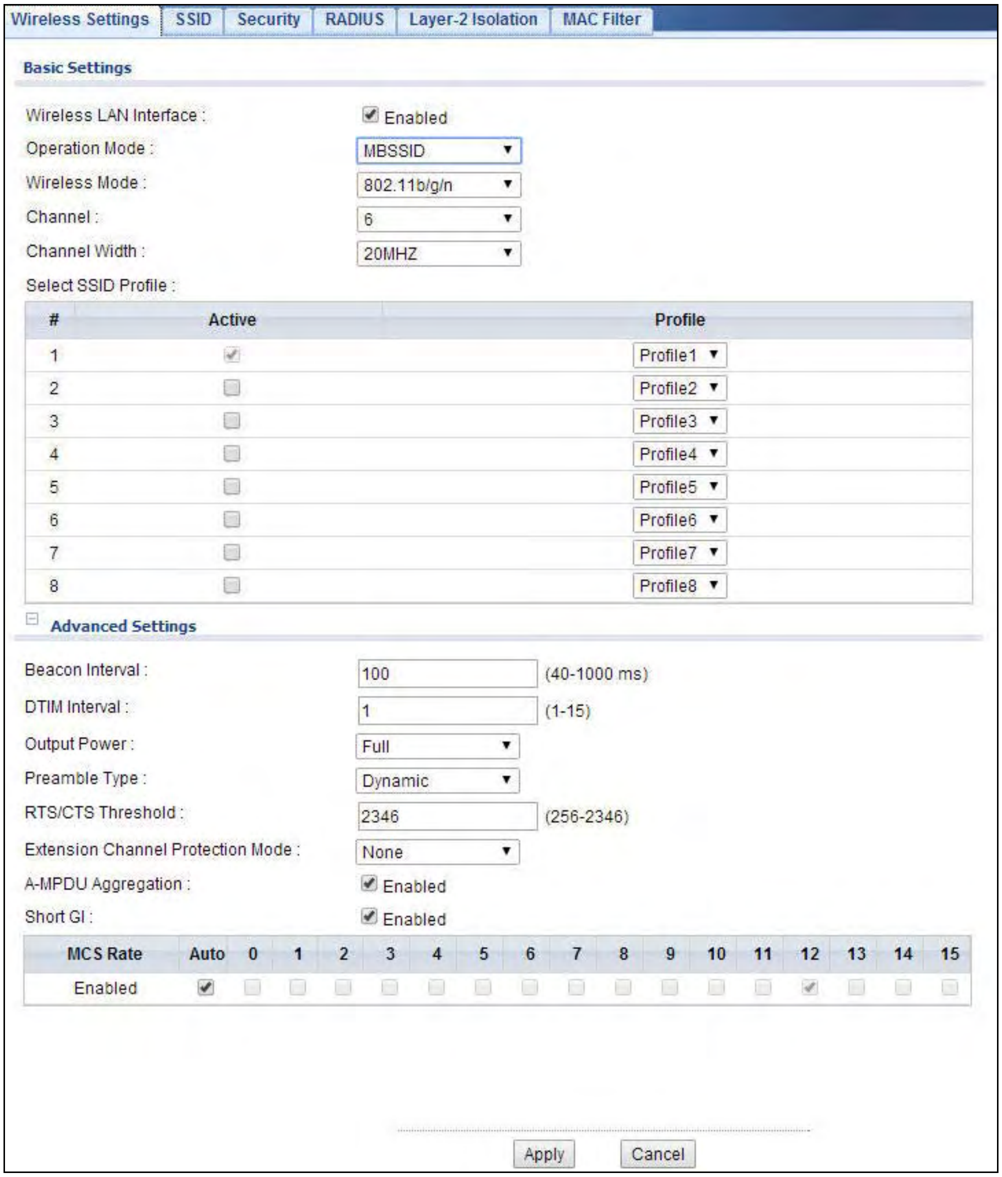
Table 13 Wireless LAN > Wireless Settings: Wireless Client (continued)

LABEL	DESCRIPTION
Short GI	This field is not available in the NWA1100-NH and NWA1123-NI. 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 NWA function in MBSSID mode. Select **MBSSID** as the **Operation Mode**. The following screen diplays.

Figure 25 Wireless LAN > Wireless Settings: MBSSID



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
1	☑	Profile1
2	□	Profile2
3	□	Profile3
4	□	Profile4
5	□	Profile5
6	□	Profile6
7	□	Profile7
8	□	Profile8

⊟ Advanced Settings

Beacon Interval : 100 (40-1000 ms)

DTIM Interval : 1 (1-15)

Output Power : Full

Preamble Type : Dynamic

RTS/CTS Threshold : 2346 (256-2346)

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	☑	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□

The following table describes the labels in this screen.

Table 14 Wireless LAN > Wireless Settings: MBSSID

LABEL	DESCRIPTION
Basic Settings	
Wireless LAN Interface	Select the check box to turn on the wireless LAN on the NWA.
Operation Mode	Select **MBSSID** from the drop-down list.

Table 14 Wireless LAN > Wireless Settings: MBSSID (continued)

LABEL	DESCRIPTION
Wireless Mode	If you are in the **Wireless LAN > Wireless Settings** or **Wireless LAN > Wireless Settings- 2.4G** screen, you can select from the following: • **802.11b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced. • **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NWA. The transmission rate of the NWA might be reduced. • **802.11n** to allow only IEEE802.11n compliant WLAN devices to associate with the NWA. If you are in the **Wireless LAN > Wireless Settings- 5G** screen, you can select from the following: • **802.11a/n** to allow IEEE802.11a and IEEE802.11n compliant WLAN devices to associate with the NWA. • **802.11a** to allow only IEEE802.11a compliant WLAN devices to associate with the NWA. • **802.11n** to allow only IEEE802.11n compliant WLAN devices to associate with the NWA. • **802.11a/n/ac** to allow IEEE802.11a, IEEE802.11n and IEEE802.11ac compliant WLAN devices to associate with the NWA. The transmission rate of the NWA might be reduced.
Channel	Select the operating frequency/channel depending on your particular region from the drop-down list box.
Channel Width	This field displays only when you select **802.11n**, **802.11a/n**, **802.11b/g/n** or **802.11a/n/ac** in the **Wireless Mode** field. 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. Select the channel bandwidth you want to use for your wireless network. 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.
Select SSID Profile	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. Note: If you are configuring the NWA from a computer connected to the wireless LAN and you change the NWA'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 NWA's new settings.
#	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 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 NWA in this field. If there is a high density of APs in an area, decrease the output power of the NWA 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 NWA's output power.

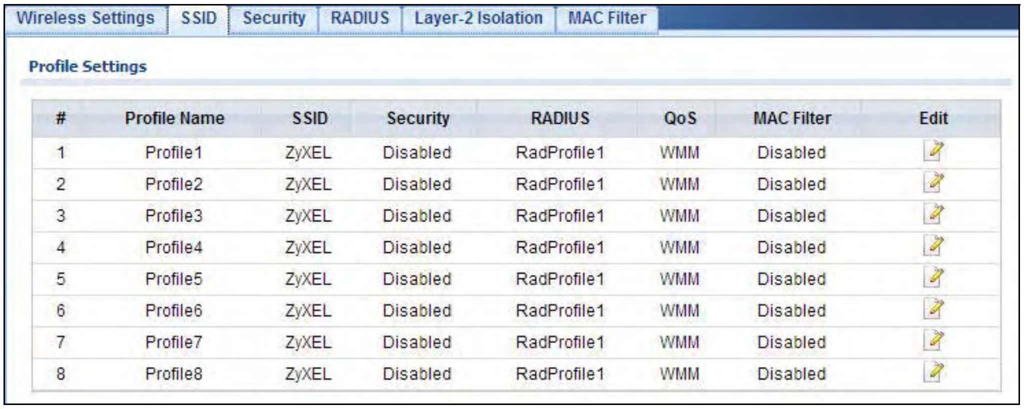
Table 14 Wireless LAN > Wireless Settings: MBSSID (continued)

LABEL	DESCRIPTION
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.
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 **802.11n**, **802.11b/g/n**, **802.11a/n** or **802.11a/n/ac** 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 **802.11n**, **802.11b/g/n**, **802.11a/n** or **802.11a/n/ac** 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 **802.11n**, **802.11b/g/n** or **802.11a/n** or **802.11a/n/ac** 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 NWA use the data rate. Clear the **Enabled** check box if you do not want the NWA to use the data rate. Turn on the **Auto** option to have the NWA set the data rates automatically to optimize the throughput. Note: You can set the NWA 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.

6.5 SSID Screen

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

Figure 26 Wireless LAN > SSID



Profile Settings

#	Profile Name	SSID	Security	RADIUS	QoS	MAC Filter	Edit
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	✎

The following table describes the labels in this screen.

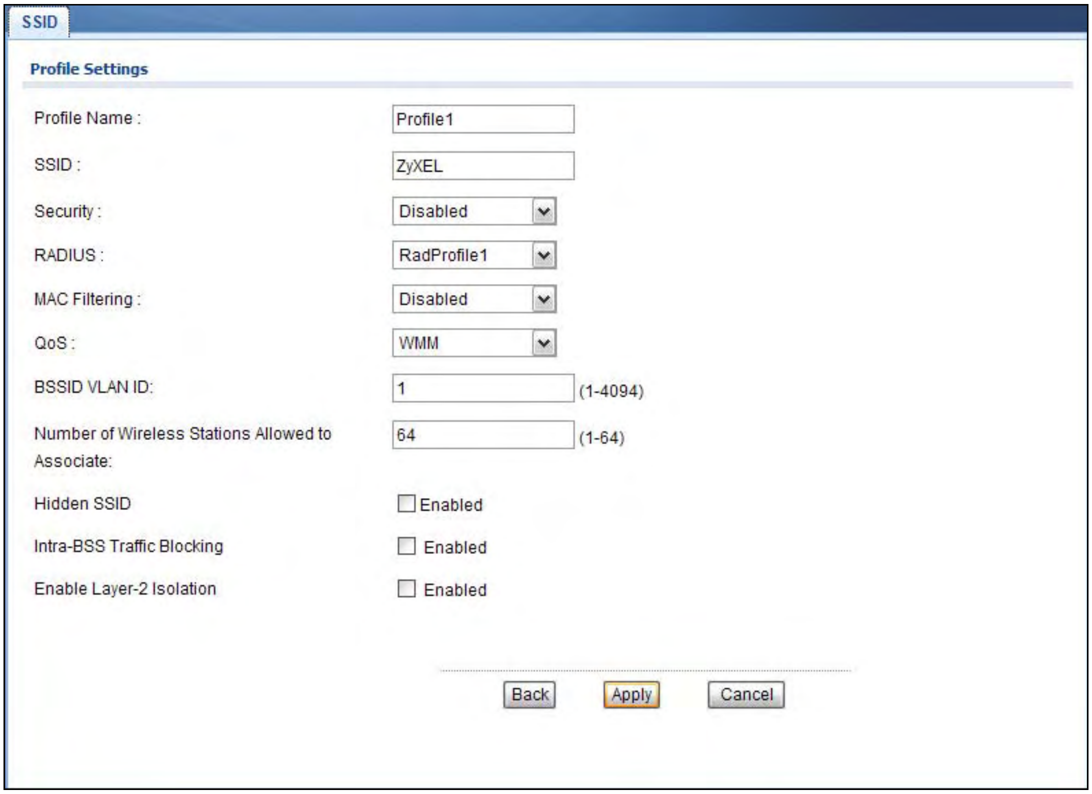
Table 15 Wireless LAN > SSID

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 NWA.
SSID	This field displays the SSID (Service Set IDentifier), that is, the name of the wireless network to which a wireless client can connect. 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 72 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.
Edit	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 27 SSID: Edit



Profile Settings

Profile Name : Profile1

SSID : ZyXEL

Security : Disabled

RADIUS : RadProfile1

MAC Filtering : Disabled

QoS : WMM

BSSID VLAN ID: 1 (1-4094)

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

Hidden SSID □ Enabled

Intra-BSS Traffic Blocking □ Enabled

Enable Layer-2 Isolation □ Enabled

The following table describes the labels in this screen.

Table 16 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 72 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 78 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**.

Table 16 SSID: Edit (continued)

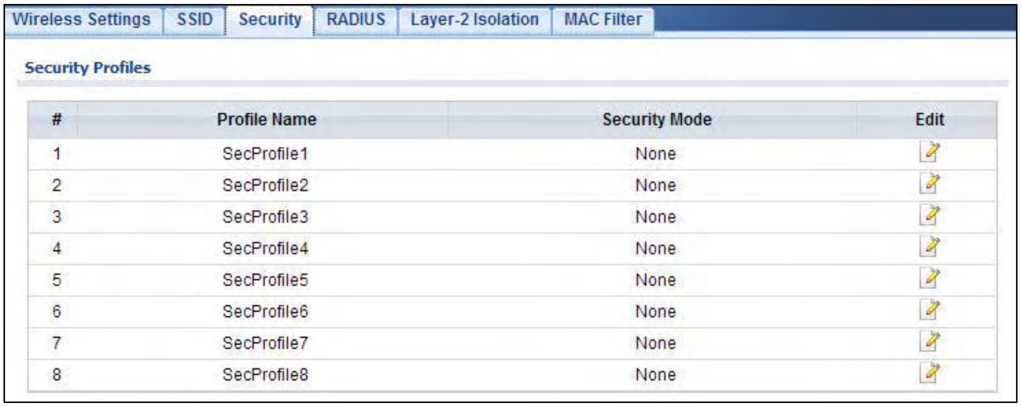
LABEL	DESCRIPTION
QoS	Select the Quality of Service priority for this BSS's traffic. • If you select **WMM** from the QoS list, the priority of a data packet depends on the packet's IEEE 802.1q or DSCP header. If a packet has no WMM value assigned to it, it is assigned the default priority. • If you select **WMM_VOICE**, **WMM_VIDEO**, **WMM_BESTEFFORT** or **WMM_BACKGROUND**, the NWA applies that QoS setting to all of that SSID's traffic. • If you select **None**, the NWA applies no priority to traffic on this SSID. Note: When you configure an SSID profile's QoS settings, the NWA applies the same QoS setting to all of the profile's traffic.
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 NWA.
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 NWA broadcasts this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, if you select the checkbox, the NWA hides this SSID (a wireless client scanning for an AP will not find this SSID).
Intra-BSS Traffic Blocking	Select this to prevent wireless clients in this profile's BSS from communicating with one another.
Enable Layer-2 Isolation	Select this to enable layer-2 isolation for this profile. Wireless clients that connect to the WLAN using this SSID can access only certain pre-defined devices. See Section 6.8 on page 80. Intra-BSS traffic blocking is enabled automatically when you enable layer-2 isolation.
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 NWA.

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

Figure 28 Wireless > Security

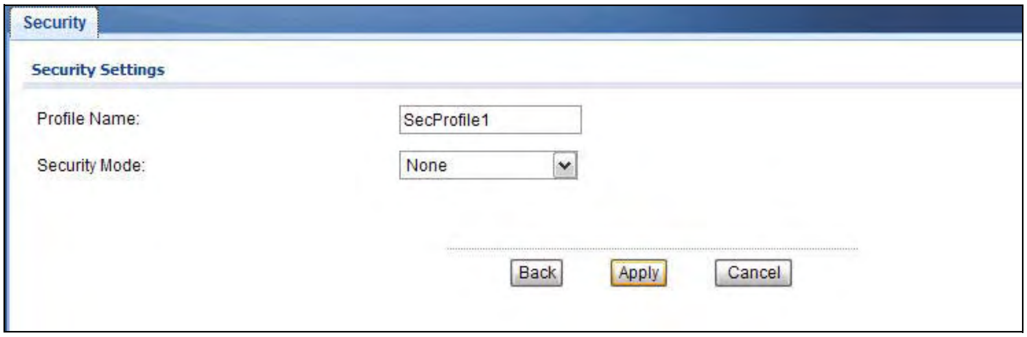


Security Profiles

#	Profile Name	Security Mode	Edit
1	SecProfile1	None	✎
2	SecProfile2	None	✎
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 29 Security: None



Security Settings

Profile Name: SecProfile1

Security Mode: None

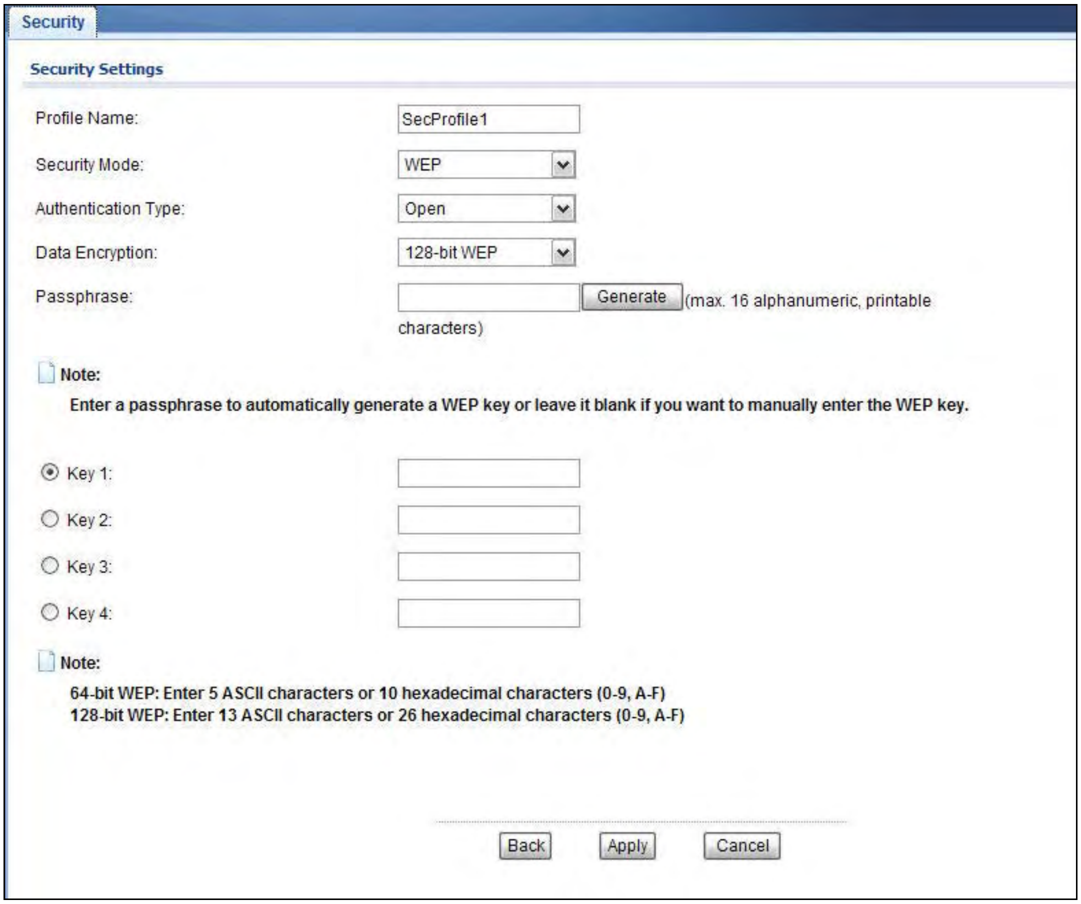
Note that some screens display differently depending on the operating mode selected in the **Wireless LAN > Wireless Settings**, **Network > Wireless LAN > Wireless Settings- 2.4G** or **Network > Wireless LAN > Wireless Settings - 5G** screen.

Note: You must enable the same wireless security settings on the NWA 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 NWA. Select **WEP** in the **Security Mode** field to display the following screen.

Figure 30 Security: WEP



Profile Name: SecProfile1

Security Mode: WEP

Authentication Type: Open

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)

The following table describes the labels in this screen.

Table 17 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 17 Security: WEP (continued)

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NWA and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You can configure up to four keys, but only one key can be activated at any one time.
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.

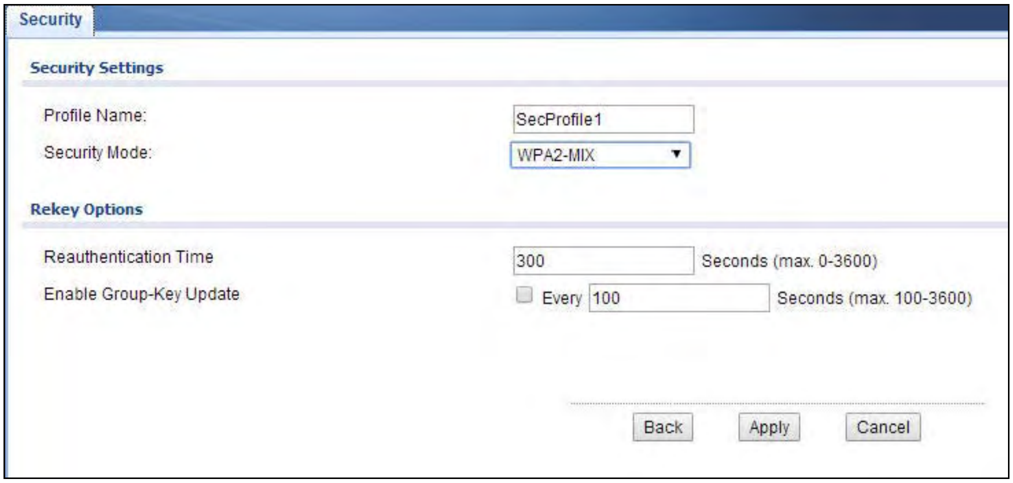
6.6.2 Security: WPA2, WPA2-MIX

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

Figure 31 Security: WPA2-MIX for Access Point



Security Settings

Profile Name: SecProfile1

Security Mode: WPA2-MIX

Rekey Options

Reauthentication Time 300 Seconds (max. 0-3600)

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

The following table describes the labels in this screen.

Table 18 Security: WPA2-MIX for Access Point

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose **WPA2** or **WPA2-MIX** in this field.
Rekey Options	

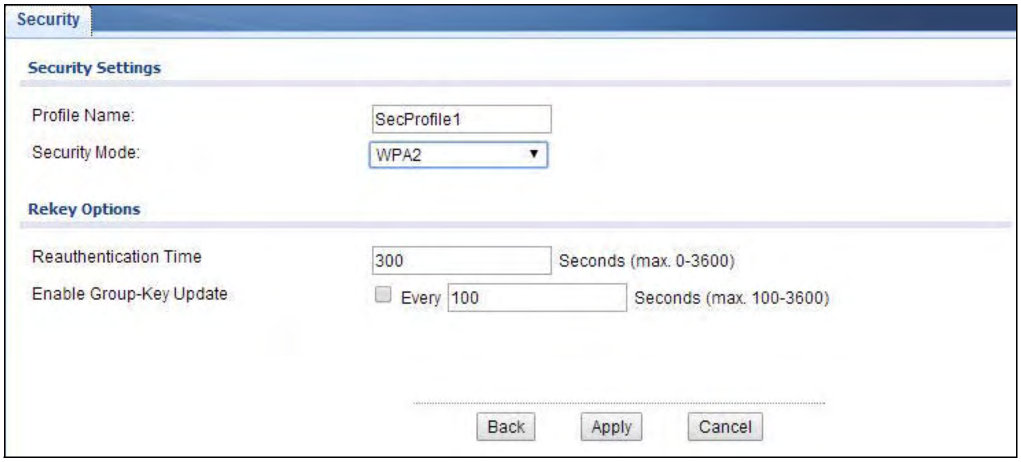
Table 18 Security: WPA2-MIX for Access Point (continued)

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 0 and 3600 seconds. 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	Group Key Timer is the rate at which the RADIUS server sends a new group key out to all clients. Click the check box to enable the **Group Key Update** and type a number between 100 and 3600 for the **time** rate.
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 employ WPA2 as the security mode for your NWA that is in wireless client operating mode. Select **WPA2** in the **Security Mode** field to display the following screen.

Figure 32 Security: WPA2 for Wireless Client



Security Settings

Profile Name: SecProfile1

Security Mode: WPA2

Rekey Options

Reauthentication Time 300 Seconds (max. 0-3600)

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

The following table describes the labels in this screen.

Table 19 Security: WPA2 for Wireless Client

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

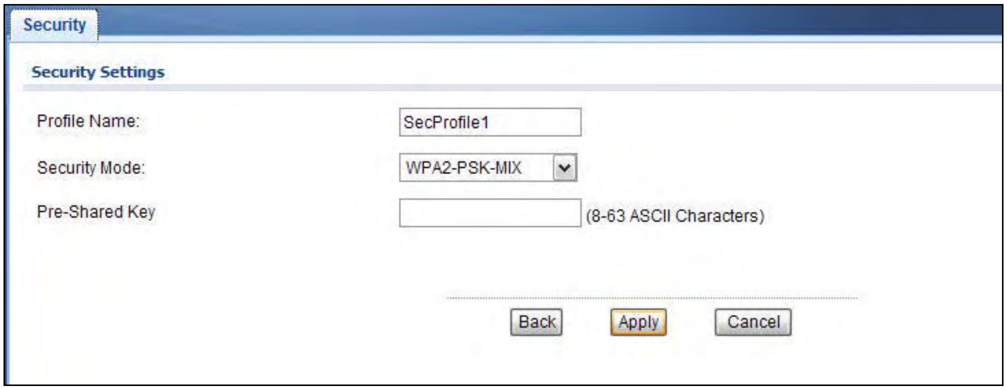
Table 19 Security: WPA2 for Wireless Client (continued)

LABEL	DESCRIPTION
Security Mode	Choose the same security mode used by the AP.
Rekey Option	
Reauthentication Time	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 0 and 3600 seconds. Enter "0" to turn reauthentication off. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.Enter how often the external authentication server requires a connected wireless client to reauthenticate itself to the server again.
Enable Group-key Update	Group Key Timer is the rate at which the RADIUS server sends a new group key out to all clients. Click the check box to enable the **Group Key Update** and type a number between 100 and 3600 for the **time** rate.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.6.3 Security: WPA2-PSK, WPA2-PSK-MIX

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

Figure 33 Security: WPA2-PSK or WPA2-PSK-MIX



Profile Name: SecProfile1

Security Mode: WPA2-PSK-MIX

Pre-Shared Key (8-63 ASCII Characters)

The following table describes the labels not previously discussed

Table 20 Security: WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Profile Name	This is the name that identifying this profile.
Security Mode	Choose **WPA2-PSK** or **WPA2-PSK-MIX** in this field.
Pre-Shared Key	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

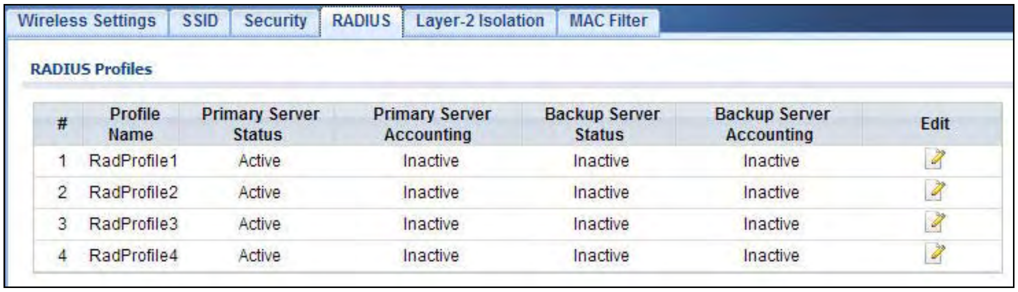
Table 20 Security: WPA2-PSK or WPA2-PSK-MIX (continued)

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.

6.7 RADIUS Screen

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

Figure 34 Wireless LAN > RADIUS

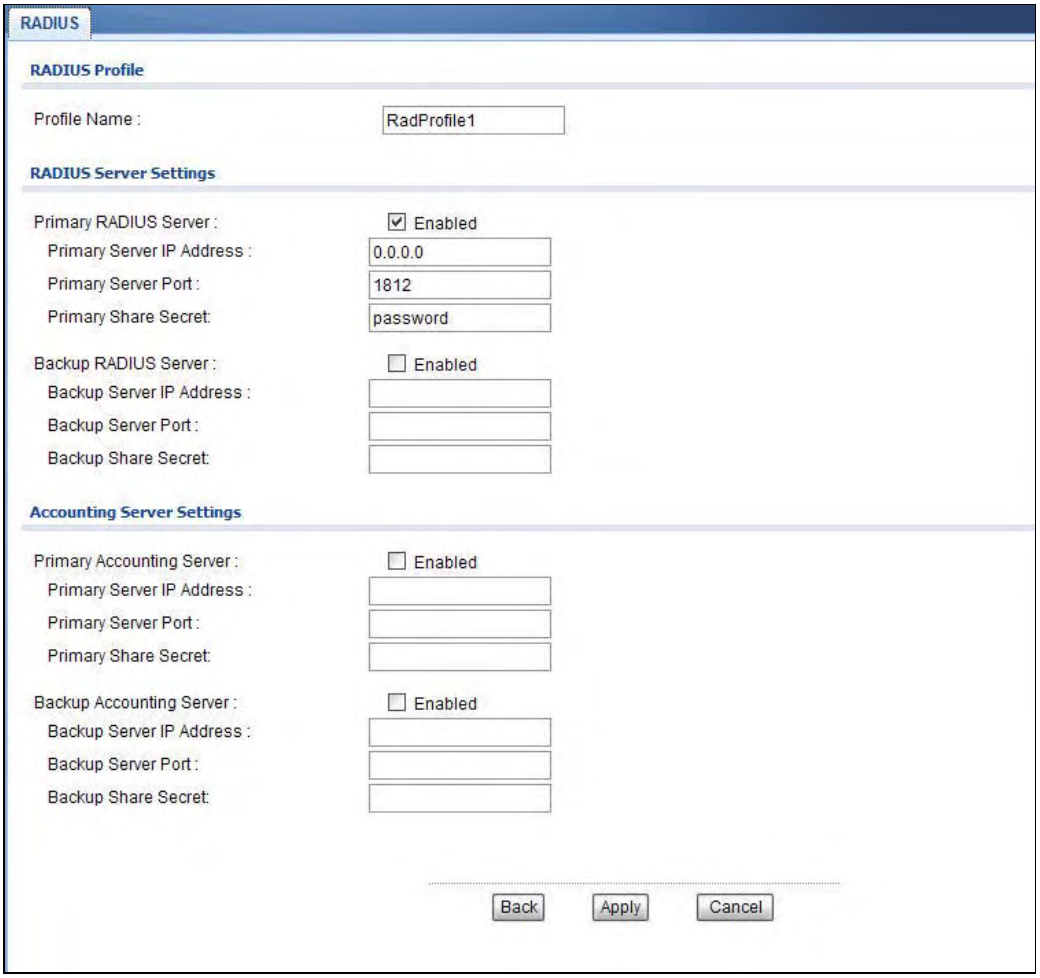


RADIUS Profiles

#	Profile Name	Primary Server Status	Primary Server Accounting	Backup Server Status	Backup Server Accounting	Edit
1	RadProfile1	Active	Inactive	Inactive	Inactive	✎
2	RadProfile2	Active	Inactive	Inactive	Inactive	✎
3	RadProfile3	Active	Inactive	Inactive	Inactive	✎
4	RadProfile4	Active	Inactive	Inactive	Inactive	✎

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

Figure 35 Wireless LAN > 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:

The following table describes the labels in this screen.

Table 21 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 64 alphanumeric characters) as the key to be shared between the external authentication server and the NWA. The key must be the same on the external authentication server and your NWA. The key is not sent over the network.

Table 21 Wireless LAN > RADIUS (continued)

LABEL	DESCRIPTION
Backup RADIUS Server	If the NWA cannot communicate with the primary RADIUS server, you can have the NWA use a backup RADIUS server. Make sure the check box is selected if you want to use the backup server. The NWA 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.
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 64 alphanumeric characters) as the key to be shared between the external authentication server and the NWA. The key must be the same on the external authentication server and your NWA. 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 64 alphanumeric characters) as the key to be shared between the external accounting server and the NWA. The key must be the same on the external accounting server and your NWA. The key is not sent over the network.
Backup Accounting Server	If the NWA cannot communicate with the primary accounting server, you can have the NWA use a backup accounting server. Make sure the check box is selected if you want to use the backup server. The NWA will attempt to communicate three times before using the backup server.
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 64 alphanumeric characters) as the key to be shared between the external accounting server and the NWA. The key must be the same on the external accounting and your NWA. The key is not sent over the network.
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.

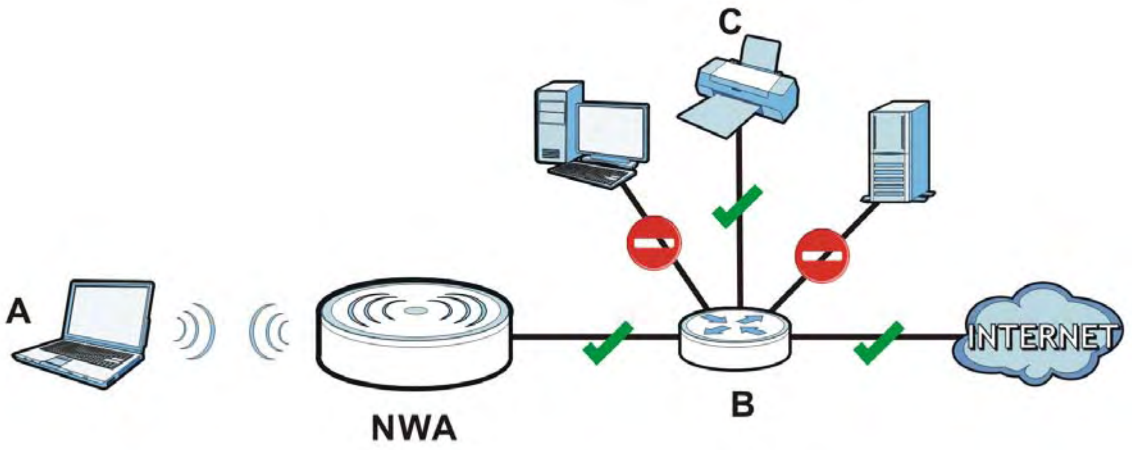
6.8 Layer-2 Isolation

Layer-2 isolation is used to prevent wireless clients associated with your NWA from communicating with other wireless clients, APs, computers or routers in a network.

In the following example, layer-2 isolation is enabled on the NWA to allow a guest wireless client (**A**) to access the main network router (**B**). The router provides access to the Internet and the network printer (**C**) while preventing the client from accessing other computers and servers on the network. The client can communicate with other wireless clients only if Intra-BSS Traffic blocking is disabled.

Note: **Intra-BSS Traffic Blocking** is activated when you enable layer-2 isolation.

Figure 36 Layer-2 Isolation Application



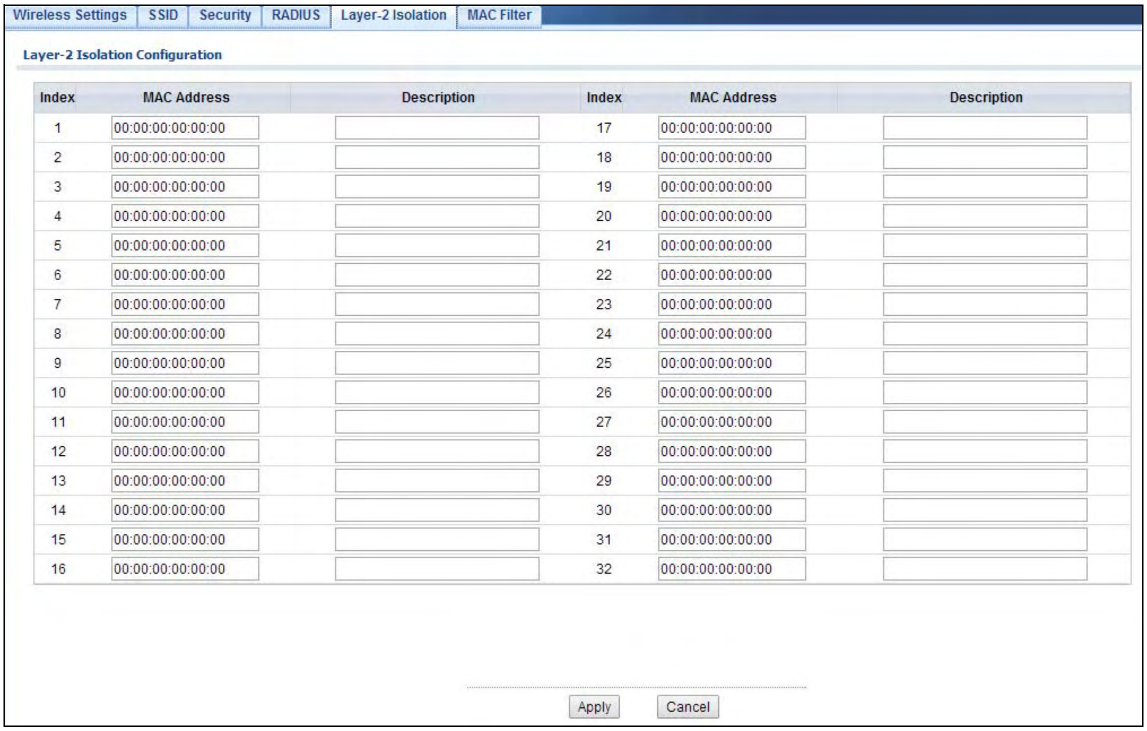
MAC addresses that are not listed in the layer-2 isolation table are blocked from communicating with the NWA's wireless clients except for broadcast packets. Layer-2 isolation does not check the traffic between wireless clients that are associated with the same AP. Intra-BSS Traffic allows wireless clients associated with the same AP to communicate with each other.

6.8.1 Layer-2 Isolation Screen

Use this screen to specify devices you want the users on your wireless networks to access. Click **Wireless LAN > Layer-2 Isolation**. The screen displays as shown.

Note: You need to know the MAC address of each wireless client, AP, computer or router that you want to allow to communicate with the NWA's wireless clients.

Figure 37 Wireless LAN > Layer-2 Isolation



Layer-2 Isolation Configuration

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

The following table describes the labels in this screen.

Table 22 Wireless LAN > Layer-2 Isolation

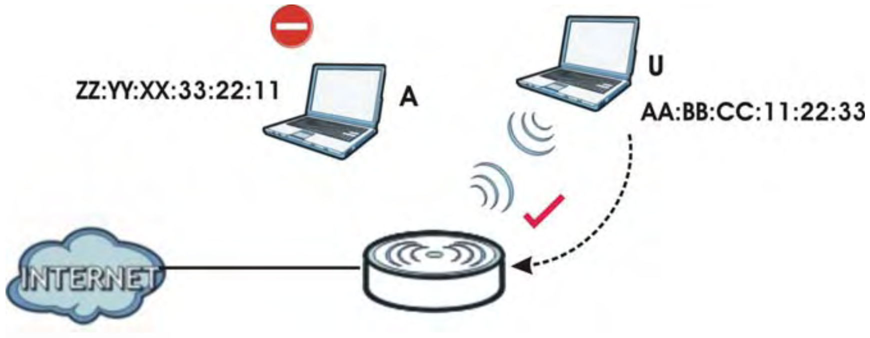
LABEL	DESCRIPTION
Index	This is the index number of the MAC address listed.
MAC Address	Enter the MAC addresses of the wireless client, AP, computer or router that you want to allow the associated wireless clients to have access to in these address fields. Enter the MAC address in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).
Description	Enter a name to identify this device.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.9 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 NWA.

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

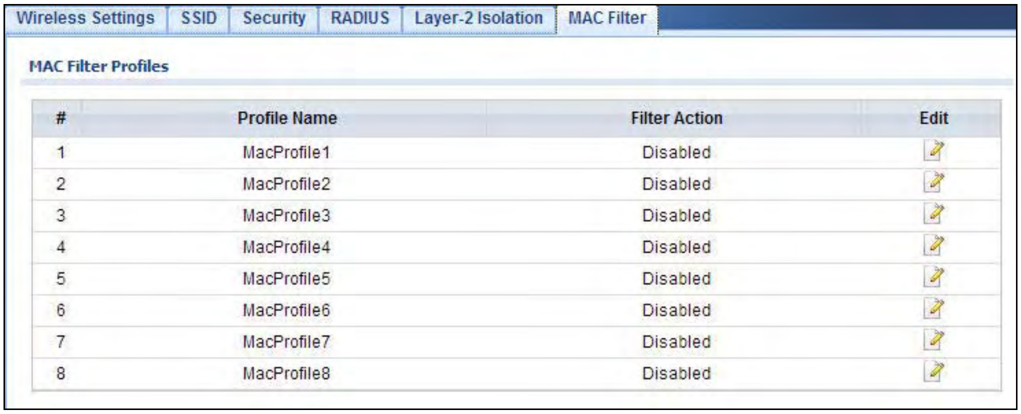
Figure 38 MAC Filtering



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 NWA. The MAC address of client A is either denied association or is not in the list of allowed wireless clients specified in the NWA.

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

Figure 39 Wireless LAN > MAC Filter

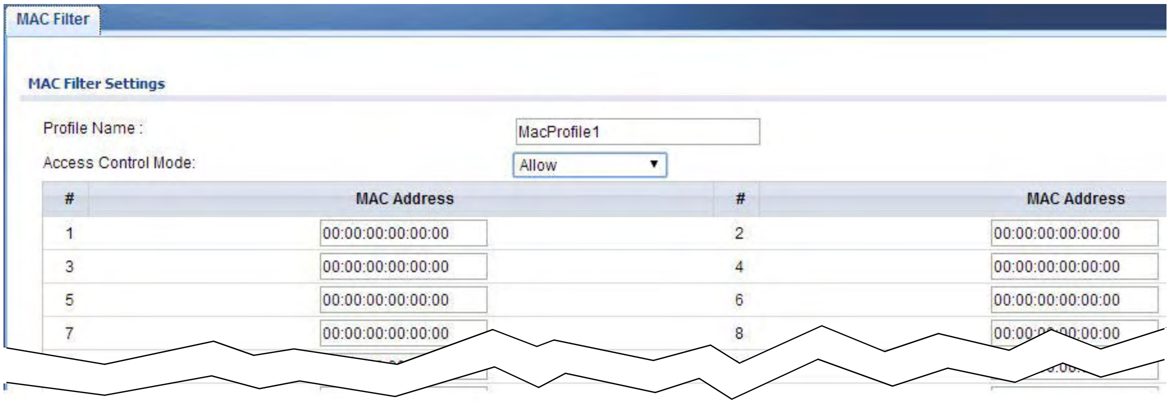


MAC Filter Profiles

#	Profile Name	Filter Action	Edit
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 40 MAC Filter: Edit



MAC Filter Settings

Profile Name : MacProfile1

Access Control Mode: Allow ▾

#	MAC Address	#	MAC Address
1	00:00:00:00:00:00	2	00:00:00:00:00:00
3	00:00:00:00:00:00	4	00:00:00:00:00:00
5	00:00:00:00:00:00	6	00:00:00:00:00:00
7	00:00:00:00:00:00	8	00:00:00:00:00:00

The following table describes the labels in this screen.

Table 23 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 NWA. MAC addresses not listed will be denied access to the NWA. Select **Deny** to block access to theNWA. MAC addresses not listed will be allowed to access the NWA.
#	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 NWA.
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.

6.10 Technical Reference

This section provides technical background information about the topics covered in this chapter. Refer to Appendix E on page 178 for further readings on Wireless LAN.

6.10.1 Additional Wireless Terms

Table 24 Additional Wireless Terms

TERM	DESCRIPTION
Intra-BSS Traffic	This describes direct communication (not through the NWA) 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 NWA. The lower the value, the more often the devices must get permission.
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 NWA does, it cannot communicate with the NWA.

TERM	DESCRIPTION
Roaming	If you have two or more NWAs (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.

6.10.2 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 NWA uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q or DSCP information in each packet's header. The NWA 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).

6.10.2.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the NWA uses.

Table 25 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.

6.10.3 Security Mode Guideline

The following is a general guideline in choosing the security mode for your NWA.

- Use WPA2-PSK if you have WPA2-aware wireless clients but no RADIUS server.
- Use WPA2 security if you have WPA2-aware wireless clients and a RADIUS server. WPA2 has user authentication and improved data encryption over WEP.
- If you don't have WPA2-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 E on page 178.

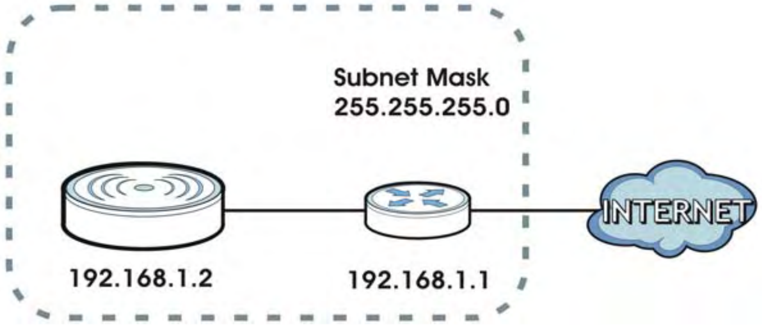
LAN and VLAN

7.1 LAN Overview

This chapter describes how you can configure the IP address of your NWA.

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 41 IPv4 Setup



The figure above illustrates one possible setup of your NWA. The gateway IPv4 address is 192.168.1.1 and the IPv4 address of the NWA 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 the LAN IP Screen

Use the **LAN IP** screen to configure the IP address of your NWA (see Section 7.6 on page 90).

7.3 What You Need to Know

The Ethernet parameters of the NWA 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 x 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 26 Link-local Unicast Address Format

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

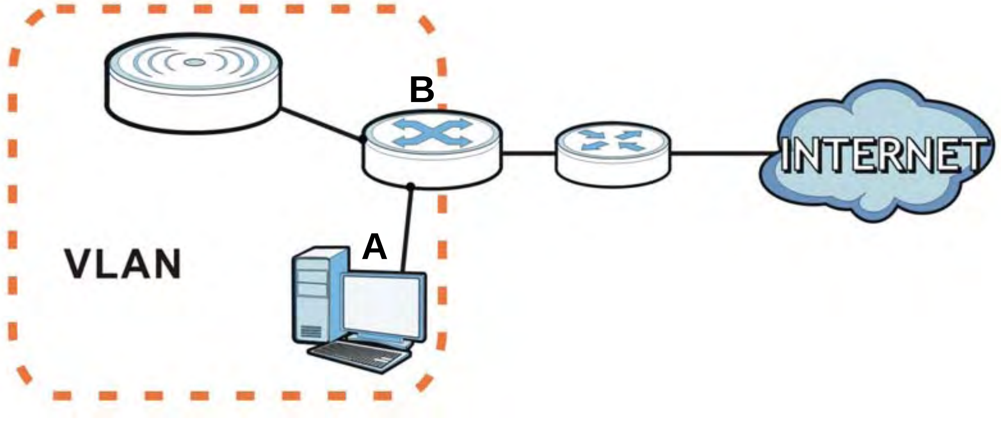
Global Address

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 VLAN Overview

This section discusses how to configure the NWA's VLAN settings.

Figure 42 Management VLAN Setup



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

7.5 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.

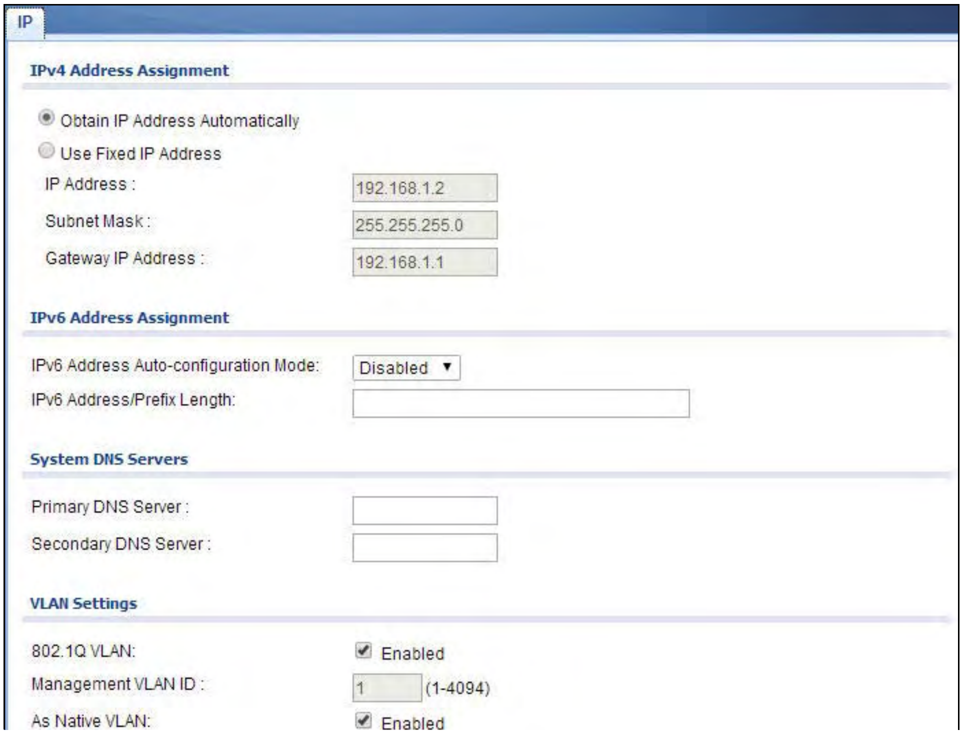
IEEE 802.1Q Tag

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.

7.6 LAN IP Screen

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

Figure 43 LAN IP



IPv4 Address Assignment

● Obtain IP Address Automatically
○ Use Fixed IP Address
IP Address : 192.168.1.2
Subnet Mask : 255.255.255.0
Gateway IP Address : 192.168.1.1

IPv6 Address Assignment

IPv6 Address Auto-configuration Mode: Disabled ▼
IPv6 Address/Prefix Length:

System DNS Servers

Primary DNS Server :
Secondary DNS Server :

VLAN Settings

802.1Q VLAN: ☑ Enabled
Management VLAN ID : 1 (1-4094)
As Native VLAN: ☑ Enabled

The following table describes the labels in this screen.

Table 27 LAN IP

LABEL	DESCRIPTION
IPv4 Address Assignment	
Obtain IP Address Automatically	Select this option if your NWA is using a dynamically assigned IPv4 address from a DHCP server each time. Note: You must know the IP address assigned to the NWA (by the DHCP server) to access the NWA again.
Use Fixed IP Address	Select this option if your NWA is using a static IPv4 address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your NWA in dotted decimal notation. Note: If you change the NWA'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 NWA that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NWA; over the WAN, the gateway must be the IP address of one of the remote nodes.

Table 27 LAN IP (continued)

LABEL	DESCRIPTION
IPv6 Address Assignment	
Enable Stateful Address Auto-configuration	Select this to turn on IPv6 stateful auto-configuration to have the NWA 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.
VLAN Settings	
802.1q VLAN	Select this to enable VLAN tagging on the NWA.
Management VLAN ID	Enter a number from 1 to 4094 to define the NWA's management VLAN group.
As Native VLAN	Click this check box to enable As Native VLAN. If enabled, only untagged packets may access to the CPU of NWA. If disabled, only tagged packets shall be forwarded to the matched VLAN. Select this check box to treat this VLAN ID as a VLAN created on the NWA and not one assigned to it from outside the network.
Green Ethernet	
Energy Efficient Ethernet (EEE)	Click the check box to enable Energy-Efficient Ethernet (EEE). When enabled, it turns on power saving mode. If disabled, only tagged packets with matched VLAN-ID may access the NWA.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8

System

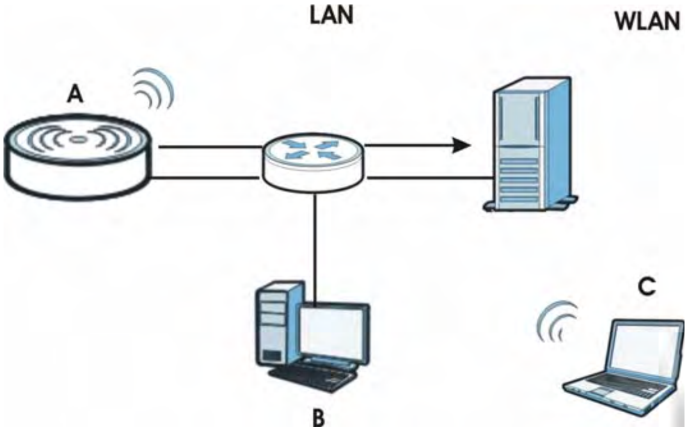
8.1 Overview

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

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

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

Figure 44 Remote Management Example



In the figure above, the NWA (**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).

8.2 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 NWA (see Section 8.4 on page 95).
- Use the **Certificates** screen to delete and import certificates (seen Section 8.5 on page 96).
- Use the **Telnet** screen to configure through which interface(s) and from which IP address(es) you can use Telnet to manage the NWA. A Telnet connection is prioritized by the NWA over other remote management sessions (see Section 8.6 on page 97).

- Use the **SNMP** screen to configure through which interface(s) and from which IP address(es) a network systems manager can access the NWA (see Section 8.7 on page 99).
- 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 NWA. You can use FTP to upload the latest firmware for example (see Section 8.8 on page 101).

8.3 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.

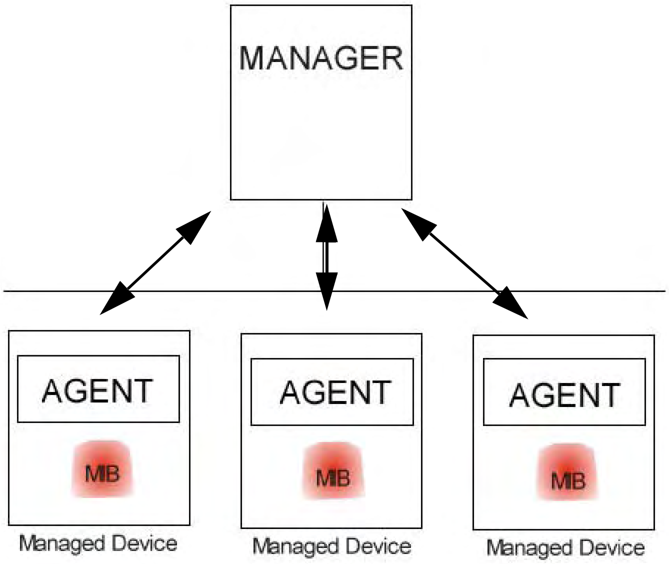
SNMP

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

Your NWA supports SNMP agent functionality, which allows a manager station to manage and monitor the NWA through the network. The NWA supports SNMP version one (SNMPv1), version two (SNMPv2c) and version three (SNMPv3).

The next figure illustrates an SNMP management operation.

Figure 45 SNMP Management Mode



A 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 NWA). 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 NWA will disconnect the session immediately.
- You may only have one remote management session running at one time. The NWA 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:

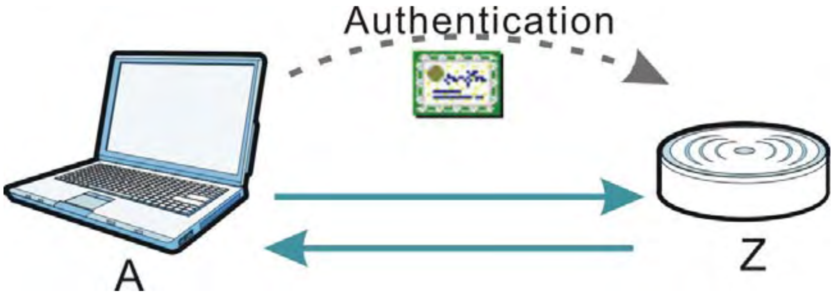
1 Telnet

2 HTTP

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 46 Certificates Example



In the figure above, the NWA (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 NWA 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 NWA, you should verify that you have the correct certificate.

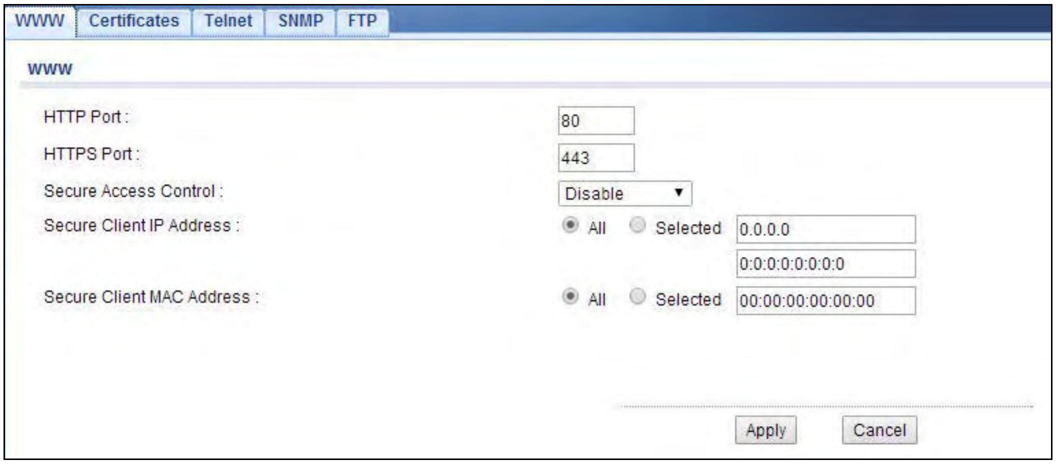
Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

8.4 WWW Screen

Use this screen to configure your NWA 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 NWA.

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

Figure 47 System > WWW



WWW

HTTP Port : 80

HTTPS Port : 443

Secure Access Control : Disable

Secure Client IP Address : ● All ○ Selected 0.0.0.0
0:0:0:0:0:0:0:0

Secure Client MAC Address : ● All ○ Selected 00:00:00:00:00:00

The following table describes the labels in this screen.

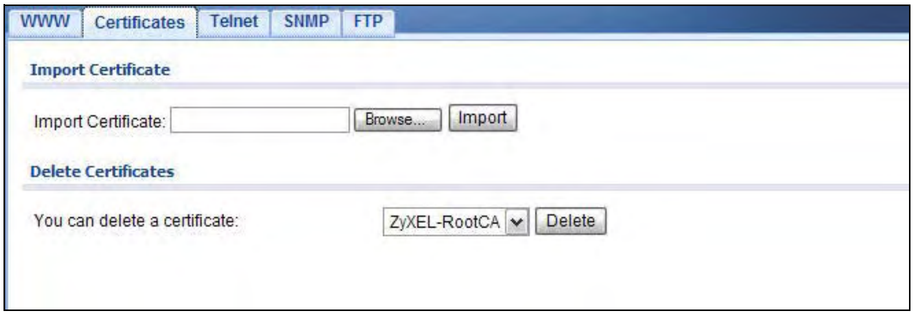
Table 28 System > WWW

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 NWA, for example 8443, then you must notify people who need to access the NWA web configurator to use "https://NWA IP Address:8443" as the URL.
Secure Access Control	Select the interface(s) through which a computer may access the NWA using WWW and to which the IP and MAC filtering rules you specified below are applied. Otherwise, select **Disable** to allow any computer to access the NWA through any interface using WWW.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NWA using this service. Select **All** to allow any computer to access the NWA using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NWA using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the NWA using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the NWA using this service.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.5 Certificates Screen

Use this screen to delete or import certificates.

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



Import Certificate

Import Certificate:

Delete Certificates

You can delete a certificate: ZyXEL-RootCA

Figure 48 System > Certificates

The following table describes the labels in this screen.

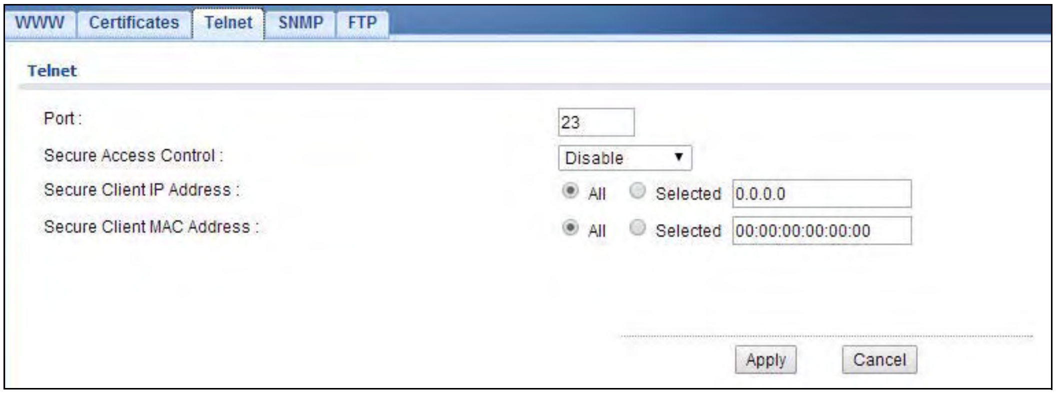
Table 29 System > Certificates

LABEL	DESCRIPTION
Import Certificate	
Import Certificate	Enter the location of a previously-saved certificate to upload to the NWA. Alternatively, click the **Browse** button to locate a list.
Browse	Click this button to locate a previously-saved certificate to upload to the NWA.
Import	Click this button to upload the previously-saved certificate displayed in the **Import Certificate** field to the NWA.
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.

8.6 Telnet Screen

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

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



Telnet

Port : 23

Secure Access Control : Disable

Secure Client IP Address : ● All ○ Selected 0.0.0.0

Secure Client MAC Address : ● All ○ Selected 00:00:00:00:00:00

Figure 49 System > Telnet

The following table describes the labels in this screen.

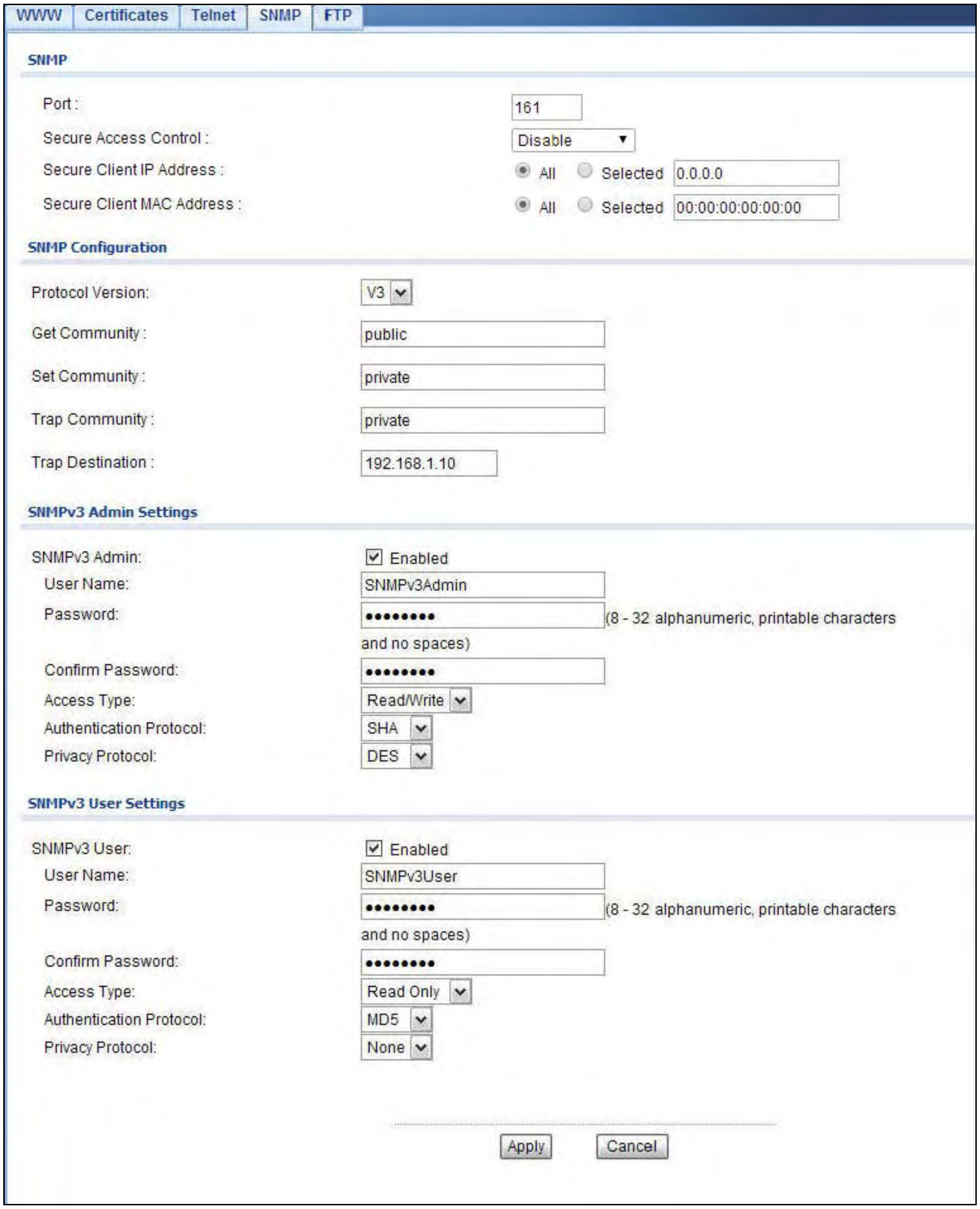
Table 30 System > Telnet

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.
Secure Access Control	Select the interface(s) through which a computer may access the NWA using Telnet and to which the IP and MAC filtering rules you specified below are applied. Otherwise, select **Disable** to allow any computer to access the NWA through any interface using Telnet.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the NWA using this service. Select **All** to allow any computer to access the NWA using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NWA using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the NWA using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the NWA using this service.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.7 SNMP Screen

Use this screen to have a manager station administrate your NWA over the network and configure SNMP accounts on the SNMP v3 manager. A SNMP administrator/user is a SNMP manager. To change your NWA's SNMP settings, click **System** > **SNMP**. The following screen displays.

Figure 50 System > SNMP



SNMP

Port : 161

Secure Access Control : Disable

Secure Client IP Address : ● All ○ Selected 0.0.0.0

Secure 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

The following table describes the labels in this screen.

Table 31 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.
Secure Access Control	Select the interface(s) through which a computer may access the NWA using SNMP and to which the IP and MAC filtering rules you specified below are applied. Otherwise, select **Disable** to allow any computer to access the NWA through any interface using SNMP.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the NWA using this service. Select **All** to allow any computer to access the NWA using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NWA using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the NWA using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the NWA using this service.
SNMP Configuration	
Protocol Version	Select the SNMP version for the NWA, which you allow the SNMP manager to use to access the NWA. The SNMP version on the NWA must match the version on the SNMP manager.
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	Specify the SNMP administrator’s access rights to MIBs. **Read/Write** - The SNMP administrator has read and write rights, meaning that the user can create and edit the MIBs on the NWA. **Read Only** - The SNMP administrator has read rights only, meaning the user can collect information from the NWA.
Authentication Protocol	Select an authentication algorithm used for SNMP communication with the SNMP administrator. **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.

Table 31 System > SNMP (continued)

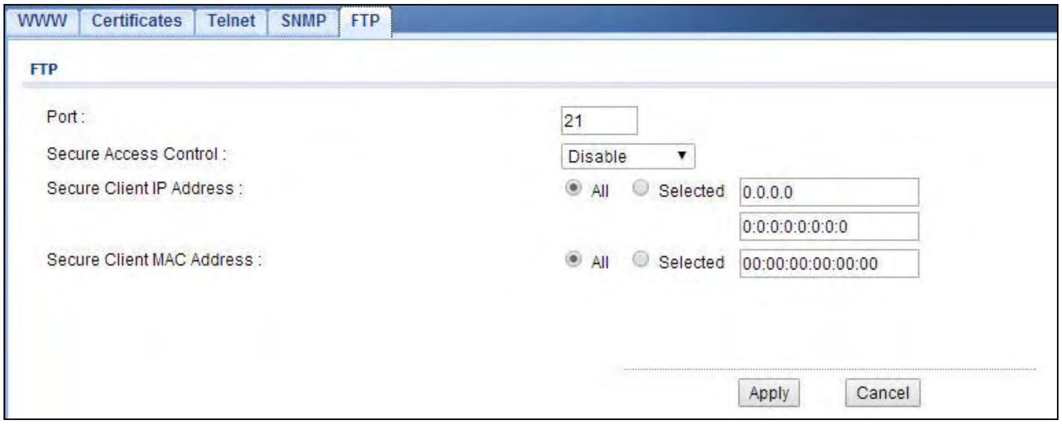
LABEL	DESCRIPTION
Privacy Protocol	Specify the encryption method used for SNMP communication with the SNMP administrator. **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. **AES** - Advanced Encryption 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.
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 NWA. **Read/Write** - The SNMP user has read and write rights, meaning that the user can create and edit the MIBs on the NWA.
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.

8.8 FTP Screen

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

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

Figure 51 System > FTP



FTP

Port : 21

Secure Access Control : Disable

Secure Client IP Address : ● All ○ Selected 0.0.0.0 0:0:0:0:0:0:0:0

Secure Client MAC Address : ● All ○ Selected 00:00:00:00:00:00

The following table describes the labels in this screen.

Table 32 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.
Secure Access Control	Select the interface(s) through which a computer may access the NWA using this service and to which the IP and MAC filtering rules you specified below are applied. Otherwise, select **Disable** to allow any computer to access the NWA through any interface using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NWA using this service. Select **All** to allow any computer to access the NWA using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NWA using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the NWA using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the NWAe using this service.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.9 Technical Reference

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

8.9.1 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.

8.9.2 Supported MIBs

The NWA 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.

8.9.3 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.

8.9.4 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 NWA to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

8.9.5 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.

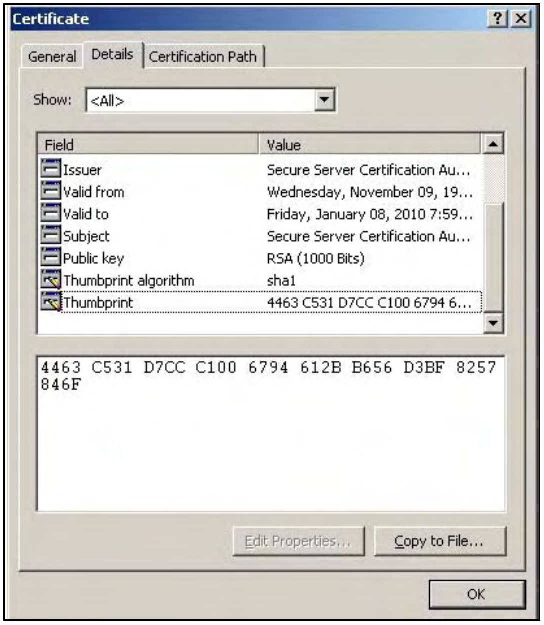
1 Browse to where you have the certificate saved on your computer.

2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 52 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 53 Certificate Details



Show: <All>

Field	Value
Issuer	Secure Server Certification Au...
Valid from	Wednesday, November 09, 19...
Valid to	Friday, January 08, 2010 7:59...
Subject	Secure Server Certification Au...
Public key	RSA (1000 Bits)
Thumbprint algorithm	sha1
Thumbprint	4463 C531 D7CC C100 6794 6...

```
4463 C531 D7CC C100 6794 612B B656 D3BF 8257
846F
```

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.

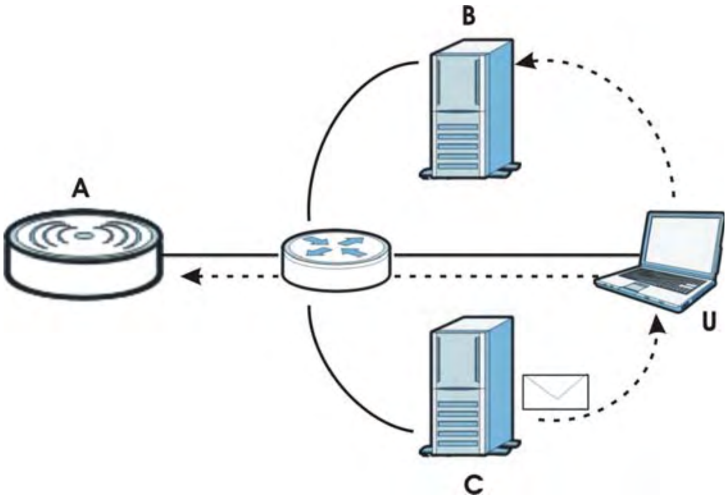
Log Settings

9.1 Overview

This chapter provides information on viewing and generating logs on your NWA.

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 54 Accessing Logs in the Network



The figure above illustrates three ways to access logs. The user (**U**) can access logs directly from the NWA (**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.

9.2 What You Can Do in this Chapter

Use the **Log Settings** screen to configure where and when the NWA will send the logs, and which logs it will send (Section 9.4 on page 106). Use the **Monitor > Logs** screen to display all logs or logs for a certain category.

9.3 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

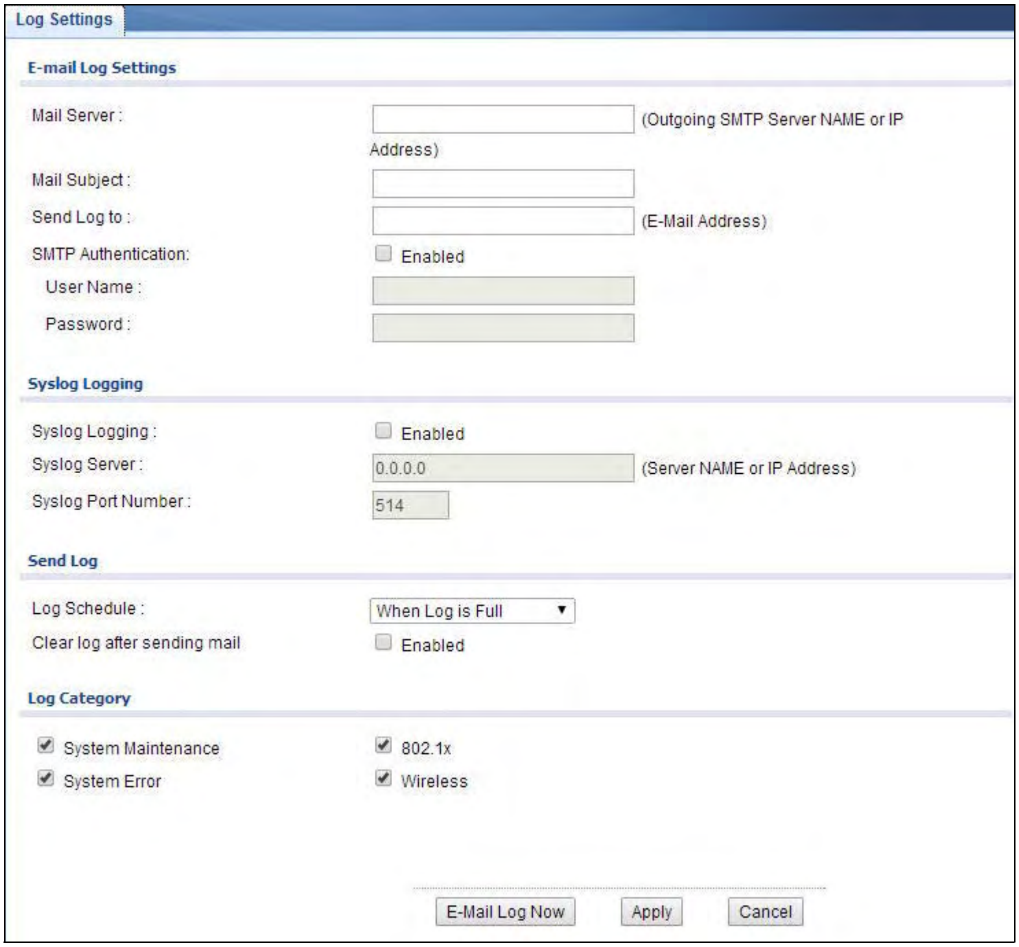
To enable Syslog Logging, obtain your Syslog server's IP address (or server name).

9.4 Log Settings Screen

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

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

Figure 55 Log Settings



Log Settings

E-mail Log Settings

Mail Server :		(Outgoing SMTP Server NAME or IP Address)
Mail Subject :		
Send Log to :		(E-Mail Address)
SMTP Authentication:	□ Enabled	
User Name :		
Password :		

Syslog Logging

Syslog Logging :	□ Enabled	
Syslog Server :	0.0.0.0	(Server NAME or IP Address)
Syslog Port Number :	514	

Send Log

Log Schedule :	When Log is Full ▼
Clear log after sending mail	□ Enabled

Log Category

☑ System Maintenance	☑ 802.1x
☑ System Error	☑ Wireless

The following table describes the labels in this screen.

Table 33 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 NWA 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 33 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 user name here.
Password	Enter the password associated with the above user name.
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: • 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.
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 NWA to immediately send e-mail alerts.
Apply	Click **Apply** to save your customized settings.
Cancel	Click **Cancel** to begin configuring this screen afresh.

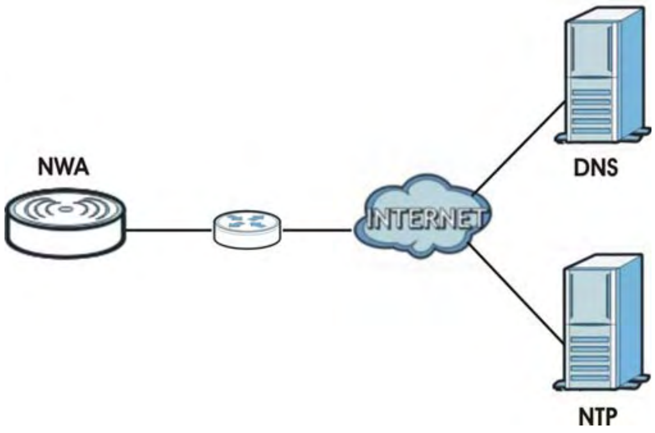
Maintenance

10.1 Overview

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

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

Figure 56 NWA Setup



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

10.2 What You Can Do in this Chapter

- Use the **General** screen to specify the system name (see Section 10.4 on page 110).
- Use the **Password** screen to manage the password for your NWA (see Section 10.5 on page 111).
- Use the **Time** screen to change your NWA's time and date. This screen allows you to configure the NWA's time based on your local time zone (see Section 10.6 on page 112).
- Use the **Firmware Upgrade** screen to upload the latest firmware for your NWA (see Section 10.7 on page 113).
- Use the **Configuration File** screen to view information related to factory defaults, backup configuration, and restoring configuration (see Section 10.8 on page 114).
- Use the **Restart** screen to reboot the NWA without turning the power off (see Section 10.9 on page 116).

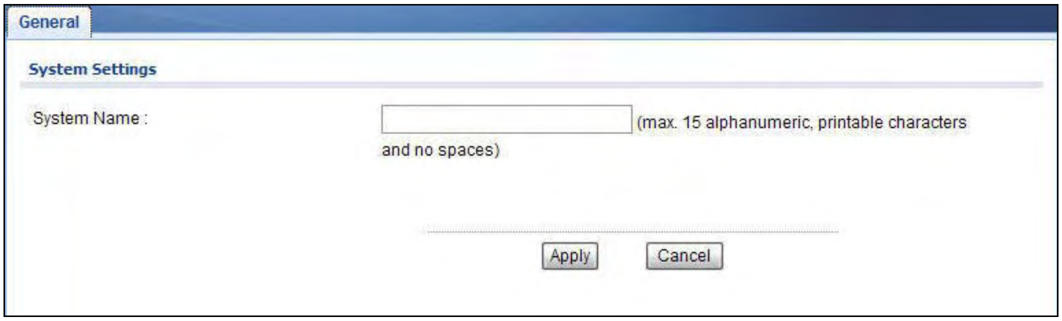
10.3 What You Need To Know

You can find the firmware for your device at www.zyxel.com. It is a file that uses the system project code with a "*.bin" extension, for example "V100AAEO0.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

10.4 General Screen

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

Figure 57 Maintenance > General



The following table describes the labels in this screen.

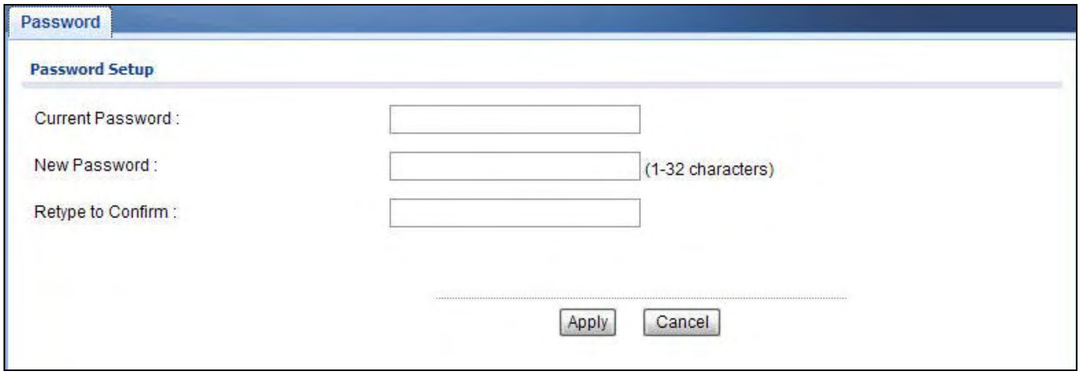
Table 34 Maintenance > General

LABEL	DESCRIPTION
System Settings	
System Name	Type a descriptive name to identify the NWA 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.

10.5 Password Screen

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

Figure 58 Maintenance > Password



The following table describes the labels in this screen.

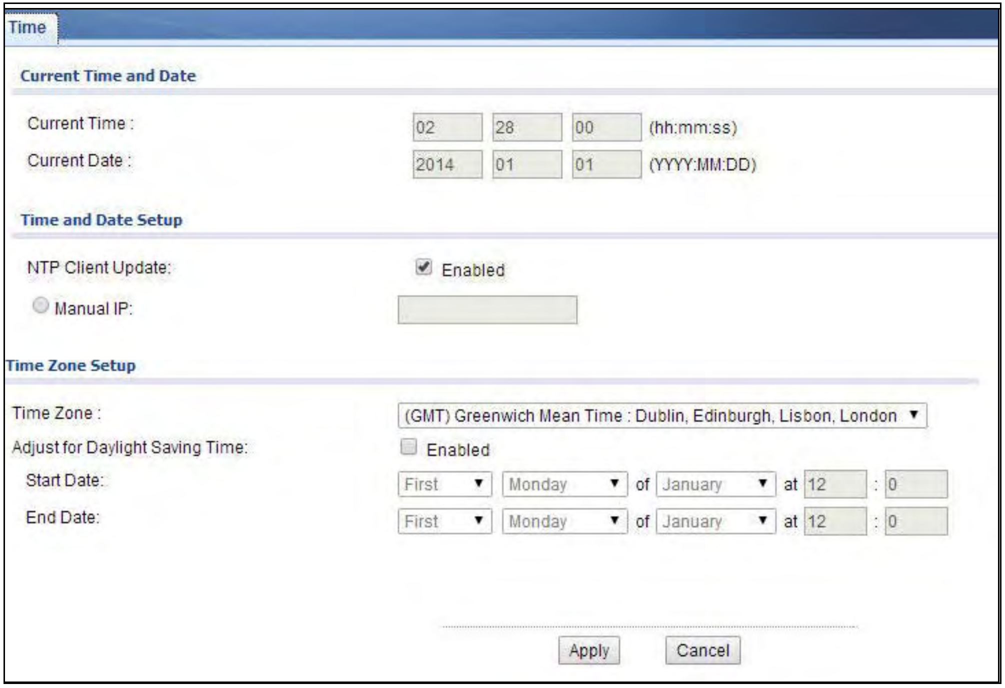
Table 35 Maintenance > Password

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.

10.6 Time Screen

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

Figure 59 Maintenance > Time



Current Time and Date

Current Time : 02 28 00 (hh:mm:ss)

Current Date : 2014 01 01 (YYYY:MM:DD)

Time and Date Setup

NTP Client Update: ☑ Enabled

○ Manual IP:

Time Zone Setup

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

Adjust for Daylight Saving Time: □ Enabled

Start Date: First Monday of January at 12 : 0

End Date: First Monday of January at 12 : 0

The following table describes the labels in this screen.

Table 36 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NWA. Each time you reload this page, the NWA 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 NWA 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	

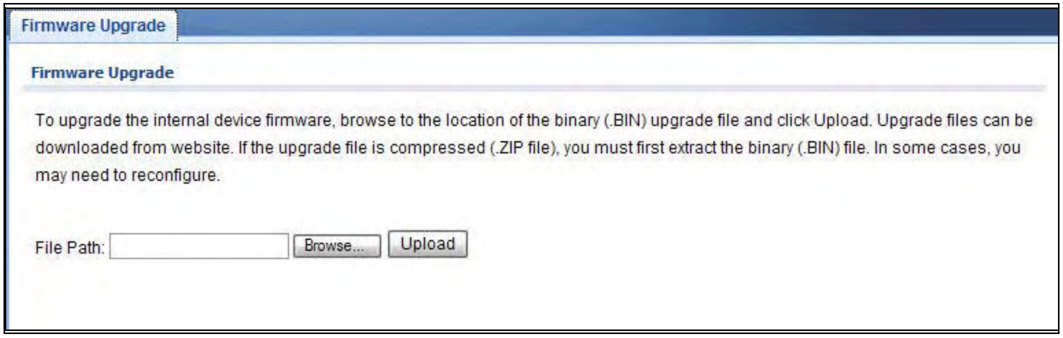
Table 36 Maintenance > Time (continued)

LABEL	DESCRIPTION
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Adjust for Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Enable Daylight Saving. The at fields uses the 24 hour format. For example: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field. In the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving at the same time (1 A.M. GMT or UTC). Therefore you should select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you will type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT +1).
End Date	Configure the day and time when Daylight Saving Time starts if you selected Enable Daylight Saving. The at fields uses the 24 hour format. For example: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field. In the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving at the same time (1 A.M. GMT or UTC). Therefore you should select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you will type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT +1).
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.7 Firmware Upgrade Screen

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

Figure 60 Maintenance > Firmware Upgrade



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

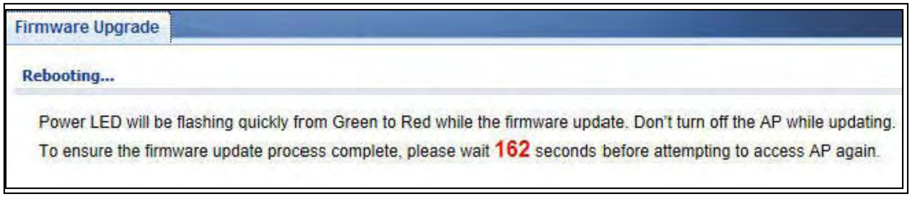
The following table describes the labels in this screen.

Table 37 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 NWA while firmware upload is in progress!

Figure 61 Firmware Upload In Process



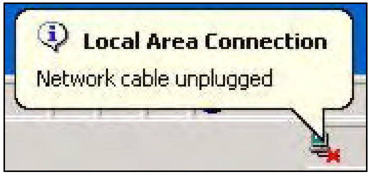
Rebooting...

Power LED will be flashing quickly from Green to Red while the firmware update. Don't turn off the AP while updating.

To ensure the firmware update process complete, please wait 162 seconds before attempting to access AP again.

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

Figure 62 Network Temporarily Disconnected



Local Area Connection

Network cable unplugged

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

10.8 Configuration File Screen

Use this screen to backup, restore and reset the configuration of your NWA.

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

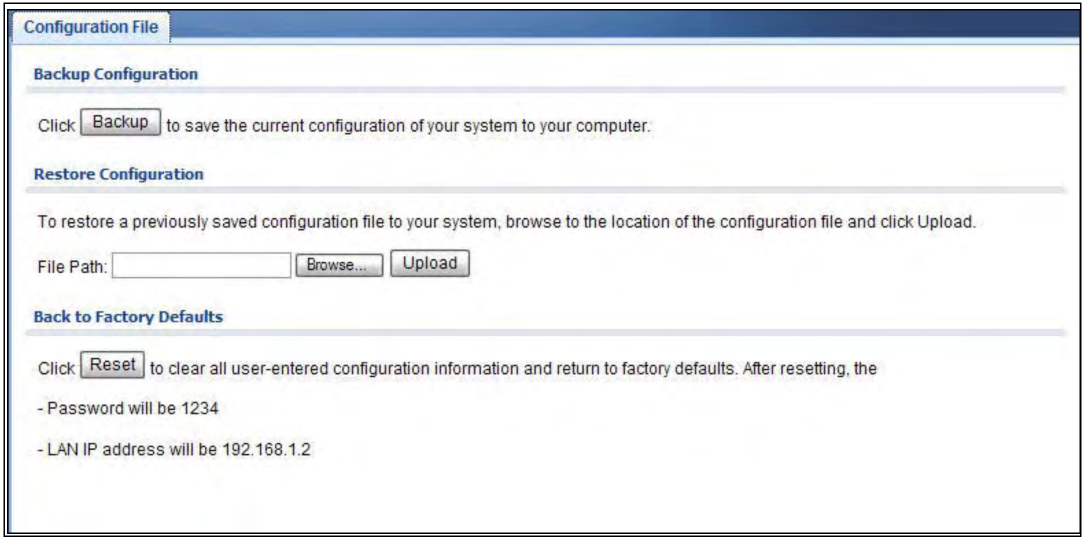


Figure 63 Maintenance > Configuration File

Backup Configuration

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

Restore Configuration

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

File Path: Browse... Upload

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- Password will be 1234

- LAN IP address will be 192.168.1.2

10.8.1 Backup Configuration

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

10.8.2 Restore Configuration

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

Table 38 Restore Configuration

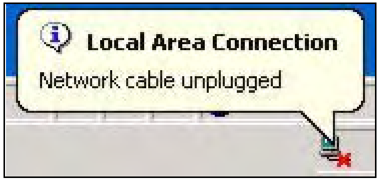
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload**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

Do not turn off the NWA while configuration file upload is in progress.

You must then wait one minute before logging into the NWA again.

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

Figure 64 Network Temporarily Disconnected



Local Area Connection

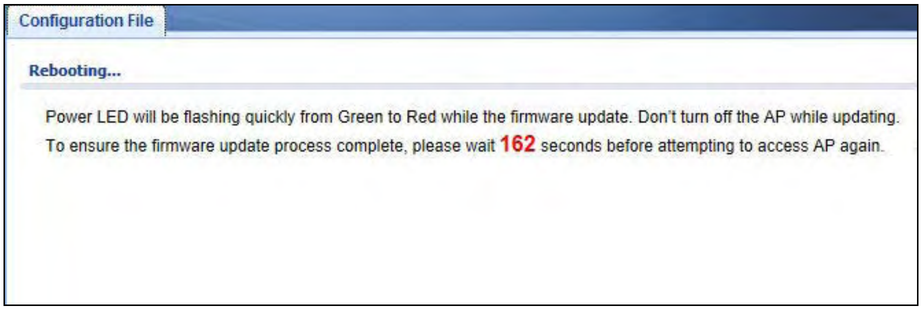
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NWA IP address (192.168.1.2). See Appendix A on page 122 for details on how to set up your computer's IP address.

10.8.3 Back to Factory Defaults

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

Figure 65 Reset Message



Rebooting...

Power LED will be flashing quickly from Green to Red while the firmware update. Don't turn off the AP while updating.

To ensure the firmware update process complete, please wait 162 seconds before attempting to access AP again.

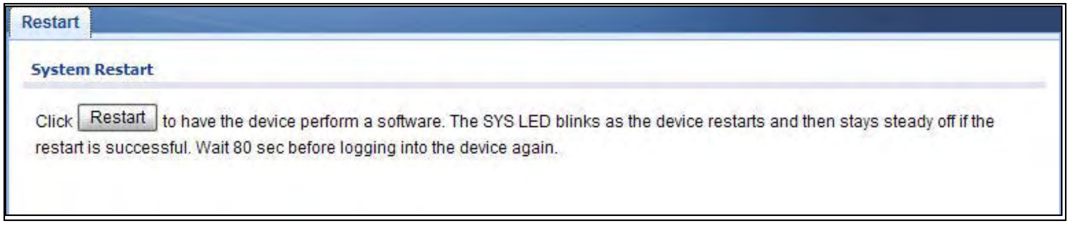
You can also press the **RESET** button to reset your NWA to its factory default settings. Refer to Section 2.3 on page 20 for more information.

10.9 Restart Screen

Use this screen to reboot the NWA without turning the power off.

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

Figure 66 Maintenance > Restart



System Restart

Click Restart to have the device perform a software. The SYS LED blinks as the device restarts and then stays steady off if the restart is successful. Wait 80 sec before logging into the device again.

Click **Restart** to have the NWA reboot. This does not affect the NWA's configuration.

11

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
- NWA Access and Login
- Internet Access
- Wireless LAN

11.1 Power, Hardware Connections, and LEDs

The NWA does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the NWA.
2. Make sure the power adaptor or cord is connected to the NWA 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 NWA.
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 16.
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 NWA.
5. If the problem continues, contact the vendor.

11.2 NWA Access and Login

I forgot the IP address for the NWA.

1 The default IP address is **192.168.1.2**.

2 If the NWA is working as a DHCP client and receives an IP address from a DHCP server, check the DHCP server for the NWA's IP address.

3 If you configured a static IP address and have forgotten it, you have to reset the device to its factory defaults. See Section 2.3 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 2.3 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 7.6 on page 90), 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 NWA.

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 16.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Section 11.1 on page 117.

4 Make sure your computer is in the same subnet as the NWA. (If you know that there are routers between your computer and the NWA, 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 NWA.

5 Reset the device to its factory defaults, and try to access the NWA 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 NWA using another service, such as Telnet. If you can access the NWA, check the remote management settings to find out why the NWA 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 NWA.

1. Make sure you have entered the user name and password correctly. The default user name is **admin** and default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
2. Disconnect and re-connect the power adaptor or cord to the NWA.
3. If this does not work, you have to reset the device to its factory defaults. See Section 2.3 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.

11.3 Internet Access

I cannot access the Internet through the NWA.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 11.1 on page 117.
2. Make sure your NWA is connected to a networking device that provides Internet access.
3. Make sure your computer is set to obtain a dynamic IP address or has an IP address which is in the same subnet as the broadband modem or router.
4. 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.
5. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
6. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NWA), 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 16.
2. Reboot the NWA.
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 16. If the NWA 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 NWA (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 NWA.
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.

11.4 Wireless LAN

I cannot access the NWA or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the NWA.
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the NWA.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the NWA.

5 Check that both the NWA and your wireless client are using the same wireless and wireless security settings.

A

Setting Up Your Computer's IP Address

Note: Your specific NWA 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.

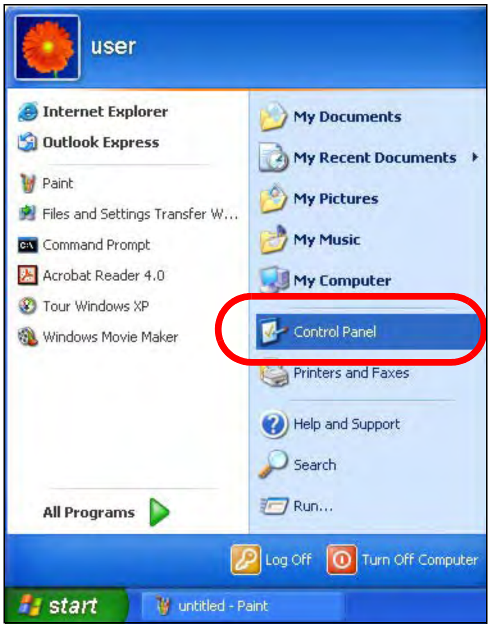
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 122
- Windows Vista on page 126
- Windows 7 on page 130
- Mac OS X: 10.3 and 10.4 on page 134
- Mac OS X: 10.5 and 10.6 on page 137
- Linux: Ubuntu 8 (GNOME) on page 140
- Linux: openSUSE 10.3 (KDE) on page 144

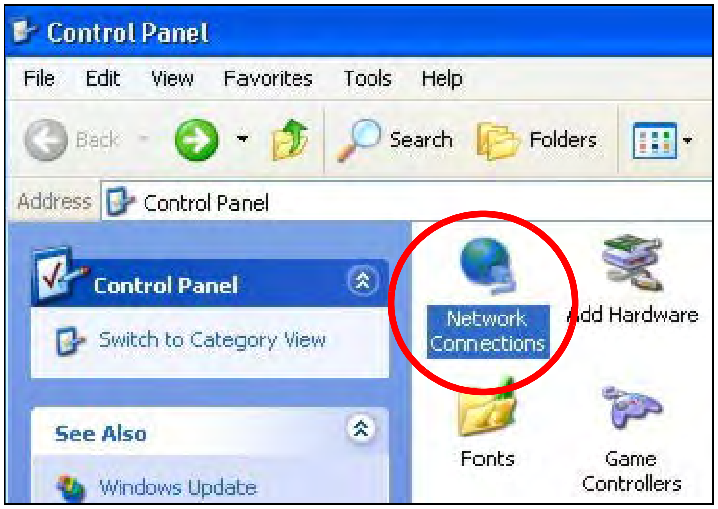
Windows XP/NT/2000

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

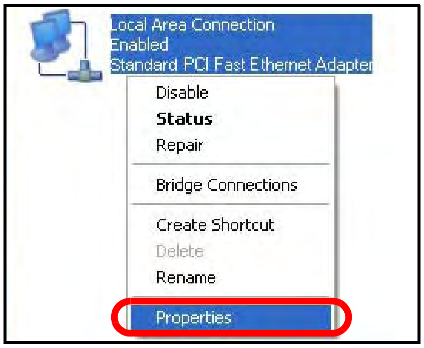
1 Click **Start** > **Control Panel**.



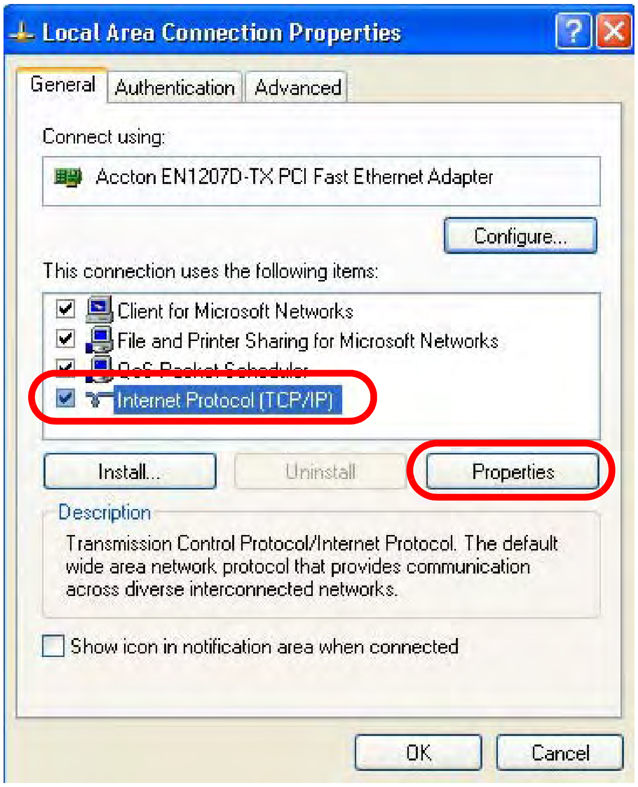
2 In the **Control Panel**, click the **Network Connections** icon.



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



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



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

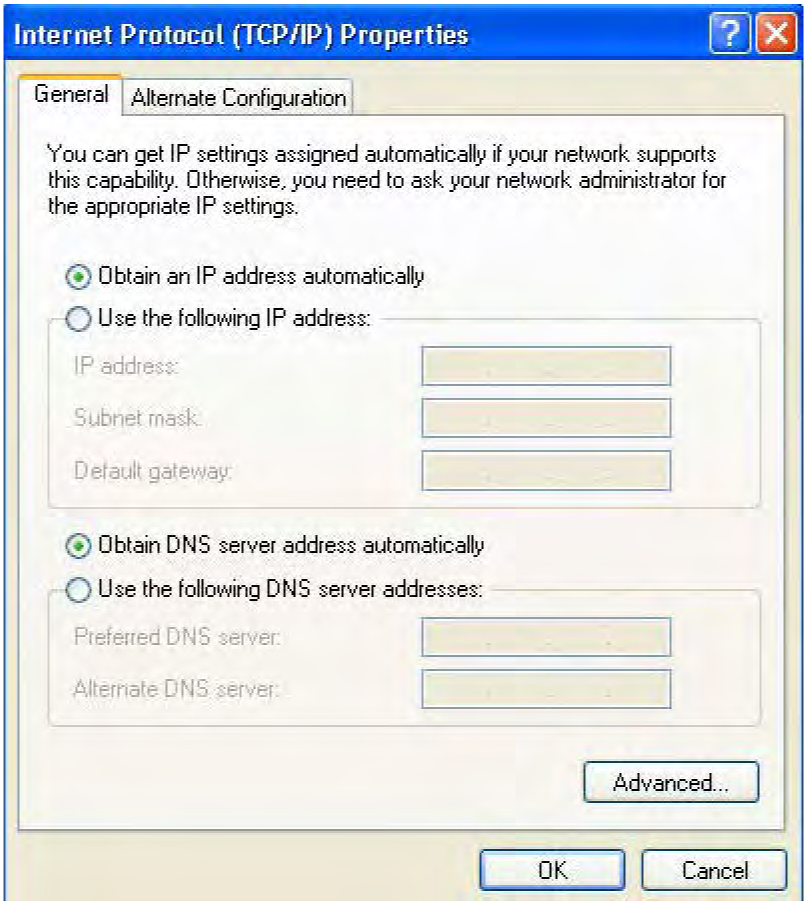
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

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



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

● Obtain an IP address automatically

○ Use the following IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

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**.

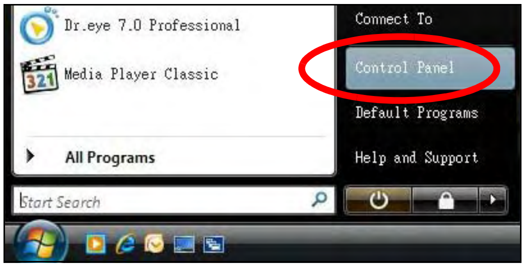
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

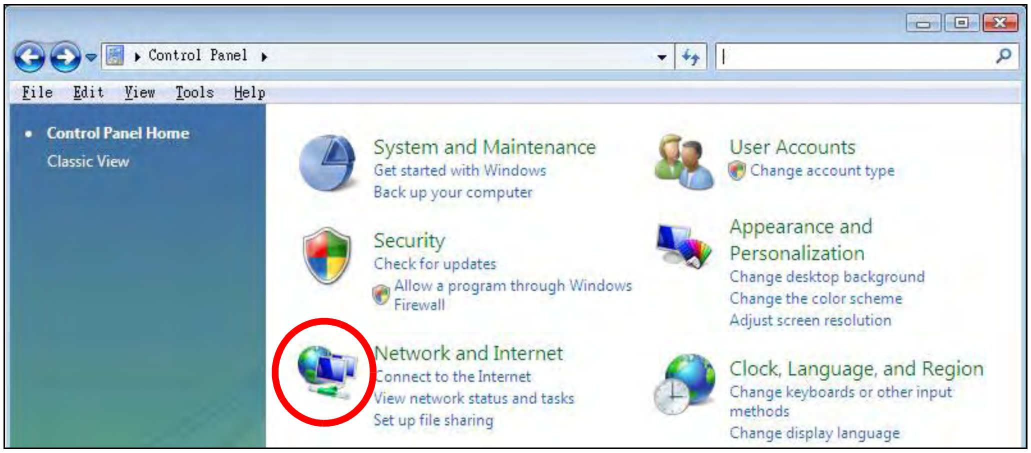
Windows Vista

This section shows screens from Windows Vista Professional.

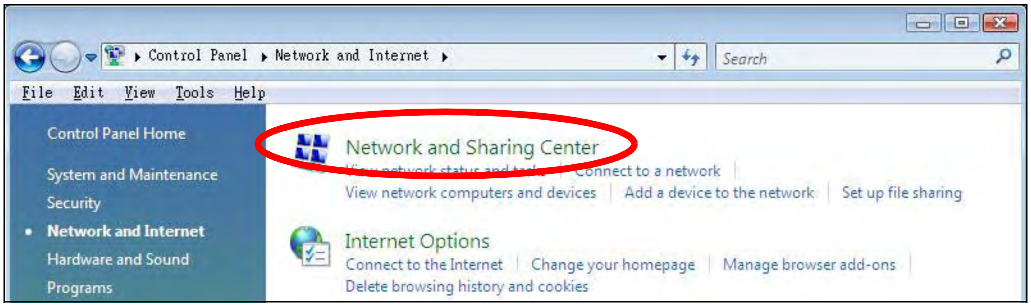
1 Click **Start** > **Control Panel**.



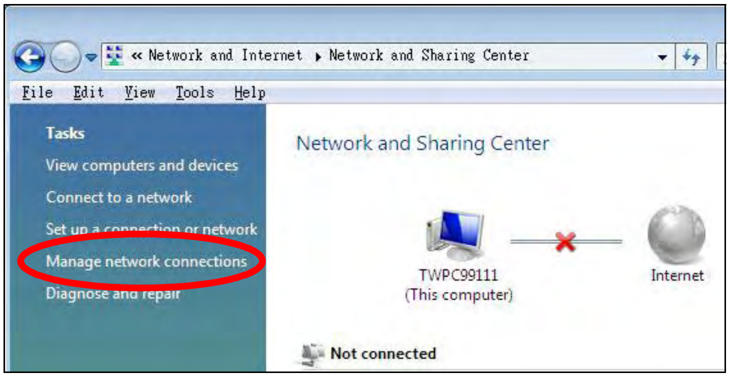
2 In the **Control Panel**, click the **Network and Internet** icon.



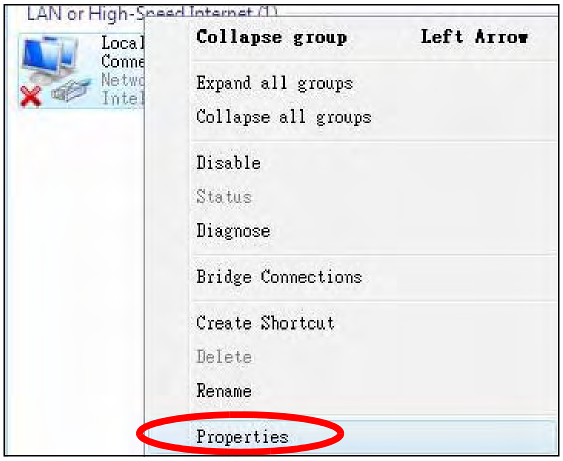
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

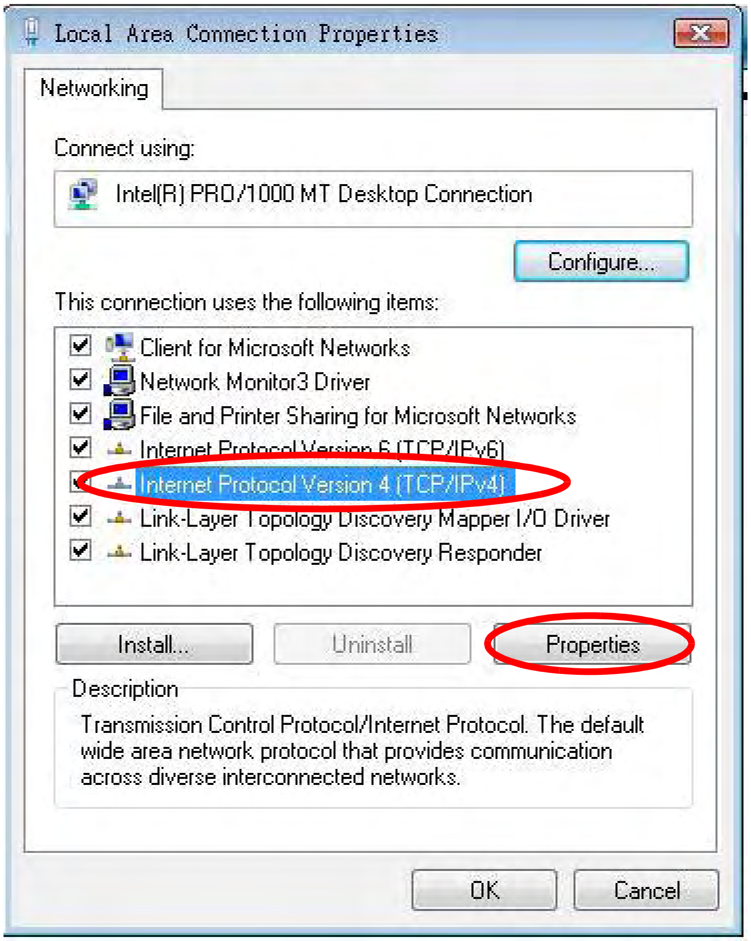

« Network and Internet ▸ Network and Sharing Center
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
TWPC99111
(This computer)
Internet
Not connected

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**.



Connect using:

Intel(R) PRO/1000 MT Desktop Connection

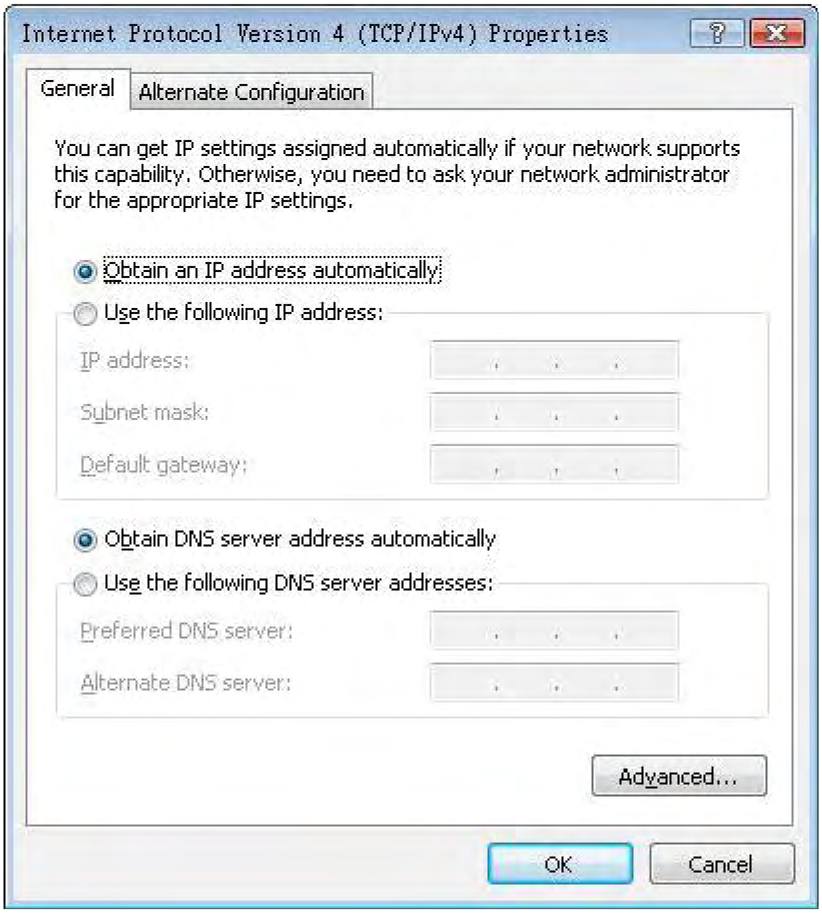
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Network Monitor3 Driver
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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**.

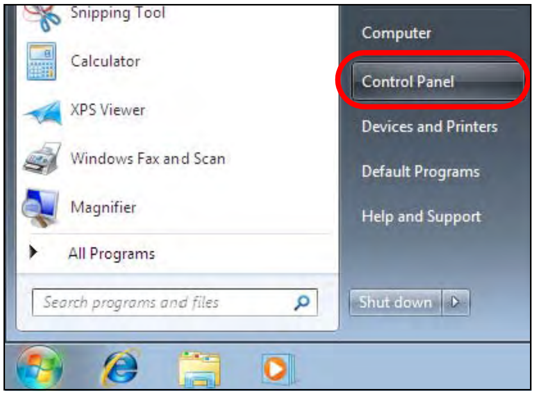
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

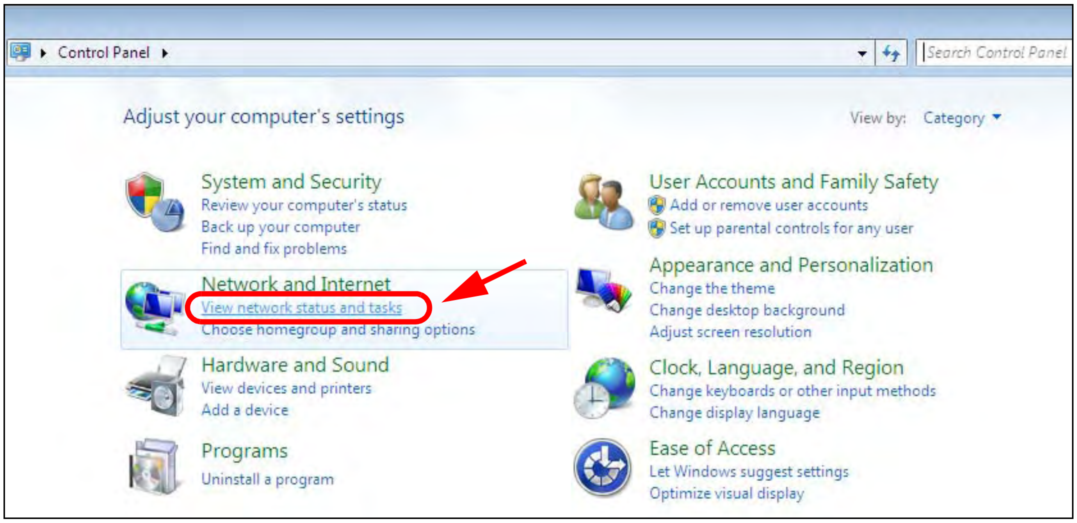
Windows 7

This section shows screens from Windows 7 Enterprise.

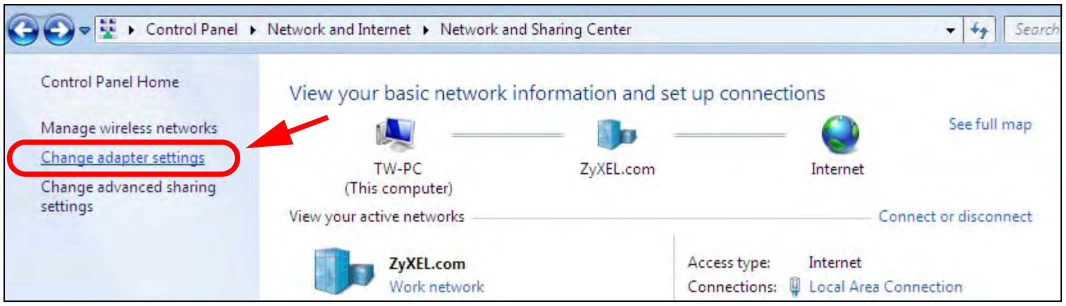
1 Click **Start** > **Control Panel**.



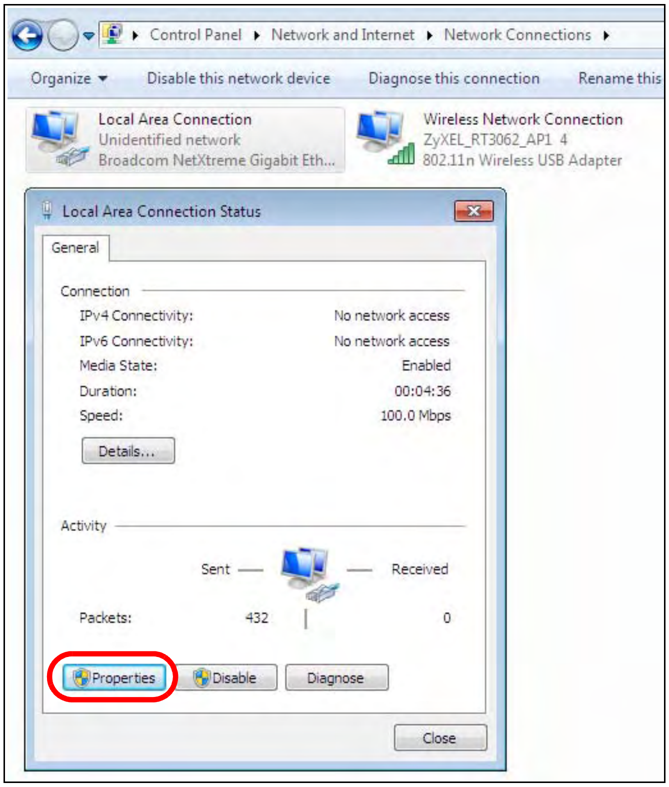
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3 Click **Change adapter settings**.


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TW-PC
(This computer)
ZyXEL.com
Internet
View your active networks
Connect or disconnect
ZyXEL.com
Work network
Access type: Internet
Connections: Local Area Connection

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



Control Panel ▸ Network and Internet ▸ Network Connections ▸
Organize ▾
Disable this network device
Diagnose this connection
Rename this
Local Area Connection
Unidentified network
Broadcom NetXtreme Gigabit Eth...
Wireless Network Connection
ZyXEL_RT3062_AP1 4
802.11n Wireless USB Adapter
Local Area Connection Status
General
Details...
Properties
Disable
Diagnose
Close

Connection

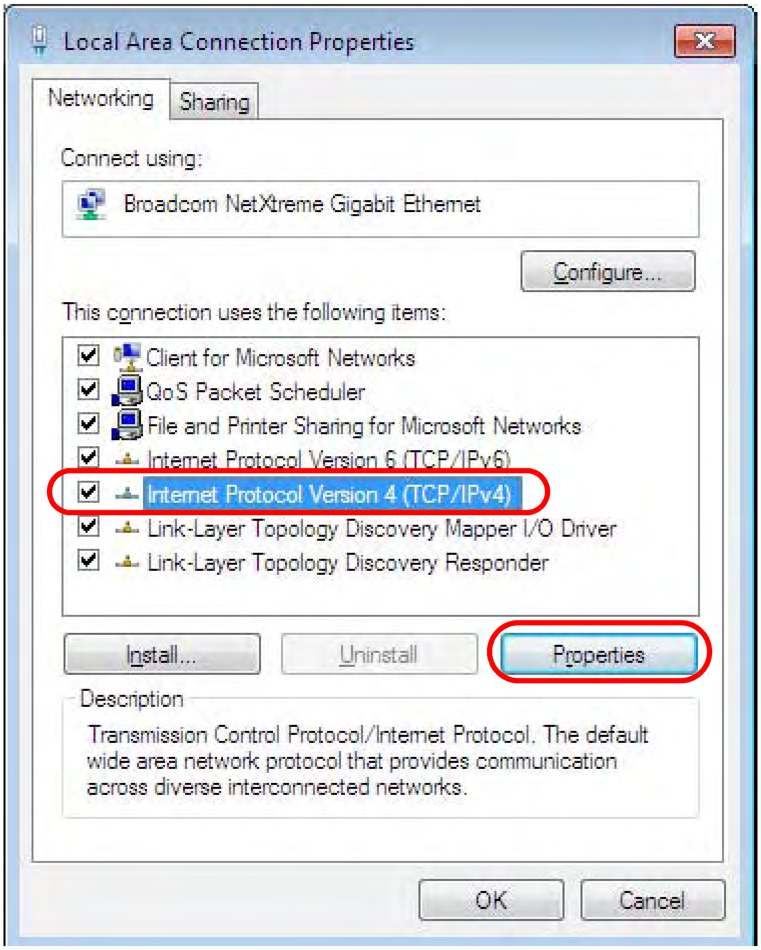
IPv4 Connectivity:	No network access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	00:04:36
Speed:	100.0 Mbps

Activity

	Sent	Received
Packets:	432	0

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

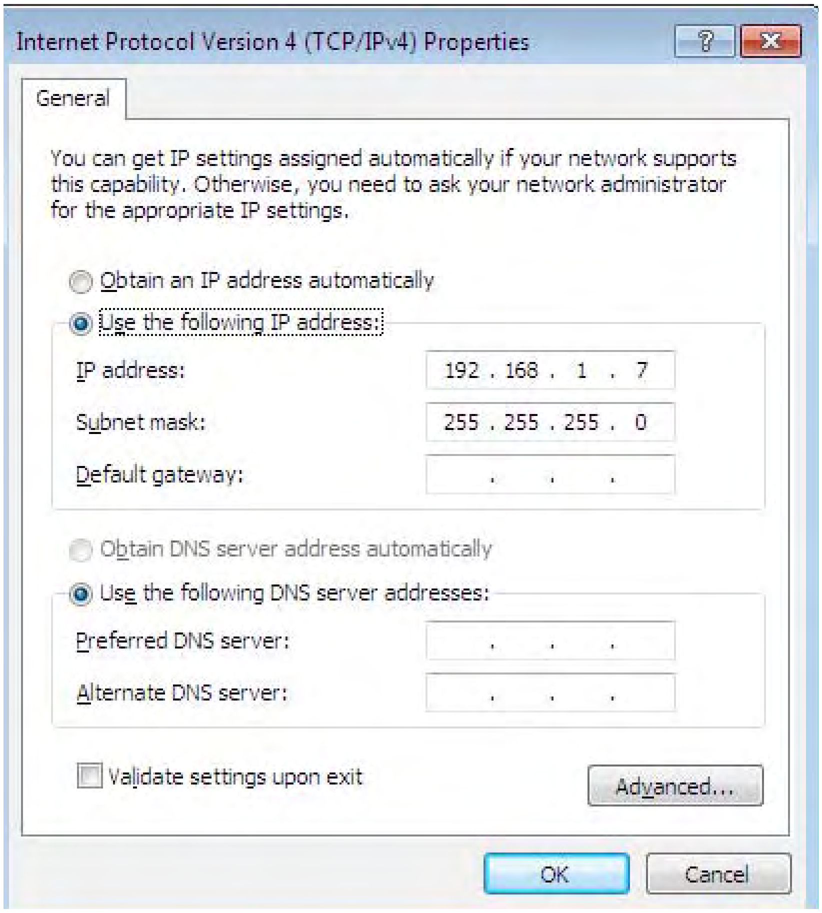
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



Local Area Connection Properties
Networking
Sharing
Connect using:
Broadcom NetXtreme Gigabit Ethernet
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
OK
Cancel

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 7
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

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.

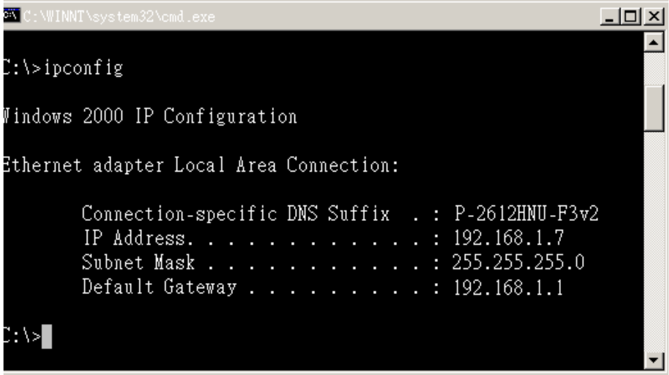
9 Click **OK** to close the **Local Area Connection Properties** window.

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.

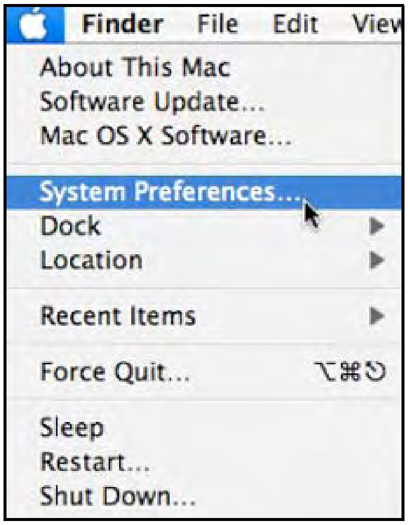


```
C:\>ipconfig

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:\>
```

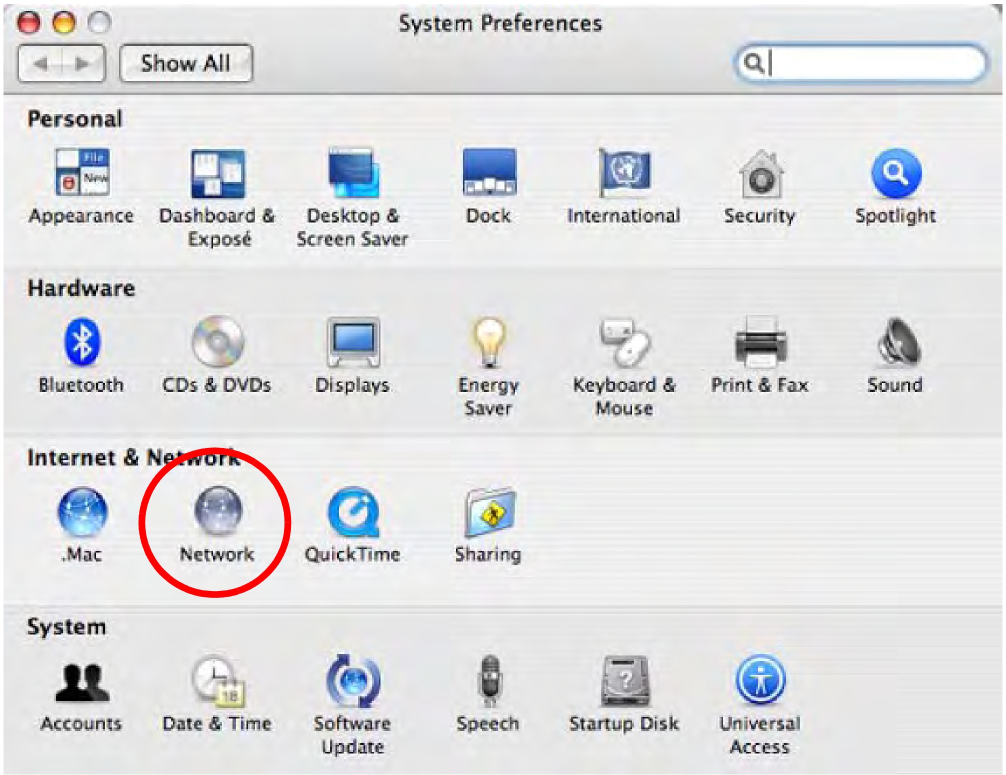
Mac OS X: 10.3 and 10.4

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

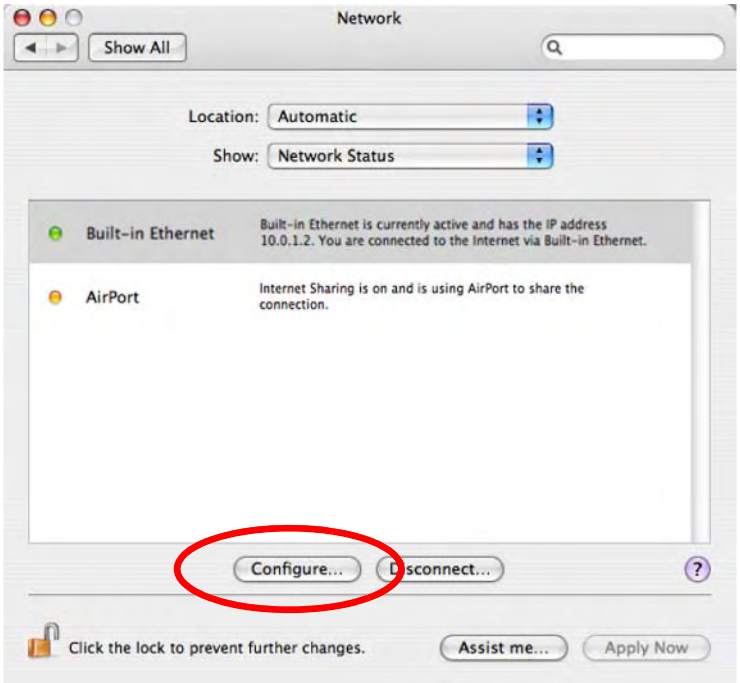
1 Click **Apple** > **System Preferences**.



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.**



Location: Automatic

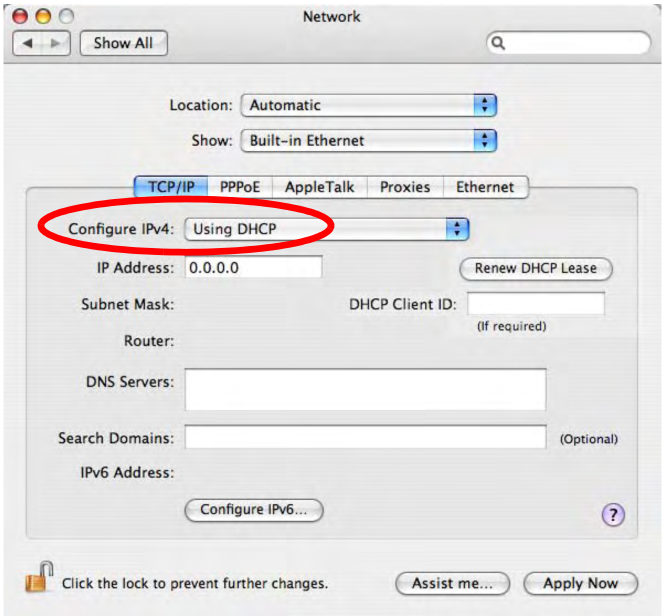
Show: Network Status

Built-in Ethernet — Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.

AirPort — Internet Sharing is on and is using AirPort to share the connection.

Click the lock to prevent further changes.

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



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 0.0.0.0

Subnet Mask:

Router:

DHCP Client ID: (If required)

DNS Servers:

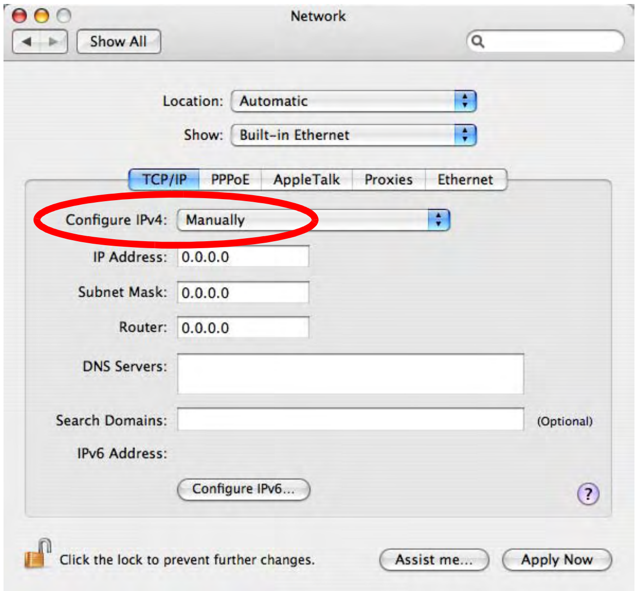
Search Domains: (Optional)

IPv6 Address:

Click the lock to prevent further changes.

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.



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Manually

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Router: 0.0.0.0

DNS Servers:

Search Domains: (Optional)

IPv6 Address:

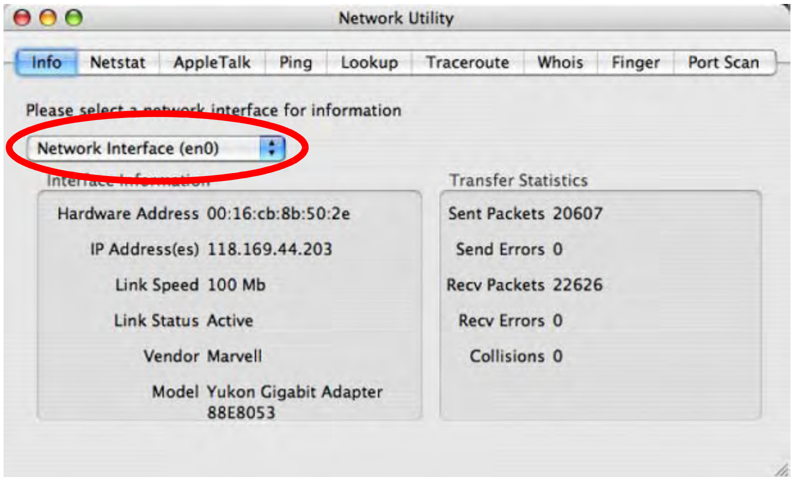
Click the lock to prevent further changes.

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 67 Mac OS X 10.4: Network Utility



Please select a network interface for information

Network Interface (en0)

Interface Information

Hardware Address 00:16:cb:8b:50:2e
IP Address(es) 118.169.44.203
Link Speed 100 Mb
Link Status Active
Vendor Marvell
Model Yukon Gigabit Adapter 88E8053

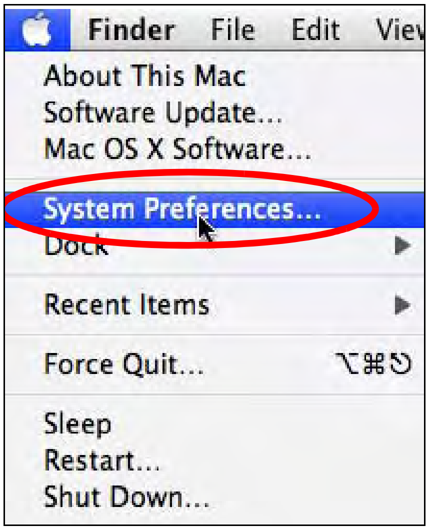
Transfer Statistics

Sent Packets 20607
Send Errors 0
Recv Packets 22626
Recv Errors 0
Collisions 0

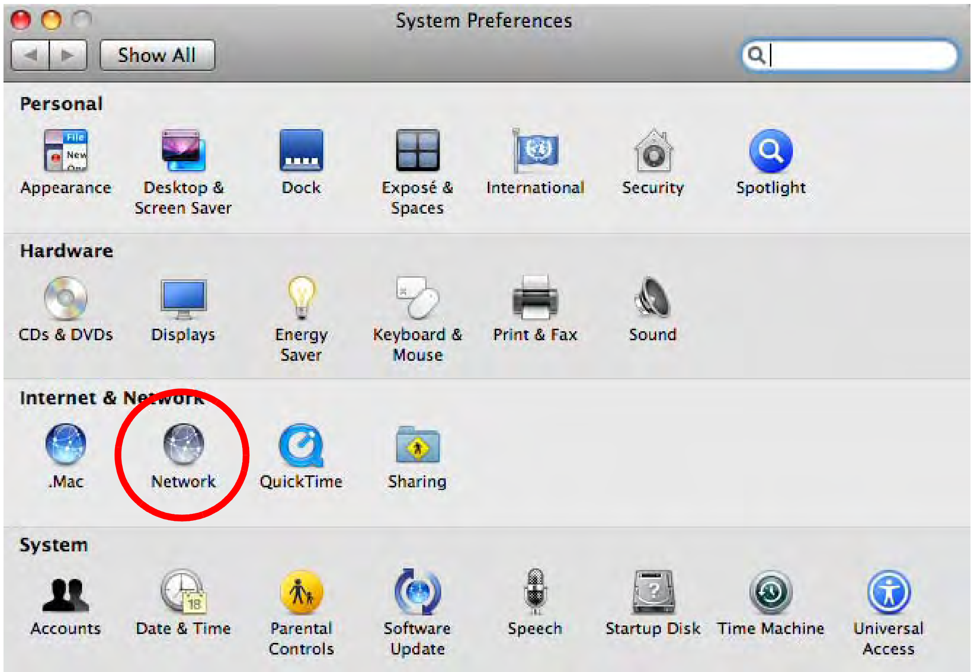
Mac OS X: 10.5 and 10.6

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

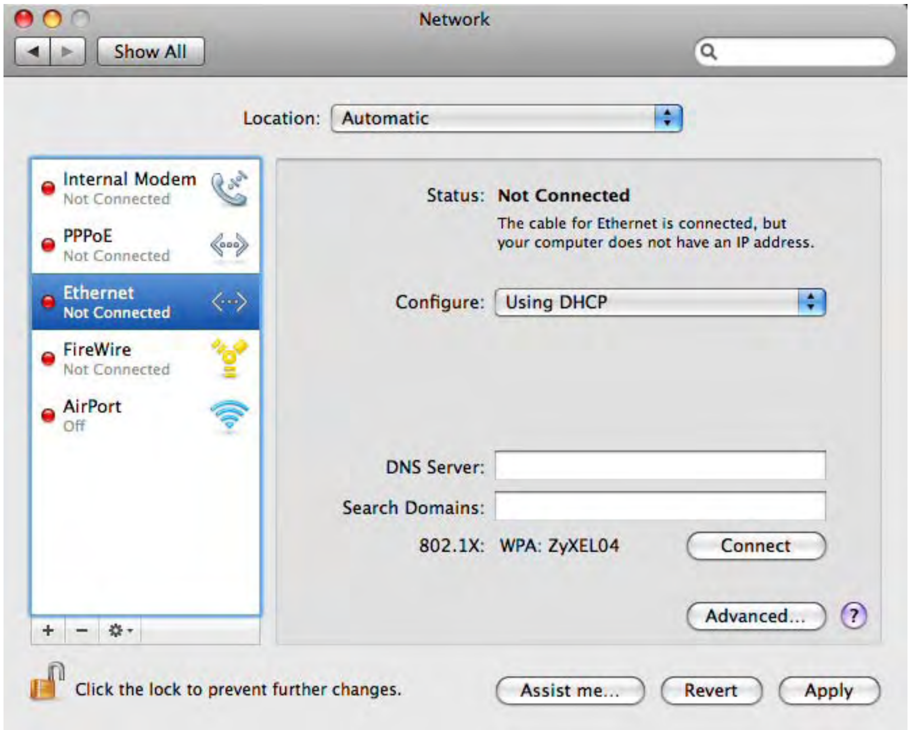
1 Click **Apple** > **System Preferences**.



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



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



Location: Automatic

Status: **Not Connected**

The cable for Ethernet is connected, but your computer does not have an IP address.

Configure: Using DHCP

DNS Server:

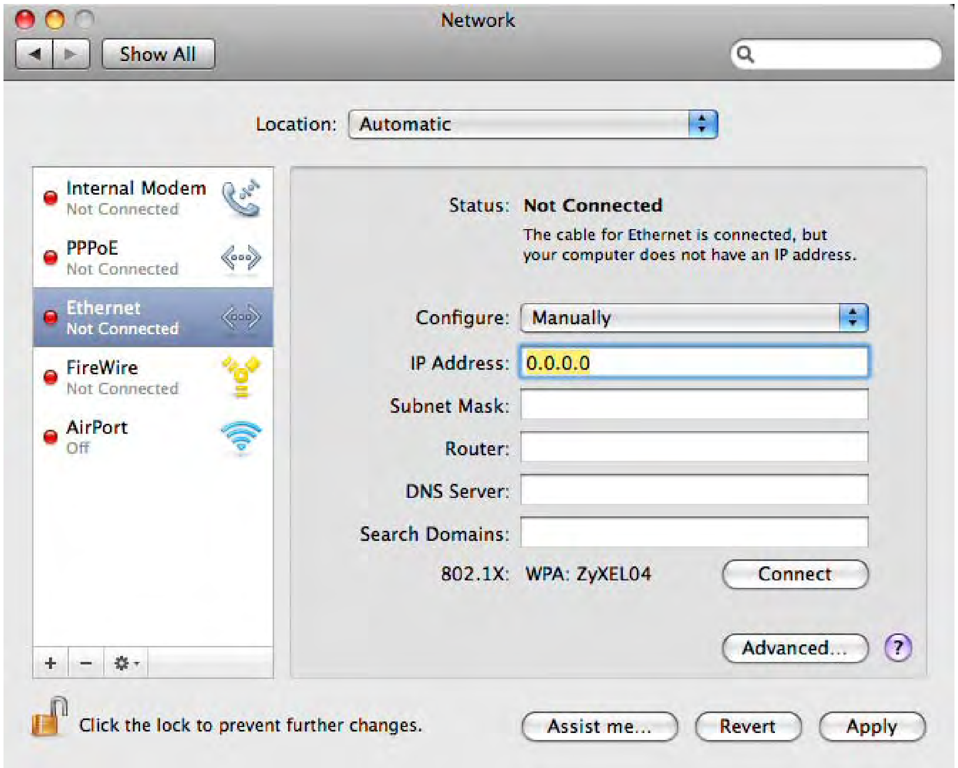
Search Domains:

802.1X: WPA: ZyXEL04

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 NWA.



Location: Automatic

Internal Modem
Not Connected

PPPoE
Not Connected

Ethernet
Not Connected

FireWire
Not Connected

AirPort
Off

Status: **Not Connected**

The cable for Ethernet is connected, but your computer does not have an IP address.

Configure: Manually

IP Address: 0.0.0.0

Subnet Mask:

Router:

DNS Server:

Search Domains:

802.1X: WPA: ZyXEL04

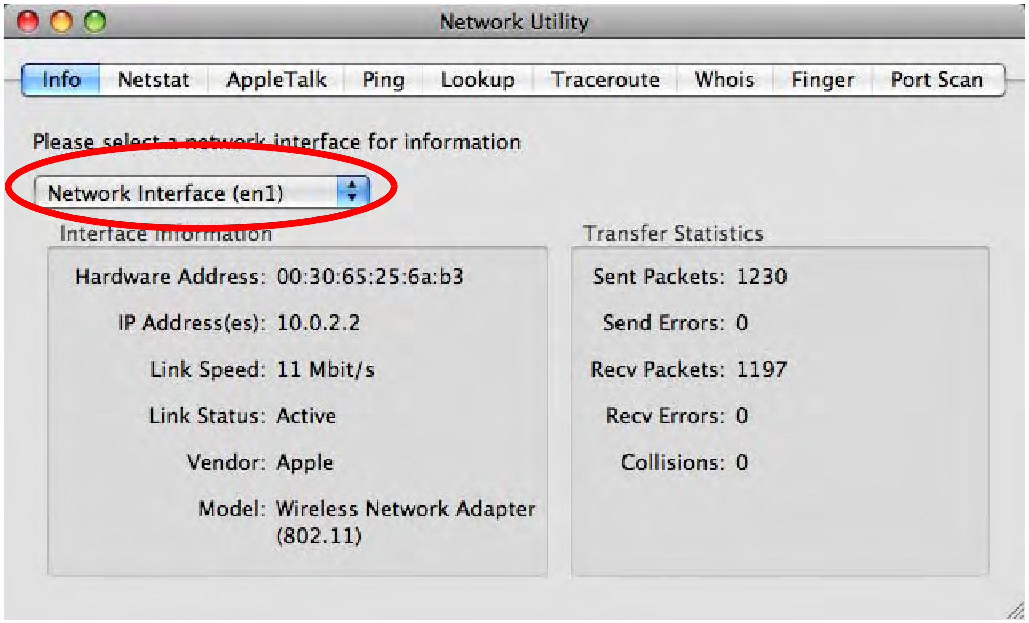
Click the lock to prevent further changes.

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 68 Mac OS X 10.5: Network Utility



Please select a network interface for information

Network Interface (en1)

Interface Information

Hardware Address: 00:30:65:25:6a:b3

IP Address(es): 10.0.2.2

Link Speed: 11 Mbit/s

Link Status: Active

Vendor: Apple

Model: Wireless Network Adapter (802.11)

Transfer Statistics

Sent Packets: 1230

Send Errors: 0

Recv Packets: 1197

Recv Errors: 0

Collisions: 0

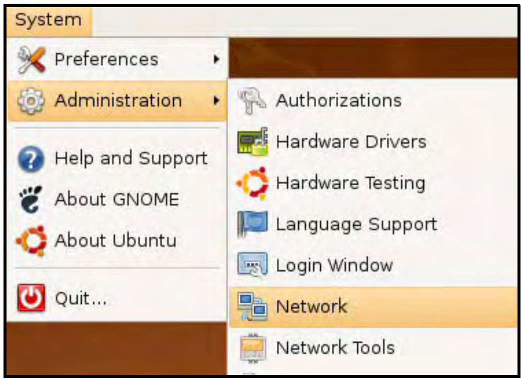
Linux: Ubuntu 8 (GNOME)

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.

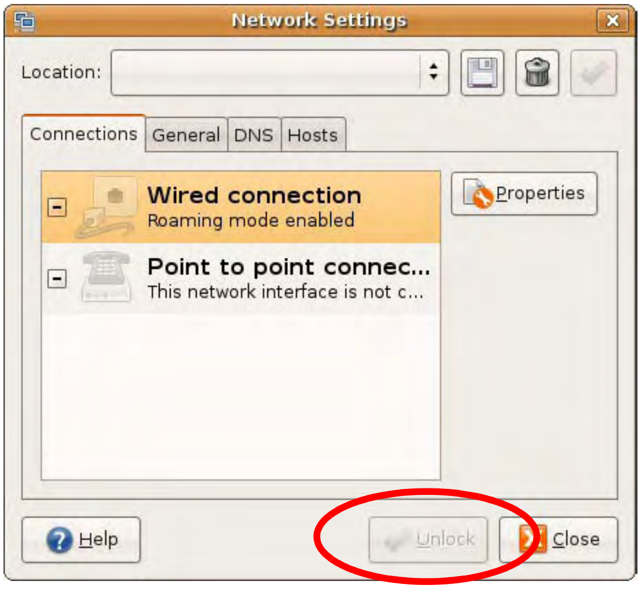
Note: Make sure you are logged in as the root administrator.

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

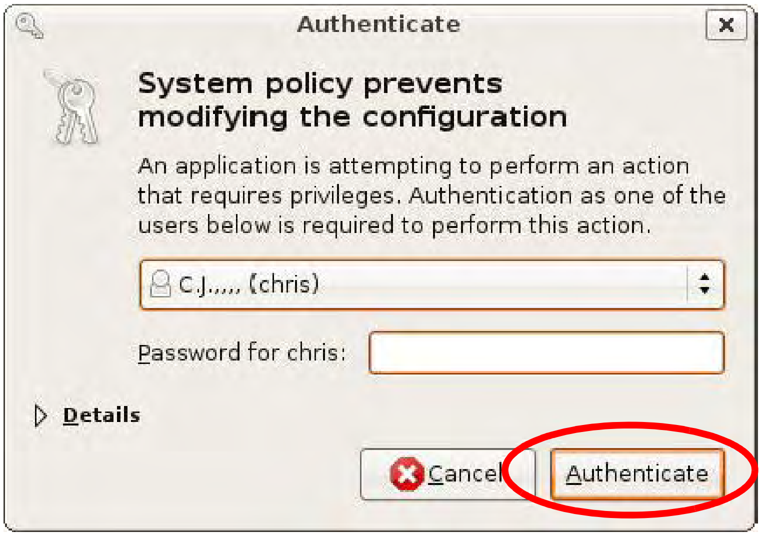
1 Click **System > Administration > Network**.



2 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.



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



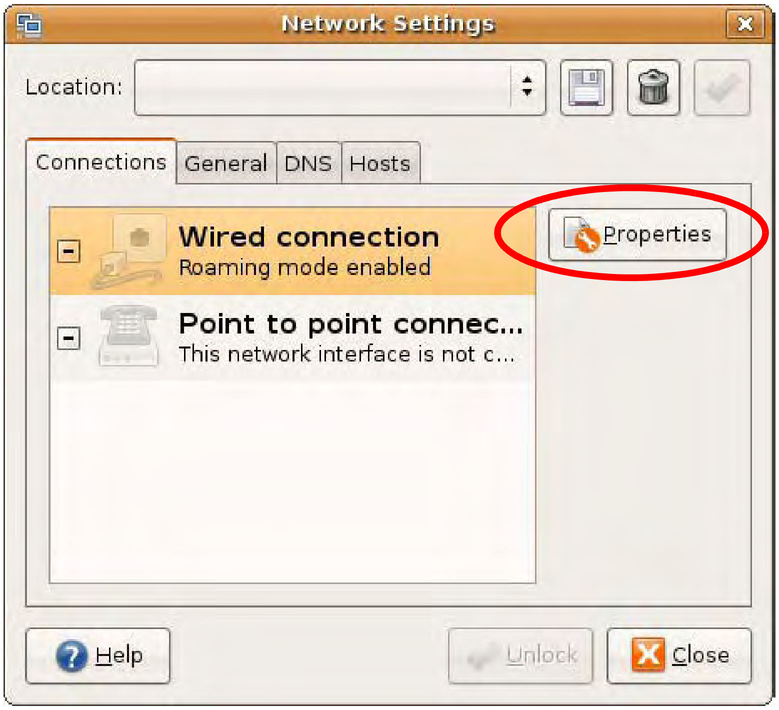
System policy prevents modifying the configuration

An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.

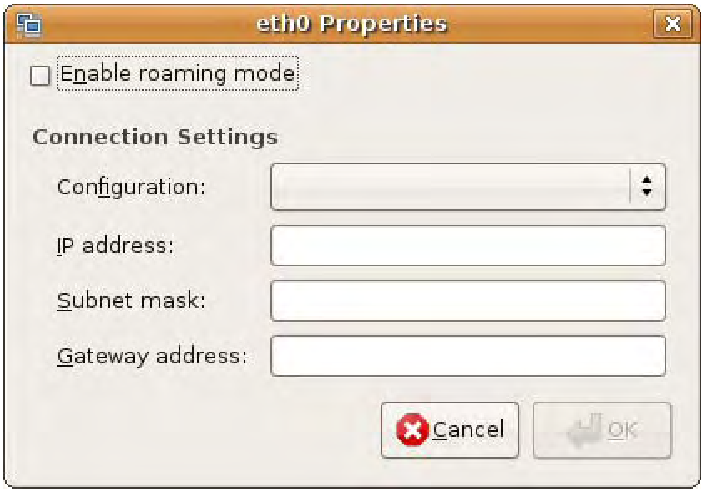
C.J....., (chris)

Password for chris:

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



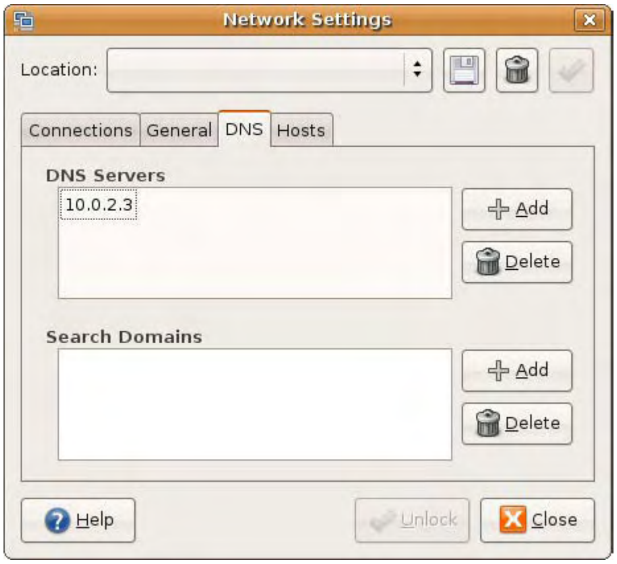
5 The **Properties** dialog box opens.



- 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.



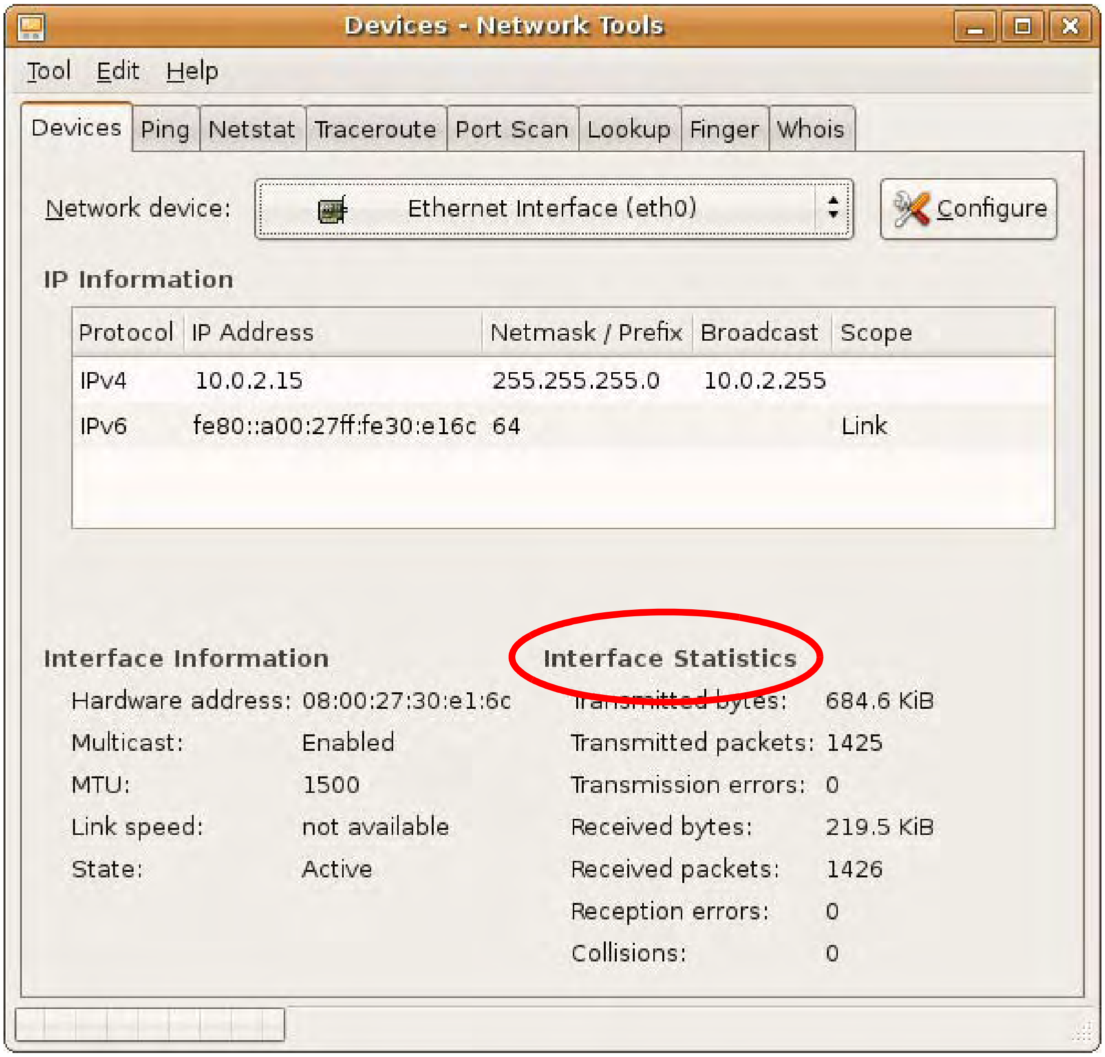
DNS Servers
10.0.2.3

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 69 Ubuntu 8: Network Tools



Network device: Ethernet Interface (eth0)

IP Information

Protocol	IP Address	Netmask / Prefix	Broadcast	Scope
IPv4	10.0.2.15	255.255.255.0	10.0.2.255	
IPv6	fe80::a00:27ff:fe30:e16c	64		Link

Interface Information

Hardware address:	08:00:27:30:e1:6c
Multicast:	Enabled
MTU:	1500
Link speed:	not available
State:	Active

Interface Statistics

Transmitted bytes:	684.6 KiB
Transmitted packets:	1425
Transmission errors:	0
Received bytes:	219.5 KiB
Received packets:	1426
Reception errors:	0
Collisions:	0

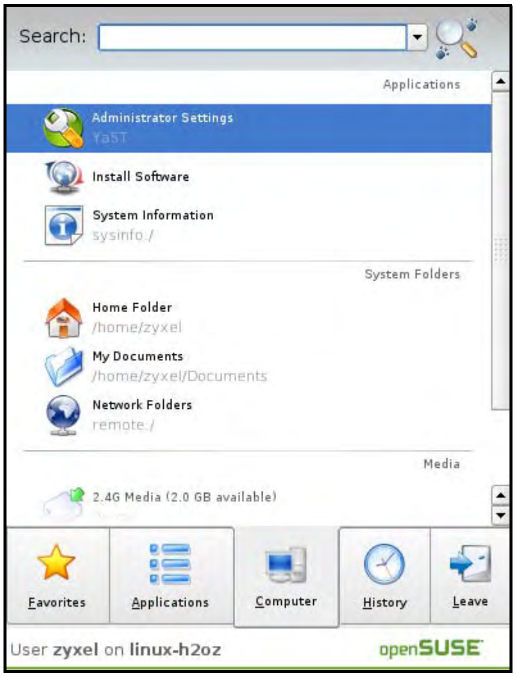
Linux: openSUSE 10.3 (KDE)

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.

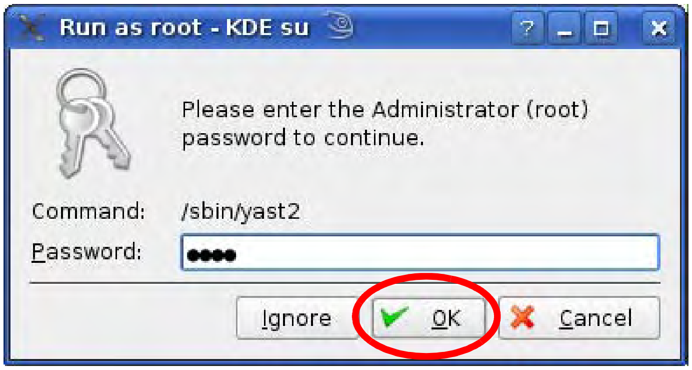
Note: Make sure you are logged in as the root administrator.

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**.

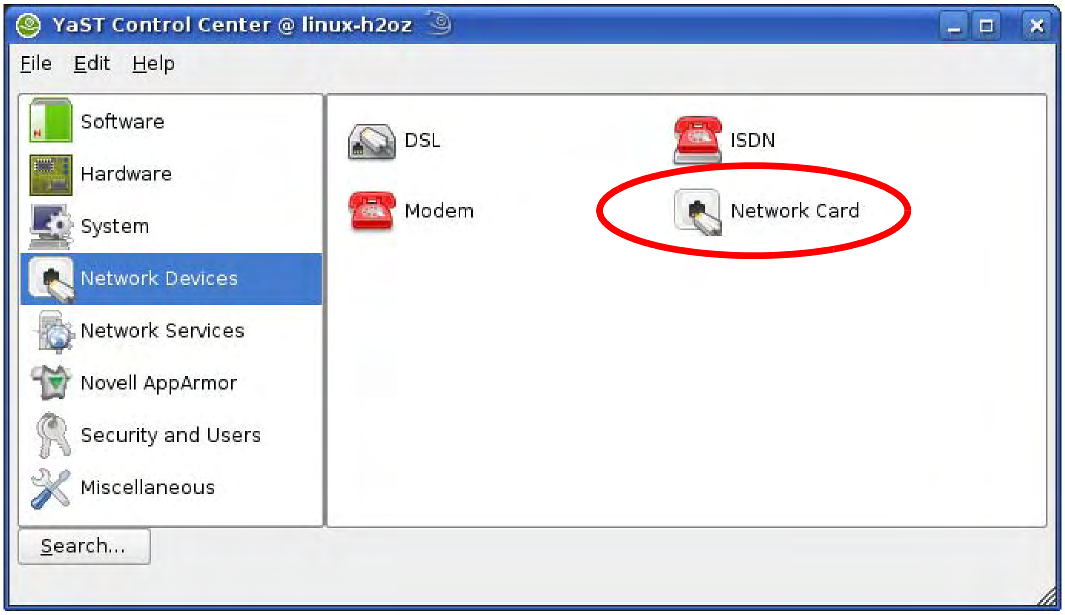


Please enter the Administrator (root) password to continue.

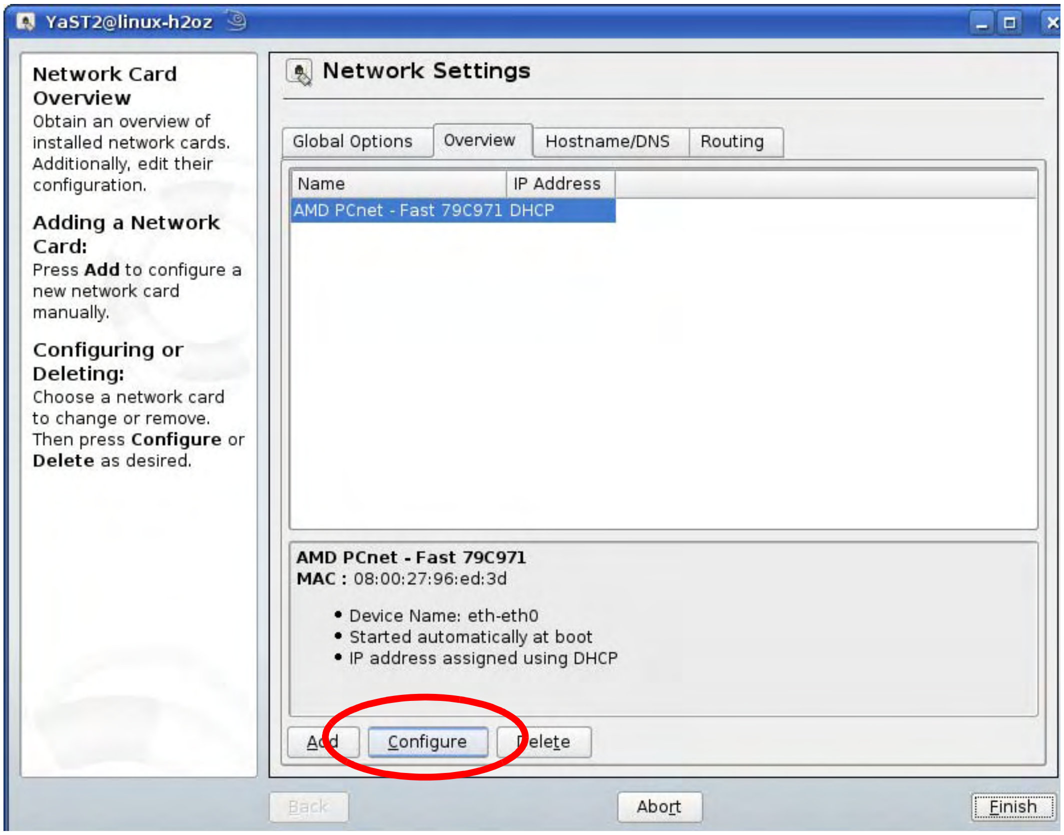
Command: /sbin/yast2

Password: ●●●●

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.



Network Card Overview
Obtain an overview of installed network cards. Additionally, edit their configuration.

Adding a Network Card:
Press **Add** to configure a new network card manually.

Configuring or Deleting:
Choose a network card to change or remove. Then press **Configure** or **Delete** as desired.

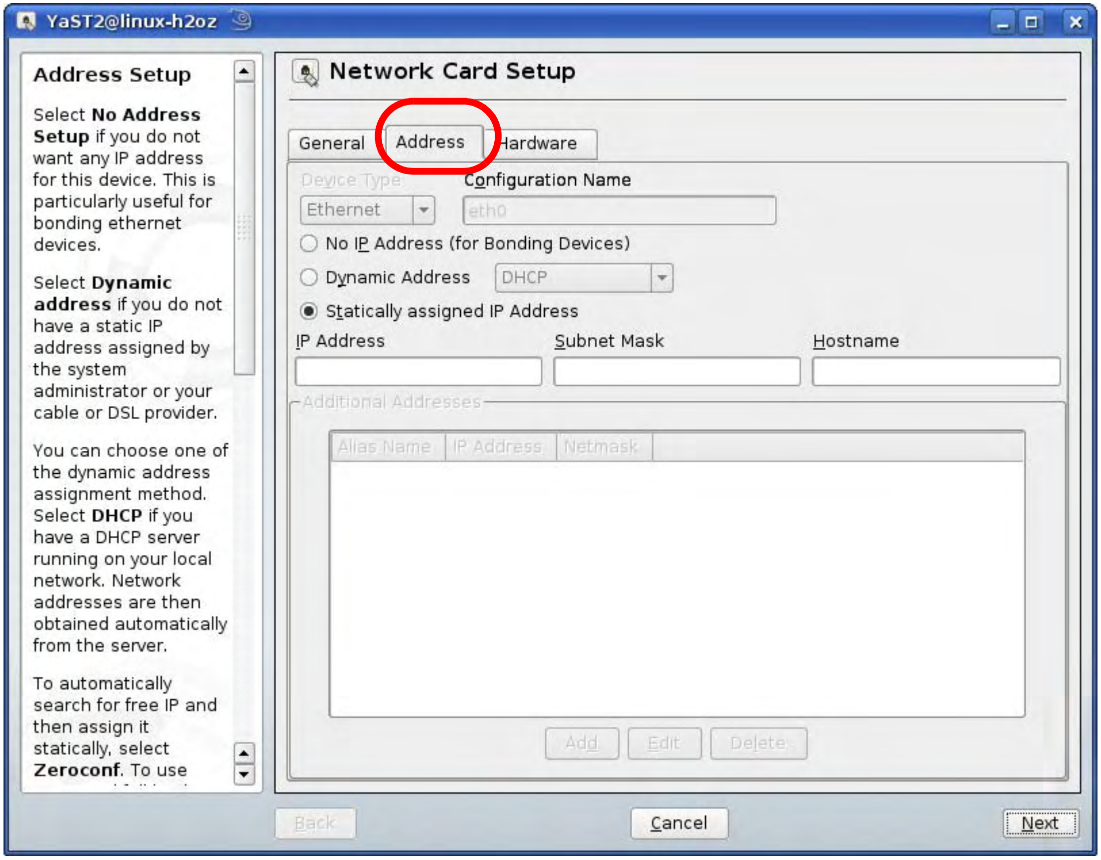
Name	IP Address
AMD PCnet - Fast 79C971	DHCP

AMD PCnet - Fast 79C971
MAC : 08:00:27:96:ed:3d

- Device Name: eth-eth0
- Started automatically at boot
- IP address assigned using DHCP

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

Figure 70 openSUSE 10.3: Network Card Setup



Address Setup

Select **No Address Setup** if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.

Select **Dynamic address** if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.

You can choose one of the dynamic address assignment method. Select **DHCP** if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.

To automatically search for free IP and then assign it statically, select **Zeroconf**. To use

Device Type: Ethernet

Configuration Name: eth0

○ No IP Address (for Bonding Devices)

○ Dynamic Address DHCP

● Statically assigned IP Address

IP Address:

Subnet Mask:

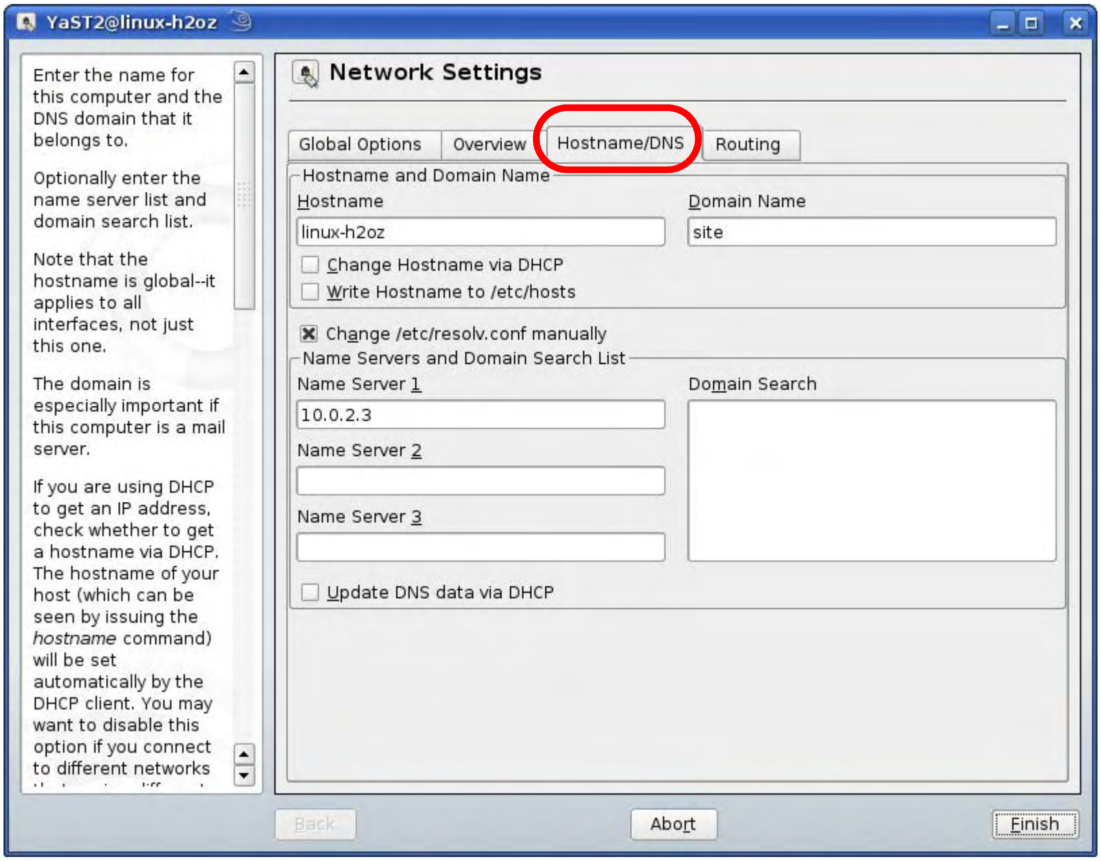
Hostname:

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.



YaST2@linux-h2oz

Enter the name for this computer and the DNS domain that it belongs to.

Optionally enter the name server list and domain search list.

Note that the hostname is global--it applies to all interfaces, not just this one.

The domain is especially important if this computer is a mail server.

If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the *hostname* command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks

Network Settings

Global Options | Overview | Hostname/DNS | Routing

Hostname and Domain Name

Hostname: linux-h2oz

Domain Name: site

□ Change Hostname via DHCP

□ Write Hostname to /etc/hosts

☒ Change /etc/resolv.conf manually

Name Servers and Domain Search List

Name Server 1: 10.0.2.3

Name Server 2:

Name Server 3:

Domain Search:

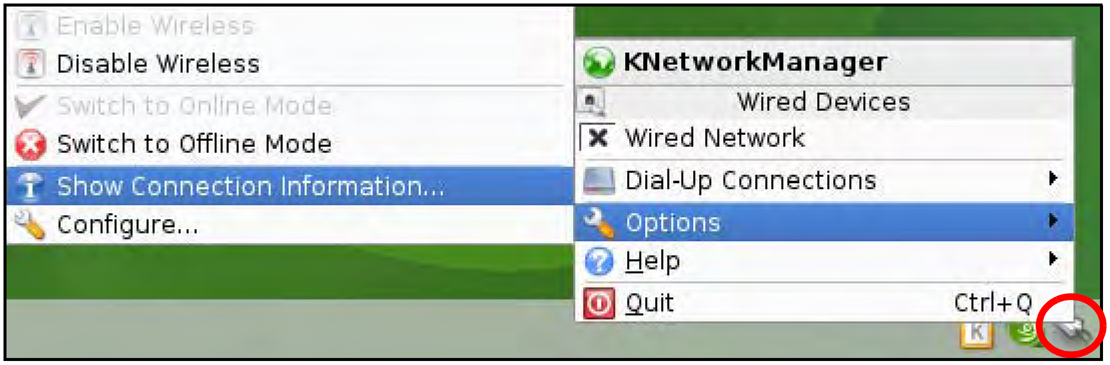
□ Update DNS data via DHCP

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

Verifying Settings

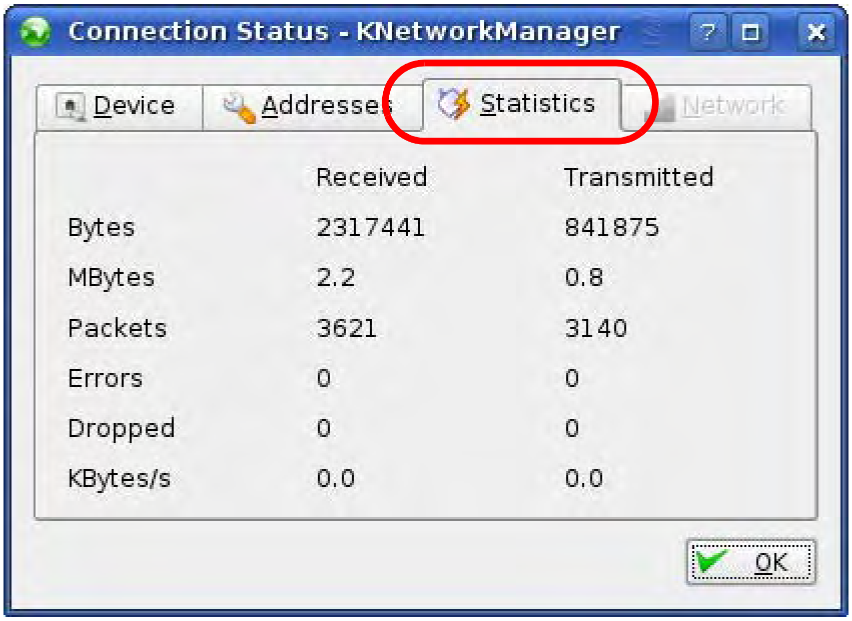
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 71 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 72 openSUSE: Connection Status - KNetwork Manager



	Received	Transmitted
Bytes	2317441	841875
MBytes	2.2	0.8
Packets	3621	3140
Errors	0	0
Dropped	0	0
KBytes/s	0.0	0.0

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

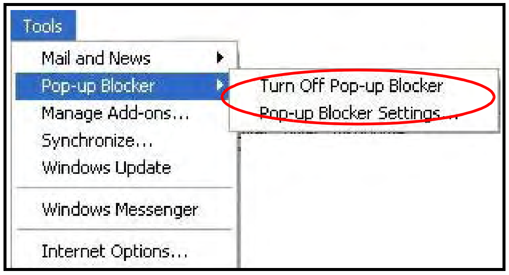
You may have to disable pop-up blocking to log into your device.

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 73 Pop-up Blocker

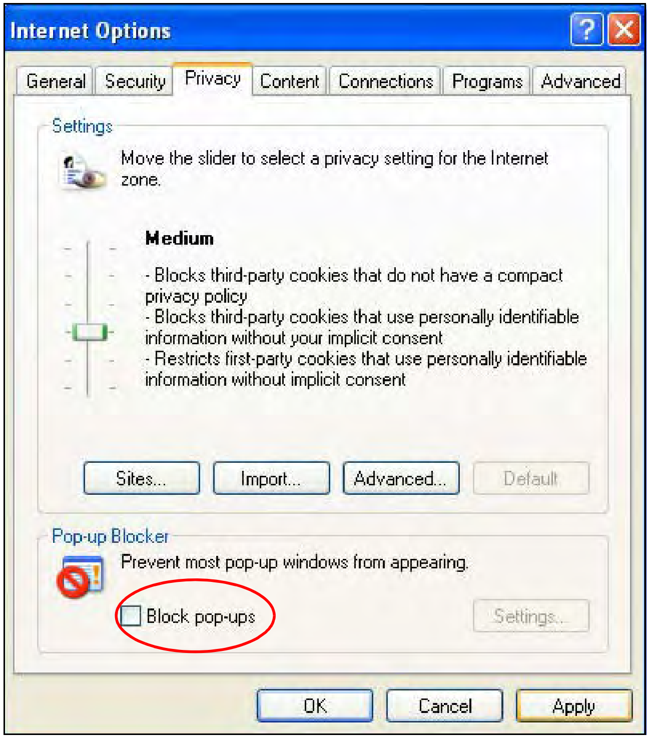


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 74 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

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

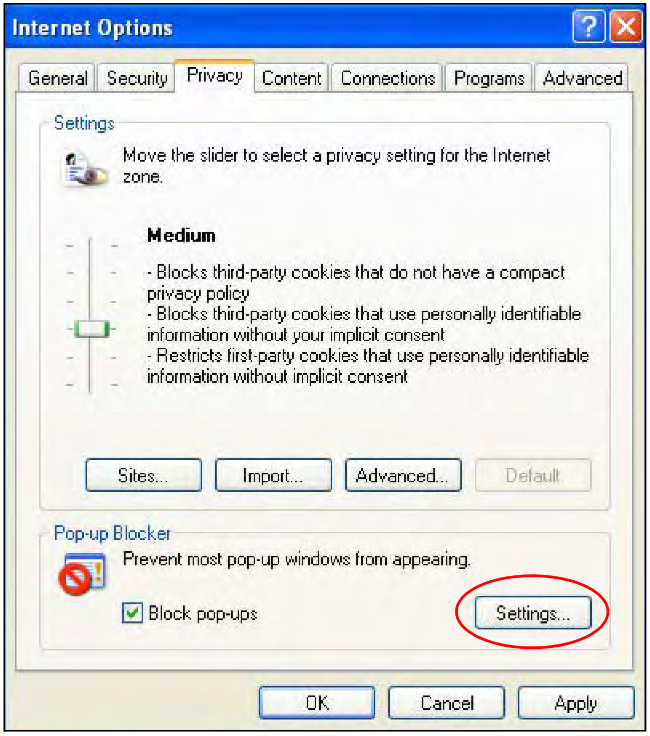
Enable Pop-up Blockers with Exceptions

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 75 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

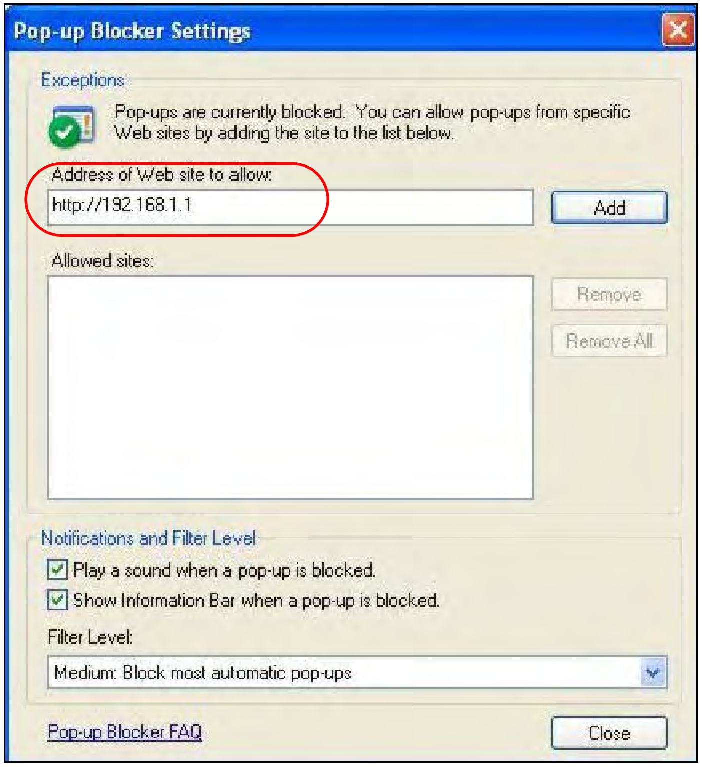
Prevent most pop-up windows from appearing.

☑ Block pop-ups

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.

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

Figure 76 Pop-up Blocker Settings



Address of Web site to allow: http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

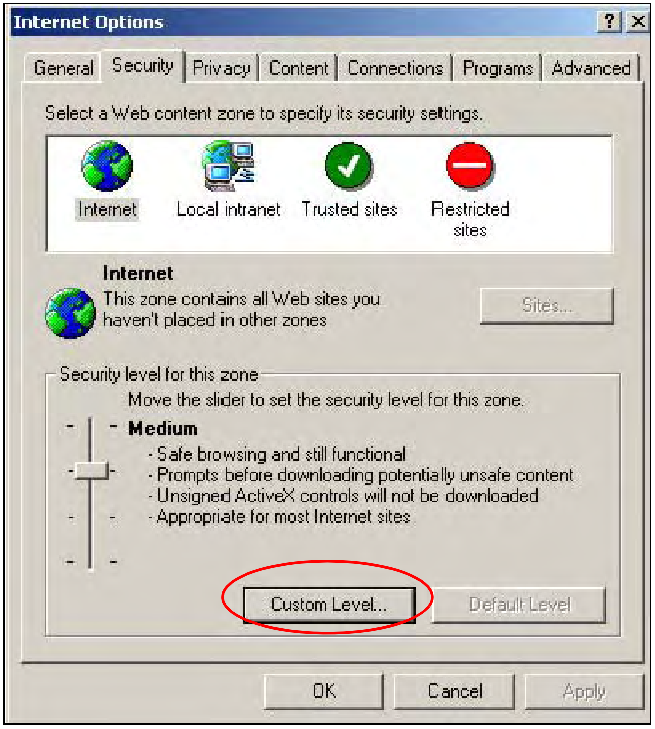
6 Click **Apply** to save this setting.

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 77 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

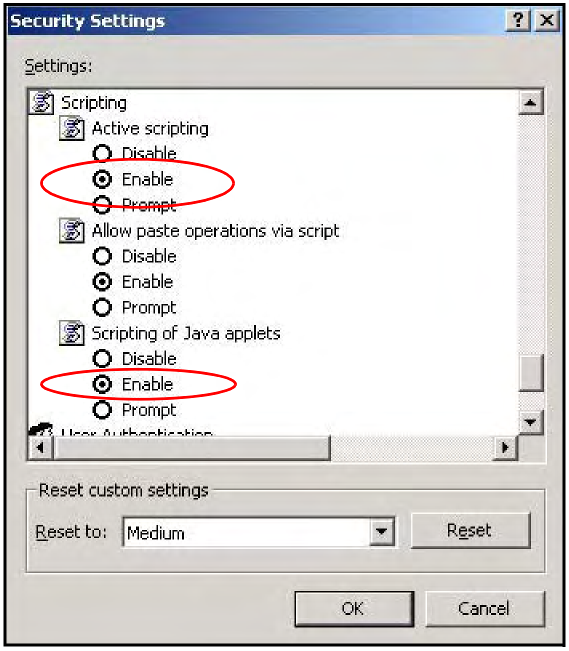
3 Scroll down to **Scripting**.

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 78 Security Settings - Java Scripting



Security Settings

Settings:

Scripting

Active scripting

○ Disable

● Enable

○ Prompt

Allow paste operations via script

○ Disable

● Enable

○ Prompt

Scripting of Java applets

○ Disable

● Enable

○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

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

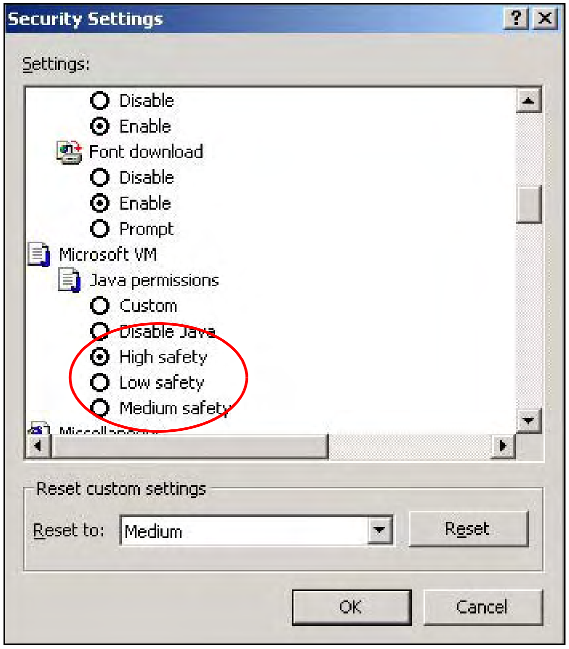
2 Click the **Custom Level...** button.

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 79 Security Settings - Java



○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

Reset to: Medium

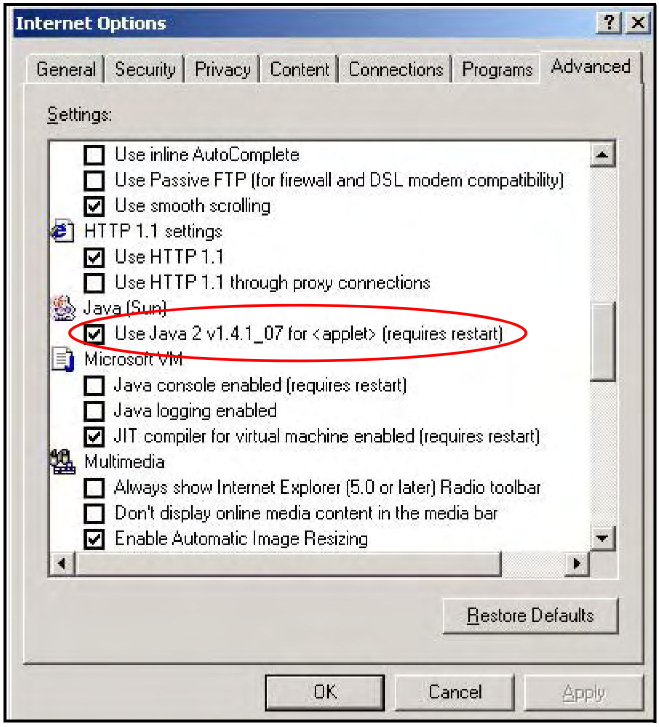
JAVA (Sun)

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 80 Java (Sun)



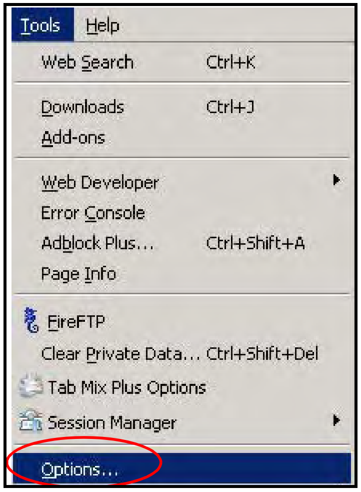
□ Use inline AutoComplete
□ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
□ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
□ Java console enabled (requires restart)
□ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
□ Always show Internet Explorer (5.0 or later) Radio toolbar
□ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

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.

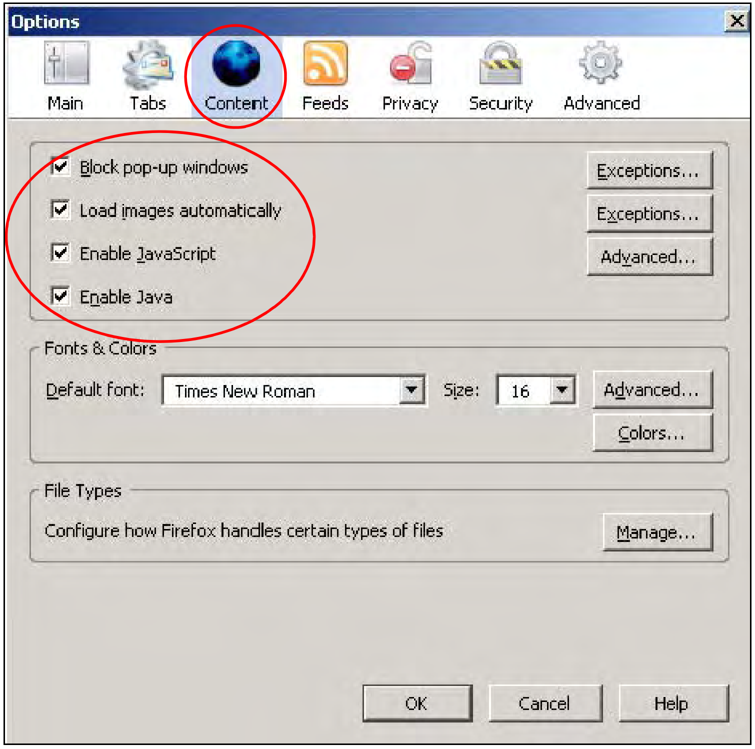
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 81 Mozilla Firefox: TOOLS > Options



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

Figure 82 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Default font: Times New Roman Size: 16

Configure how Firefox handles certain types of files

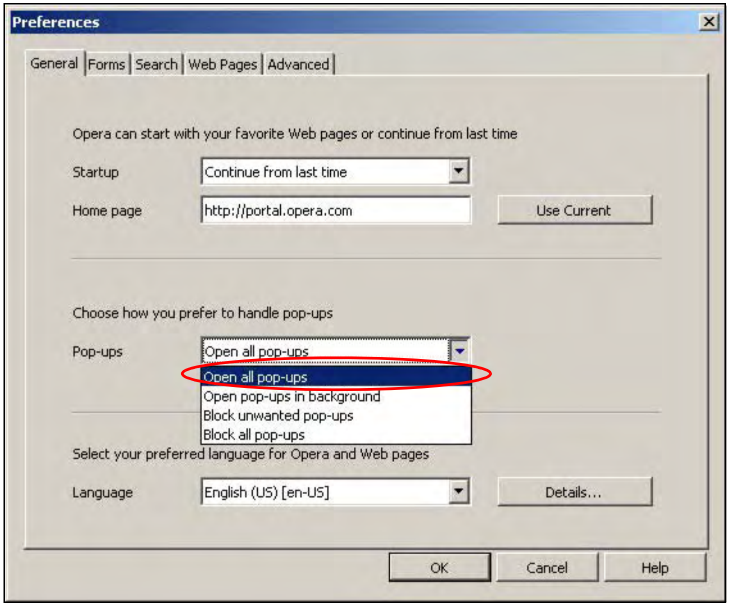
Opera

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 83 Opera: Allowing Pop-Ups



Preferences

General | Forms | Search | Web Pages | Advanced

Opera can start with your favorite Web pages or continue from last time

Startup: Continue from last time

Home page: http://portal.opera.com

Use Current

Choose how you prefer to handle pop-ups

Pop-ups: Open all pop-ups

- Open all pop-ups
- Open pop-ups in background
- Block unwanted pop-ups
- Block all pop-ups

Select your preferred language for Opera and Web pages

Language: English (US) [en-US]

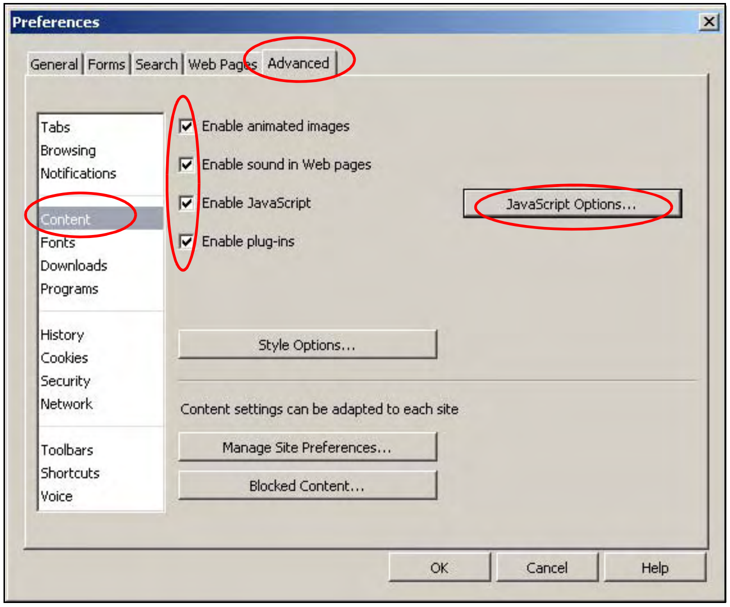
Details...

OK | Cancel | Help

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 84 Opera: Enabling Java



Preferences

General | Forms | Search | Web Pages | Advanced

Tabs
Browsing
Notifications
Content
Fonts
Downloads
Programs
History
Cookies
Security
Network
Toolbars
Shortcuts
Voice

☑ Enable animated images

☑ Enable sound in Web pages

☑ Enable JavaScript

☑ Enable plug-ins

JavaScript Options...

Style Options...

Content settings can be adapted to each site

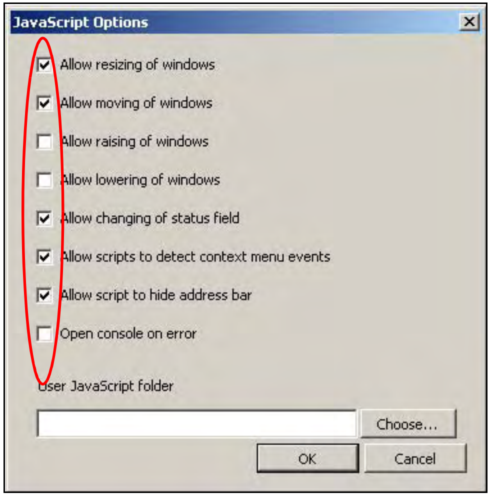
Manage Site Preferences...

Blocked Content...

OK | Cancel | Help

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

Figure 85 Opera: JavaScript Options



☑ Allow resizing of windows

☑ Allow moving of windows

☐ Allow raising of windows

☐ Allow lowering of windows

☑ Allow changing of status field

☑ Allow scripts to detect context menu events

☑ Allow script to hide address bar

☐ Open console on error

User JavaScript folder

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.

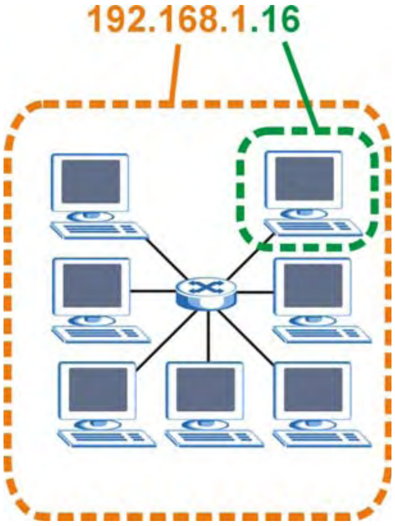
Structure

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 86 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 39 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 40 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 41 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 42 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

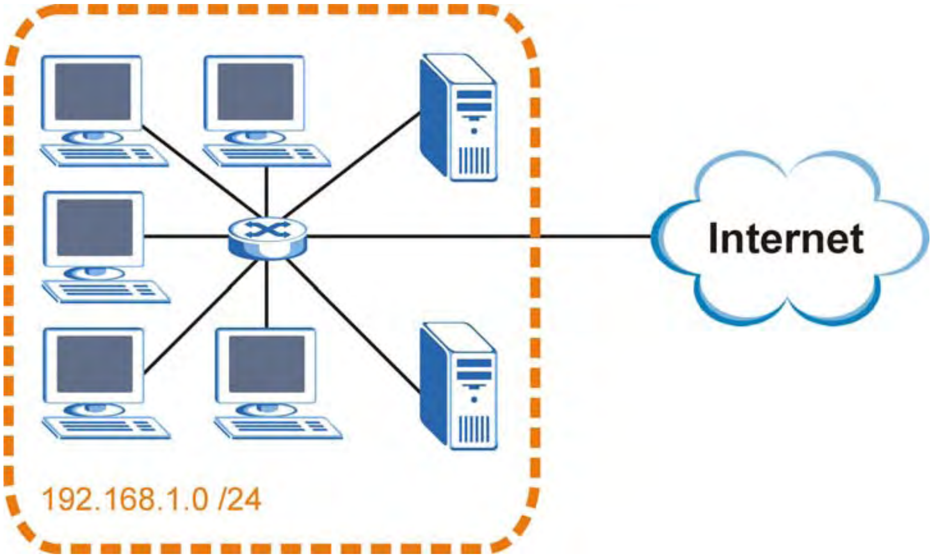
Subnetting

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 87 Subnetting Example: Before Subnetting

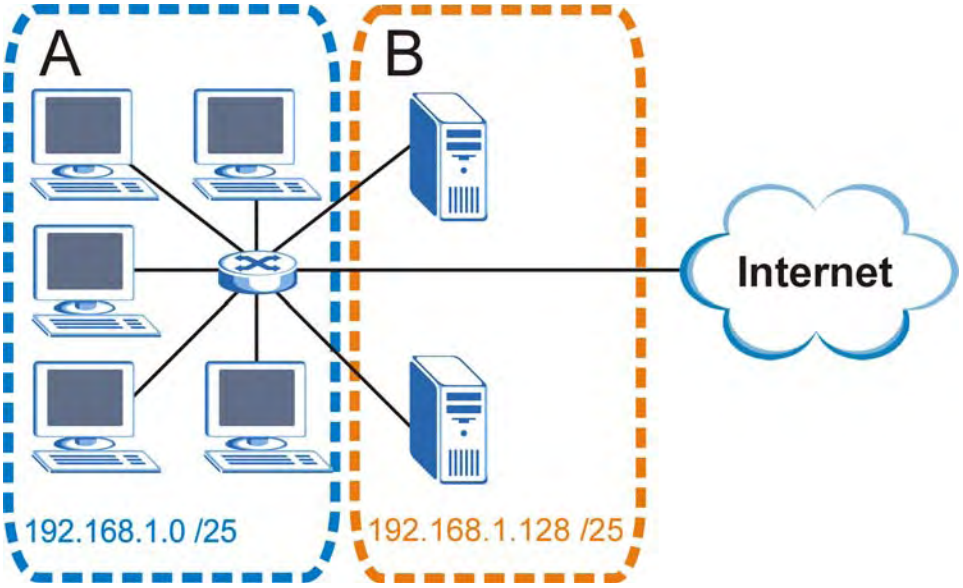


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 88 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.**11**000000) 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 43 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 43 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 44 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 45 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 46 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
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 47 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 48 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 49 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 49 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 NWA.

Once you have decided on the network number, pick an IP address for your NWA 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 NWA 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 NWA 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.*

D

IPv6

Overview

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 x 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 50 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.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 51 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 52 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0

Table 52 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block’s 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 53

MAC	00	:	13	:	49 : 12	:	34	:	56

Table 54

EUI-64	02	:	13	:	49 :	FF	:	FE	: 12	:	34	:	56

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don’t need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see Interface ID and EUI-64) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the NWA is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates [1]another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

DHCPv6

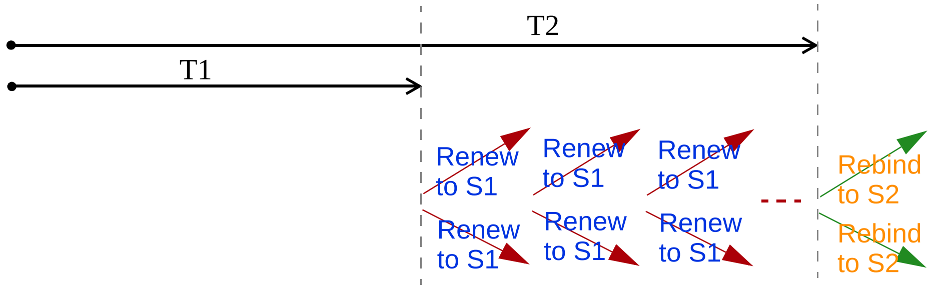
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique IDentifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string,

[1] In IPv6, all network interfaces can be associated with several addresses.

such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The NWA uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the NWA passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor’s reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor’s link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being “reachable” means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The NWA maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the NWA configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the NWA also sends out a neighbor solicitation message. When the NWA receives a neighbor advertisement in response, it stores the neighbor’s link-layer address in the neighbor cache. When the NWA uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router’s information to the neighbor cache, prefix list and destination cache. The NWA creates an entry in the default router list cache if the router can be used as a default router.

When the NWA needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the NWA uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the NWA determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the NWA looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the NWA cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

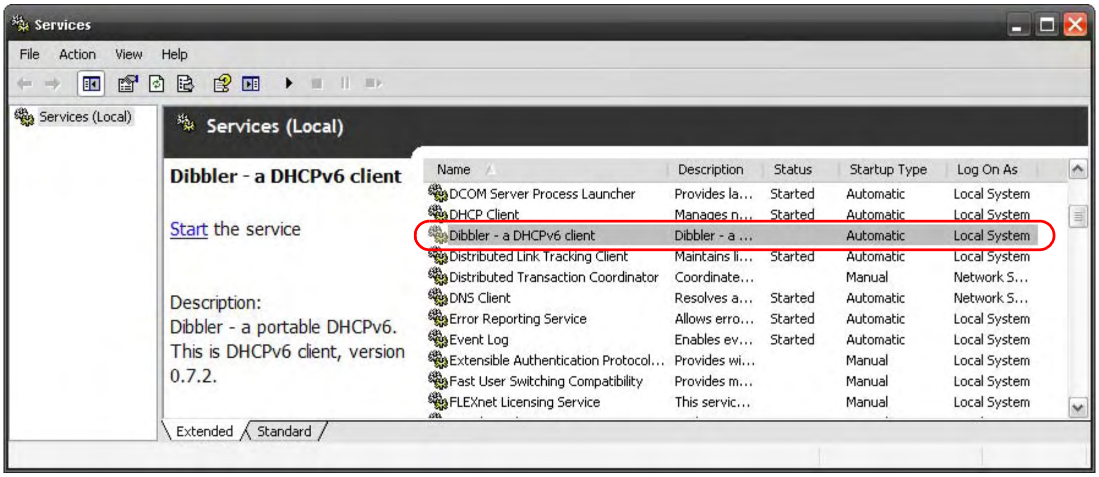
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1 Install Dibbler and select the DHCPv6 client option on your computer.

2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

3 Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



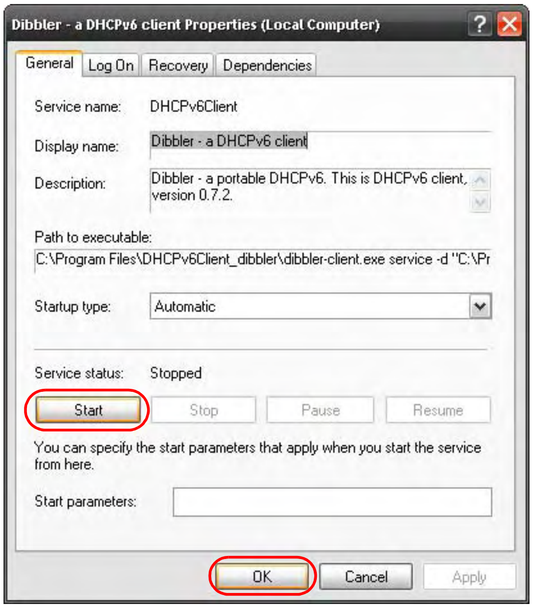
Dibbler - a DHCPv6 client

Start the service

Description:
Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Name	Description	Status	Startup Type	Log On As
DCOM Server Process Launcher	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Dibbler - a DHCPv6 client	Dibbler - a ...		Automatic	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Service	Allows erro...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
Extensible Authentication Protocol...	Provides wi...		Manual	Local System
Fast User Switching Compatibility	Provides m...		Manual	Local System
FLEXnet Licensing Service	This servic...		Manual	Local System

5 Click **Start** and then **OK**.



Service name: DHCPv6Client

Display name: Dibbler - a DHCPv6 client

Description: Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Path to executable:
C:\Program Files\DHCPv6Client_dibbler\dibbler-client.exe service -d "C:\Pr

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

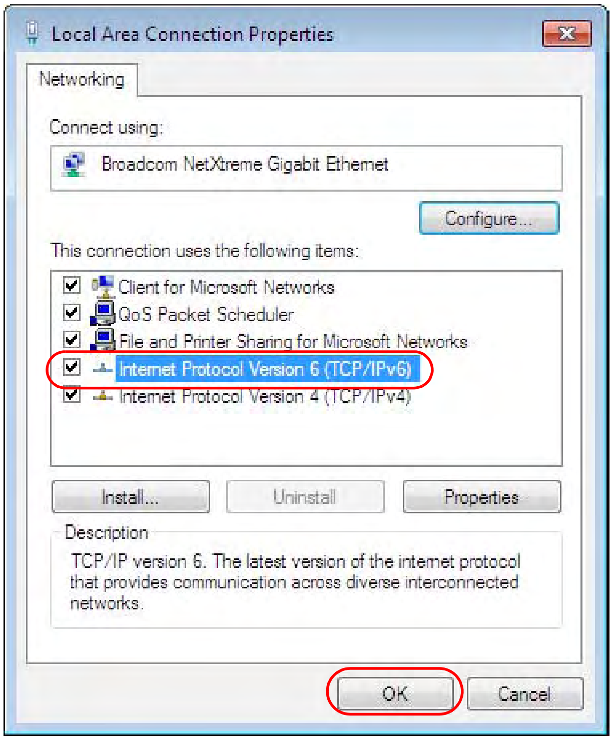
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.



Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the ipconfig command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

Wireless LANs

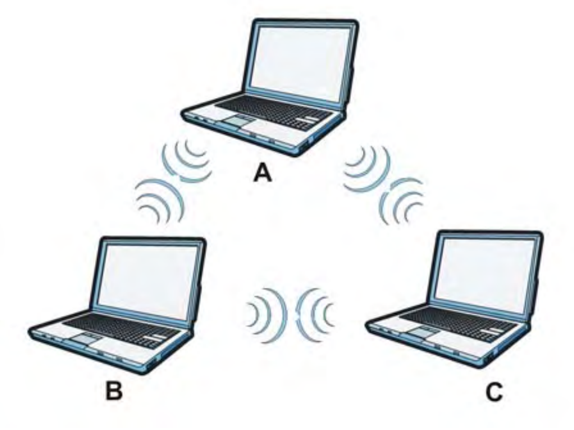
Wireless LAN Topologies

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 89 Peer-to-Peer Communication in an Ad-hoc Network

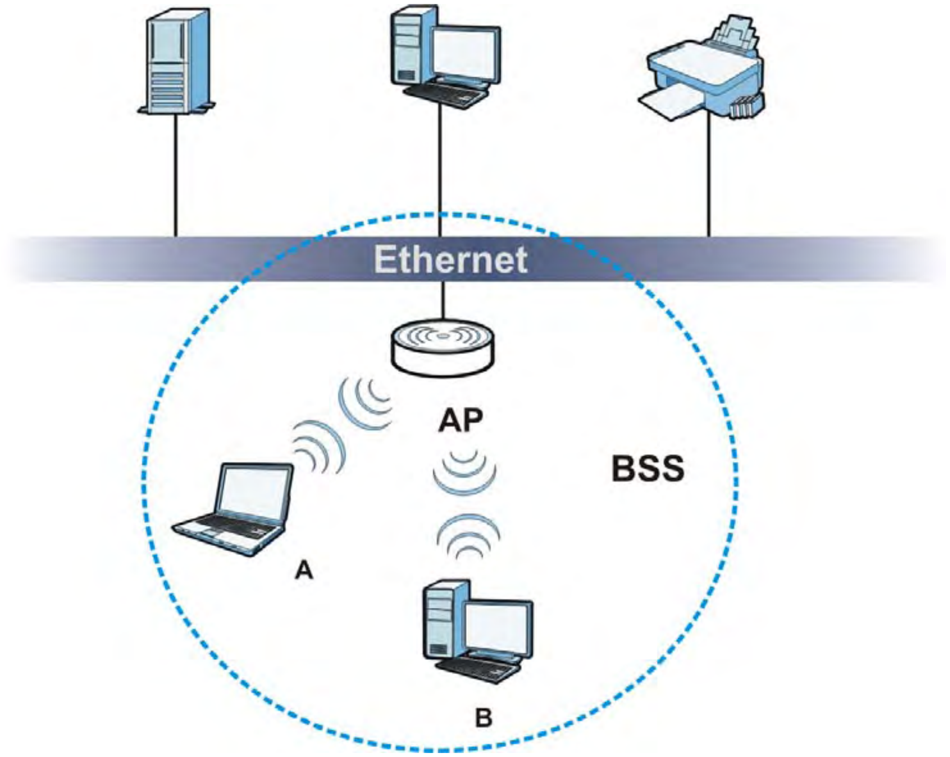


BSS

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 90 Basic Service Set



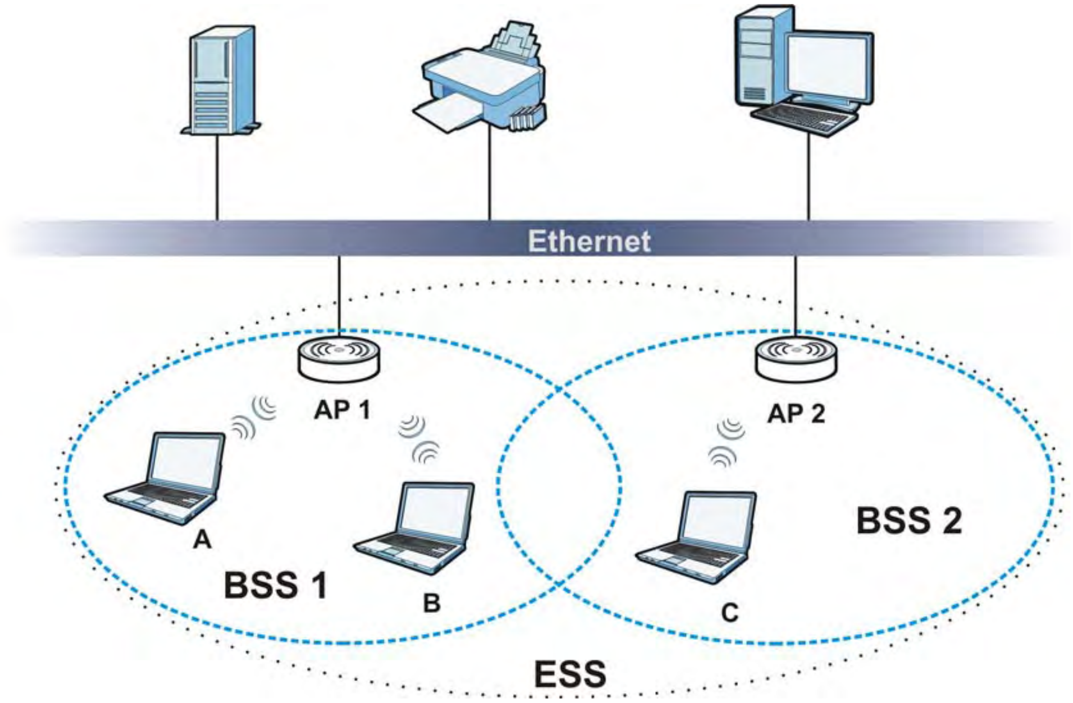
ESS

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 91 Infrastructure WLAN



Channel

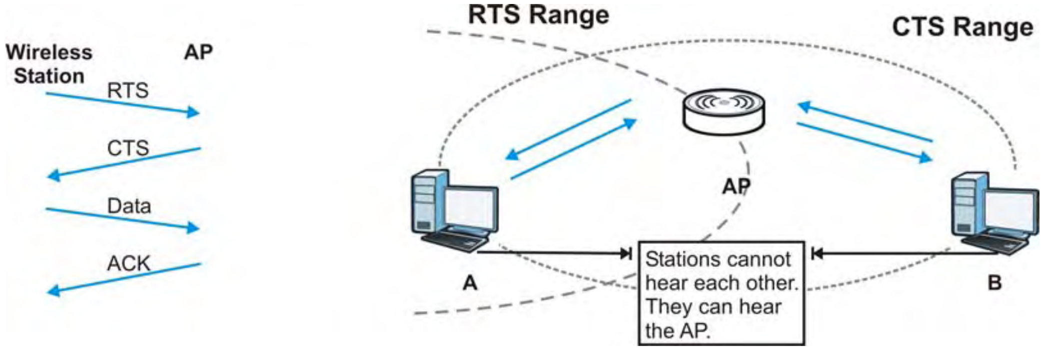
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 92 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.

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

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 NWA uses long preamble.

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

Wireless LAN Standards

The IEEE 802.11b wireless access standard was first published in 1999. IEEE 802.11b has a maximum data rate of 11 Mbps and uses the 2.4 GHz band.

IEEE 802.11g also works in the 2.4 GHz band and 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 (54 Mbps and 1 Mbps respectively).

IEEE 802.11a has a data rate of up to 54 Mbps using the 5 GHz band. IEEE 802.11a is not interoperable with IEEE 802.11b or IEEE 802.11g.

IEEE 802.11n can operate both in the 2.4 GHz and 5 GHz bands and is backward compatible with the IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g standards. It improves network throughput and increases the maximum raw data rate from 54 Mbps to 300 Mbps by using multiple-input multiple-output (MIMO), a channel width of 40 MHz, frame aggregation and short guard interval.

Table 55 Wireless LAN Standards Comparison Table

WIRELESS LAN STANDARD	MAXIMUM NET DATA RATE	FREQUENCY BAND	COMPATIBILITY
IEEE 802.11b	11 Mbps	2.4 GHz	IEEE 802.11g IEEE 802.11n
IEEE 802.11g	54 Mbps	2.4 GHz	IEEE 802.11b IEEE 802.11n
IEEE 802.11a	54 Mbps	5 GHz	IEEE 802.11n
IEEE 802.11n	300 Mbps	2.4 GHz, 5 GHz	IEEE 802.11b IEEE 802.11g IEEE 802.11a

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 NWA are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NWA identity.

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

Table 56 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
Most Secure	WPA2

Note: You must enable the same wireless security settings on the NWA 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 57 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

WPA2

WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management.

Key differences between 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.

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

Encryption

WPA2 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.

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 WPA2 and WPA2-PSK are the same. The only difference between the two is that WPA2-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA2-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 prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

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. 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 with 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 WPA2 Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA2. At the time of writing, the most widely available supplicant is the WPA2 patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA2 capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA2 with RADIUS Application Example

To set up WPA2, you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA2 application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

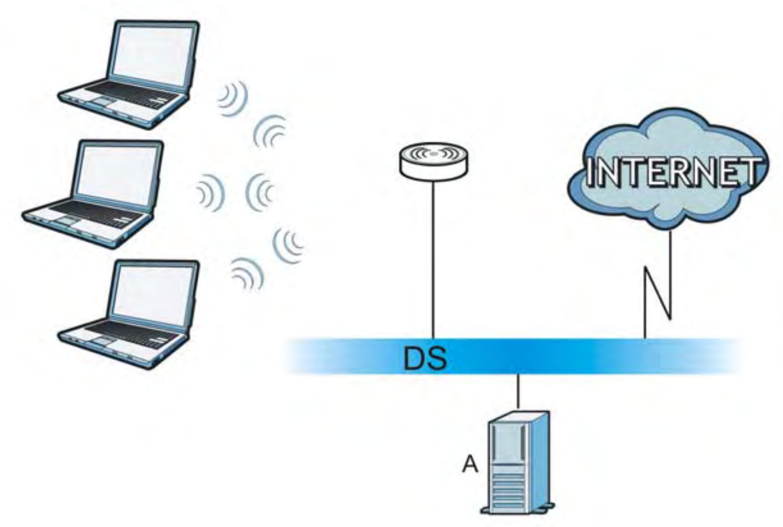
1 The AP passes the wireless client's authentication request to the RADIUS server.

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 93 WPA2 with RADIUS Application Example



WPA2-PSK Application Example

A WPA2-PSK application looks as follows.

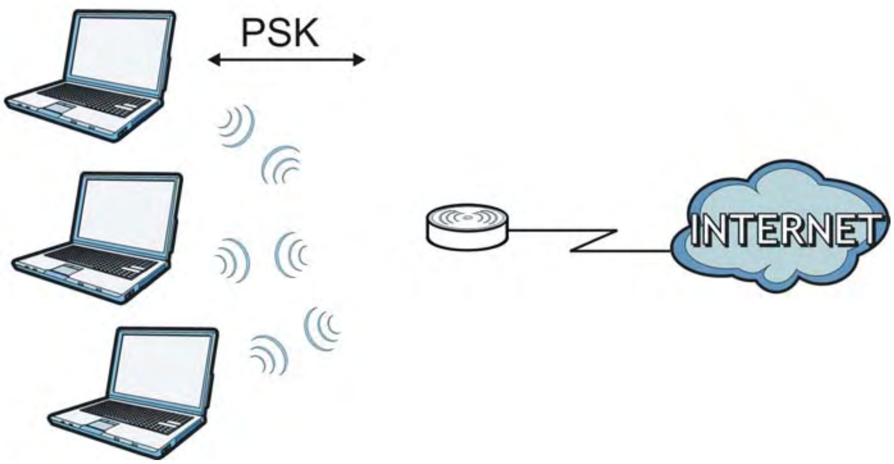
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

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 94 WPA2-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 58 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTIO N 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
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.