NWA1100-N

802.11b/g/n PoE Access Point

User's Guide

Default Login Details

IP Address	http://192.168.1.2
Password	1234

Firmware Version 1.00
Edition 1, 3/2011

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NWA using the web configurator.

Tips for Reading User’s Guides On-Screen

When reading a ZyXEL User’s Guide On-Screen, keep the following in mind:

- If you don’t already have the latest version of Adobe Reader, you can download it from http://www.adobe.com.
- Use the PDF’s bookmarks to quickly navigate to the areas that interest you. Adobe Reader’s bookmarks pane opens by default in all ZyXEL User’s Guide PDFs.
- If you know the page number or know vaguely which page-range you want to view, you can enter a number in the toolbar in Reader, then press [ENTER] to jump directly to that page.
- Type [CTRL]+[F] to open the Adobe Reader search utility and enter a word or phrase. This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader.
- To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a “hand” with which you can grab the page and move it around freely on your screen.
- Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User’s Guide PDF.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get your NWA up and running right away. It contains information on setting up your network and configuring for Internet access.
- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

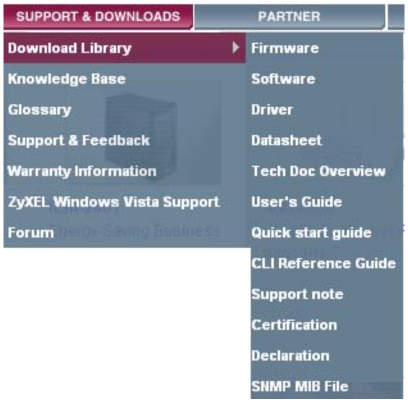
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the documentation in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your NWA.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

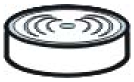
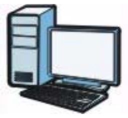
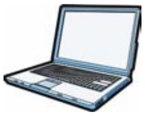
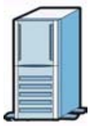
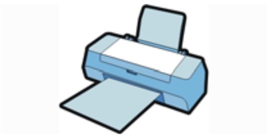
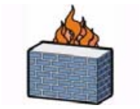
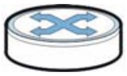
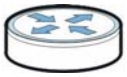
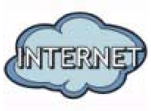
- The NWA1100-N may be referred to as the "NWA", the "device", or the "ZyXEL Device" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide use the following generic icons. The NWA icon is not an exact representation of your NWA.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Table 1 Common Icons

NWA 	Computer 	Notebook 
Server 	Printer 	Firewall 
Switch 	Router 	Internet Cloud 

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- This product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

Table of Contents

PART I
User's Guide

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

Your NWA extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

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

Your 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.

1.2 Applications for the NWA

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

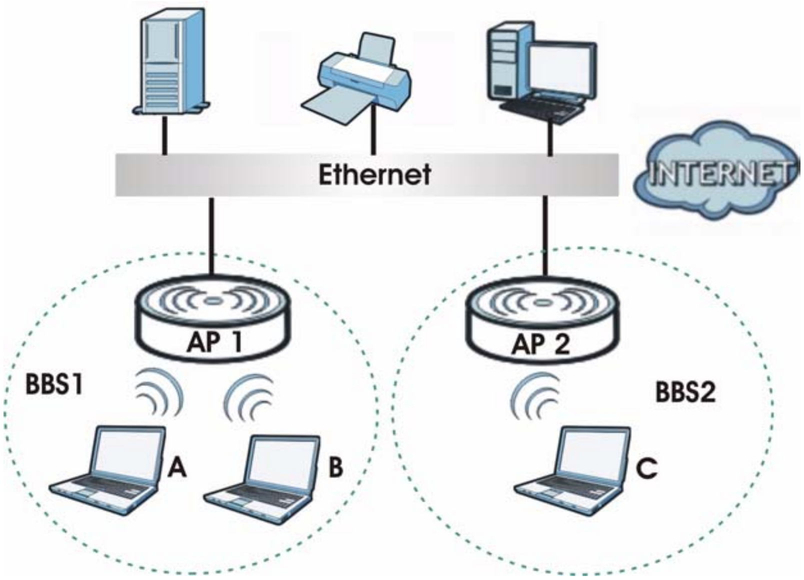
1. Access Point
2. Bridge/Repeater
3. AP + Bridge
4. Wireless Client
5. MBSSID

Applications for each operating mode are shown below.

1.2.1 Access Point

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

Figure 1 Access Point Application



1.2.2 Bridge / Repeater

The NWA can act as a wireless network bridge and establish wireless links with other APs. In the figure below, the two NWAs (**A** and **B**) are connected to independent wired networks and have a bridge connection (**A** can communicate with **B**) at the same time. A NWA in repeater mode (**C** in Figure 3) has no Ethernet connection. When the NWA is in bridge mode, you should enable Spanning Tree Protocol (STP) to prevent bridge loops.

When the NWA is in **Bridge / Repeater mode**, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See Section 6.4.2 on page 65 for more details.

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

At the time of writing, WDS security is compatible with other ZyXEL NWA-series access points only. Refer to your other access point's documentation for details.

Figure 2 Bridge Application

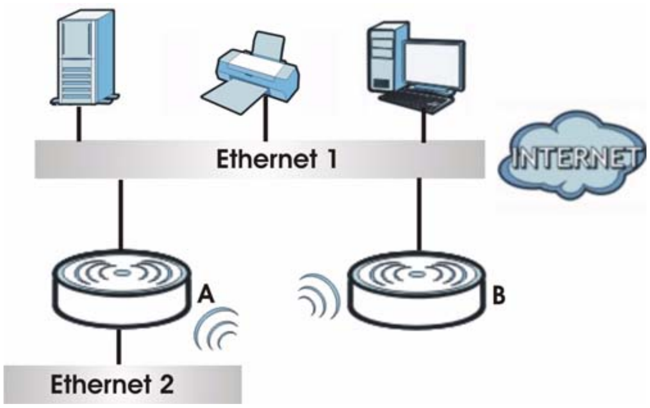
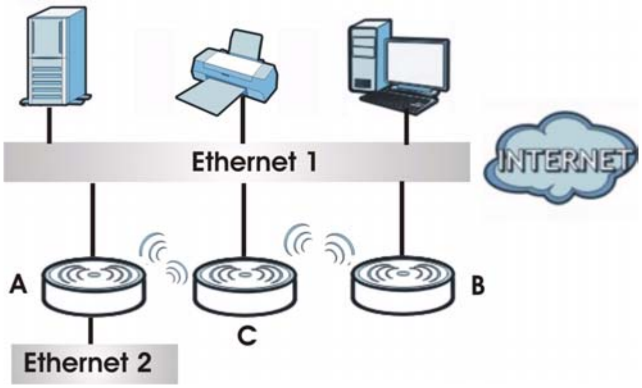


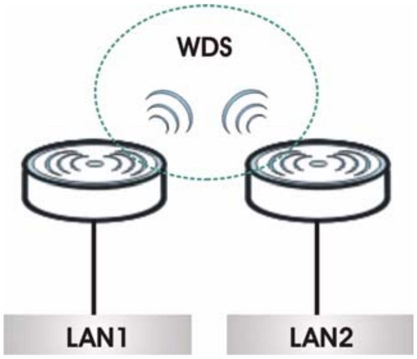
Figure 3 Repeater Application



1.2.2.1 Bridge / Repeater Mode Example

In the example below, when both NWAs are in **Bridge mode**, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

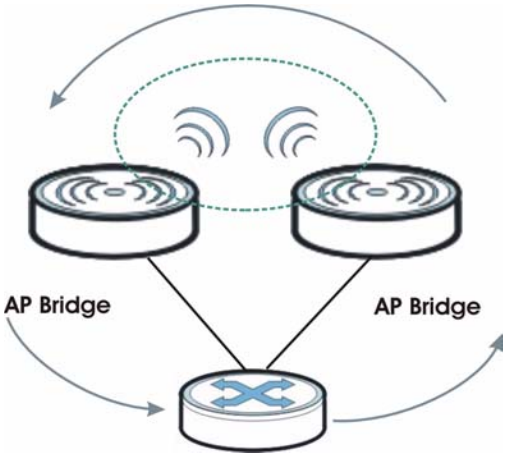
Figure 4 Bridging Example



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

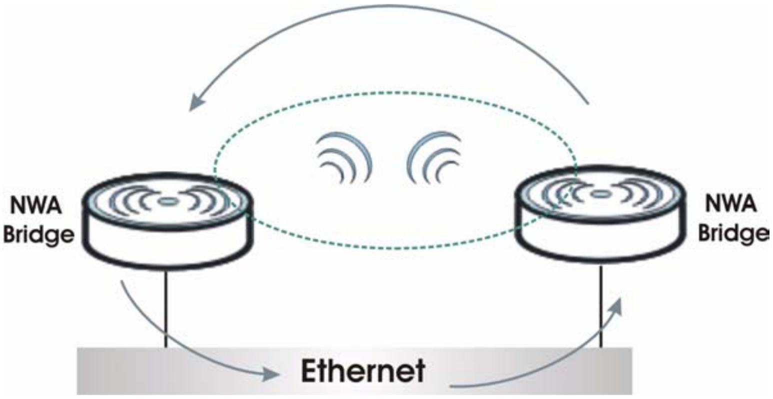
- If two or more NWAs (in bridge mode) are connected to the same hub.

Figure 5 Bridge Loop: Two Bridges Connected to Hub



- If your NWA (in **Bridge mode**) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN.

Figure 6 Bridge Loop: Bridge Connected to Wired LAN



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

1.2.3 AP + Bridge

In **AP+Bridge mode**, the NWA supports both AP and bridge connection at the same time.

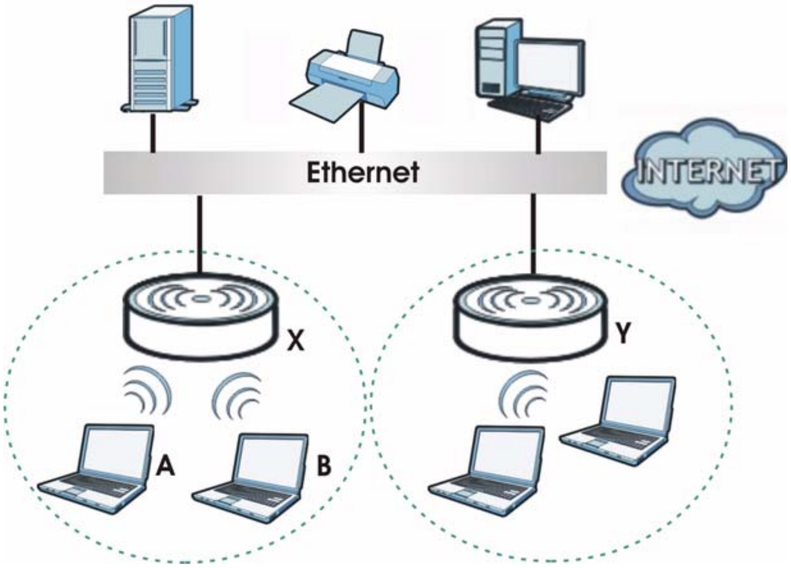
In the figure below, **A** and **B** use **X** as an AP to access the wired network, while **X** and **Y** communicate in bridge mode.

Using **AP + Bridge mode**, your NWA can extend the range of the WLAN. In the figure below, **A** and **B** act as AP + Bridge devices that forward traffic between associated wireless workstations and the wired LAN.

When the NWA is in **AP+Bridge** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See Section 6.4.3 on page 69 for more details.

Unless specified, the term “security settings” refers to the traffic between the wireless stations and the NWA.

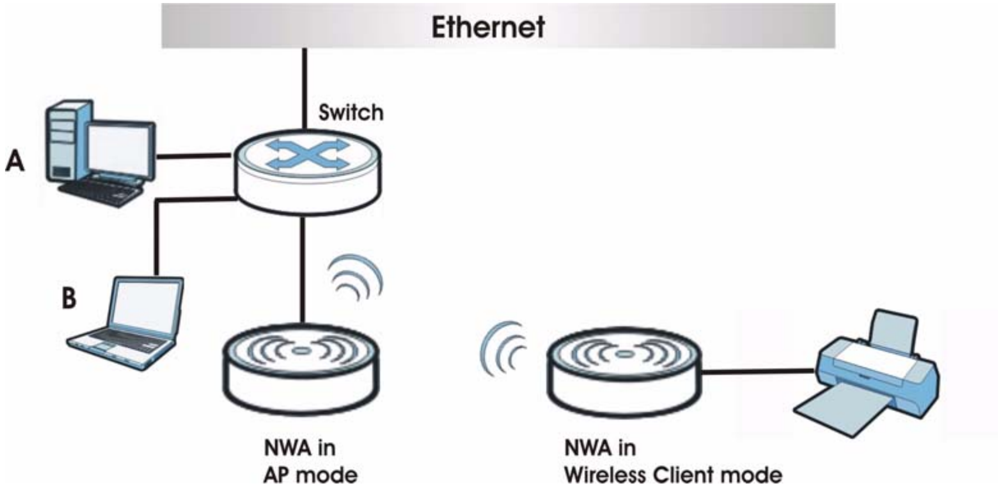
Figure 7 AP + Bridge Application



1.2.4 Wireless Client

The NWA can be used as a wireless client to communicate with an existing network. In the figure below, the printer can receive requests from the wired computer clients A and B via the NWA in Wireless Client mode.

Figure 8 Wireless Client Application



1.2.5 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.

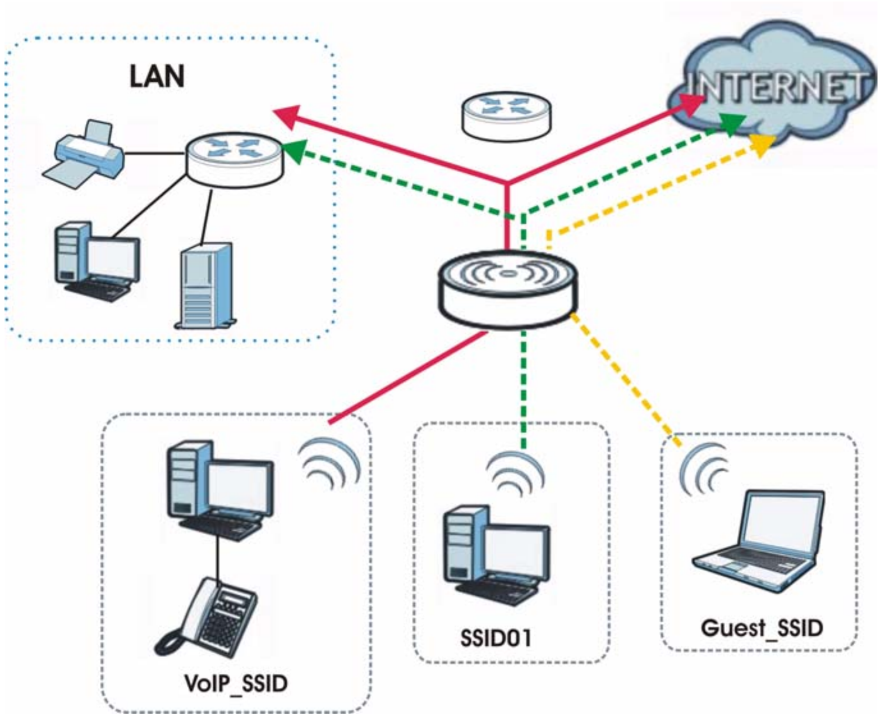
You can configure up to eight SSID profiles, and have up to four active at any one time.

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 9 Multiple BSSs



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.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP (File Transfer Protocol) for firmware upgrades.
- SNMP (Simple Network Management Protocol). The device can be monitored by an SNMP manager.

1.4 Configuring Your 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.
- Avoid setting a long timeout period before the NWA’s web configurator automatically times out. A short timeout reduces the risk of unauthorized person accessing the web configurator while it is left idle.
- See Chapter 5 on page 55 for instructions on changing your password and setting the timeout period.
- Configure remote management to control who can manage your NWA. See Chapter 12 on page 109 for more information. If you enable remote management, ensure you have enabled remote management only on the IP addresses, services or interfaces you intended and that other remote management settings are disabled.

1.4.2 Wireless Security

Wireless devices are especially vulnerable to attack. If your NWA has a wireless function, 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 8.4 on page 87 for directions on configuring encryption. If you have a RADIUS server, enable IEEE 802.1x or WPA(2) user identification on your network so users must log in. This method is more common in business environments.

- Hide your wireless network name (SSID). The SSID can be regularly broadcast and unauthorized users may use this information to access your network. See Section 6.4 on page 62 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 10.4 on page 103 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.

1.6 Hardware Connections

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

1.7 LEDs

Figure 10 LEDs

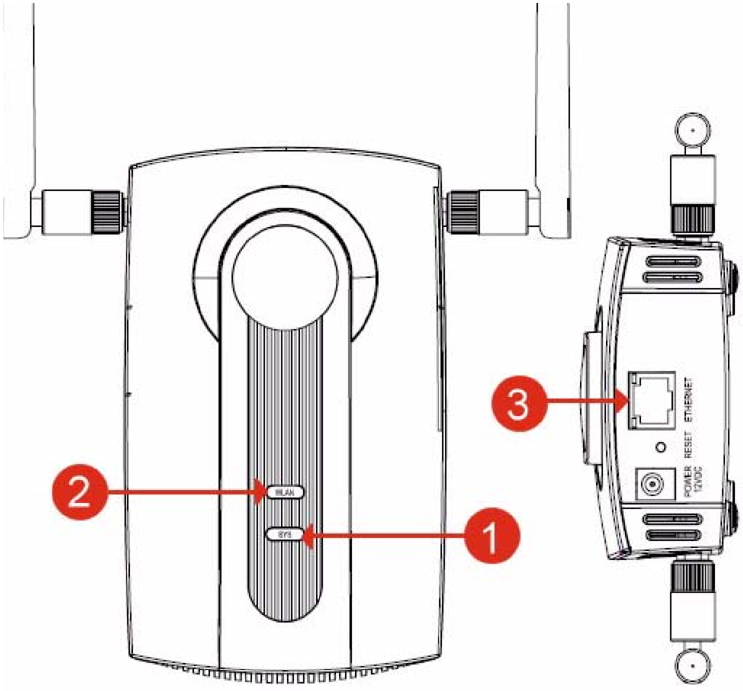


Table 2 LEDs

LABEL	LED	COLOR	STATUS	DESCRIPTION
1	SYS	Green	On	The NWA is receiving power and ready for use.
		Red	Flashing	There is system error and the NWA cannot boot up.
			Off	The NWA is not receiving power.
2	WLAN	Green	On	The wireless adaptor WLAN is active.
			Blinking	The wireless adaptor WLAN is active, and transmitting or receiving data.
			Off	The wireless adaptor WLAN is not active.
3	ETHERNET	Green	On	The NWA has a 10/100 Mbps Ethernet connection.
			Blinking	The NWA has a 10/100 Mbps Ethernet connection and is sending or receiving data.
		Yellow	On	The NWA has a 1000 Mbps Ethernet connection.
			Blinking	The NWA has a 1000 Mbps Ethernet connection and is sending/receiving data.
			Off	The NWA does not have an Ethernet connection.

Introducing the Web Configurator

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

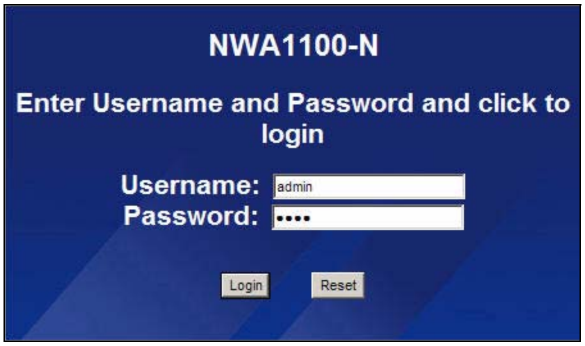
2.1 Accessing the Web Configurator

1 Make sure your hardware is properly connected and prepare your computer or computer network to connect to the 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 11 The Login Screen



NWA1100-N

Enter Username and Password and click to login

Username: admin

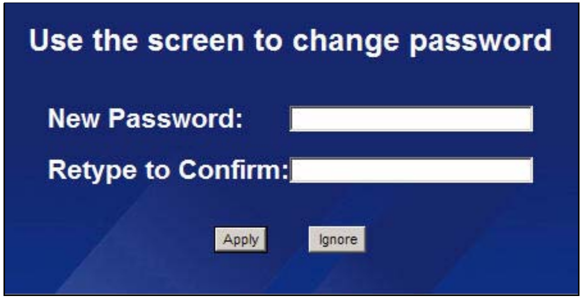
Password: ••••

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 12 Change Password Screen



Use the screen to change password

New Password:

Retype to Confirm:

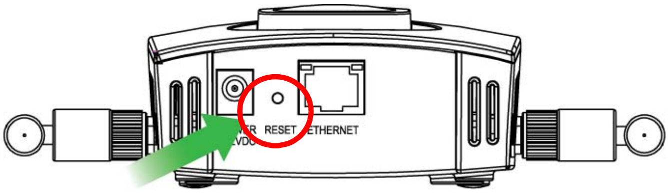
You should now see the **Status** screen. See Chapter 2 on page 29 for details about the **Status** screen.

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

2.2 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 13 The RESET Button



2.2.1 Methods of Restoring Factory-Defaults

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

Use the **RESET** button to upload the default configuration file. Hold this button in for about 10 seconds (the lights will begin to blink). Use this method for cases when the password or IP address of the NWA is not known.

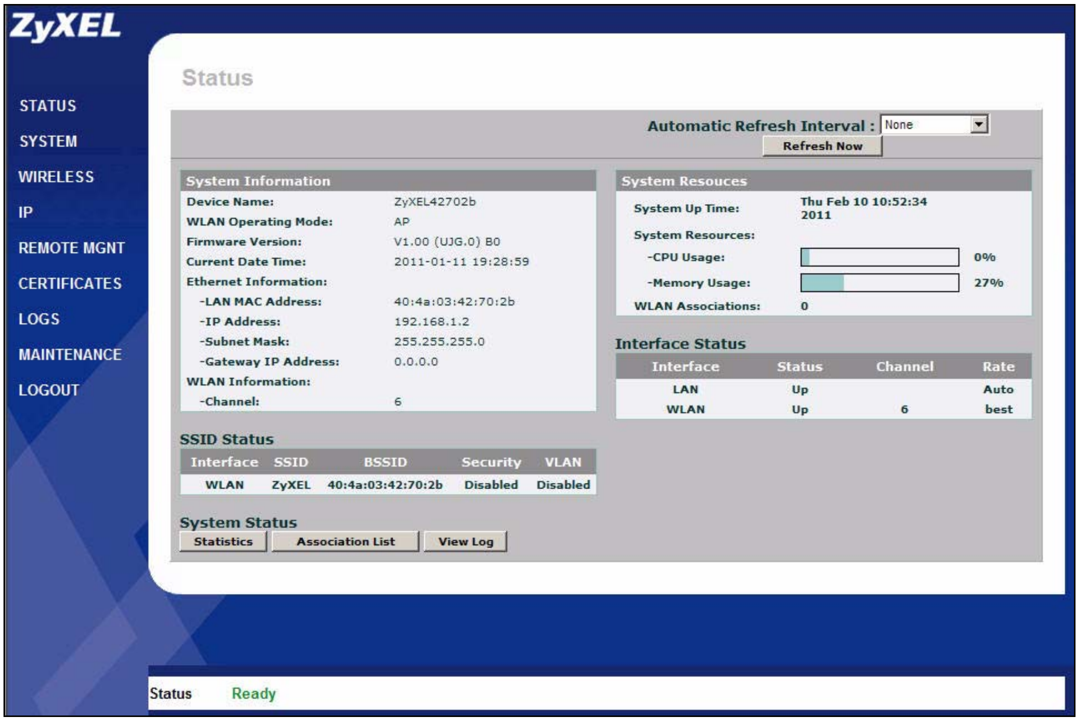
Use the web configurator to restore defaults (refer to Section 15.7 on page 133).

2.3 Navigating the Web Configurator

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

Check the status bar at the bottom of the screen when you click **Apply** or **OK** to verify that the configuration has been updated.

Figure 14 Status Screen of the Web Configurator



Status

Automatic Refresh Interval : None

System Information

Device Name:	ZyXEL42702b
WLAN Operating Mode:	AP
Firmware Version:	V1.00 (UJG.0) B0
Current Date Time:	2011-01-11 19:28:59
Ethernet Information:	
-LAN MAC Address:	40:4a:03:42:70:2b
-IP Address:	192.168.1.2
-Subnet Mask:	255.255.255.0
-Gateway IP Address:	0.0.0.0
WLAN Information:	
-Channel:	6

System Resouces

System Up Time:	Thu Feb 10 10:52:34 2011
System Resources:	
-CPU Usage:	0%
-Memory Usage:	27%
WLAN Associations:	0

Interface Status

Interface	Status	Channel	Rate
LAN	Up		Auto
WLAN	Up	6	best

SSID Status

Interface	SSID	BSSID	Security	VLAN
WLAN	ZyXEL	40:4a:03:42:70:2b	Disabled	Disabled

System Status

Status Ready

- Click the links on the left of the screen to configure advanced features such as **SYSTEM** (General, Password and Time), **WIRELESS** (Wireless Settings, SSID, Security, RADIUS, MAC Filter), **IP**, **REMOTE MGNT** (Telnet, FTP, WWW and SNMP), **CERTIFICATES**, and **LOGS** (View Log and Log Settings).
- Click **MAINTENANCE** to view information about your NWA or upgrade configuration and firmware files. Maintenance features include **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration File** (Backup, Restore and Default) and **Restart**.
- Click **LOGOUT** at any time to exit the web configurator.

Status Screens

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

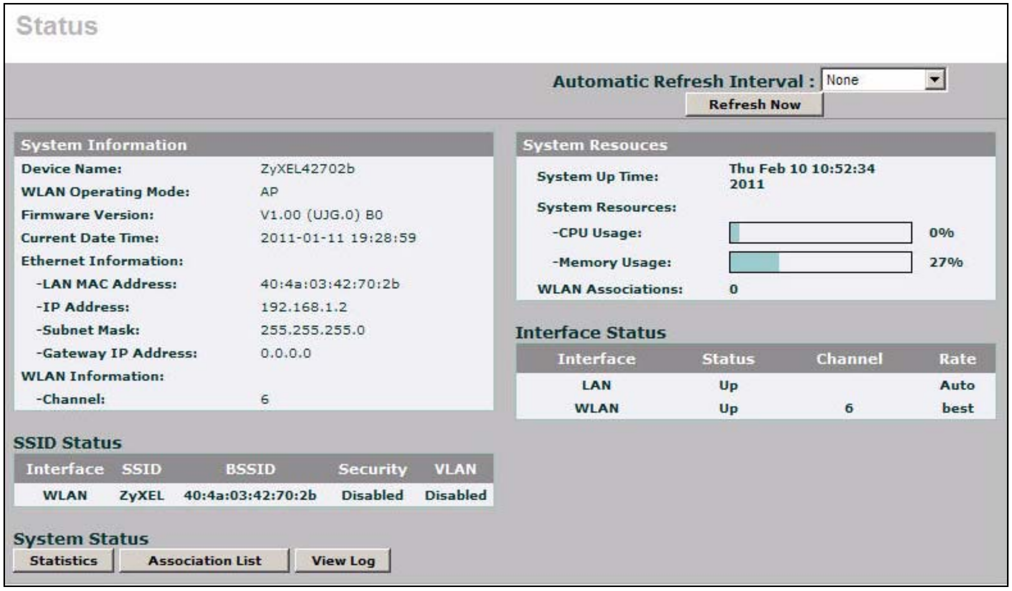
Use the **Status** screens to look at the current status of the device, system resources, and interfaces. The **Status** screens also provide detailed information about system statistics, associated wireless clients, and logs.

3.1 The Status Screen

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

Click **Status**. The following screen displays.

Figure 15 The Status Screen



Status

Automatic Refresh Interval : None

System Information

Device Name: ZyXEL42702b
WLAN Operating Mode: AP
Firmware Version: V1.00 (UJG.0) B0
Current Date Time: 2011-01-11 19:28:59
Ethernet Information:
-LAN MAC Address: 40:4a:03:42:70:2b
-IP Address: 192.168.1.2
-Subnet Mask: 255.255.255.0
-Gateway IP Address: 0.0.0.0
WLAN Information:
-Channel: 6

System Resouces

System Up Time: Thu Feb 10 10:52:34 2011
System Resources:
-CPU Usage: 0%
-Memory Usage: 27%
WLAN Associations: 0

Interface Status

Interface	Status	Channel	Rate
LAN	Up		Auto
WLAN	Up	6	best

SSID Status

Interface	SSID	BSSID	Security	VLAN
WLAN	ZyXEL	40:4a:03:42:70:2b	Disabled	Disabled

System Status

The following table describes the labels in this screen.

Table 3 The Status Screen

LABEL	DESCRIPTION
Automatic Refresh Interval	Select how often you want the NWA to update this screen.
Refresh Now	Click this to update this screen immediately.
System Information	

Table 3 The Status Screen (continued)

LABEL	DESCRIPTION
Device Name	This field displays the NWA system name. It is used for identification. You can change this in the **System > General** screen's **Device Name** field.
WLAN Operation Mode	This field displays the current operating mode of the first wireless module (**Access Point**, **Bridge/Repeater**, **AP+Bridge**, **Wireless Client**, or **MBSSID**). You can change the operating mode in the **Wireless > Wireless Settings** screen.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in **Maintenance > F/W Upload**.
Current Date Time	This field displays the date and time configured on the NWA. You can change this in the **System > Time Setting** screen.
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.
IP Address	This field displays the current IP 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.
WLAN Information	
SSID	This field displays the SSID (Service Set Identifier). This is available only when the WLAN Operation Mode is **Wireless Client**.
Channel	The channel or frequency used by the NWA to send and receive information.
Status	This shows the current status of the wireless LAN. This is available only when the WLAN Operation Mode is **Wireless Client**.
Security Mode	This displays the security mode the NWA is using.
System Resources	
System Up Time	This field displays the elapsed time since the NWA was turned on.
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	Click this to see which wireless channels are currently in use in the local area. See Section 15.5 on page 130.
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.

Table 3 The Status Screen (continued)

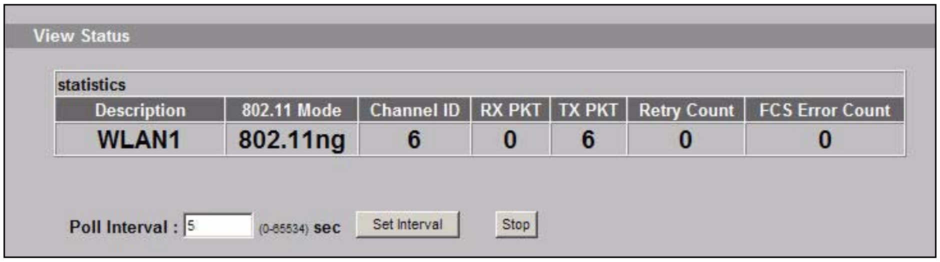
LABEL	DESCRIPTION
LAN	This field displays the number of wireless clients currently associated to the first wireless module. Each wireless module supports up to 32 concurrent associations.
WLAN	This field displays the number of wireless clients currently associated to the second wireless module. Each wireless module supports up to 32 concurrent associations.
System Status	
Statistics	Click this link to view port status and packet specific statistics. See Section 3.1.1 on page 35.
Association List	Click this to see a list of wireless clients currently associated to each of the NWA’s wireless modules. See Section 15.4 on page 129.
View Log	Click this to see a list of logs produced by the NWA. See Chapter 14 on page 123.

3.1.1 System Statistics Screen

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. The fields in this screen vary according to the current wireless mode of each WLAN adaptor.

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

Figure 16 System Status: Statistics



Description	802.11 Mode	Channel ID	RX PKT	TX PKT	Retry Count	FCS Error Count
WLAN1	802.11ng	6	0	6	0	0

Poll Interval : 5 (0-65534) sec

The following table describes the labels in this screen.

Table 4 System Status: Show Statistics

LABEL	DESCRIPTION
Description	This is the wireless LAN adaptor.
802.11 Mode	This field shows which 802.11 mode the NWA is using.
Channel ID	Click this to see which wireless channels are currently in use in the local area. See Section 15.5 on page 130.
RX PKT	This is the number of received packets on this port.
TX PKT	This is the number of transmitted packets on this port.
Retry Count	This is the total number of retries for transmitted packets (TX).
FCS Error Count	This is the ratio percentage showing the total number of checksum error of received packets (RX) over total RX.
Poll Interval	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.
Stop	Click this button to stop refreshing statistics.

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 4.1.3 on page 38 for links to more information on each step.

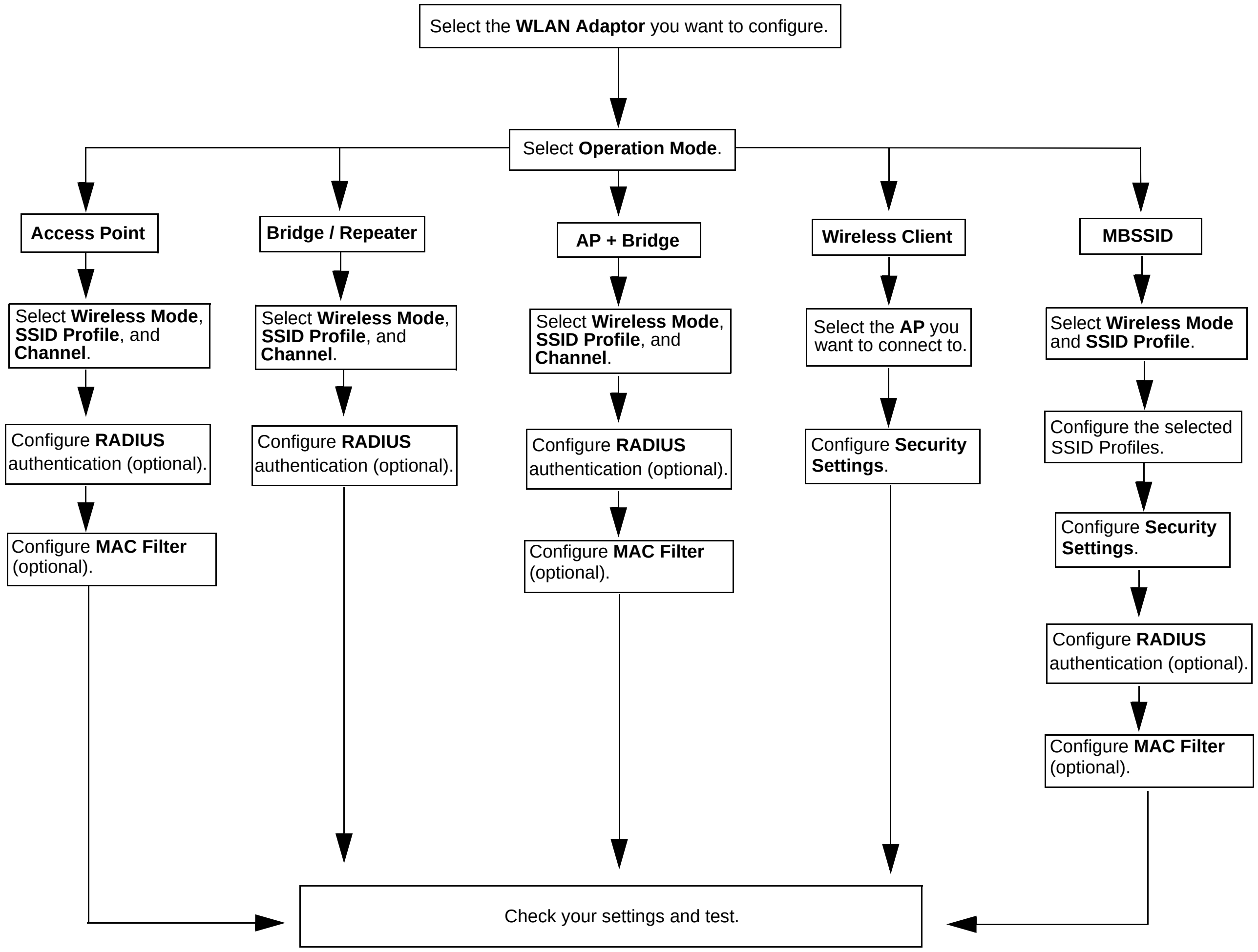
4.1.1 Choosing the Wireless Mode

- Use **Access Point** operating mode if you want to allow wireless clients to access your wired network, all using the same security and Quality of Service (QoS) settings. See Section 1.2.1 on page 20 for details.
- Use **Bridge / Repeater** operating mode if you want to use the NWA to communicate with other access points. See Section 1.2.2 on page 20 for details.
- Use **AP + Bridge** operating mode if you want to use the NWA as an access point (see above) while also communicating with other access points. See Section 1.2.3 on page 22 for details.
- Use **Wireless Client** operating mode if you want to use the NWA to access a wireless network. See Section 1.2.4 on page 23 for details.

  The NWA is a bridge when other APs access your wired Ethernet network through the NWA.
- 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 1.2.5 on page 24 for details.

4.1.2 Wireless LAN Configuration Overview

The following figure shows the steps you should take to configure the wireless settings according to the operating mode you select. Use the Web Configurator to set up your NWA's wireless network (see your Quick Start Guide for information on setting up your NWA and accessing the Web Configurator).


Select the **WLAN Adaptor** you want to configure.
Select **Operation Mode**.
Access Point
Bridge / Repeater
AP + Bridge
Wireless Client
MBSSID
Select **Wireless Mode**, **SSID Profile**, and **Channel**.
Select **Wireless Mode**, **SSID Profile**, and **Channel**.
Select **Wireless Mode**, **SSID Profile**, and **Channel**.
Select the **AP** you want to connect to.
Select **Wireless Mode** and **SSID Profile**.
Configure **RADIUS** authentication (optional).
Configure **RADIUS** authentication (optional).
Configure **RADIUS** authentication (optional).
Configure **Security Settings**.
Configure the selected SSID Profiles.
Configure **MAC Filter** (optional).
Configure **MAC Filter** (optional).
Configure **Security Settings**.
Configure **RADIUS** authentication (optional).
Configure **MAC Filter** (optional).
Check your settings and test.

4.1.3 Further Reading

Use these links to find more information on the steps:

- Selecting a **WLAN Adaptor**: see Section 6.4.1 on page 63.
- Choosing **802.11 Mode**: see Section 6.4.1 on page 63.
- Choosing a wireless **Channel ID**: see Section 6.4.1 on page 63.
- Choosing a **Security** mode: see Section 8.4.1 on page 89.
- Configuring an external **RADIUS** server: see Section 9.4 on page 100.
- Configuring **MAC Filtering**: see Section 10.1 on page 102.

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 (See your Quick Start Guide for information on how to set up your NWA in Access Point mode). Now your network is expanding and you want to make use of the MBSSID feature (see Section 8.2.4 on page 139) 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 **Access Point** to **MBSSID** and reactivate the standard network.

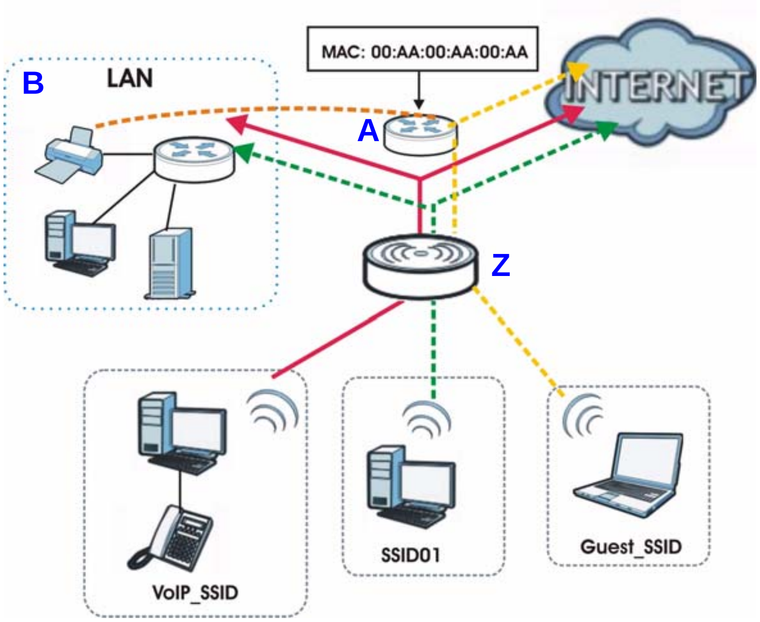
3 Configure different security modes for the networks.

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.

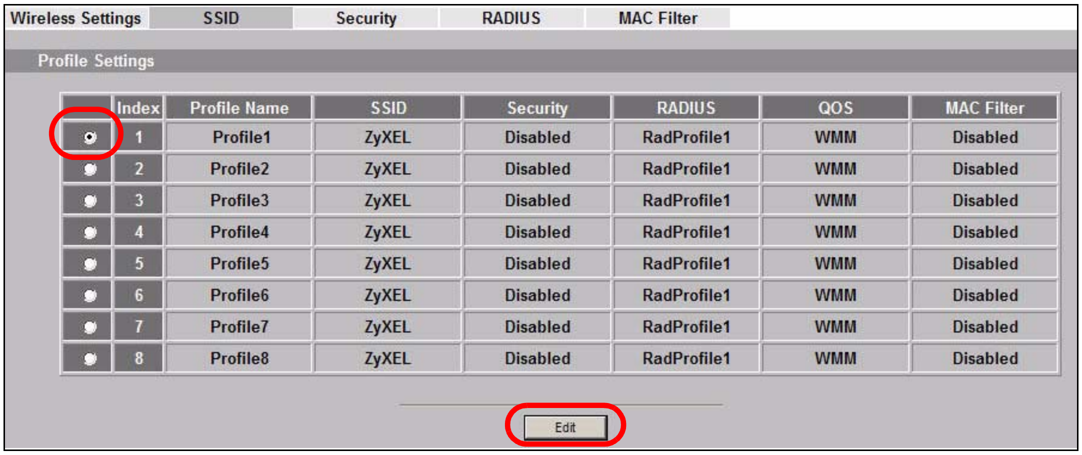
Table 5 Tutorial: Example Information

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

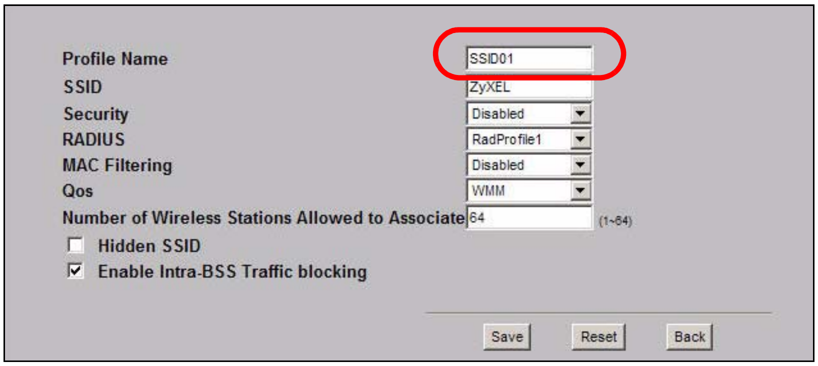
1 Log in to the NWA (see Section 2.2 on page 35). Click **Wireless > SSID**. The **SSID** screen appears.

2 Select the **Profile1** check-box and click **Edit**.



	Index	Profile Name	SSID	Security	RADIUS	QOS	MAC Filter
●	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** as **SSID01**. Click **Save**.



Profile Name	SSID01
SSID	ZyXEL
Security	Disabled
RADIUS	RadProfile1
MAC Filtering	Disabled
Qos	WMM
Number of Wireless Stations Allowed to Associate	64 (1~64)

□ Hidden SSID

☑ Enable Intra-BSS Traffic blocking

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

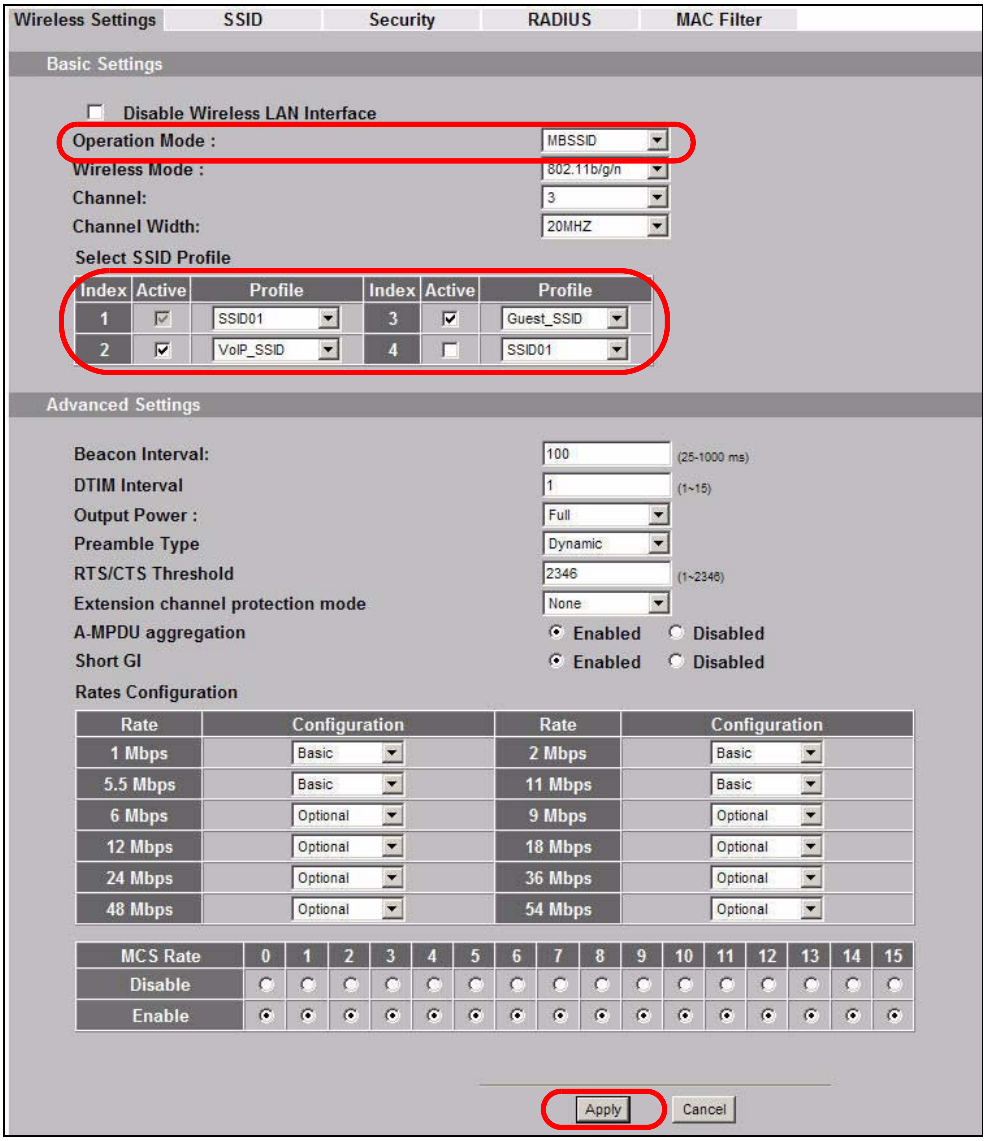
4.2.1.1 MBSSID

1 Go to **Wireless > Wireless Settings**. Select **MBSSID** from the **Operating 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

□ Disable Wireless LAN Interface

Operation Mode : MBSSID

Wireless Mode : 802.11b/g/n

Channel: 3

Channel Width: 20MHZ

Select SSID Profile

Index	Active	Profile	Index	Active	Profile
1	☑	SSID01	3	☑	Guest_SSID
2	☑	VoIP_SSID	4	□	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 ○ Disabled

Short GI ● Enabled ○ Disabled

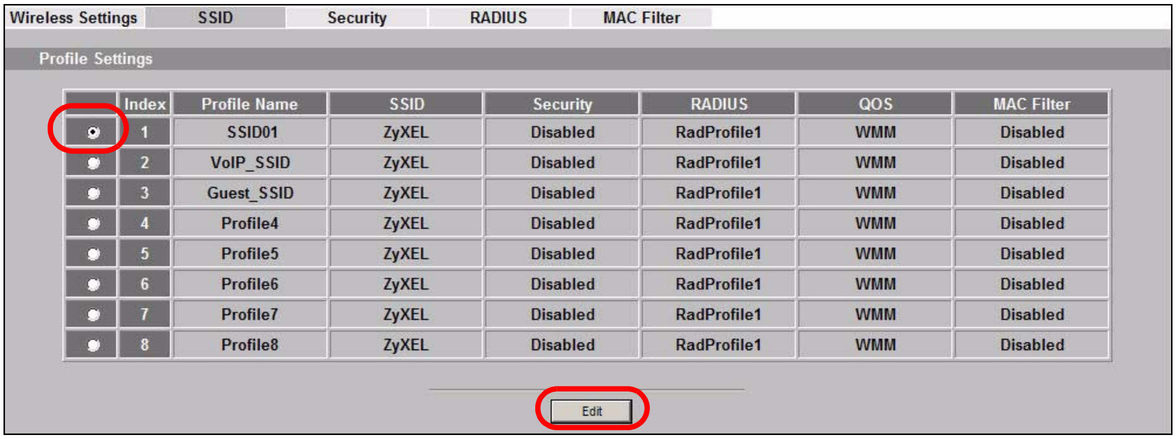
Rates Configuration

Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional

MCS Rate	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Enable	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

4.2.2 Configure the Standard Network

1 Click **Wireless** > **SSID**. Select **SSID01** and click **Edit**.

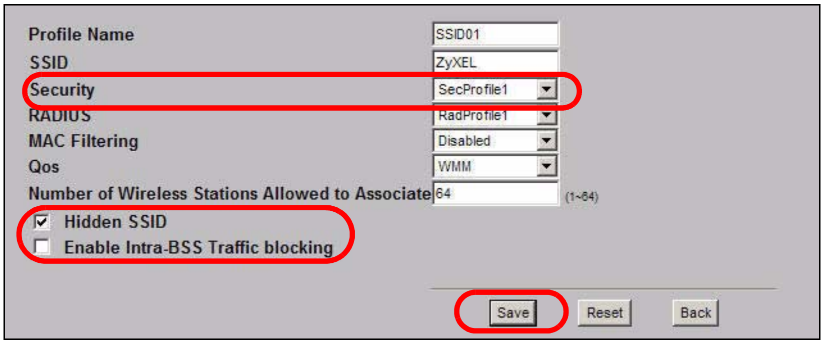


	Index	Profile Name	SSID	Security	RADIUS	QOS	MAC Filter
●	1	SSID01	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	2	VoIP_SSID	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	3	Guest_SSID	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	4	Profile4	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	5	Profile5	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	6	Profile6	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	7	Profile7	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	8	Profile8	ZyXEL	Disabled	RadProfile1	WMM	Disabled

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 **Enable Intra-BSS Traffic blocking** check-box.

Click **Save**.

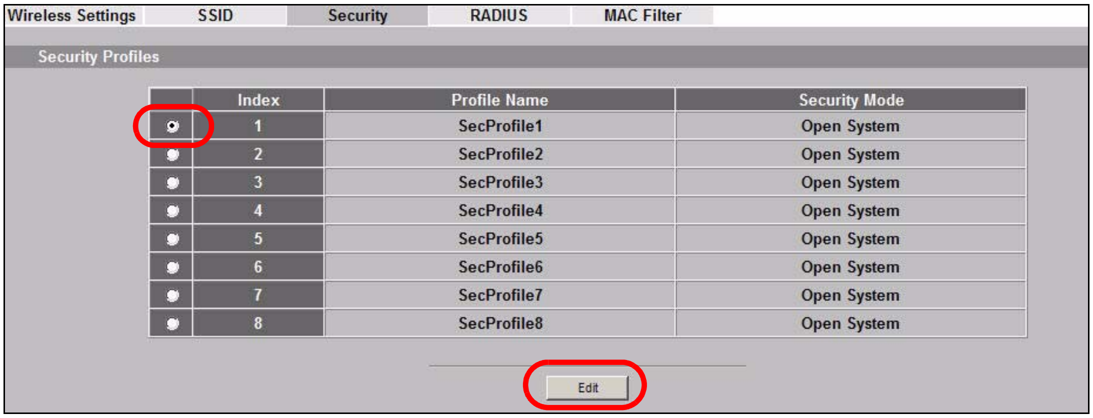


Profile Name	SSID01
SSID	ZyXEL
Security	SecProfile1
RADIUS	RadProfile1
MAC Filtering	Disabled
Qos	WMM
Number of Wireless Stations Allowed to Associate	64 (1~64)

☑ Hidden SSID

☐ Enable Intra-BSS Traffic blocking

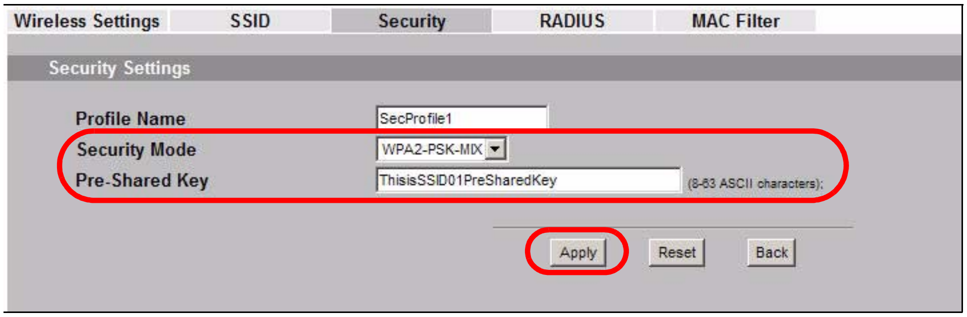
3 Next, click **Wireless > Security**. Select **SecProfile1** and click **Edit**.



Security Profiles

	Index	Profile Name	Security Mode
●	1	SecProfile1	Open System
○	2	SecProfile2	Open System
○	3	SecProfile3	Open System
○	4	SecProfile4	Open System
○	5	SecProfile5	Open System
○	6	SecProfile6	Open System
○	7	SecProfile7	Open System
○	8	SecProfile8	Open System

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**.



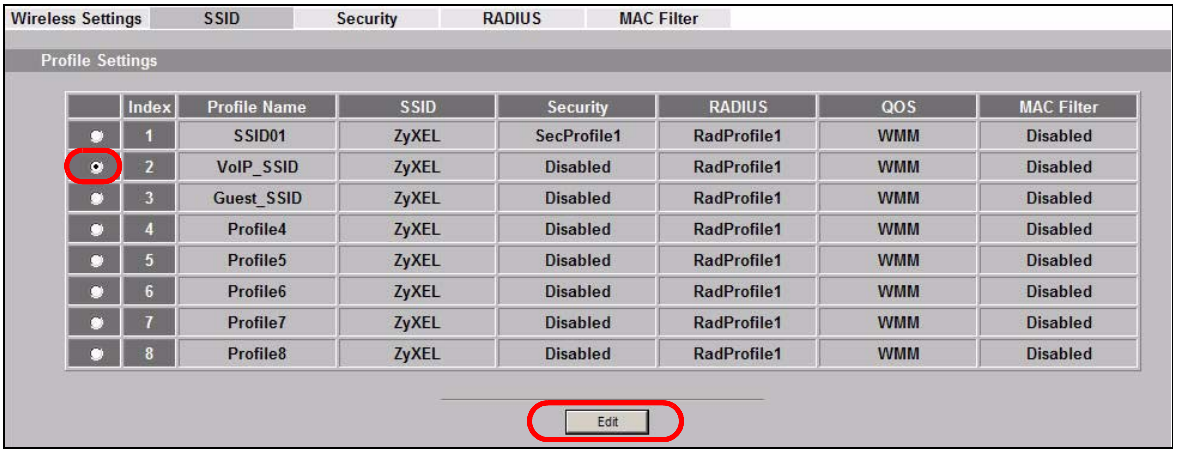
Security Settings

Profile Name	SecProfile1
Security Mode	WPA2-PSK-MIX
Pre-Shared Key	ThisisSSID01PreSharedKey (8-63 ASCII characters);

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

4.2.3 Configure the VoIP Network

1 Go to **Wireless** > **SSID**. Select **VoIP_SSID** and click **Edit**.

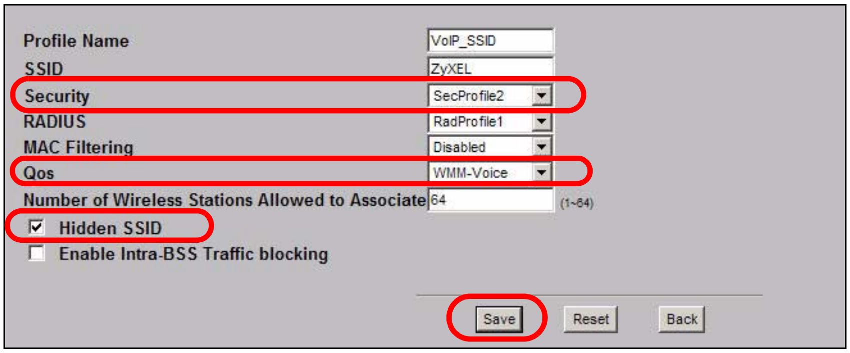


Profile Settings

	Index	Profile Name	SSID	Security	RADIUS	QOS	MAC Filter
○	1	SSID01	ZyXEL	SecProfile1	RadProfile1	WMM	Disabled
●	2	VoIP_SSID	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	3	Guest_SSID	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

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

3 Select **WMM-Voice** in the **QoS** field to give VoIP the highest priority in the wireless network. Click **Save**.

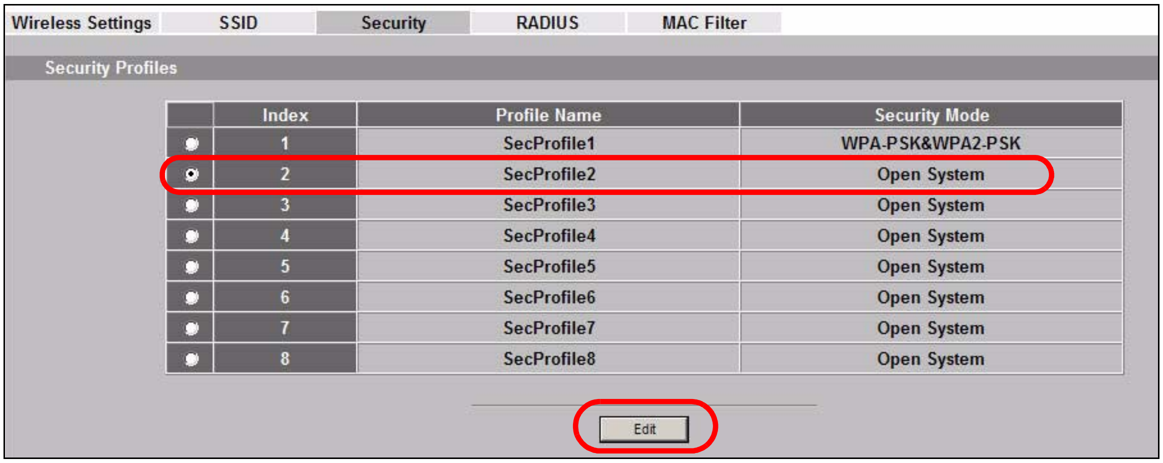


Profile Name	VoIP_SSID
SSID	ZyXEL
Security	SecProfile2
RADIUS	RadProfile1
MAC Filtering	Disabled
Qos	WMM-Voice
Number of Wireless Stations Allowed to Associate	64 (1~64)

☑ Hidden SSID

□ Enable Intra-BSS Traffic blocking

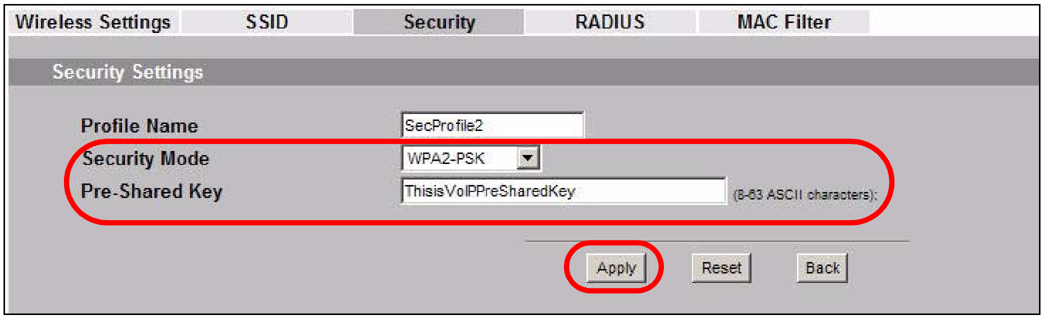
4 Next, click **Wireless > Security**. Select **SecProfile2** and click **Edit**.



Security Profiles

	Index	Profile Name	Security Mode
○	1	SecProfile1	WPA-PSK&WPA2-PSK
●	2	SecProfile2	Open System
○	3	SecProfile3	Open System
○	4	SecProfile4	Open System
○	5	SecProfile5	Open System
○	6	SecProfile6	Open System
○	7	SecProfile7	Open System
○	8	SecProfile8	Open System

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



Security Settings

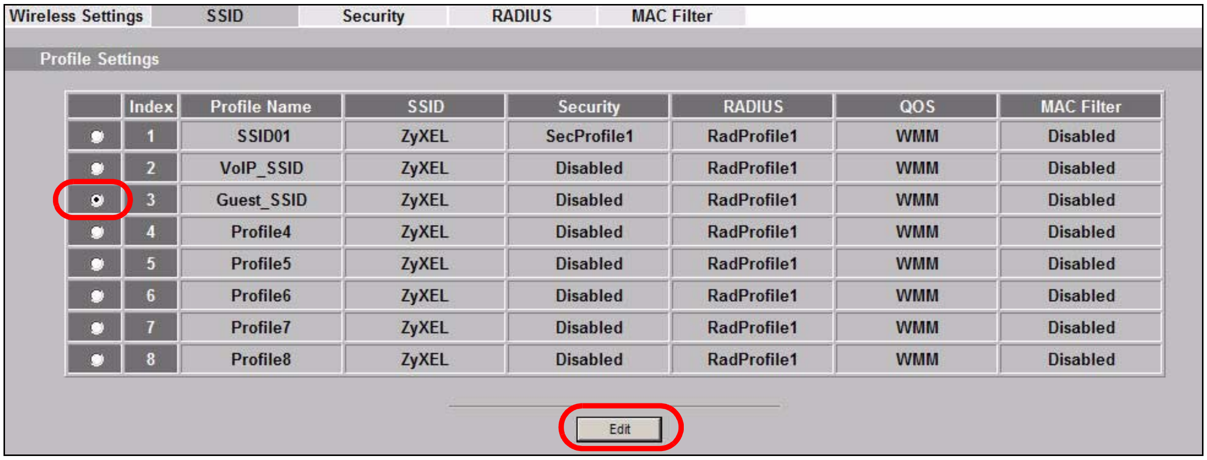
Profile Name	SecProfile2
Security Mode	WPA2-PSK
Pre-Shared Key	ThisisVoIPPreSharedKey (8-63 ASCII characters);

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** > **SSID**. Select **Guest_SSID** and click **Edit**.



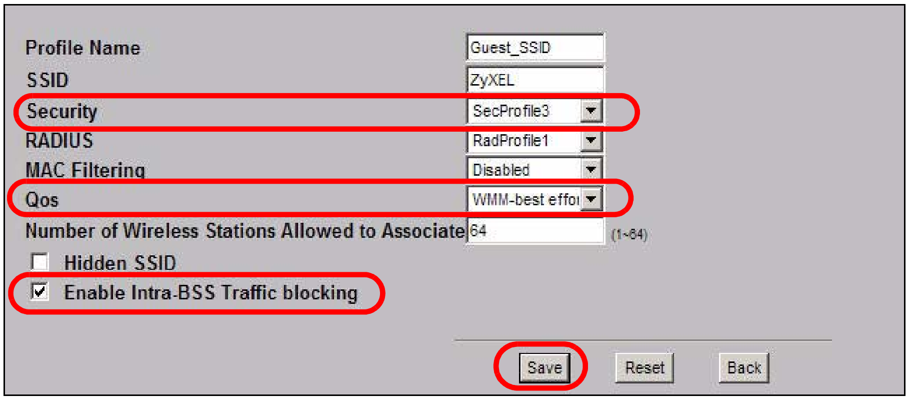
Profile Settings

	Index	Profile Name	SSID	Security	RADIUS	QOS	MAC Filter
○	1	SSID01	ZyXEL	SecProfile1	RadProfile1	WMM	Disabled
○	2	VoIP_SSID	ZyXEL	Disabled	RadProfile1	WMM	Disabled
●	3	Guest_SSID	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

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-best effort** in the **QoS** field to give the guest a lower QoS priority.

4 Select the check-box of **Enable Intra-BSS Traffic blocking**. Click **Save**.

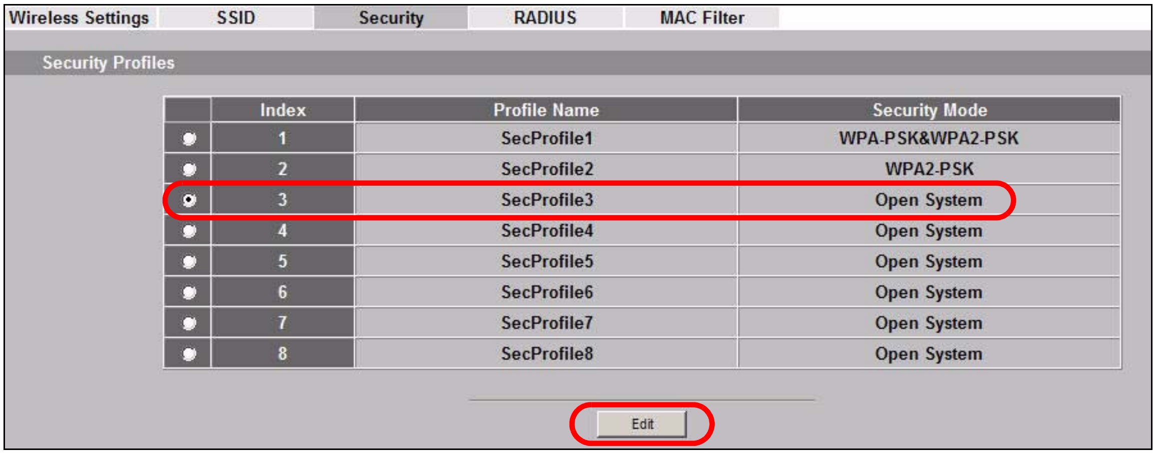


Profile Name	Guest_SSID
SSID	ZyXEL
Security	SecProfile3
RADIUS	RadProfile1
MAC Filtering	Disabled
Qos	WMM-best effor
Number of Wireless Stations Allowed to Associate	64 (1~64)

□ Hidden SSID

☑ Enable Intra-BSS Traffic blocking

5 Next, click **Wireless > Security**. Select **SecProfile3** and click **Edit**.

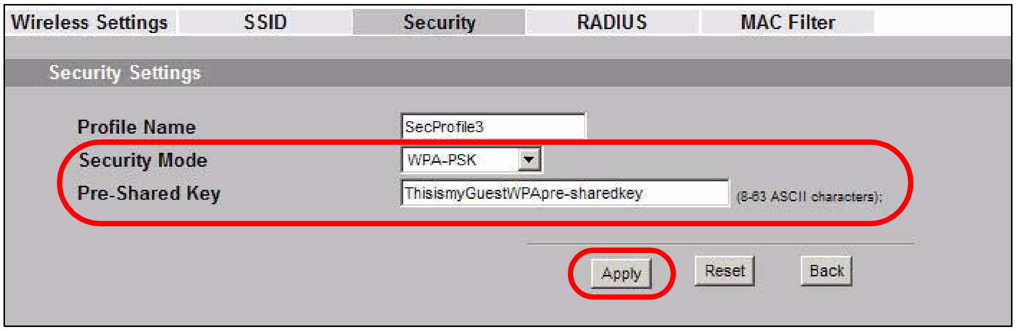


Security Profiles

	Index	Profile Name	Security Mode
○	1	SecProfile1	WPA-PSK&WPA2-PSK
○	2	SecProfile2	WPA2-PSK
●	3	SecProfile3	Open System
○	4	SecProfile4	Open System
○	5	SecProfile5	Open System
○	6	SecProfile6	Open System
○	7	SecProfile7	Open System
○	8	SecProfile8	Open System

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

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



Security Settings

Profile Name	SecProfile3
Security Mode	WPA-PSK
Pre-Shared Key	ThisismyGuestWPApre-sharedkey (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 **Save**.
- Try to access each network using the correct security settings, and then using incorrect security settings, such as the WPA-PSK for another active network. If the behavior is different from expected (for example, if you can access the **SSID01** or **VoIP_SSID** wireless network using the security settings for the **Guest_SSID** wireless network) check that the SSID profile is set to use the correct security profile, and that the settings of the security profile are correct.

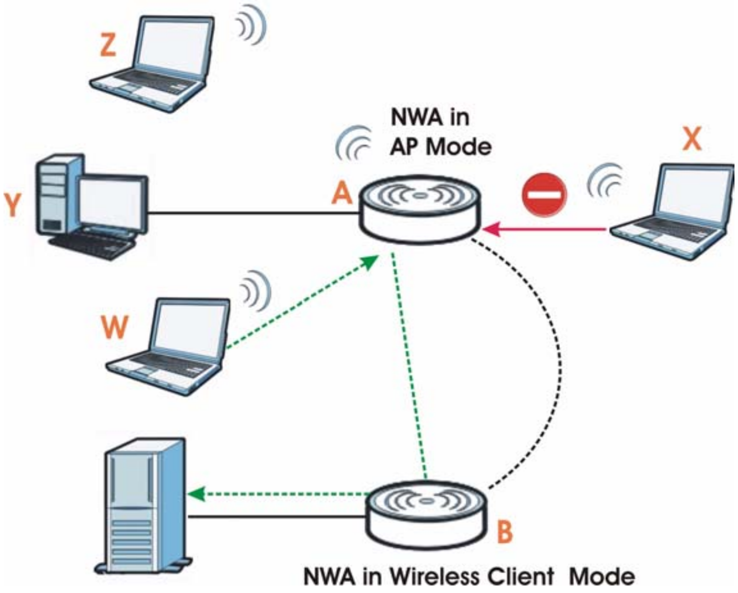
4.3 NWA Setup in AP and Wireless Client Modes

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 Access Point (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.

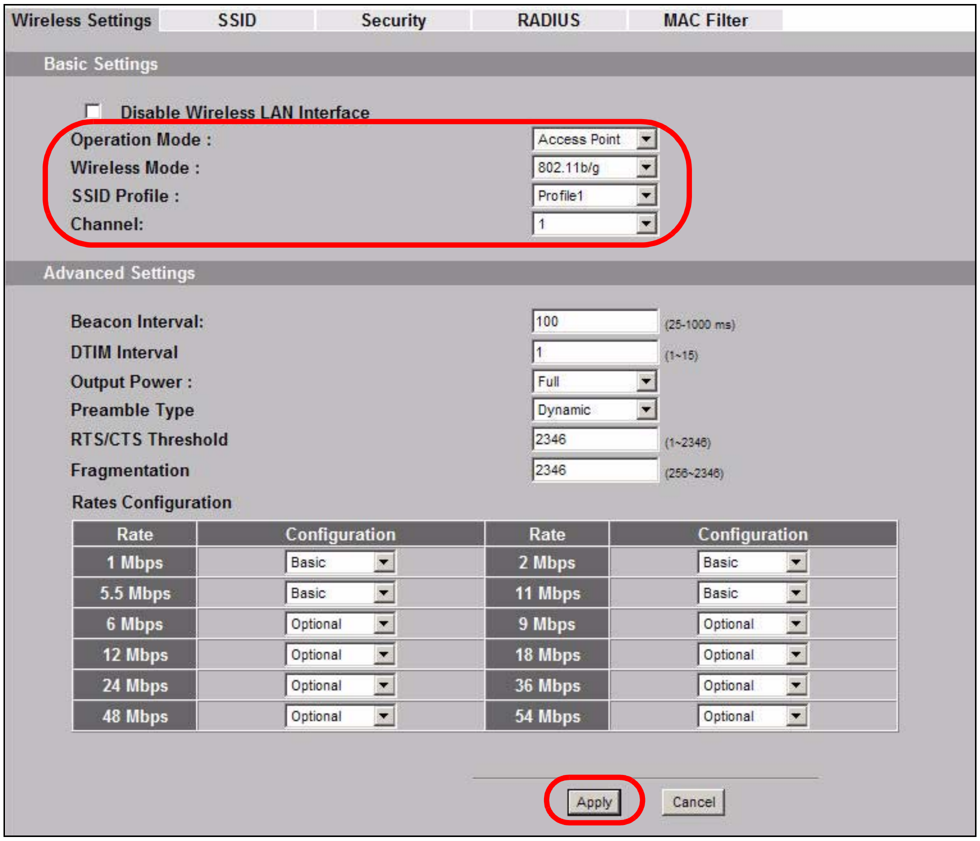
Figure 17 FTP Server Connected to a Wireless Client



4.3.2 Configuring the NWA in Access Point 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 > Wireless Settings** screen.



Basic Settings

□ Disable Wireless LAN Interface

Operation Mode : Access Point

Wireless Mode : 802.11b/g

SSID Profile : Profile1

Channel: 1

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)

Fragmentation 2346 (256~2346)

Rates Configuration

Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional

1 Set the **Operation Mode** to **Access Point**.

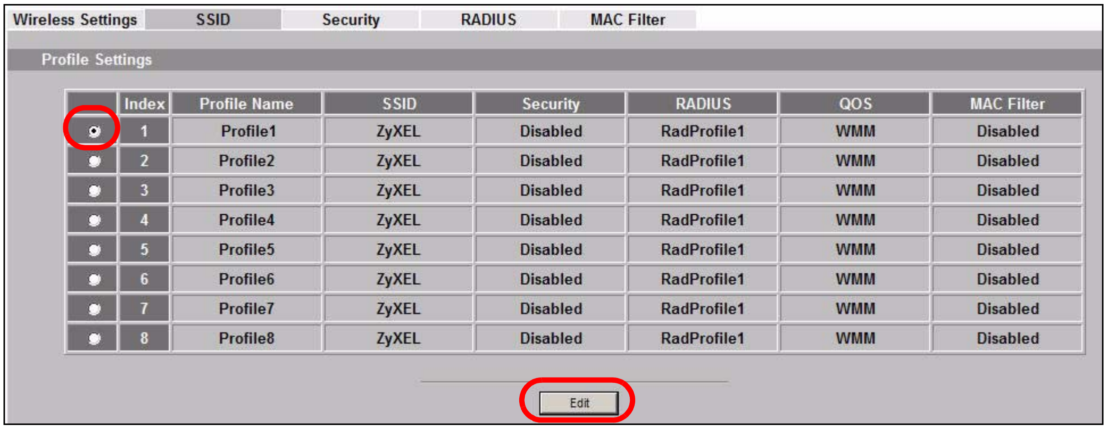
2 Select the **Wireless Mode**. In this example, select **802.11b/g**.

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

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

5 Click **Apply**.

6 Go to **Wireless > SSID**. Select **Profile1** and click **Edit**.



Profile Settings

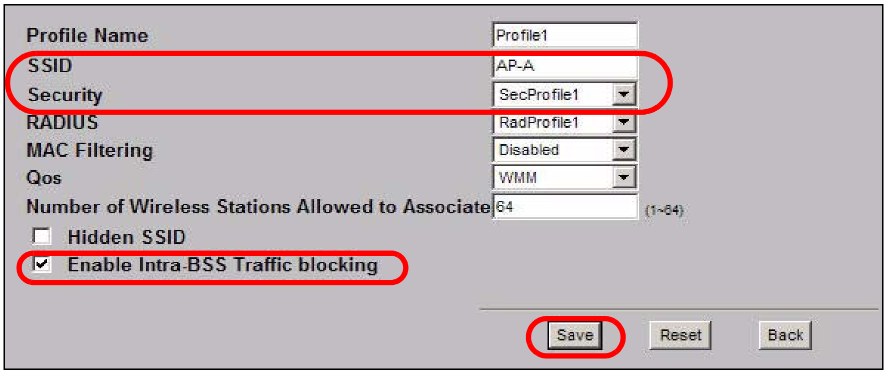
	Index	Profile Name	SSID	Security	RADIUS	QOS	MAC Filter
●	1	Profile1	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	2	Profile2	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	3	Profile3	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	4	Profile4	ZyXEL	Disabled	RadProfile1	WMM	Disabled
○	5	Profile5	ZyXEL	Disabled	RadProfile1	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 **Enable Intra-BSS Traffic blocking** so the client cannot access other clients on the same wireless network.

10 Click **Save**.

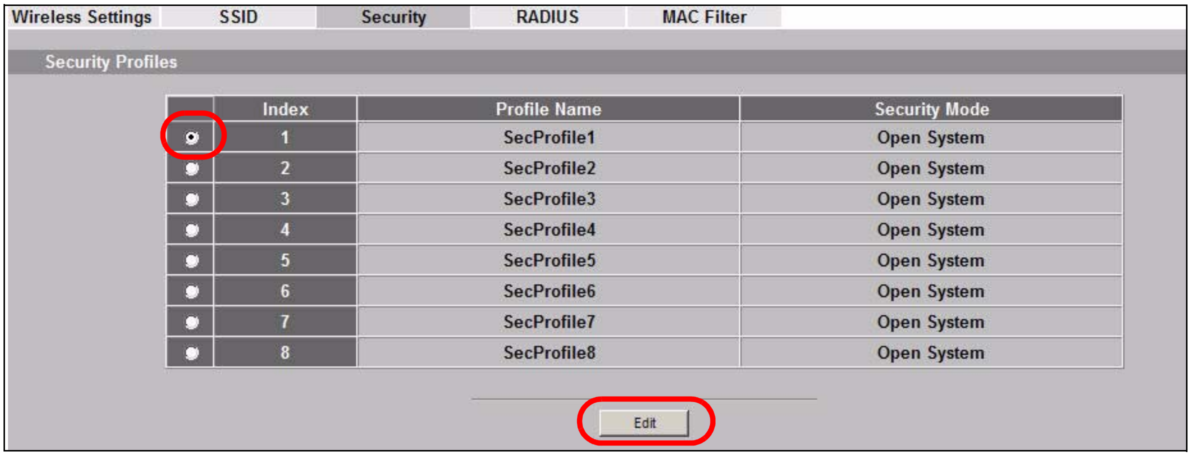


Profile Name	Profile1	
SSID	AP-A	
Security	SecProfile1	
RADIUS	RadProfile1	
MAC Filtering	Disabled	
Qos	WMM	
Number of Wireless Stations Allowed to Associate	64	(1~64)

□ Hidden SSID

☑ Enable Intra-BSS Traffic blocking

11 Go to **Wireless > Security**. Select **SecProfile1**. Click **Edit**.

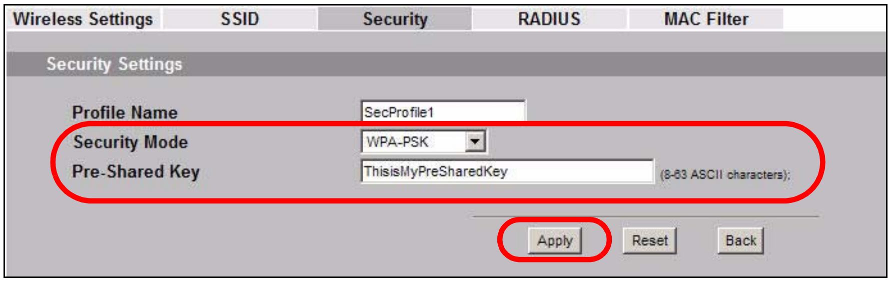


Security Profiles

	Index	Profile Name	Security Mode
●	1	SecProfile1	Open System
○	2	SecProfile2	Open System
○	3	SecProfile3	Open System
○	4	SecProfile4	Open System
○	5	SecProfile5	Open System
○	6	SecProfile6	Open System
○	7	SecProfile7	Open System
○	8	SecProfile8	Open System

12 Configure **WPA-PSK** as the **Security Mode** and enter **ThisisMyPreSharedKey** in the **Pre-Shared Key** field.

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



Profile Name: SecProfile1

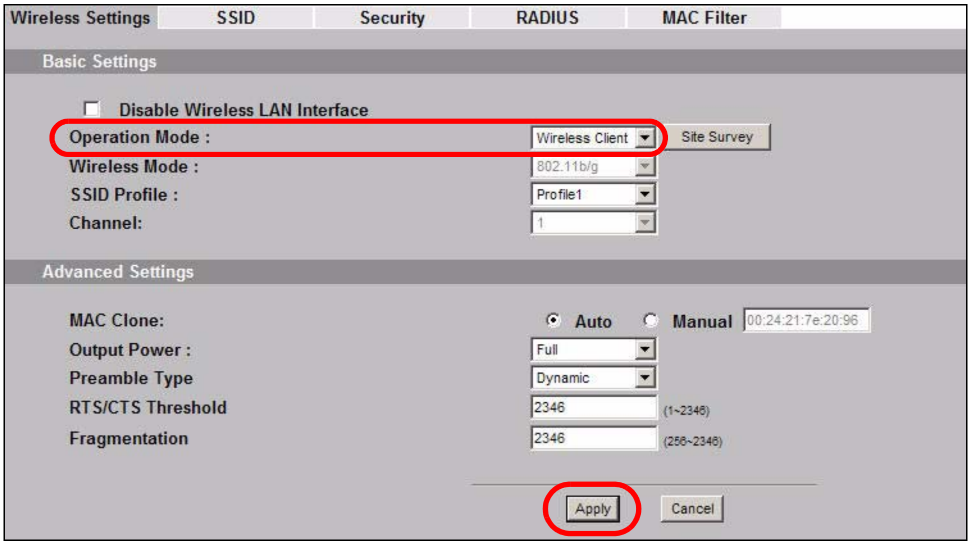
Security Mode: WPA-PSK

Pre-Shared Key: ThisisMyPreSharedKey (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 > Wireless Settings** screen. Follow these steps to configure station **B**.

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



□ Disable Wireless LAN Interface

Operation Mode : Wireless Client

Wireless Mode : 802.11b/g

SSID Profile : Profile1

Channel: 1

MAC Clone: ● Auto ○ Manual 00:24:21:7e:20:96

Output Power : Full

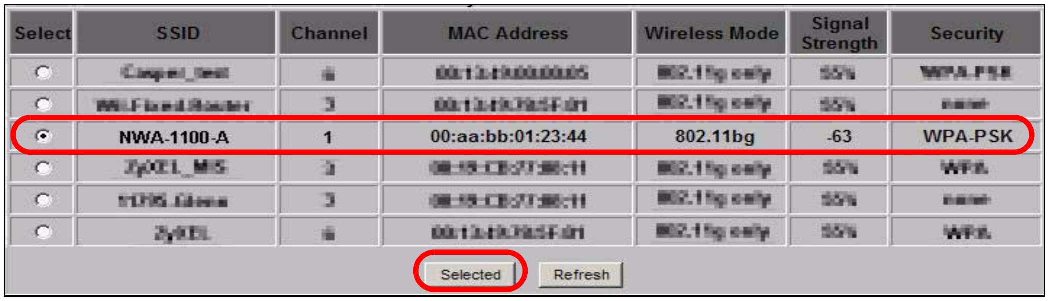
Preamble Type: Dynamic

RTS/CTS Threshold: 2346 (1~2346)

Fragmentation: 2346 (256~2346)

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

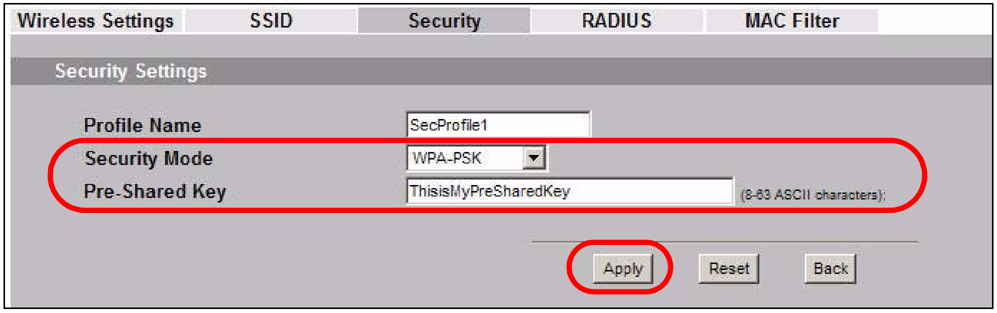
3 Find and select NWA1100-N-A's SSID: **NWA-1100-A**. Click **Selected**.



Select	SSID	Channel	MAC Address	Wireless Mode	Signal Strength	Security
○	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
○	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
●	NWA-1100-A	1	00:aa:bb:01:23:44	802.11bg	-63	WPA-PSK
○	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
○	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
○	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

4 Go to **Wireless > Security** to configure the NWA to use the same security mode and Pre-Shared Key as NWA1100-N-A: **WPA-PSK / ThisisMyPreSharedKey**. Click **Apply**.

Figure 18



Security Settings

Profile Name: SecProfile1

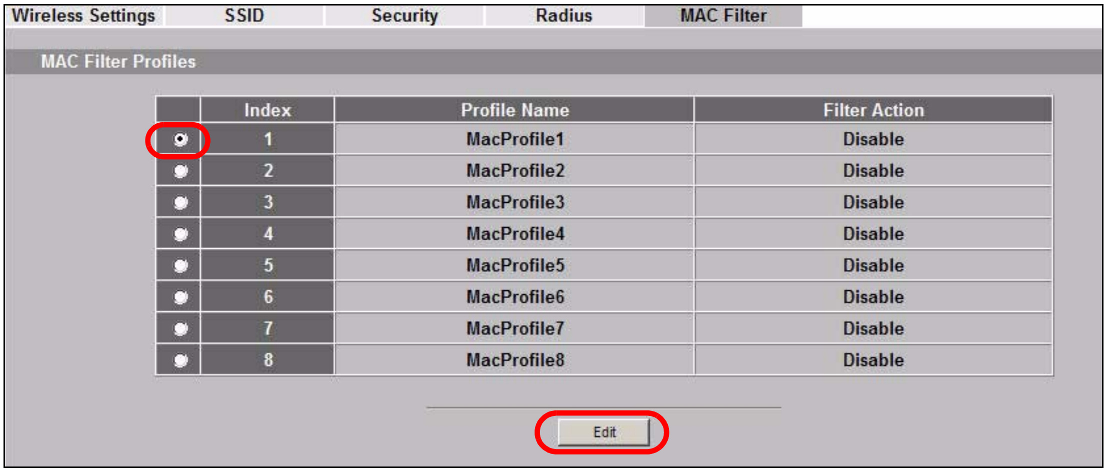
Security Mode: WPA-PSK

Pre-Shared Key: ThisisMyPreSharedKey (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 Chapter 10 on page 102 for more information on MAC Filter).

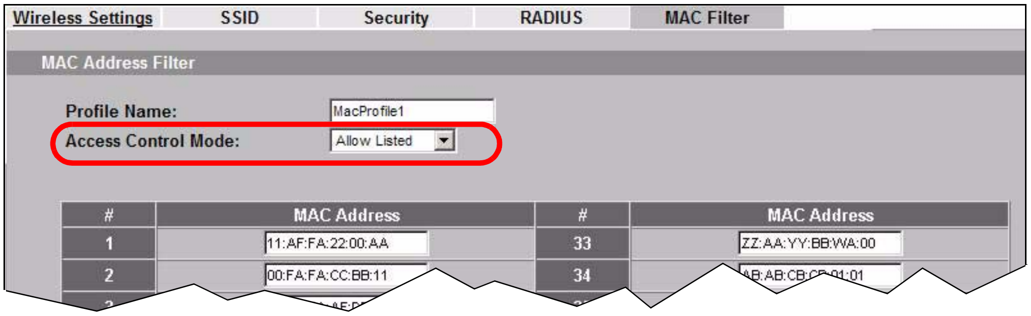
1 Go to **Wireless > MAC Filter**. Select **MacProfile1** and click **Edit**.



MAC Filter Profiles

	Index	Profile Name	Filter Action
●	1	MacProfile1	Disable
○	2	MacProfile2	Disable
○	3	MacProfile3	Disable
○	4	MacProfile4	Disable
○	5	MacProfile5	Disable
○	6	MacProfile6	Disable
○	7	MacProfile7	Disable
○	8	MacProfile8	Disable

2 Select **Allow Listed** 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 Address Filter

Profile Name: MacProfile1

Access Control Mode: Allow Listed

#	MAC Address	#	MAC Address
1	11:AF:FA:22:00:AA	33	ZZ:AA:YY:BB:WA:00
2	00:FA:FA:CC:BB:11	34	AB:AB:CB:CD:01:01

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

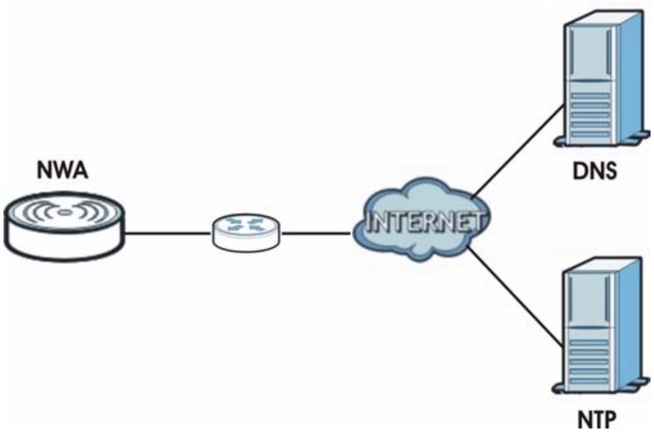
The appendices provide general information. Some details may not apply to your NWA.

System Screens

5.1 Overview

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

Figure 19 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 an Network Time Protocol (NTP) server to set the time on the device.

5.2 What You Can Do in this Chapter

- Use the **System > General** screen to specify the **System Name** and **Ethernet Data Rate** value (see Section 5.4 on page 57) .
- Use the **System > Password** screen to manage the password for your NWA (see Section 5.4.1 on page 57).
- Use the **System > Time Setting** 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 5.5 on page 58).

5.3 What You Need To Know

IP Address Assignment

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

Table 6 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

IP Address and Subnet Mask

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

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

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

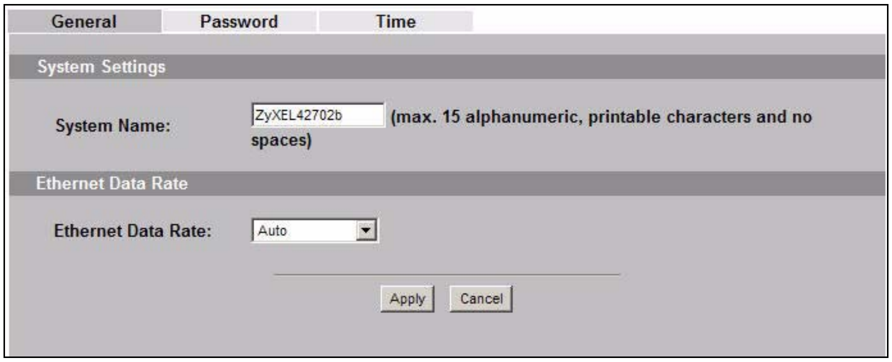
Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your device 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 device unless you are instructed to do otherwise.

5.4 General Screen

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

Figure 20 System > General



System Name: ZyXEL42702b (max. 15 alphanumeric, printable characters and no spaces)

Ethernet Data Rate: Auto

The following table describes the labels in this screen.

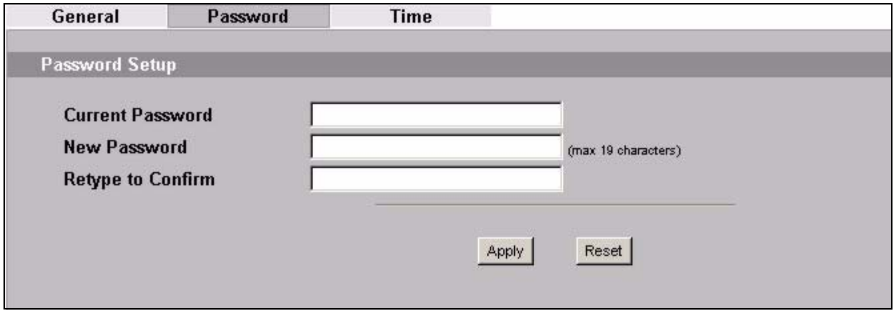
Table 7 System > General

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.
Ethernet Data Rate	
Ethernet Data Rate	Select an Ethernet port speed and duplex mode from the drop-down list. Select **Auto** if you would like to have the system configure this automatically.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

5.4.1 Password Screen

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

Figure 21 System > Password



Current Password

New Password (max 19 characters)

Retype to Confirm

The following table describes the labels in this screen.

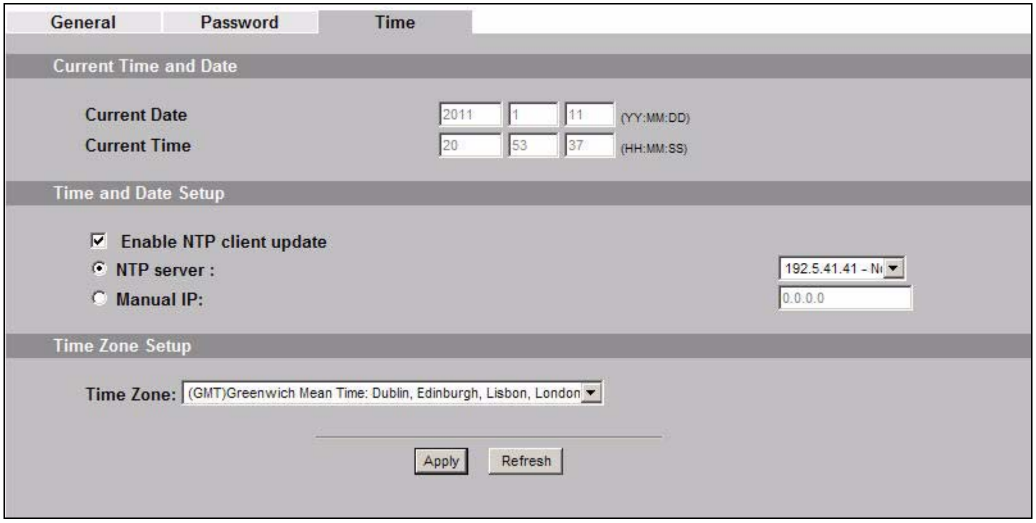
Table 8 System > Password

LABEL	DESCRIPTIONS
Current Password	Type in your existing system password.
New Password	Type your new system password (max 19 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.5 Time Screen

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

Figure 22 System > Time



Current Date 2011 1 11 (YY:MM:DD)

Current Time 20 53 37 (HH:MM:SS)

☑ Enable NTP client update

● NTP server : 192.5.41.41 - N

○ Manual IP: 0.0.0.0

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

The following table describes the labels in this screen.

Table 9 System > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Date	This field displays the last updated date from the time server.
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).
Time and Date Setup	
Enable NTP client update	Select this to have the NWA use the predefined list of Network Time Protocol (NTP) servers.
NTP server	Select an NTP server from the drop-list box.

Table 9 System > Time (continued)

LABEL	DESCRIPTION
Manual IP	Enter the IP address or URL of your time server. Check with your ISP/ network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Apply	Click **Apply** to save your changes.
Refresh	Click **Refresh** to reload the previous configuration for this screen.

5.6 Technical Reference

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

5.6.1 Pre-defined NTP Time Servers List

When you turn on the NWA for the first time, the date and time start at 2000-01-01 00:00:00. When you select **Auto** in the **System** > **Time Setting** screen, the NWA then attempts to synchronize with one of the following pre-defined list of NTP time servers.

The NWA continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 10 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

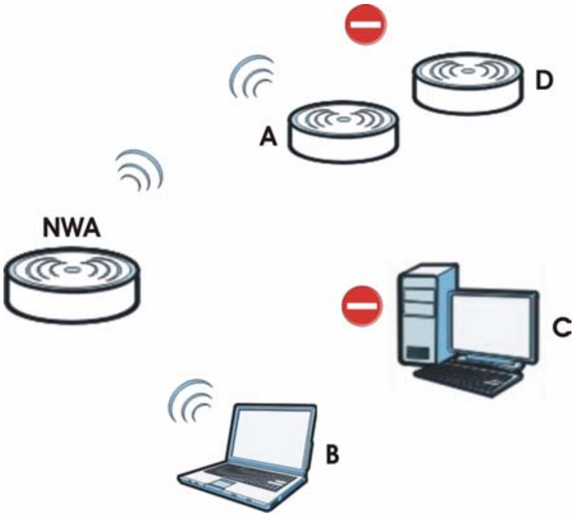
When the NWA uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the NWA goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

Wireless Settings Screen

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 23 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 > Wireless Settings** screen to configure the NWA's operation mode (see Section 6.4 on page 62).

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:

- **AP (Access Point)**. The NWA is wireless access point that allows wireless communication to other devices in the network.
- **Bridge/Repeater.** The NWA acts as a wireless network bridge and establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The NWA can establish up to five wireless links with other APs.
- **AP+Bridge.** The NWA functions as a bridge and access point simultaneously.
- **Wireless Client.** The NWA acts as a wireless client to access a wireless network.
- **MBSSID Mode**. 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 19 for illustrations of these wireless applications.

SSID

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.

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

Wireless Mode

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

MBSSID

Traditionally, you needed to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there was also the possibility of channel interference. The 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.

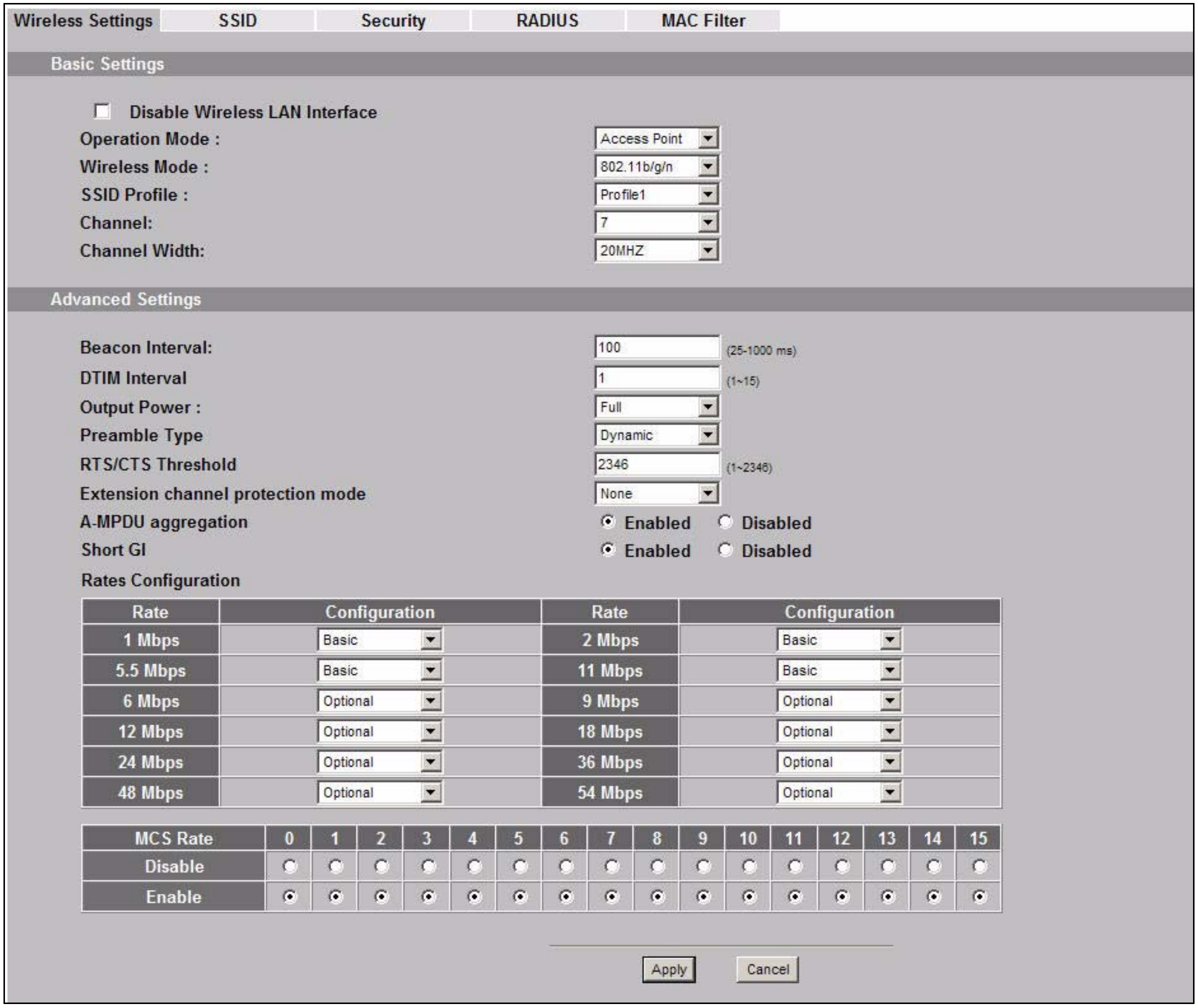
6.4 Wireless Settings Screen

Use this screen to choose the operating mode for your NWA. Click **Wireless > Wireless Settings**. The screen varies depending upon the operating mode you select.

6.4.1 Access Point Mode

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

Figure 24 Wireless > Wireless Settings: Access Point



Basic Settings

☐ Disable Wireless LAN Interface

Operation Mode : Access Point

Wireless Mode : 802.11b/g/n

SSID Profile : Profile1

Channel: 7

Channel Width: 20MHZ

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 ○ Disabled

Short GI ● Enabled ○ Disabled

Rates Configuration

Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional

MCS Rate	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Enable	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

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

Table 11 Wireless > Wireless Settings: Access Point

LABEL	DESCRIPTION
Basic Settings	
Operation Mode	Select **Access Point** from the drop-down list.
Wireless Mode	Select **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. Select **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the Device. The transmission rate of the NWA might be reduced.

Table 11 Wireless > Wireless Settings: Access Point (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. Select an **SSID Profile** from the drop-down list box. 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	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 **802.11 b/g/n** in the **802.11 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 **20/40** (20/40 MHz). This allows the NWA to adjust the channel bandwidth depending on network conditions. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood.
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%**, **12.5%** or **Min** (Minimum). 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.
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.

Table 11 Wireless > Wireless Settings: Access Point (continued)

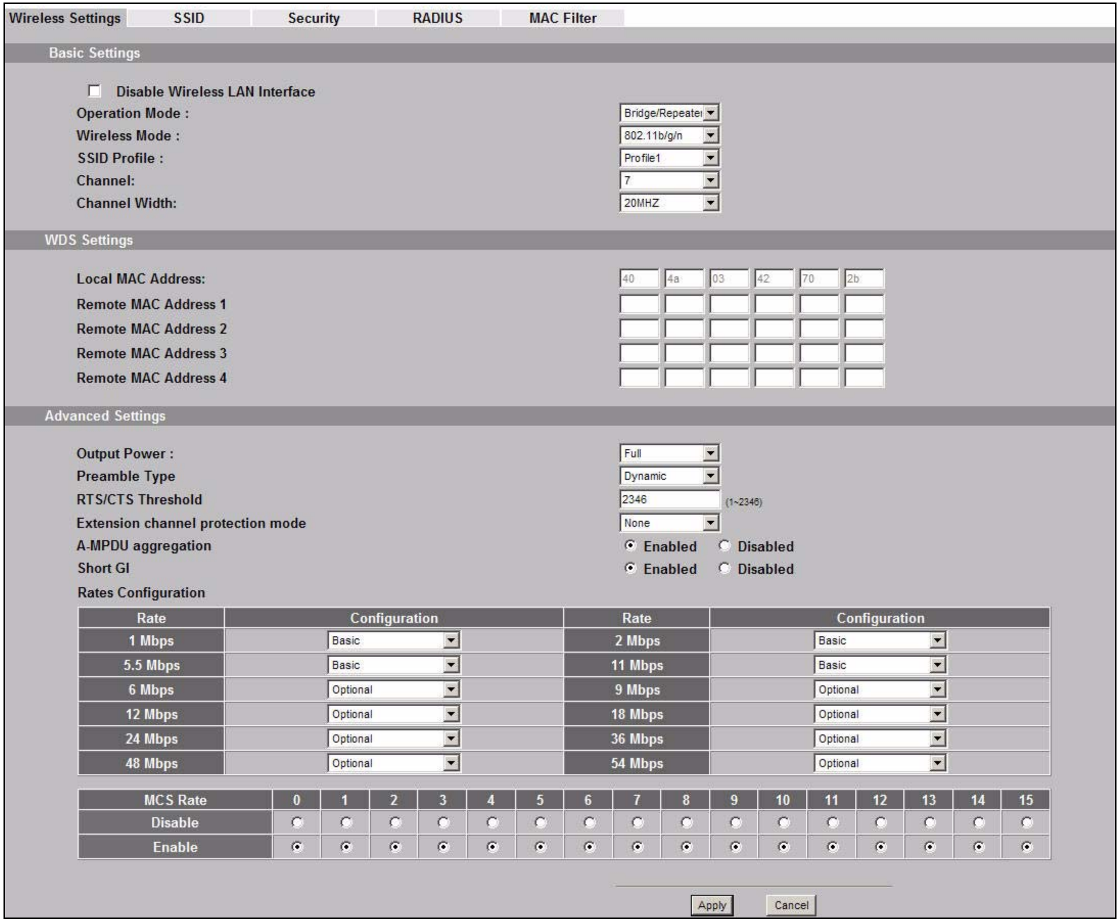
LABEL	DESCRIPTION
Rates Configuration	This section controls the data rates permitted for clients. For each **Rate**, select an option from the **Configuration** list. The options are: • **Basic** (1~11 Mbps only): Clients can always connect to the access point at this speed. • **Optional**: Clients can connect to the access point at this speed, when permitted to do so by the AP. • **Disable**: Clients cannot connect to the access point at this speed.
MCS Table	The **MCS Rate** table is available only when **802.11 b/g/n** is selected in the **802.11 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 **Enable** (default) to have the NWA use the data rate. Select **Disable** if you do not want the NWA to use the data rate.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.4.2 Bridge / Repeater Mode

Use this screen to have the NWA act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

Use this screen to use the NWA as a wireless bridge. Select **Bridge/Repeater** as the **Operation Mode**.

Figure 25 Wireless > Wireless Settings: Bridge/Repeater



Basic Settings

□ Disable Wireless LAN Interface

Operation Mode :	Bridge/Repeater
Wireless Mode :	802.11b/g/n
SSID Profile :	Profile1
Channel:	7
Channel Width:	20MHZ

WDS Settings

Local MAC Address:	40	4a	03	42	70	2b
Remote MAC Address 1						
Remote MAC Address 2						
Remote MAC Address 3						
Remote MAC Address 4						

Advanced Settings

Output Power :	Full
Preamble Type	Dynamic
RTS/CTS Threshold	2346 (1~2346)
Extension channel protection mode	None
A-MPDU aggregation	● Enabled ○ Disabled
Short GI	● Enabled ○ Disabled

Rates Configuration

Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional

MCS Rate	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Enable	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

The following table describes the bridge labels in this screen.

Table 12 Wireless > Wireless Settings: Bridge/Repeater

LABEL	DESCRIPTIONS
Basic Settings	
Operation Mode	Select **Bridge/Repeater** in this field.
Wireless Mode	Select **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. Select **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.

Table 12 Wireless > Wireless Settings: Bridge/Repeater (continued)

LABEL	DESCRIPTIONS
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. Select an **SSID Profile** from the drop-down list box. 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	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 **802.11 b/g/n** in the **802.11 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 **20/40** (20/40 MHz). This allows the NWA to adjust the channel bandwidth depending on network conditions. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood.
WDS Settings	
Local Mac Address Remote MAC Address 1 - 4	A Wireless Distribution System is a wireless connection between two or more APs. Note: WDS security is independent of the security settings between the NWA and any wireless clients. **Local MAC Address** is the MAC address of your NWA. You can specify up to 4 remote devices' MAC addresses in this section.
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%**, **12.5%** or **Min** (Minimum). 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.
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.

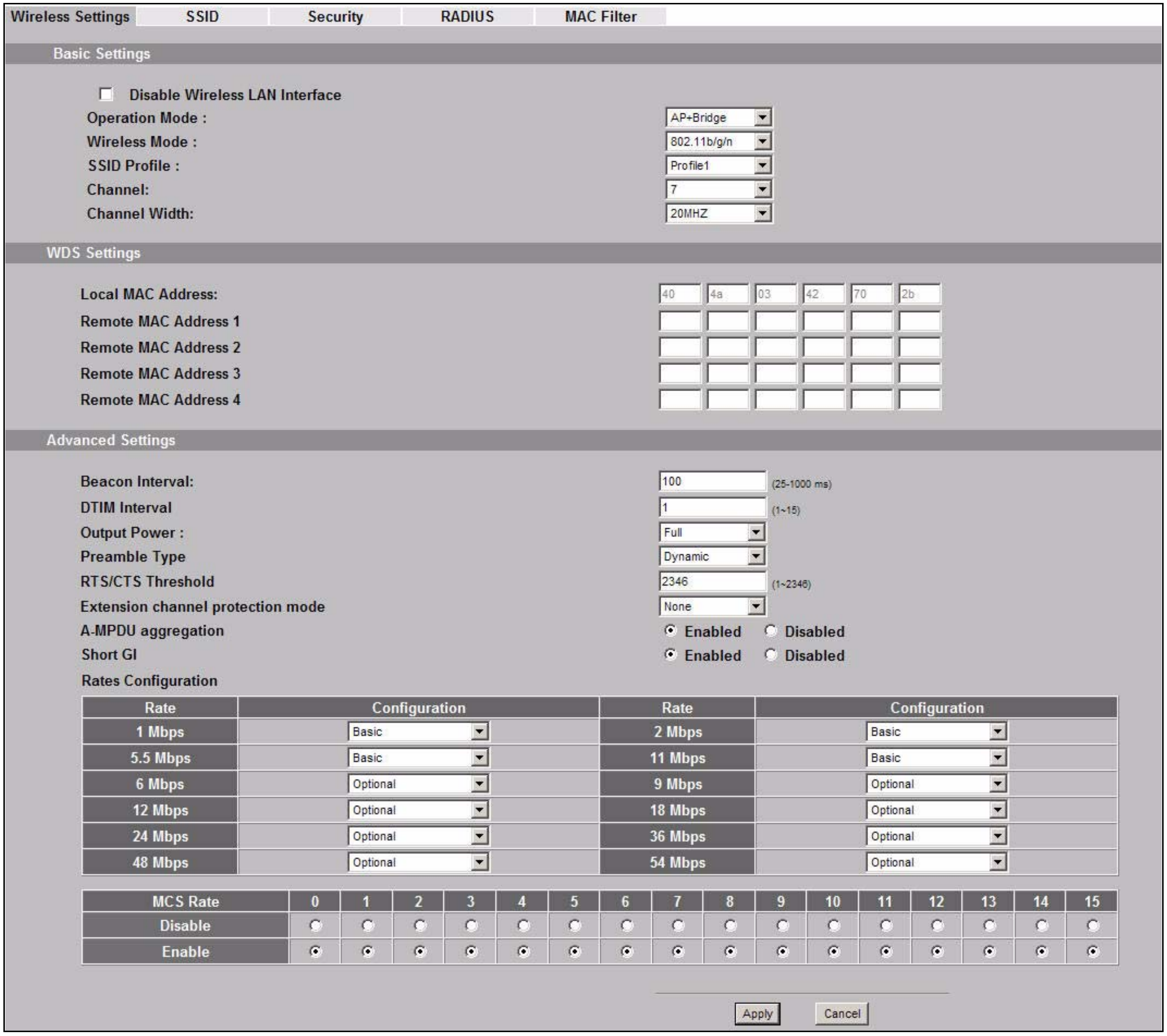
Table 12 Wireless > Wireless Settings: Bridge/Repeater (continued)

LABEL	DESCRIPTIONS
Rates Configuration	This section controls the data rates permitted for clients. For each **Rate**, select an option from the **Configuration** list. The options are: • **Basic** (1~11 Mbps only): Clients can always connect to the access point at this speed. • **Optional**: Clients can connect to the access point at this speed, when permitted to do so by the AP. • **Disable**: Clients cannot connect to the access point at this speed.
MCS Table	The **MCS Rate** table is available only when **802.11 b/g/n** is selected in the **802.11 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 **Enable** (default) to have the NWA use the data rate. Select **Disable** if you do not want the NWA to use the data rate.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.4.3 AP + Bridge Mode

Use this screen to have the NWA function as a bridge and access point simultaneously. Select **AP+Bridge** as the **Operation Mode**. The following screen displays.

Figure 26 Wireless > Wireless Settings: AP+Bridge



Basic Settings

☐ Disable Wireless LAN Interface

Operation Mode :	AP+Bridge
Wireless Mode :	802.11b/g/n
SSID Profile :	Profile1
Channel:	7
Channel Width:	20MHZ

WDS Settings

Local MAC Address:	40	4a	03	42	70	2b
Remote MAC Address 1						
Remote MAC Address 2						
Remote MAC Address 3						
Remote MAC Address 4						

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 ○ Disabled	
Short GI	● Enabled ○ Disabled	

Rates Configuration

Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional

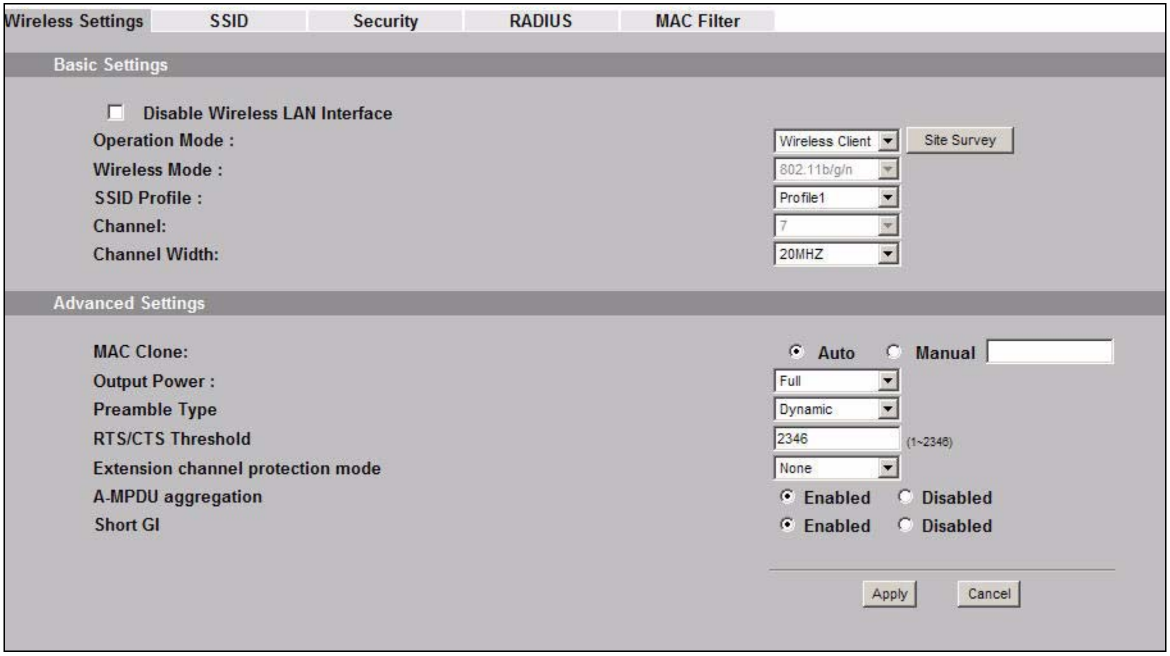
MCS Rate	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Enable	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

See the tables describing the fields in the **Access Point** and **Bridge / Repeater** operating modes for descriptions of the fields in this screen.

6.4.4 Wireless Client Mode

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

Figure 27 Wireless > Wireless Settings: Wireless Client



Basic Settings

□ Disable Wireless LAN Interface

Operation Mode : Wireless Client

Wireless Mode : 802.11b/g/n

SSID Profile : Profile1

Channel: 7

Channel Width: 20MHZ

Advanced Settings

MAC Clone: ● Auto ○ Manual

Output Power : Full

Preamble Type Dynamic

RTS/CTS Threshold 2346 (1~2346)

Extension channel protection mode None

A-MPDU aggregation ● Enabled ○ Disabled

Short GI ● Enabled ○ Disabled

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

Table 13 Wireless > Wireless Settings: Wireless Client

LABEL	DESCRIPTION
Basic Settings	
Operation Mode	Select **Wireless 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 and click **Selected**. Note: After selecting **Wireless Client** as the **Operation Mode** in the **Basic Settings** section, you must click **Apply** to be able to select from the AP list.
Wireless Mode	Select **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. Select **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.

Table 13 Wireless > 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 of the AP you want to use (click **Site Survey** button for a list of available APs). Click **Apply**. Set the security configuration for this operating mode in the **Wireless > Security** screen. Check the **Status** 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 **Wireless Client** as your operation mode.
Channel Width	This field displays only when you select **802.11 b/g/n** in the **802.11 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 **20/40** (20/40 MHz). This allows the NWA to adjust the channel bandwidth depending on network conditions. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood.
Advanced Settings	
MAC Clone	Choose **Manual** to configure the NWA's MAC address by cloning the MAC address from a computer on your LAN. Choose **Auto** to use the factory default MAC address of your NWA.
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%**, **12.5%** or **Min** (Minimum). 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.

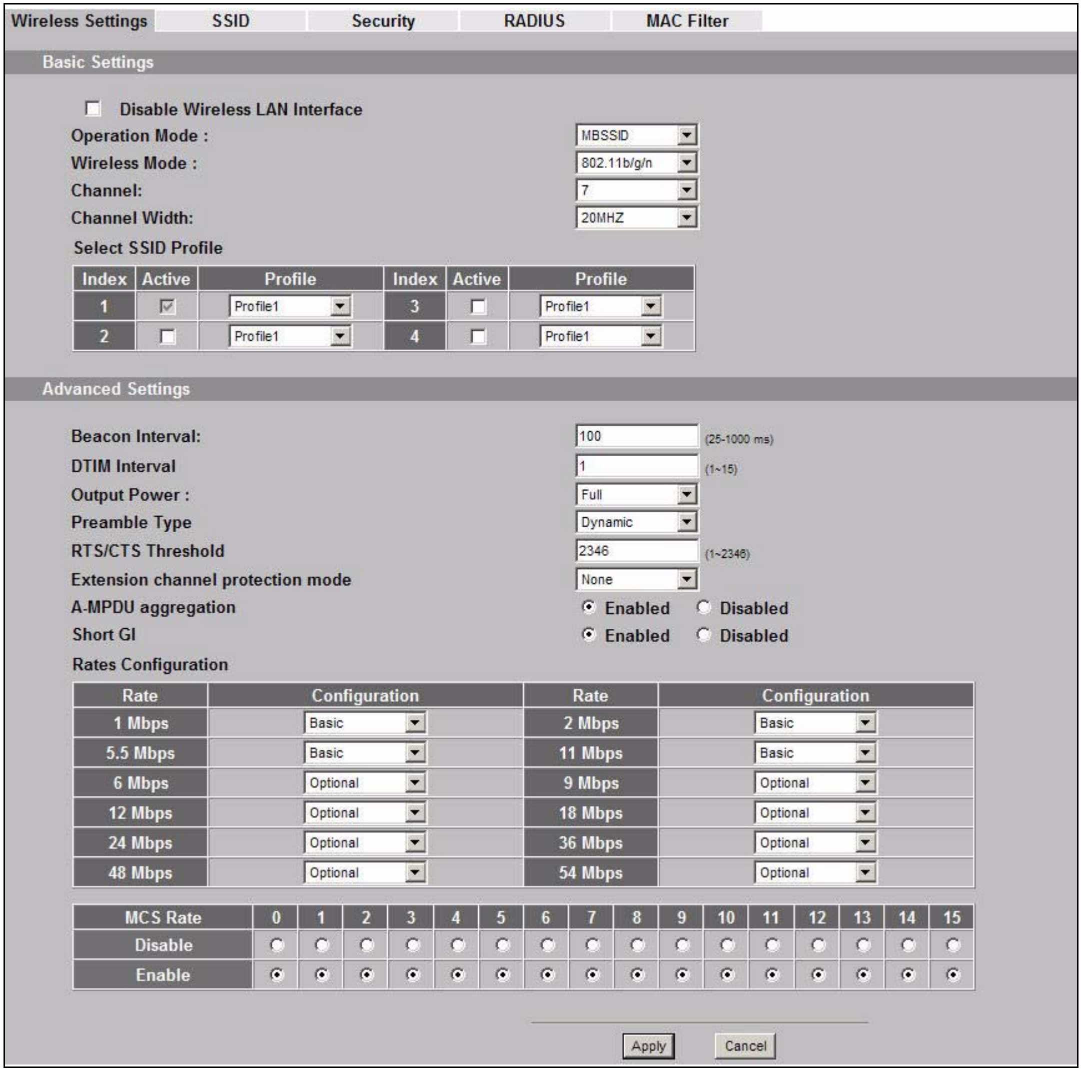
Table 13 Wireless > Wireless Settings: Wireless Client (continued)

LABEL	DESCRIPTION
A-MPDU aggregation	This field is available only when **802.11 b/g/n** is selected as the **Wireless Mode**. Select **Enable** to allow the grouping of several A-MSDUs (Aggregate MAC Service Data Units) into one large A-MPDU (Aggregate MAC Protocol Data Unit). This function allows faster data transfer rates.
Short GI	This field is available only when **802.11 b/g/n** is selected as the **Wireless Mode**. Select **Enable** 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.

6.4.5 MBSSID Mode

Use this screen to have the NWA function in MBSSID mode. Select **MBSSID** as the **Operating Mode**. The following screen diplays.

Figure 28 Wireless > Wireless Settings: MBSSID



Basic Settings

□ Disable Wireless LAN Interface

Operation Mode : MBSSID

Wireless Mode : 802.11b/g/n

Channel: 7

Channel Width: 20MHZ

Select SSID Profile

Index	Active	Profile	Index	Active	Profile
1	☑	Profile1	3	□	Profile1
2	□	Profile1	4	□	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 ○ Disabled

Short GI ● Enabled ○ Disabled

Rates Configuration

Rate	Configuration	Rate	Configuration
1 Mbps	Basic	2 Mbps	Basic
5.5 Mbps	Basic	11 Mbps	Basic
6 Mbps	Optional	9 Mbps	Optional
12 Mbps	Optional	18 Mbps	Optional
24 Mbps	Optional	36 Mbps	Optional
48 Mbps	Optional	54 Mbps	Optional

MCS Rate	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Enable	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

The following table describes the labels in this screen.

Table 14 Wireless > Wireless Settings: MBSSID

LABEL	DESCRIPTION
Operating Mode	Select **MBSSID** in this field.
802.11 Mode	Select **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. Select **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.
Channel	Select the operating frequency/channel depending on your particular region from the drop-down list box.

Table 14 Wireless > Wireless Settings: MBSSID (continued)

LABEL	DESCRIPTION
Channel Width	This field displays only when you select **802.11 b/g/n** in the **802.11 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 **20/40** (20/40 MHz). This allows the NWA to adjust the channel bandwidth depending on network conditions. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood.
Select SSID Profile	An SSID profile is the set of parameters relating to one of the NWA's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating with the access point (AP) must have the same SSID. 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.
Index	Select the check box to activate an SSID profile.
Active	Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it. The first profile is always active.
Profile	Select the profile(s) of the SSIDs you want to use in your wireless network. You can have up to four BSSs running on the NWA simultaneously. Configure SSID profiles in the **SSID** screen.
Advanced Settings	
Beacon Interval	When a wirelessly networked 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%**, **12.5%** or **Min** (Minimum). 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.

Table 14 Wireless > Wireless Settings: MBSSID (continued)

LABEL	DESCRIPTION
Extension channel protection mode	You can use **CTS to self** or **RTS-CTS** protection mechanism to reduce conflicts with other wireless networks or hidden wireless clients. The throughput of **RTS-CTS** is much lower than **CTS to self**. Using this mode may decrease your wireless performance.
A-MPDU aggregation	This field is available only when **802.11 b/g/n** is selected as the **Wireless Mode**. Select **Enable** to allow the grouping of several A-MSDUs (Aggregate MAC Service Data Units) into one large A-MPDU (Aggregate MAC Protocol Data Unit). This function allows faster data transfer rates.
Short GI	This field is available only when **802.11 b/g/n** is selected as the **Wireless Mode**. Select **Enable** 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.
Rates Configuration	This section controls the data rates permitted for clients. For each **Rate**, select an option from the **Configuration** list. The options are: • **Basic** (1~11 Mbps only): Clients can always connect to the access point at this speed. • **Optional**: Clients can connect to the access point at this speed, when permitted to do so by the AP. • **Disable**: Clients cannot connect to the access point at this speed.
MCS Table	The **MCS Rate** table is available only when **802.11 b/g/n** is selected in the **802.11 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 **Enable** (default) to have the NWA use the data rate. Select **Disable** if you do not want the NWA to use the data rate.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.5 Technical Reference

This section provides technical background information about the topics covered in this chapter. Refer to Appendix E on page 191 for further readings on Wireless LAN.

6.5.1 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).

6.5.2 Spanning Tree Protocol (STP)

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

6.5.2.1 Rapid STP

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

6.5.2.2 STP Terminology

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

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

Table 15 STP Path Costs

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

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

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

6.5.2.3 How STP Works

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

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

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

6.5.2.4 STP Port States

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

Table 16 STP Port States

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

6.5.3 Additional Wireless Terms

Table 17 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. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the NWA.
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
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.
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.

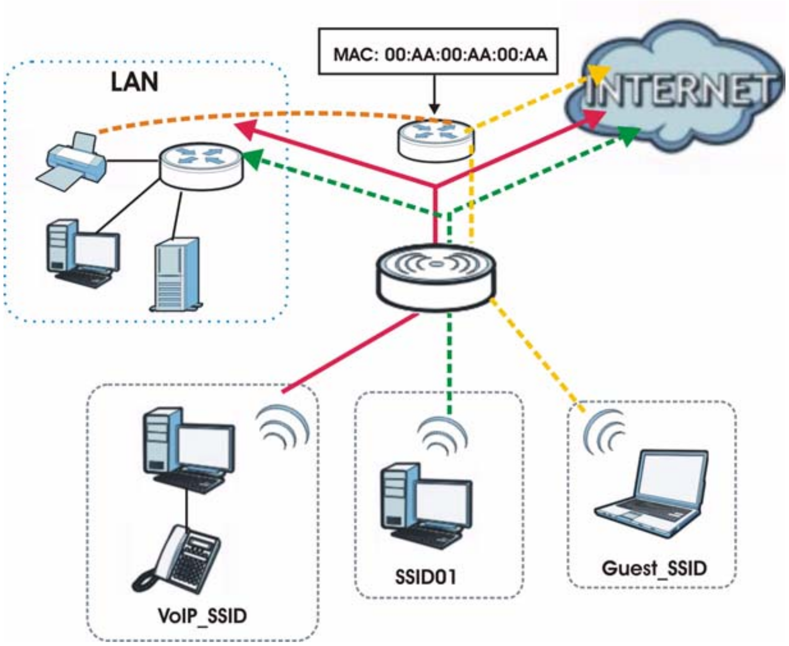
7

SSID Screen

7.1 Overview

This chapter describes how you can configure Service Set Identifier (SSID) profiles in your NWA.

Figure 29 Sample SSID Profiles



In the figure above, the NWA has three SSID profiles configured: a standard profile (**SSID01**), a profile with high QoS settings for Voice over IP (VoIP) users (**VoIP_SSID**), and a guest profile that allows visitors access only the Internet and the network printer (**Guest_SSID**).

7.1.1 What You Can Do in this Chapter

Use the **Wireless > SSID** screen to configure up to 16 SSID profiles for your NWA (see Section 7.2 on page 80).

7.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

When the NWA is set to Access Point, AP + Bridge or MBSSID mode, you need to choose the SSID profile(s) you want to use in your wireless network (see Section 6.4 on page 62 for more information on operating modes).

To configure the settings of your SSID profile, you need to know the Media Access Control (MAC) addresses of the devices you want to allow access to it.

Each SSID profile references the settings configured in the following screens:

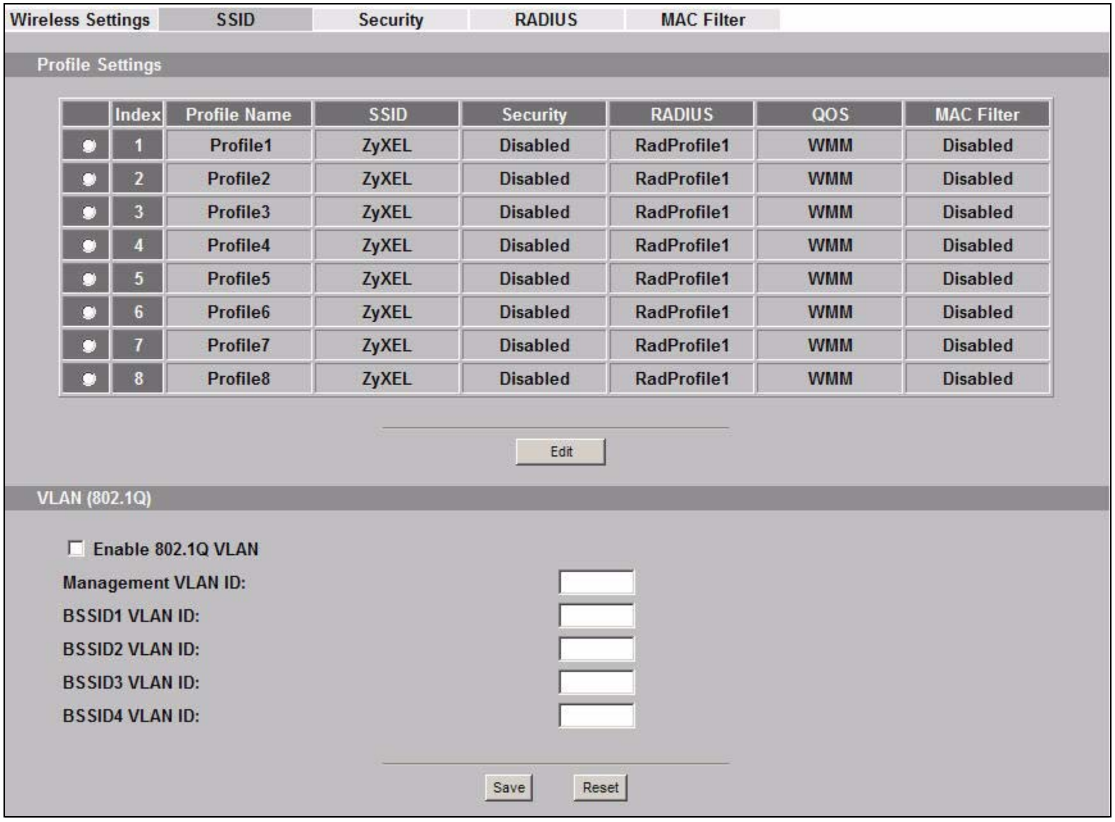
- **Wireless** > **Security** (one of the security profiles)
- **Wireless** > **RADIUS** (one of the RADIUS profiles)
- **Wireless** > **MAC Filter** (the MAC filter list, if activated in the SSID profile)
- Also, use the **VLAN** screen to set up wireless VLANs based on SSID

Configure the fields in the above screens to use the settings in an SSID profile.

7.2 The SSID Screen

Use this screen to select the SSID profile you want to configure. Click **Wireless** > **SSID** to display the screen as shown.

Figure 30 Wireless > SSID



Profile Settings

	Index	Profile Name	SSID	Security	RADIUS	QOS	MAC Filter
○	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

VLAN (802.1Q)

□ Enable 802.1Q VLAN

Management VLAN ID:

BSSID1 VLAN ID:

BSSID2 VLAN ID:

BSSID3 VLAN ID:

BSSID4 VLAN ID:

The following table describes the labels in this screen.

Figure 31 Wireless > SSID

LABEL	DESCRIPTION
Profile Settings	
Index	This field displays the index number of each SSID profile.

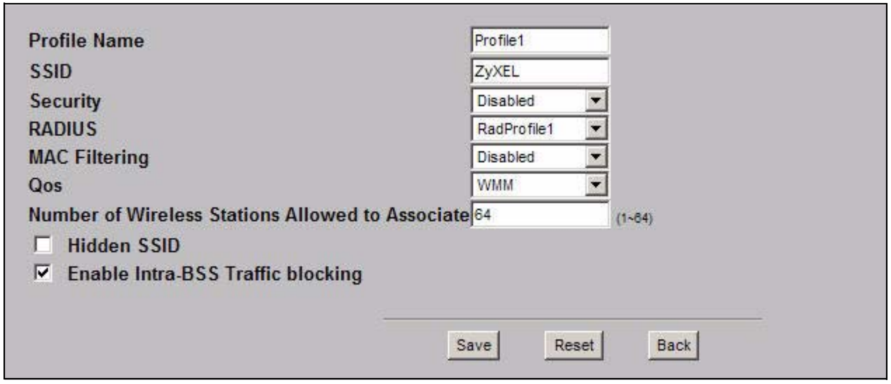
Figure 31 Wireless > SSID (continued)

LABEL	DESCRIPTION
Profile Name	This field displays the identification name of each SSID profile on the NWA.
SSID	This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates which security profile is currently associated with each SSID profile. See Section 8.4.1 on page 89 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 the radio button next to the profile you want to configure and click **Edit** to go to the SSID configuration screen.
VLAN (802.1Q)	
Enable 802.1Q VLAN	Select this to enable VLAN tagging.
Management VLAN ID	Enter a number from 1 to 4094 to define this VLAN group. At least one device in your network must belong to this VLAN group in order to manage the NWA.
BSSID1~4 VLAN ID	Enter a VLAN ID number from 1 to 4094. Packets coming from the WLAN using this BSSID profile are tagged with the VLAN ID number by the NWA. Different BSSID profiles can use the same or different VLAN IDs. This allows you to split wireless stations into groups using similar VLAN IDs.
Save	Click **Save** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.2.1 Configuring SSID

Use this screen to configure an SSID profile. In the **Wireless > SSID** screen, select an SSID profile and click **Edit** to display the following screen.

Figure 32 SSID: Edit



Profile Name	Profile1
SSID	ZyXEL
Security	Disabled
RADIUS	RadProfile1
MAC Filtering	Disabled
Qos	WMM
Number of Wireless Stations Allowed to Associate	64 (1~64)

□ Hidden SSID

☑ Enable Intra-BSS Traffic blocking

The following table describes the labels in this screen.

Table 18 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 8.4.1 on page 89 for more information.
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 9.4 on page 100 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 **Disable**.
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_BEST_EFFORT** 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.
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 to broadcast this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, if you select the checkbox, the NWA hide this SSID (a wireless client scanning for an AP will not find this SSID).
Enable Intra-BSS Traffic blocking	Select the checkbox to prevent wireless clients in this profile's BSS from communicating with one another.
Save	Click **Save** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

7.3 Technical Reference

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

7.3.1 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).

7.3.1.1 WMM QoS Priorities

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

Table 19 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_BEST_EFFORT)	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.

7.3.2 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the NWA) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

7.3.2.1 ToS (Type of Service) and WMM QoS

The DSCP value of outgoing packets is between 0 and 255. 0 is the default priority. WMM QoS checks the DSCP value in the header of data packets. It gives the traffic a priority according to this number.

In order to control which priority level is given to traffic, the device sending the traffic must set the DSCP value in the header. If the DSCP value is not specified, then the traffic is treated as best-effort. This means the wireless clients and the devices with which they are communicating must both set the DSCP value in order to make the best use of WMM QoS. A Voice over IP (VoIP) device for example may allow you to define the DSCP value.

The following table lists which WMM QoS priority level the NWA uses for specific DSCP values.

Table 20 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping

Dscp Value	WMM qos Priority Level
224, 192	voice
160, 128	video

Table 20 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping

Dscp Value	WMM qos Priority Level
96, 0 [A]	besteffort
64, 32	background

[A] The NWA also uses best effort for any DSCP value for which another WMM QoS priority is not specified (255, 158 or 37 for example).

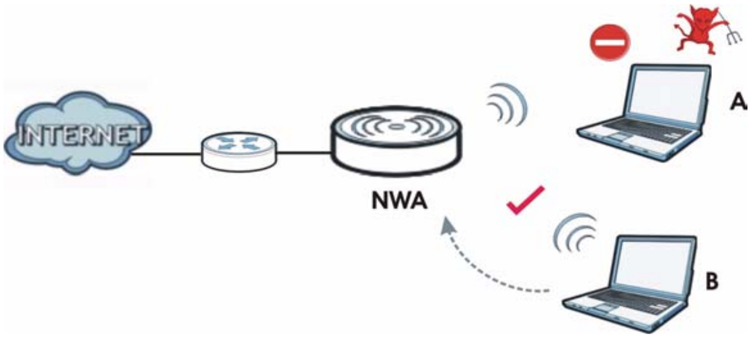
Wireless Security Screen

8.1 Overview

This chapter describes how to use the **Wireless Security** screen. This screen allows you to configure the security mode for your NWA.

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

Figure 33 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.

8.2 What You Can Do in this Chapter

Use the **Wireless > Security** screen to choose the security mode for your NWA (see Section 8.4 on page 87).

8.3 What You Need To Know

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 21 Wireless Security Levels

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

The available security modes in your 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.
- **802.1x-Only.** This is a standard that extends the features of IEEE 802.11 to support extended authentication. It provides additional accounting and control features. This option does not support data encryption.
- **802.1x-Static64.** This provides 802.1x-Only authentication with a static 64bit WEP key and an authentication server.
- **802.1x-Static128**. This provides 802.1x-Only authentication with a static 128bit WEP key and an authentication server.
- **802.1x-Static152**. This provides 802.1x-Only authentication with a static 152bit WEP key and an authentication server.
- **WPA.** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard.
- **WPA2.** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
- **WPA2-MIX.** This commands the NWA to use either WPA2 or WPA depending on which security mode the wireless client uses.

- **WPA2-PSK**. This adds a pre-shared key on top of WPA2 standard.
- **WPA2-PSK-MIX**. This commands the NWA to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.

Note: In **Bridge/Repeater** and **AP+Bridge** operating modes, the only available security modes are **WEP**, **WPA-PSK**, and **WPA2-PSK**.

Note: To guarantee 802.11n wireless speed, please only use WPA2 or WPA2-PSK security mode. Other security modes may degrate 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).

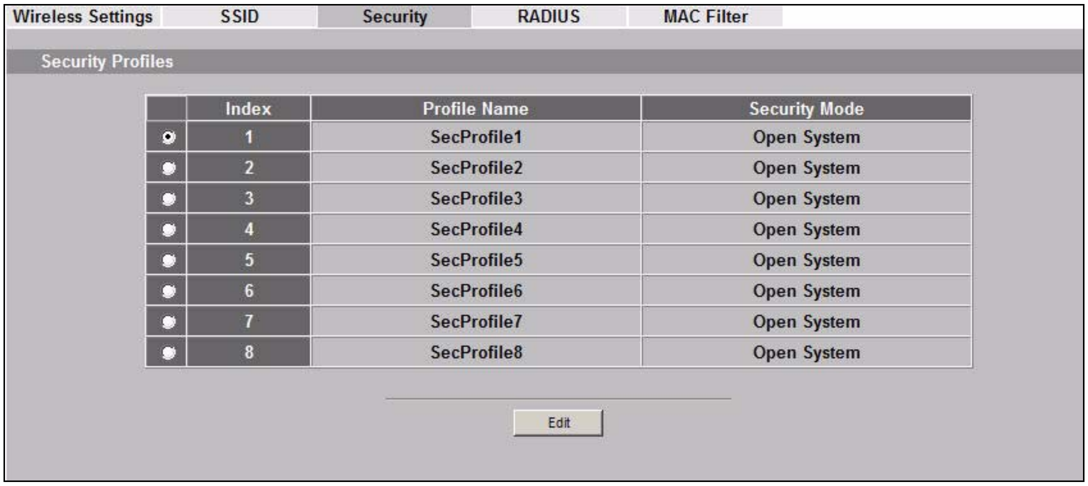
Further information on these terms can be found in Appendix E on page 191.

8.4 The Security Screen

Use this screen to choose the security mode for your NWA.

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

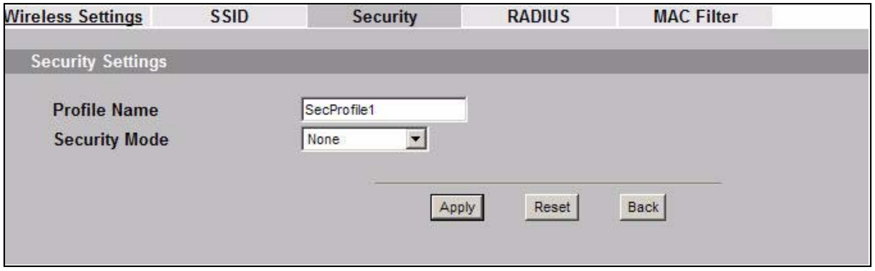
Figure 34 Wireless > Security



	Index	Profile Name	Security Mode
●	1	SecProfile1	Open System
○	2	SecProfile2	Open System
○	3	SecProfile3	Open System
○	4	SecProfile4	Open System
○	5	SecProfile5	Open System
○	6	SecProfile6	Open System
○	7	SecProfile7	Open System
○	8	SecProfile8	Open System

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

Figure 35 Security: None



Profile Name: SecProfile1
Security Mode: None

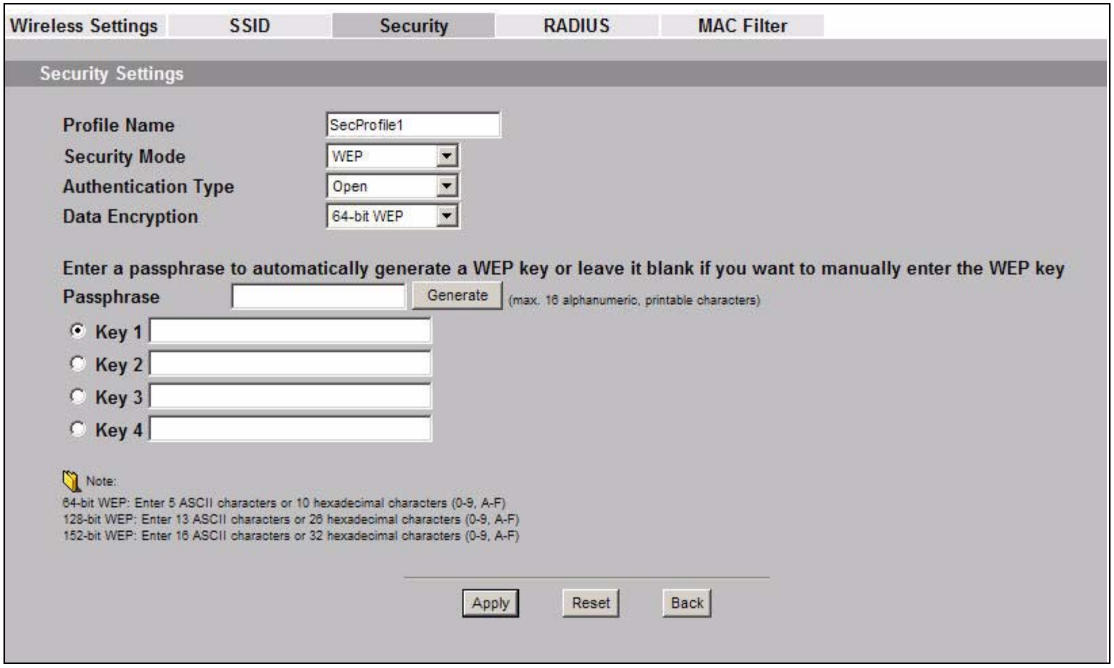
Note that some screens display differently depending on the operating mode selected in the **Wireless > Wireless Settings** screen.

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

8.4.1 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 36 Security: WEP



Profile Name: SecProfile1

Security Mode: WEP

Authentication Type: Open

Data Encryption: 64-bit WEP

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

Passphrase (max. 16 alphanumeric, printable characters)

● 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)
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters (0-9, A-F)

The following table describes the labels in this screen.

Table 22 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 Key** from the drop-down list box.
Data Encryption	Select **64-bit WEP**, **128-bit WEP** or **152-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.
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"). If you chose **152-bit WEP**, then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time.
Apply	Click **Apply** to save your changes.

Table 22 Security: WEP (continued)

LABEL	DESCRIPTION
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

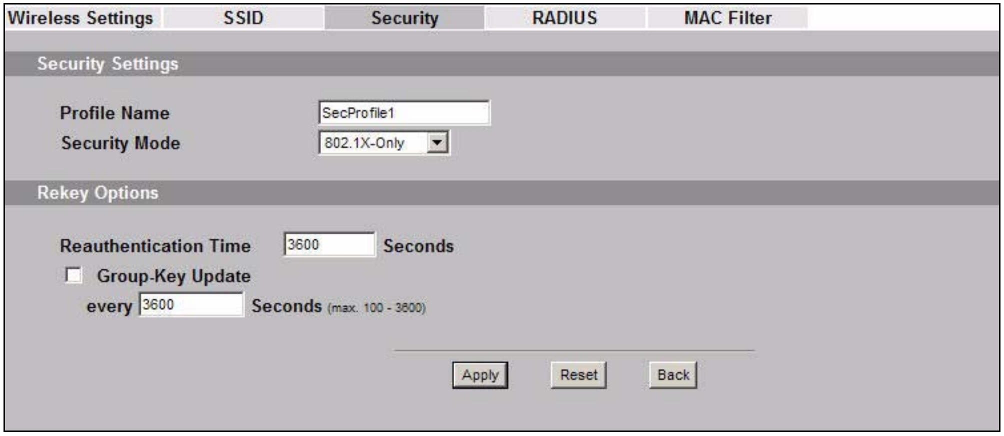
8.4.2 Security: 802.1x Only

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

8.4.2.1 Access Point

Use this screen to use 802.1x-Only security mode for your NWA that is in Access Point operating mode. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

Figure 37 Security: 802.1x Only for Access Point



Profile Name: SecProfile1

Security Mode: 802.1X-Only

Reauthentication Time: 3600 Seconds

□ Group-Key Update

every 3600 Seconds (max. 100 - 3600)

The following table describes the labels in this screen.

Table 23 Security: 802.1x Only for Access Point

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose **802.1x Only** in this field.
Rekey Options	
ReAuthentication Time	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. Alternatively, enter “0” to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group-Key Update	The NWA automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.
Apply	Click **Apply** to save your changes.

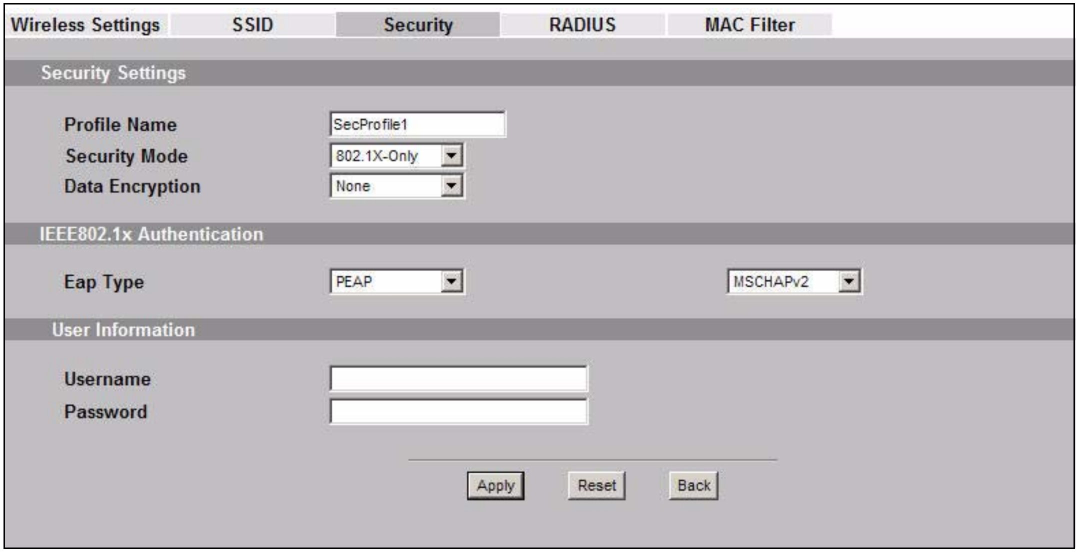
Table 23 Security: 802.1x Only for Access Point (continued)

LABEL	DESCRIPTION
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

8.4.2.2 Wireless Client

Use this screen to use 802.1x-Only security mode for your NWA that is in Wireless Client operating mode. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

Figure 38 Security: 802.1x Only for Wireless Client



Security Settings

Profile Name: SecProfile1
Security Mode: 802.1X-Only
Data Encryption: None

IEEE802.1x Authentication

Eap Type: PEAP MSCHAPv2

User Information

Username:
Password:

The following table describes the labels in this screen.

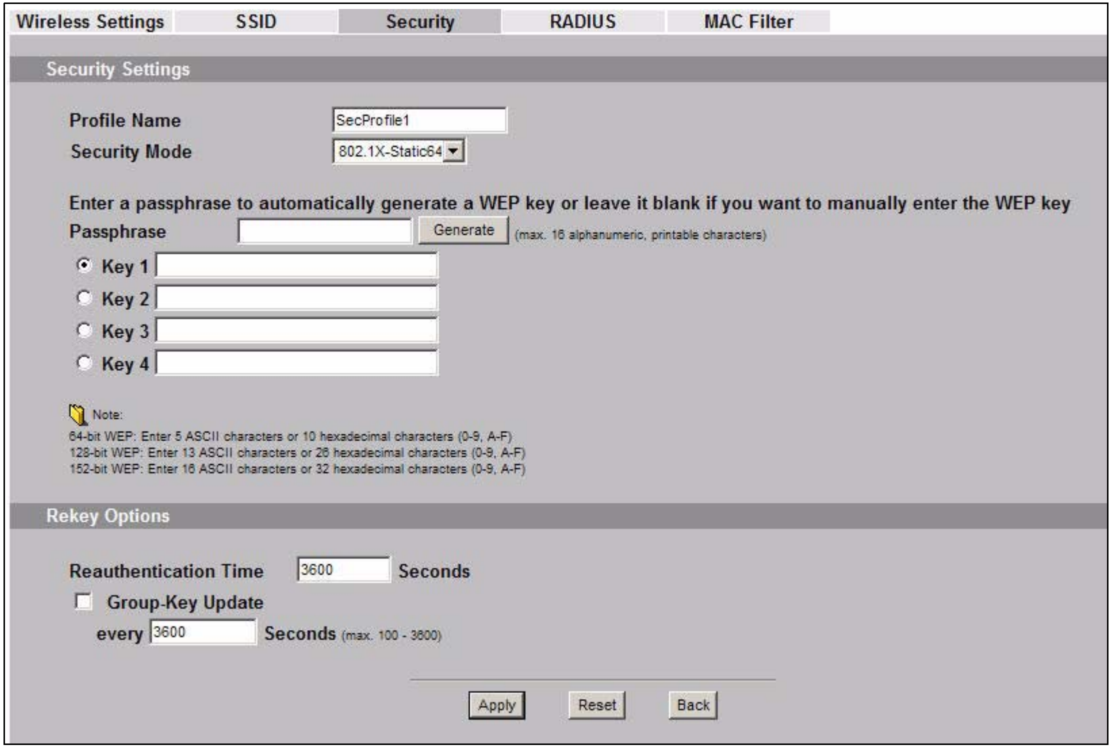
Table 24 Security: 802.1x Only for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose the same security mode used by the AP.
Data Encryption	Select between **None** and **Dynamic WEP**. Refer to Appendix E on page 198 for information on using Dynamic WEP.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

8.4.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit, 802.1x Static 152-bit

Use this screen to use 802.1x Static 64, 802.1x Static 128, or 802.1x Static 152 security mode for your NWA. Select **802.1x Static 64**, **802.1x Static 128**, or **802.1x Static 152** in the **Security Mode** field to display the following screen.

Figure 39 Security: 802.1x Static 64-bit, 802.1x Static 128-bit, 802.1x Static 152-bit (AP mode)



Security Settings

Profile Name: SecProfile1

Security Mode: 802.1X-Static64

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

Passphrase Generate (max. 16 alphanumeric, printable characters)

● 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)
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters (0-9, A-F)

Rekey Options

Reauthentication Time: 3600 Seconds

□ Group-Key Update

every 3600 Seconds (max. 100 - 3600)

The following table describes the labels in this screen.

Table 25 Security: 802.1x Static 64-bit, 802.1x Static 128-bit, 802.1x Static 152-bit

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose **802.1x Static 64**, **802.1x Static 128**, or **802.1x Static 152** in this field.
Passphrase	Enter the passphrase or string of text used for automatic WEP key generation on wireless client adapters (AP mode).
Generate	Click this to get the keys from the **Passphrase** you entered (AP mode).

Table 25 Security: 802.1x Static 64-bit, 802.1x Static 128-bit, 802.1x Static 152-bit (continued)

LABEL	DESCRIPTION
Key 1 to Key 4	If you chose **802.1x Static 64**, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **802.1x Static 128-bit**, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations. The preceding “0x” is entered automatically. You must configure all four keys, but only one key can be activated at any one time.
Rekey Options	
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. Alternatively, enter “0” to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group-Key Update	The NWA automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

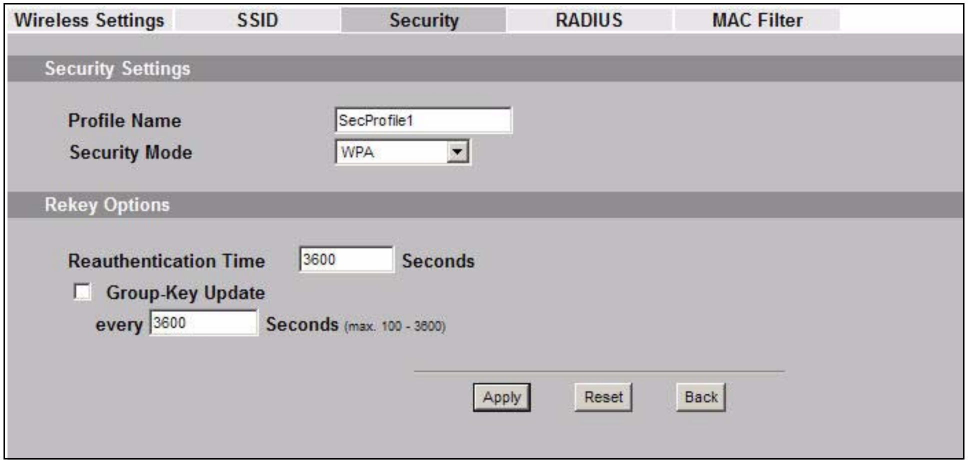
8.4.4 Security: WPA

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

8.4.4.1 Access Point

Use this screen to employ WPA as the security mode for your NWA that is in Access Point operating mode. Select **WPA** in the **Security Mode** field to display the following screen.

Figure 40 Security: WPA for Access Point



Security Settings

Profile Name: SecProfile1

Security Mode: WPA

Rekey Options

Reauthentication Time: 3600 Seconds

□ Group-Key Update

every 3600 Seconds (max. 100 - 3600)

The following table describes the labels in this screen.

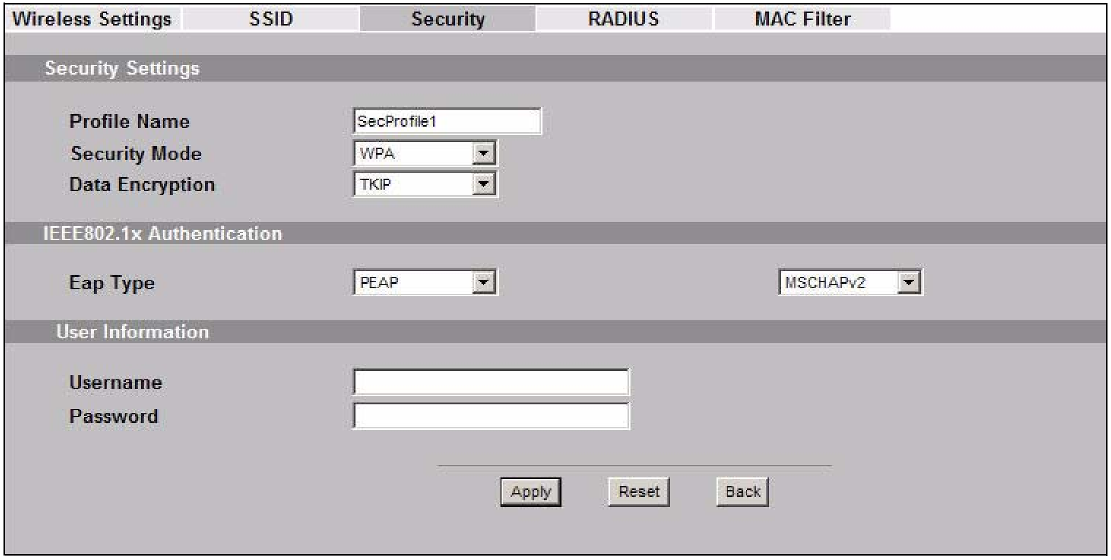
Table 26 Security: WPA for Access Point

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose **WPA** in this field.
Rekey Options	
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. Alternatively, enter "0" to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

8.4.4.2 Wireless Client

Use this screen to employ WPA as the security mode for your NWA that is in Wireless Client operating mode. Select **WPA** in the **Security Mode** field to display the following screen.

Figure 41 Security: WPA for Wireless Client



Security Settings

Profile Name: SecProfile1
Security Mode: WPA
Data Encryption: TKIP

IEEE802.1x Authentication

Eap Type: PEAP MSCHAPv2

User Information

Username:
Password:

The following table describes the labels in this screen.

Table 27 Security: WPA for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose the same security mode used by the AP.
Data Encryption	Select between **None** and **TKIP**.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

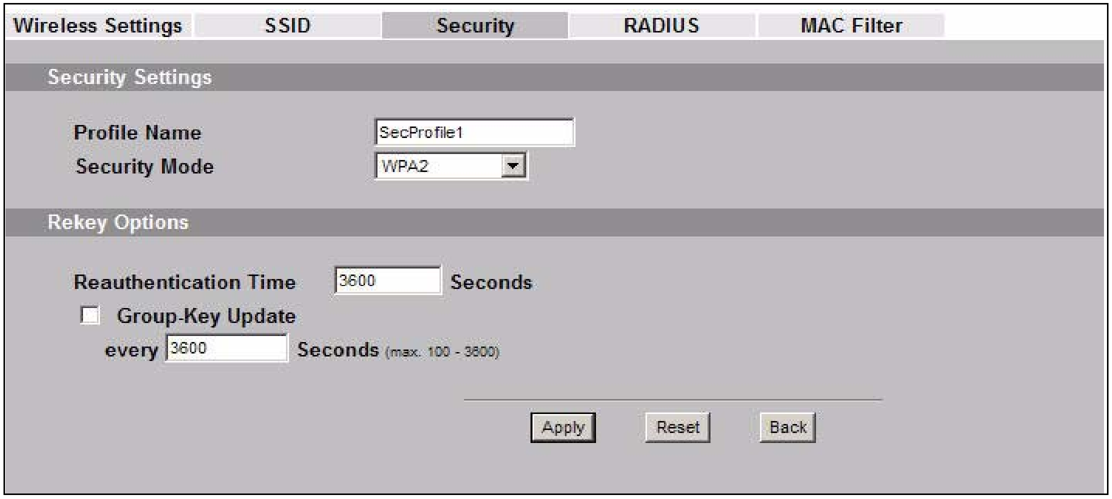
8.4.5 Security: WPA2 or WPA2-MIX

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

8.4.5.1 Access Point

Use this screen to use WAP2 or WPA2-MIX as the security mode for your NWA that is in Access Point operating mode. Select **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 42 Security:WPA2 or WPA2-MIX for Access Point



Profile Name: SecProfile1
Security Mode: WPA2
Reauthentication Time: 3600 Seconds
□ Group-Key Update
every 3600 Seconds (max. 100 - 3600)

The following table describes the labels not previously discussed

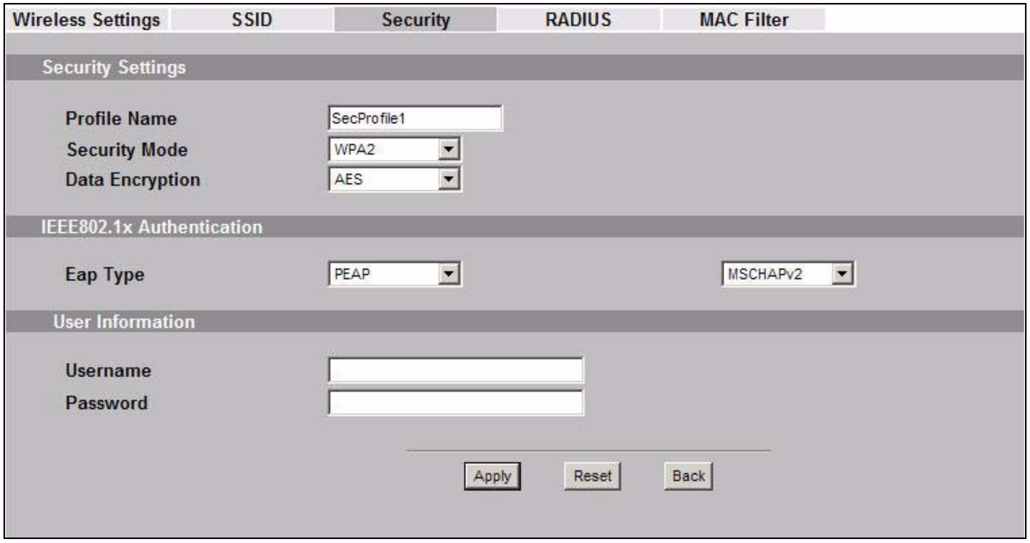
Table 28 Security: WPA2 or WPA2-MIX for Access Point

LABEL	DESCRIPTIONS
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose **WPA2** or **WPA2-MIX** in this field.
Rekey Options	
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. Alternatively, enter "0" to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

8.4.5.2 Wireless Client

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

Figure 43 Security: WPA2 or WPA2-MIX for Wireless Client



Security Settings

Profile Name: SecProfile1

Security Mode: WPA2

Data Encryption: AES

IEEE802.1x Authentication

Eap Type: PEAP MSCHAPv2

User Information

Username

Password

The following table describes the labels in this screen.

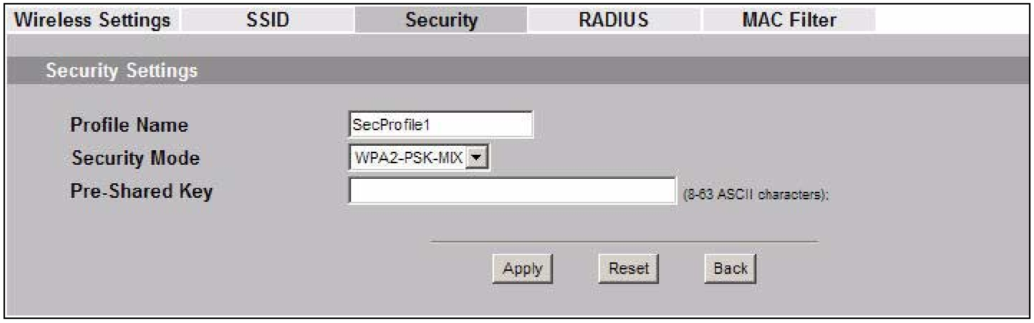
Table 29 Security: WPA2 or WPA2-MIX for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Profile Name	This is the name that identifying this profile.
Security Mode	Choose the same security mode used by the AP.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

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

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

Figure 44 Security: WPA-PSK, 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 30 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Profile Name	This is the name that identifying this profile.
Security Mode	Choose **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click **Apply** to save your changes.

Table 30 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX (continued)

LABEL	DESCRIPTION
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

8.5 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

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

- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.Use WPA(2) security if you have WPA(2)-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.
- If you don’t have WPA(2)-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security. You can manually enter 64-bit, 128-bit or 152-bit WEP keys.

More information on Wireless Security can be found in Appendix E on page 191.

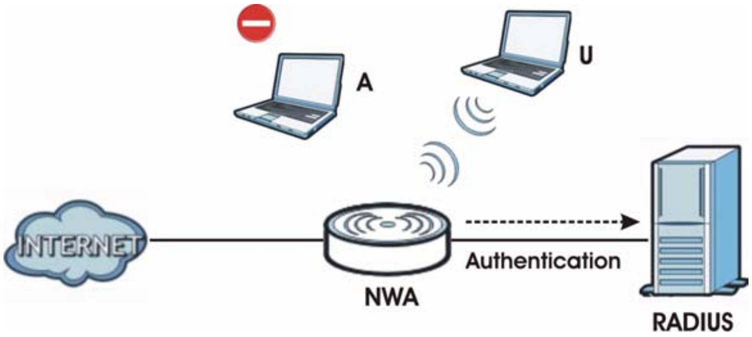
RADIUS Screen

9.1 Overview

This chapter describes how you can use the **Wireless > RADIUS** screen.

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 45 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.

9.2 What You Can Do in this Chapter

Use the **Security > RADIUS** screen if you want to authenticate wireless users using a RADIUS Server and/or Accounting Server (see Section 8.4.1 on page 89).

9.3 What You Need to Know

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.

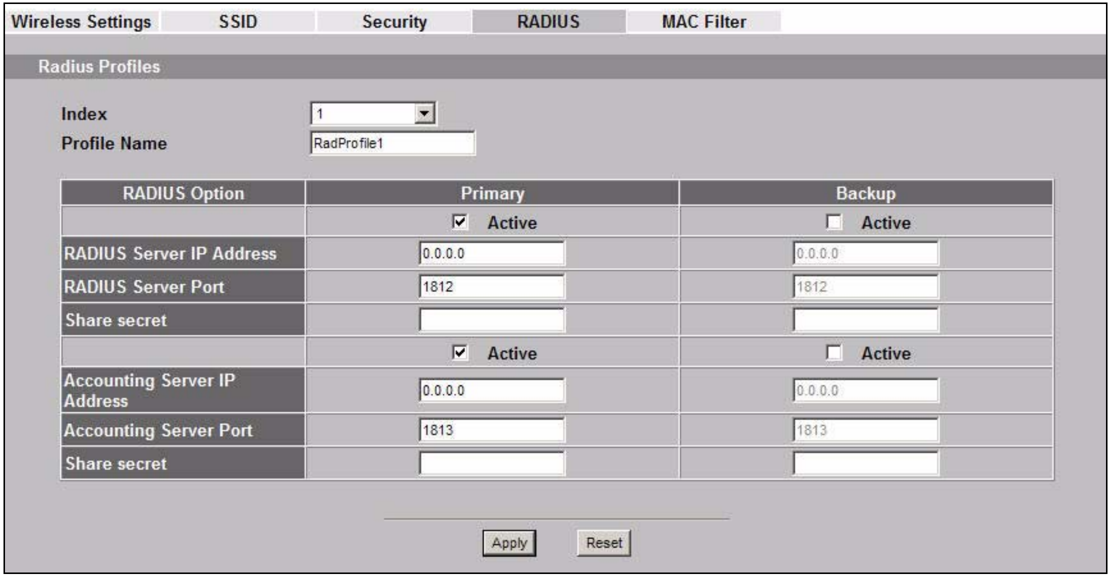
RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

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.

9.4 The RADIUS Screen

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

Figure 46 Wireless > RADIUS



Index	1
Profile Name	RadProfile1

RADIUS Option	Primary	Backup
	☑ Active	□ Active
RADIUS Server IP Address	0.0.0.0	0.0.0.0
RADIUS Server Port	1812	1812
Share secret		
	☑ Active	□ Active
Accounting Server IP Address	0.0.0.0	0.0.0.0
Accounting Server Port	1813	1813
Share secret		

The following table describes the labels in this screen.

Table 31 Wireless > RADIUS

LABEL	DESCRIPTION
Index	Select an index number.
ProfileName	This is the name that identifying this RADIUS.
Primary	Configure the fields below to set up user authentication and accounting.
Backup	If the NWA cannot communicate with the **Primary** accounting server, you can have the NWA use a **Backup** RADIUS server. Make sure the **Active** check boxes are selected if you want to use backup servers. The NWA will attempt to communicate three times before using the **Backup** servers. 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 Timer** field in the **Security Settings** screen.
RADIUS Option	

Table 31 Wireless > RADIUS (continued)

LABEL	DESCRIPTION
Active	Select the check box to enable user authentication through an external authentication server. This check box is not available when you select **Internal**.
RADIUS Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation. This field is not available when you select **Internal**.
RADIUS Server Port	Enter the port number of the external authentication server. You do not need to this value unless your network administrator instructs you to do so. This field is not available when you select **Internal**.
Share Secret	Enter a password (up to 128 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. This field is not available when you select **Internal**.
Active	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. You do not need to change this value unless your network administrator instructs you to do so with additional information.
Share Secret	Enter a password (up to 128 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.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

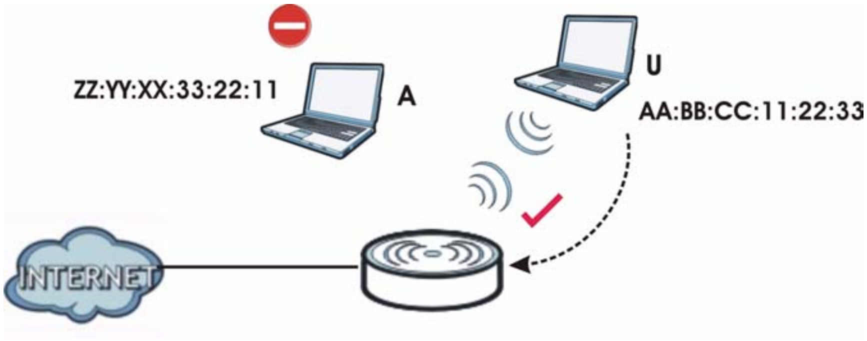
MAC Filter Screen

10.1 Overview

This chapter discusses how you can use the **Wireless > MAC Filter** screen.

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 47 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.

10.2 What You Can Do in this Chapter

Use the **Wireless > MAC Filter** screen to specify which wireless station is allowed or denied access to the NWA (see Section 10.4 on page 103).

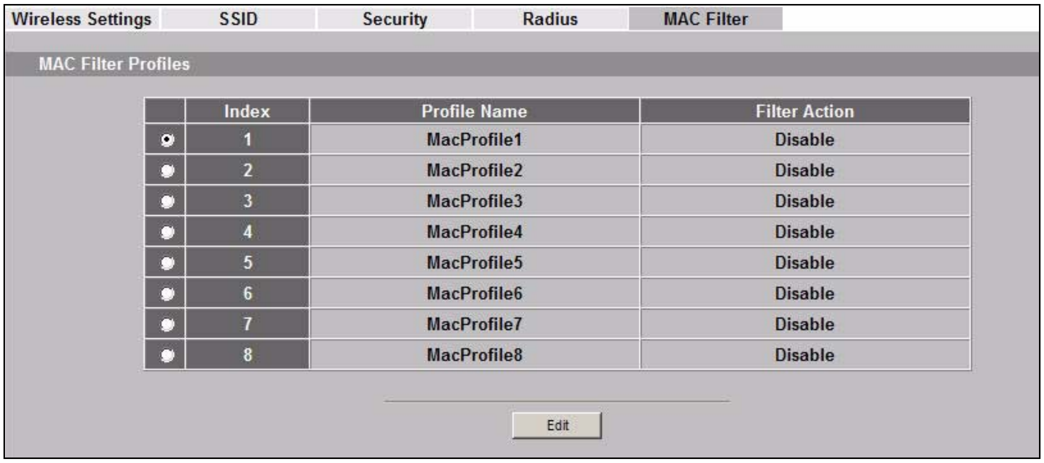
10.3 What You Need To Know

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.

10.4 MAC Filter Screen

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 > MAC Filter**. The screen displays as shown.

Figure 48 Wireless > MAC Filter

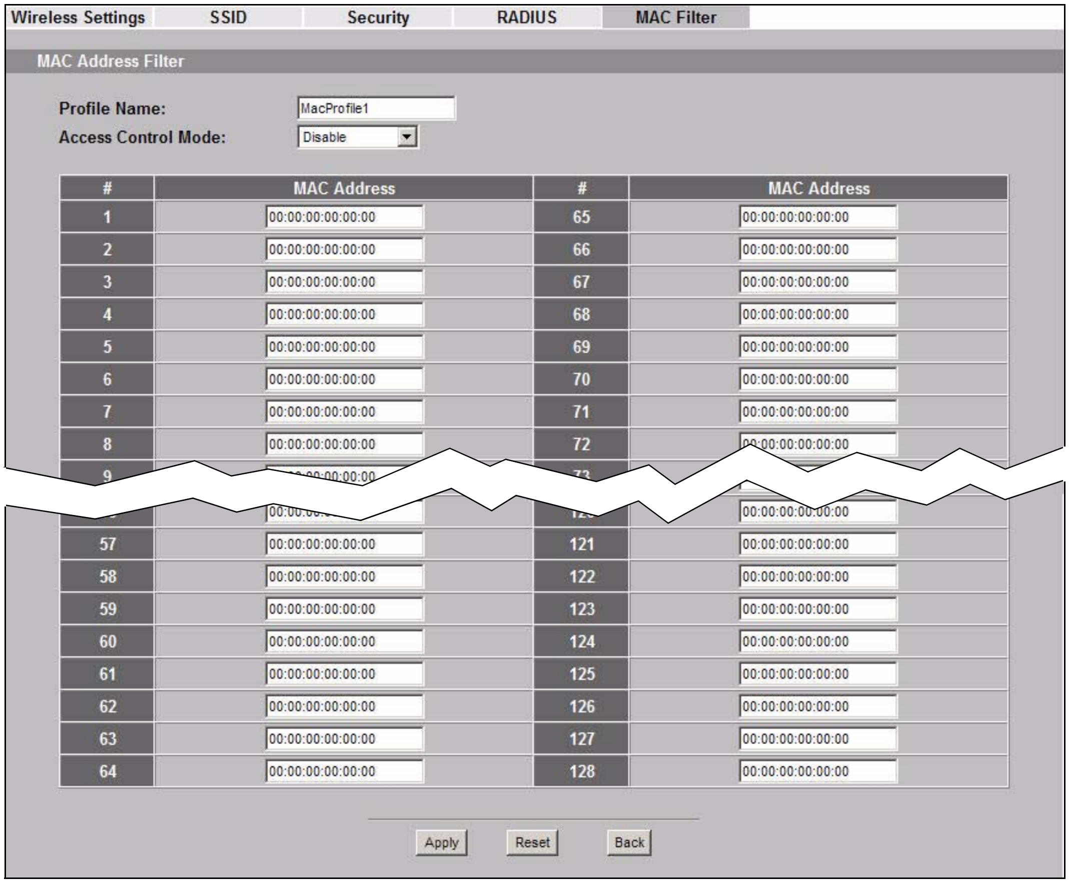


MAC Filter Profiles

	Index	Profile Name	Filter Action
◉	1	MacProfile1	Disable
○	2	MacProfile2	Disable
○	3	MacProfile3	Disable
○	4	MacProfile4	Disable
○	5	MacProfile5	Disable
○	6	MacProfile6	Disable
○	7	MacProfile7	Disable
○	8	MacProfile8	Disable

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

Figure 49 MAC Filter: Edit



MAC Address Filter

Profile Name: MacProfile1

Access Control Mode: Disable

#	MAC Address	#	MAC Address
1	00:00:00:00:00:00	65	00:00:00:00:00:00
2	00:00:00:00:00:00	66	00:00:00:00:00:00
3	00:00:00:00:00:00	67	00:00:00:00:00:00
4	00:00:00:00:00:00	68	00:00:00:00:00:00
5	00:00:00:00:00:00	69	00:00:00:00:00:00
6	00:00:00:00:00:00	70	00:00:00:00:00:00
7	00:00:00:00:00:00	71	00:00:00:00:00:00
8	00:00:00:00:00:00	72	00:00:00:00:00:00
57	00:00:00:00:00:00	121	00:00:00:00:00:00
58	00:00:00:00:00:00	122	00:00:00:00:00:00
59	00:00:00:00:00:00	123	00:00:00:00:00:00
60	00:00:00:00:00:00	124	00:00:00:00:00:00
61	00:00:00:00:00:00	125	00:00:00:00:00:00
62	00:00:00:00:00:00	126	00:00:00:00:00:00
63	00:00:00:00:00:00	127	00:00:00:00:00:00
64	00:00:00:00:00:00	128	00:00:00:00:00:00

The following table describes the labels in this screen.

Table 32 Wireless > MAC Filter

LABEL	DESCRIPTION
ProfileName	This is the name that identifying this RADIUS.
Access Control Mode	Select Disable if you do not want to use this feature. Select Allow Listed to permit access to the NWA. MAC addresses not listed will be denied access to the NWA. Select Deny Listed 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.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Back	Click **Back** to return to the previous screen.

11

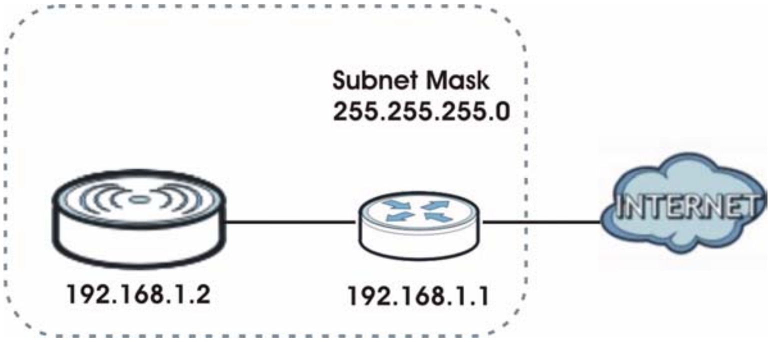
IP Screen

11.1 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 50 IP Setup



The figure above illustrates one possible setup of your NWA. The gateway IP address is 192.168.1.2 and the IP 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.

11.2 What You Can Do in this Chapter

Use the **IP** screen to configure the IP address of your NWA (see Section 11.4 on page 106).

11.3 What You Need to Know

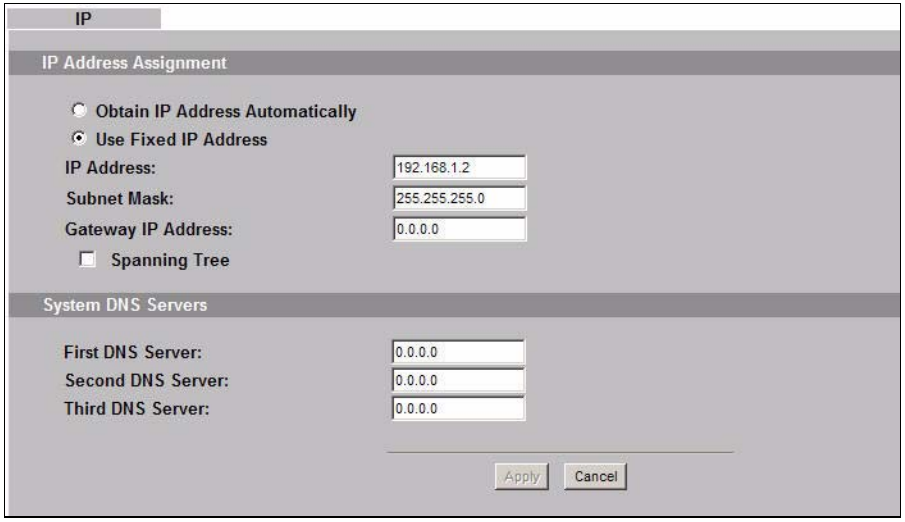
The Ethernet parameters of the NWA are preset in the factory with the following values:

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

11.4 IP Screen

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

Figure 51 IP Setup



IP

IP 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: 0.0.0.0
□ Spanning Tree

System DNS Servers

First DNS Server: 0.0.0.0
Second DNS Server: 0.0.0.0
Third DNS Server: 0.0.0.0

The following table describes the labels in this screen.

Table 33 IP Setup

LABEL	DESCRIPTION
Obtain IP Address Automatically	Select this option if your NWA is using a dynamically assigned IP 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 IP 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 IP 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.
Spanning Tree	(R)STP (Section 11.5.2 on page 107) detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the NWA.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 Technical Reference

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

11.5.1 WAN IP Address Assignment

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

Table 34 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

11.5.2 Spanning Tree Protocol (STP)

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

11.5.2.1 Rapid STP

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

11.5.2.2 STP Terminology

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

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

Table 35 STP Path Costs

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

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

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

11.5.2.3 How STP Works

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

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

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

11.5.2.4 STP Port States

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

Table 36 STP Port States

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

12

Remote Management

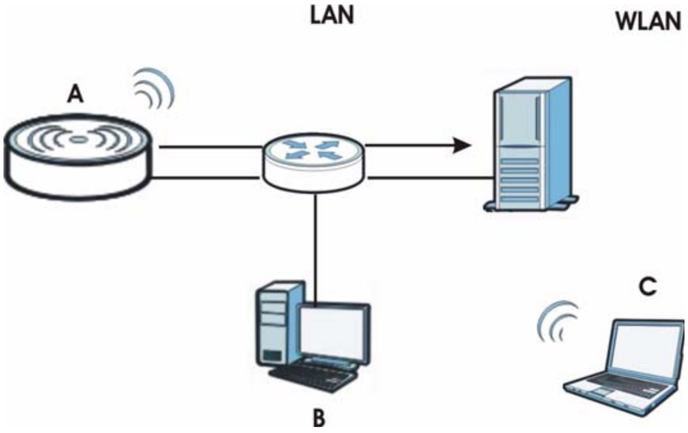
12.1 Overview

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 52 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).

12.2 What You Can Do in this Chapter

- 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 12.4 on page 112).
- 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 12.5 on page 112).

- 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 12.6 on page 113).
- 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 12.7 on page 115).

12.3 What You Need To Know

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.

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).

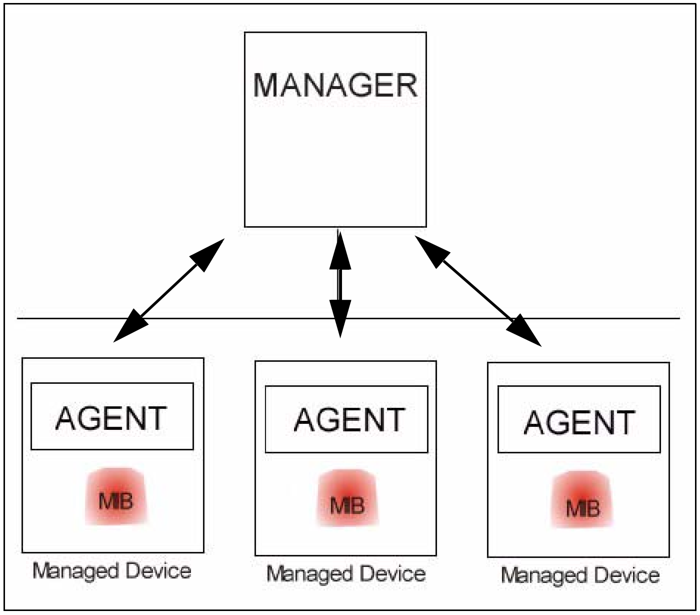
SNMP

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) and version two (SNMPv2c). The next figure illustrates an SNMP management operation. .

Note: SNMP is only available if TCP/IP is configured.

Figure 53 SNMP Management Mode



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

An agent is a management software module that resides in a managed device (the 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.

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** 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

System Timeout

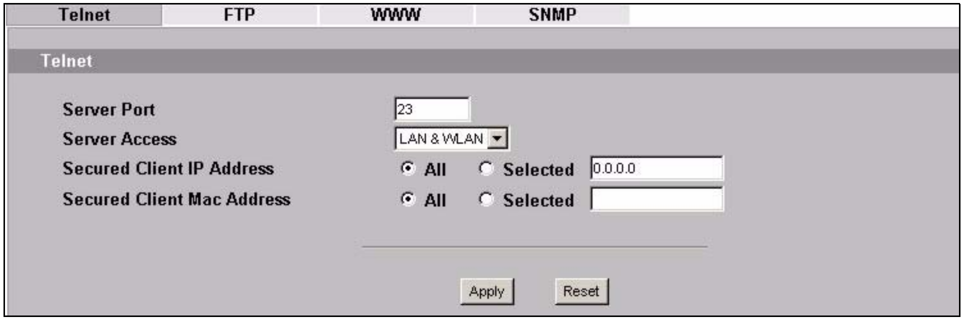
There is a default system management idle timeout of five minutes (three hundred seconds). The NWA automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout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

12.4 The 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 **REMOTE MGNT** > **TELNET**. The following screen displays.

Figure 54 Remote Management: Telnet



Server Port: 23

Server Access: LAN & WLAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Secured Client Mac Address: ● All ○ Selected

The following table describes the labels in this screen.

Table 37 Remote Management: Telnet

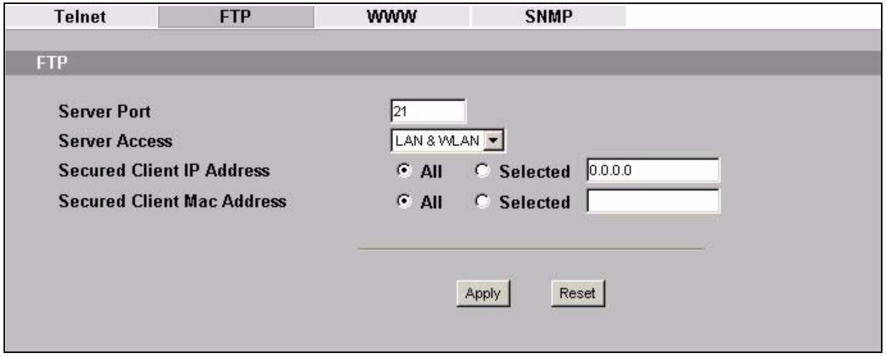
LABEL	DESCRIPTION
TELNET	
Server Port	You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NWA using Telnet.
Secured Client 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 and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

12.5 The 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 **REMOTE MGMT** > **FTP**. The following screen displays.

Figure 55 Remote Management: FTP



Server Port: 21

Server Access: LAN & WLAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Secured Client Mac Address: ● All ○ Selected

The following table describes the labels in this screen.

Table 38 Remote Management: FTP

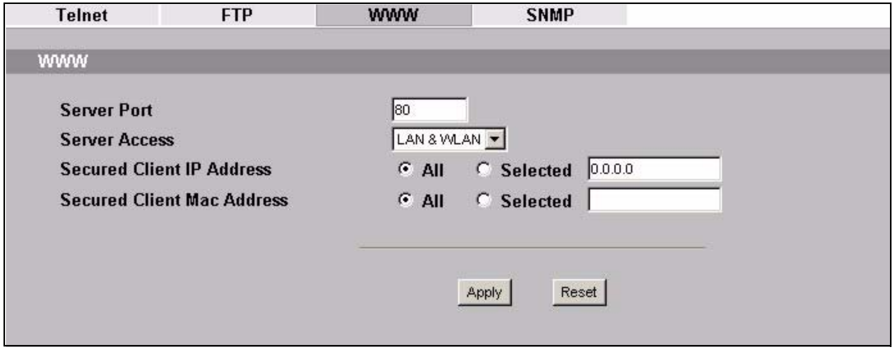
LABEL	DESCRIPTION
FTP	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NWA using this service.
Secured 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 and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

12.6 The 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 **REMOTE MGNT** > **WWW**. The following screen shows.

Figure 56 Remote Management: WWW



Server Port: 80

Server Access: LAN & WLAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Secured Client Mac Address: ● All ○ Selected

The following table describes the labels in this screen.

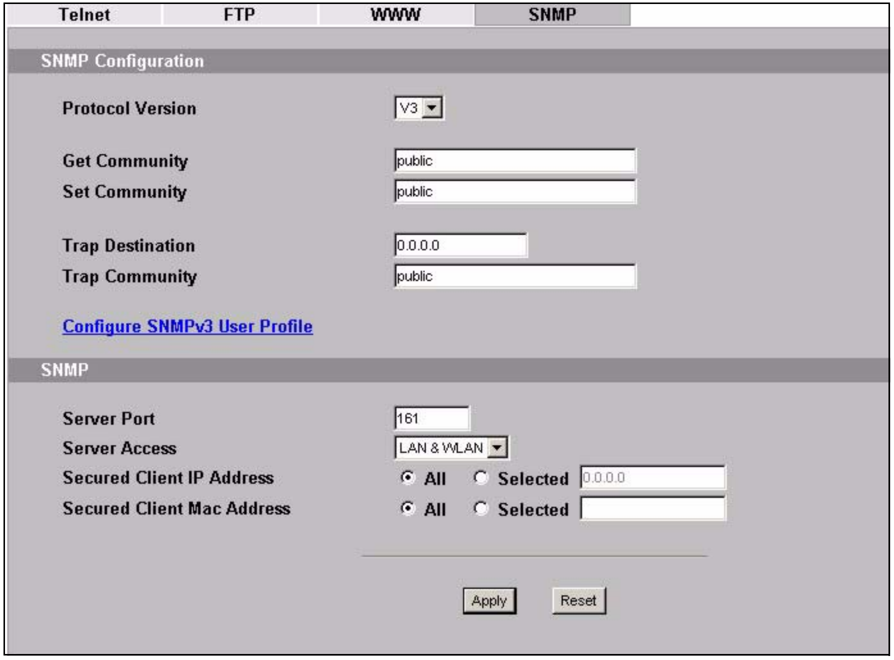
Table 39 Remote Management: WWW

LABEL	DESCRIPTION
WWW	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NWA 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 NWA using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

12.7 The SNMP Screen

Use this screen to have a manager station administrate your NWA over the network. To change your NWA's SNMP settings, click **REMOTE MGMT** > **SNMP**. The following screen displays.

Figure 57 Remote Management: SNMP



SNMP Configuration

Protocol Version: V3

Get Community: public

Set Community: public

Trap Destination: 0.0.0.0

Trap Community: public

Configure SNMPv3 User Profile

SNMP

Server Port: 161

Server Access: LAN & WLAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Secured Client Mac Address: ● All ○ Selected

The following table describes the labels in this screen.

Table 40 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
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 Destination	Type the IP address of the station to send your SNMP traps to.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. This field is available only when **SNMPv1** or **SNMPv2** is selected in the **SNMP Version** field.
Configure SNMPv3 User Profile	Click this to go to the **SNMPv3 User Profile** screen, where you can configure administration and user login details.
SNMP	
Service 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.
Service Access	Select the interface(s) through which a computer may access the NWA using this service.

Table 40 Remote Management: SNMP (continued)

LABEL	DESCRIPTION
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 and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

12.8 Technical Reference

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

12.8.1 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.

12.8.2 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.

12.8.3 SNMP Traps

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

Table 41 SNMP Traps

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

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

Table 42 SNMP Interface Index to Physical and Virtual Port Mapping

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

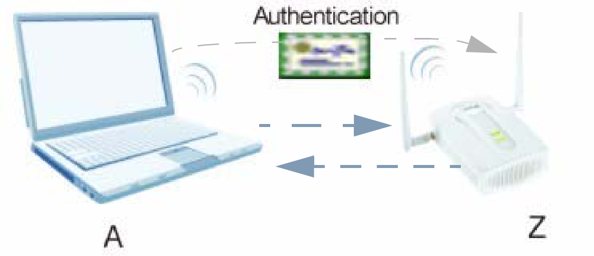
Certificate Screen

13.1 Overview

This chapter describes how your NWA can use certificates as a means of authenticating wireless clients. It gives background information about public-key certificates and explains how to use them.

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

Figure 58 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.

13.2 What You Can Do in this Chapter

Use the **CERTIFICATES > Certificate** screen to view, delete and import certificates (seen Section 13.4 on page 120).

13.3 What You Need To Know

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.

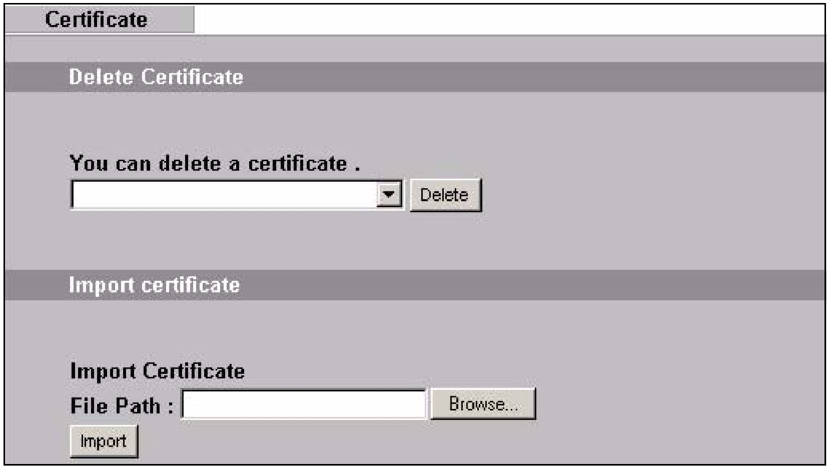
Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

13.4 Certificate Screen

Use this screen to view, delete and import certificates.

Click **CERTIFICATE** to open the NWA's summary list of certificates and to import a new certificate. See the following figure.

Figure 59 Certificate



The following table describes the labels in this screen.

Table 43 Certificate

LABEL	DESCRIPTION
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.
Import Certificate	
File Path	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 **File Path** field to the NWA.

13.5 Technical Reference

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

13.5.1 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.

13.5.2 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.

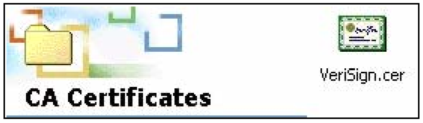
13.5.3 Checking the Fingerprint of a Certificate on Your Computer

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.

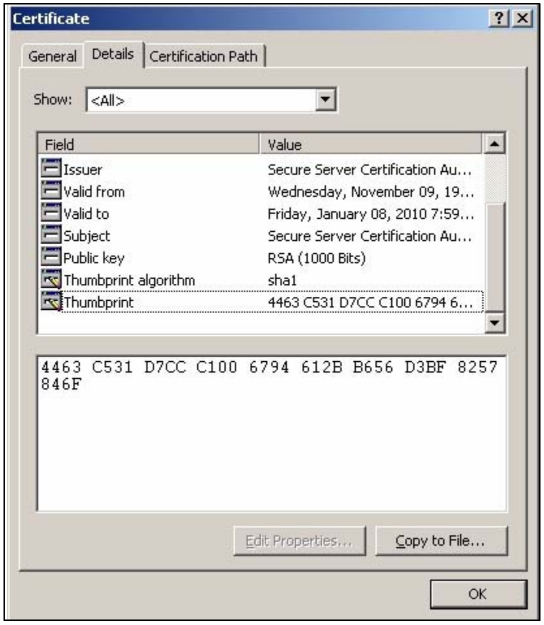
2 Make sure that the certificate has a “.cer” or “.crt” file name extension.

Figure 60 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 61 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.

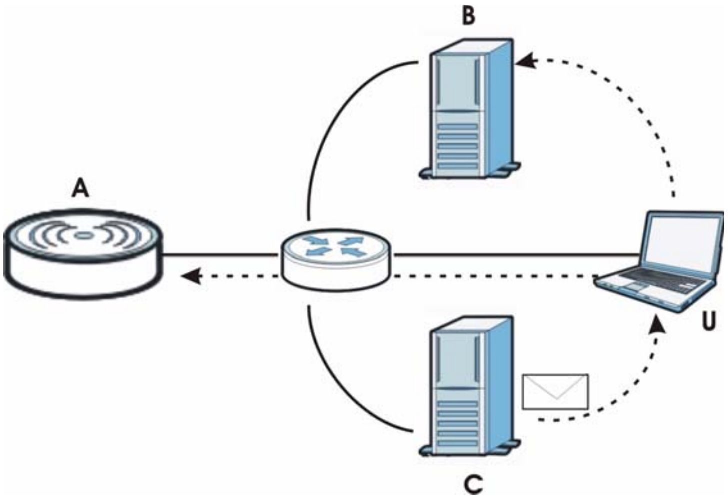
Log Screens

14.1 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 62 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.

14.2 What You Can Do in this Chapter

- Use the **View Log** screen to display all logs or logs for a certain category. You can view logs and alert messages in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted (Section 14.4 on page 124).
- Use the **Log Settings** screen to configure where and when the NWA will send the logs, and which logs and/or immediate alerts it will send (Section 14.5 on page 125).

14.3 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 Errors** consist of both logs and alerts. You can differentiate them by their color in the **View Log** 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).

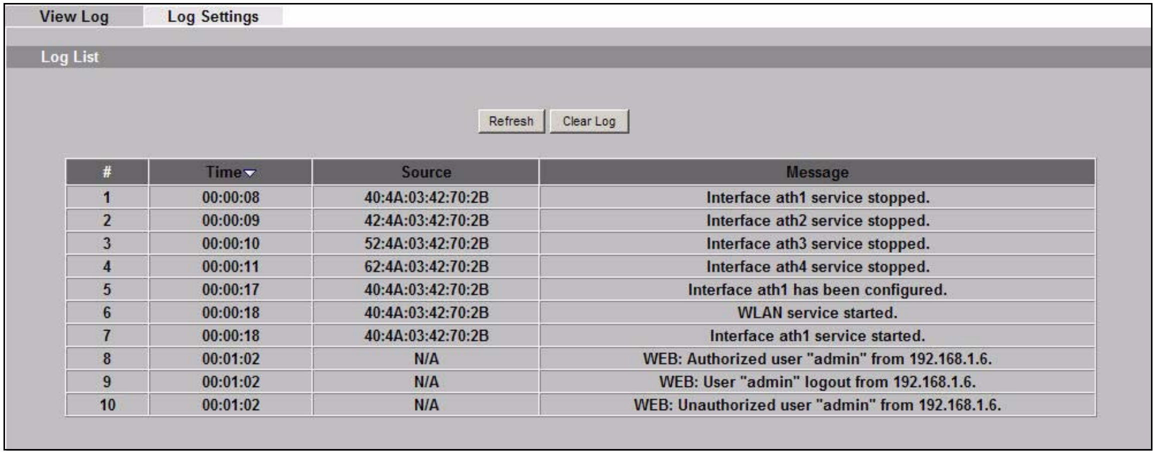
14.4 View Log Screen

Use this screen to view all the NWA’s logs in one location.

Click **Logs > View Log**. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Figure 64 on page 125). Options include logs about system maintenance, system errors and access control.

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

Figure 63 View Log



#	Time▽	Source	Message
1	00:00:08	40:4A:03:42:70:2B	Interface ath1 service stopped.
2	00:00:09	42:4A:03:42:70:2B	Interface ath2 service stopped.
3	00:00:10	52:4A:03:42:70:2B	Interface ath3 service stopped.
4	00:00:11	62:4A:03:42:70:2B	Interface ath4 service stopped.
5	00:00:17	40:4A:03:42:70:2B	Interface ath1 has been configured.
6	00:00:18	40:4A:03:42:70:2B	WLAN service started.
7	00:00:18	40:4A:03:42:70:2B	Interface ath1 service started.
8	00:01:02	N/A	WEB: Authorized user "admin" from 192.168.1.6.
9	00:01:02	N/A	WEB: User "admin" logout from 192.168.1.6.
10	00:01:02	N/A	WEB: Unauthorized user "admin" from 192.168.1.6.

The following table describes the labels in this screen.

Table 44 View Log

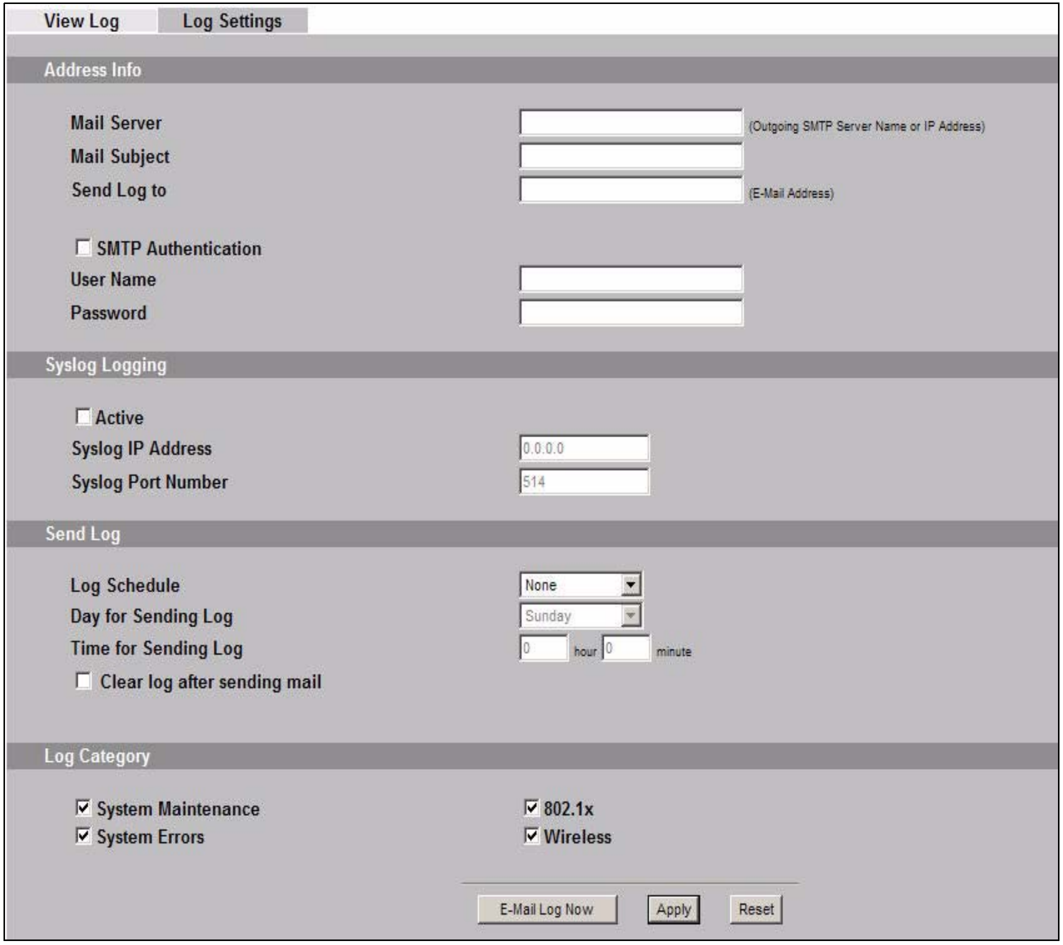
LABEL	DESCRIPTION
Time	This field displays the time the log was recorded.
Source	This field lists the source IP address and the port number of the incoming packet.
Message	This field states the reason for the log.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.

14.5 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 **LOGS** > **Log Settings**. The screen appears as shown.

Figure 64 Log Settings



Address Info

Mail Server (Outgoing SMTP Server Name or IP Address)

Mail Subject

Send Log to (E-Mail Address)

☐ SMTP Authentication

User Name

Password

Syslog Logging

☐ Active

Syslog IP Address 0.0.0.0

Syslog Port Number 514

Send Log

Log Schedule None

Day for Sending Log Sunday

Time for Sending Log 0 hour 0 minute

☐ Clear log after sending mail

Log Category

☑ System Maintenance

☑ System Errors

☑ 802.1x

☑ Wireless

The following table describes the labels in this screen.

Table 45 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the 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.
SMTP Authentication	If you use SMTP authentication, the mail receiver should be the owner of the SMTP account.
User Name	If your e-mail account requires SMTP authentication, enter the username here.
Password	Enter the password associated with the above username.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog 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: • Daily • Weekly • Hourly • When Log is Full • None. If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	
System Maintenance	Click this to receive logs related to system maintenance.
System Errors	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.

Table 45 Log Settings (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to reconfigure all the fields in this screen.

15

Maintenance

15.1 Overview

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

15.2 What You Can Do in this Chapter

- Use the **Association List** screen to view the wireless stations that are currently associated with the NWA (see Section 15.4 on page 129) .
- 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 15.5 on page 130).
- Use the **F/W Upload** screen to upload the latest firmware for your NWA (see Section 15.6 on page 131).
- Use the **Configuration File** screen to view information related to factory defaults, backup configuration, and restoring configuration (see Section 15.7 on page 133).
- Use **Restart** screen to reboot the NWA without turning the power off (see Section 15.8 on page 135).

15.3 What You Need To Know

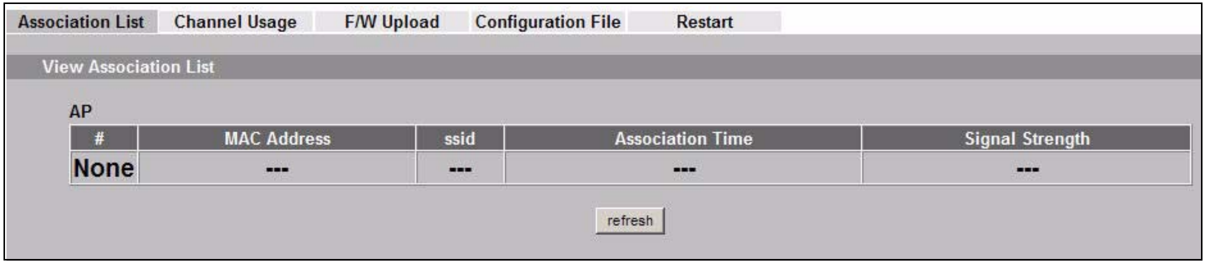
You can find the firmware for your device at www.zyxel.com. It is a file that (usually) uses the system model name with a "*.bin" extension, for example "[Model #].bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will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

15.4 Association List Screen

Use this screen to view the wireless stations that are currently associated with the NWA.

Click **Maintenance** > **Association List**. The following screen displays.

Figure 65 Association List



#	MAC Address	ssid	Association Time	Signal Strength
None	---	---	---	---

The following table describes the labels in this screen.

Table 46 Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
ssid	This field displays the SSID to which the wireless station is associated.
Association Time	This field displays the time a wireless station first associated with the NWA.
Signal Strength	This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection.
Refresh	Click **Refresh** to reload the screen.

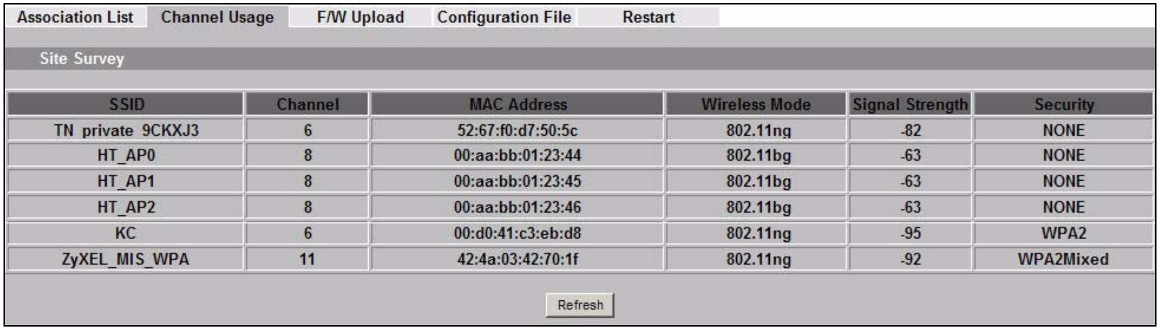
15.5 Channel Usage Screen

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 **Maintenance** > **Channel Usage** to display the screen shown next.

Wait a moment while the NWA compiles the information.

Figure 66 Channel Usage



SSID	Channel	MAC Address	Wireless Mode	Signal Strength	Security
TN private 9CKXJ3	6	52:67:f0:d7:50:5c	802.11ng	-82	NONE
HT_AP0	8	00:aa:bb:01:23:44	802.11bg	-63	NONE
HT_AP1	8	00:aa:bb:01:23:45	802.11bg	-63	NONE
HT_AP2	8	00:aa:bb:01:23:46	802.11bg	-63	NONE
KC	6	00:d0:41:c3:eb:d8	802.11ng	-95	WPA2
ZyXEL_MIS_WPA	11	42:4a:03:42:70:1f	802.11ng	-92	WPA2Mixed

The following table describes the labels in this screen.

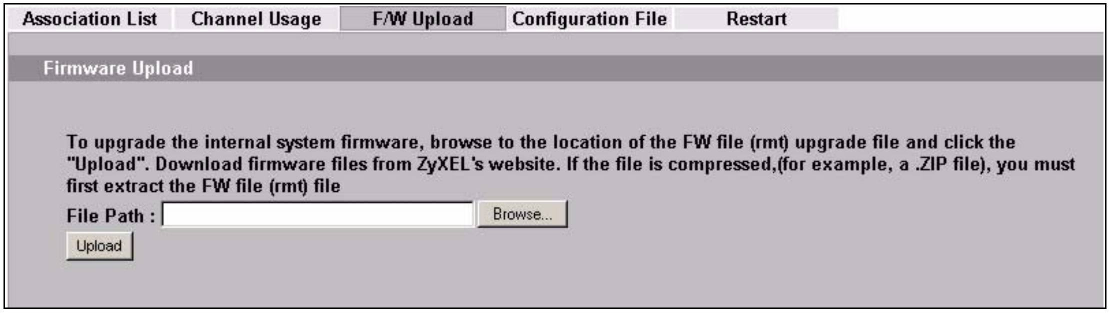
Table 47 Channel Usage

LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the chapter on wireless configuration for more information on basic service sets (BSS) and extended service sets (ESS).
MAC Address	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Wireless Mode	This is the IEEE 802.1x standard used by your NWA to apply enhanced security methods for both the authentication of wireless stations and encryption key management.
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 your NWA protect wireless communication between wireless stations, access points and the wired network.
Refresh	Click **Refresh** to reload the screen.

15.6 F/W Upload Screen

Use this screen to upload a firmware to your NWA. Click **Maintenance** > **F/W Upload**. Follow the instructions in this section to upload firmware to your NWA.

Figure 67 Firmware Upload



To upgrade the internal system firmware, browse to the location of the FW file (rmt) upgrade file and click the "Upload". Download firmware files from ZyXEL's website. If the file is compressed,(for example, a .ZIP file), you must first extract the FW file (rmt) file

File Path :

The following table describes the labels in this screen.

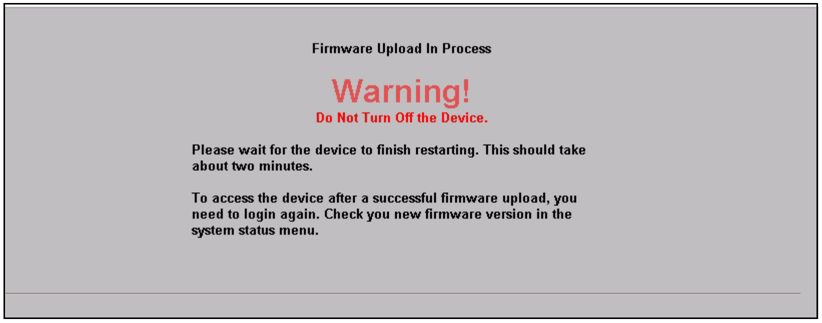
Table 48 Firmware Upload

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

Do not turn off the NWA while firmware upload is in progress!

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

Figure 68 Firmware Upload In Process



Firmware Upload In Process

Warning!

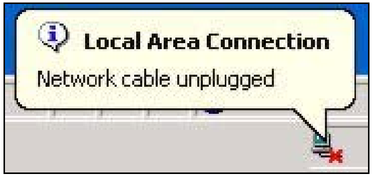
Do Not Turn Off the Device.

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

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

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 69 Network Temporarily Disconnected



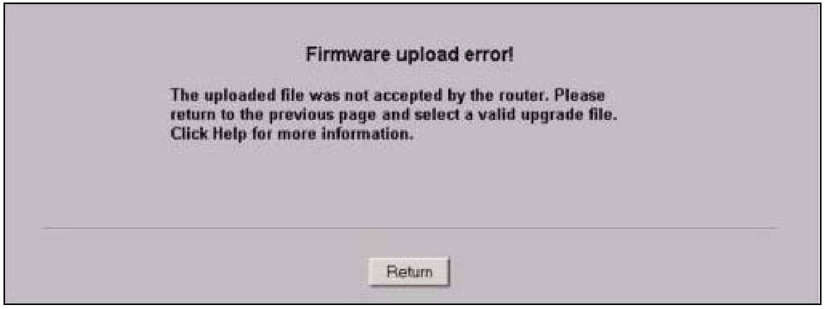
Local Area Connection

Network cable unplugged

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

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

Figure 70 Firmware Upload Error



Firmware upload error!

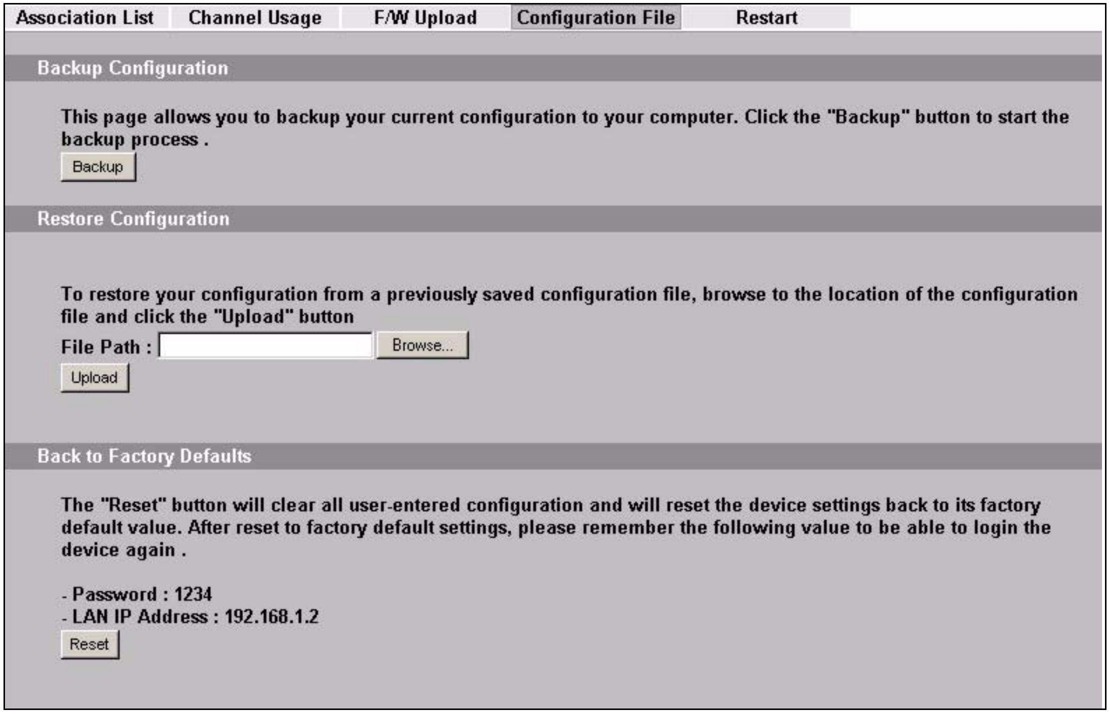
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

15.7 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 71 Configuration File



Backup Configuration

This page allows you to backup your current configuration to your computer. Click the "Backup" button to start the backup process .

Restore Configuration

To restore your configuration from a previously saved configuration file, browse to the location of the configuration file and click the "Upload" button

File Path :

Back to Factory Defaults

The "Reset" button will clear all user-entered configuration and will reset the device settings back to its factory default value. After reset to factory default settings, please remember the following value to be able to login the device again .

- Password : 1234
- LAN IP Address : 192.168.1.2

15.7.1 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.

15.7.2 Restore Configuration

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

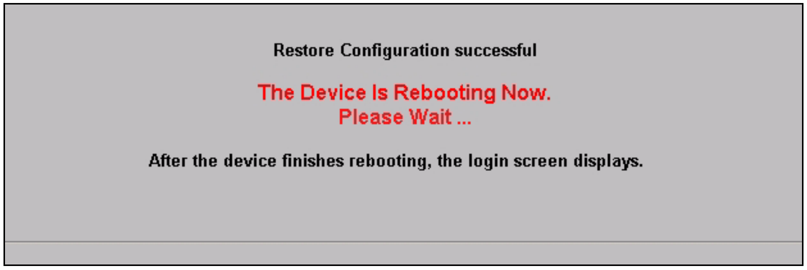
Table 49 Restore Configuration

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.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the NWA again.

Figure 72 Configuration Upload Successful



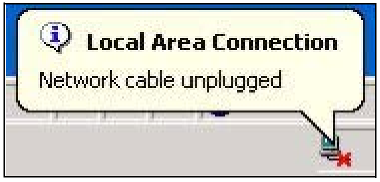
Restore Configuration successful

The Device Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

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 73 Network Temporarily Disconnected

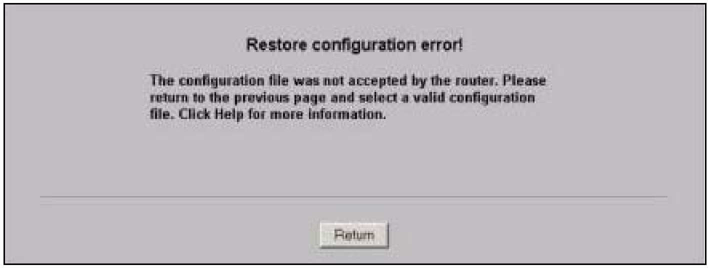


Local Area Connection
Network cable unplugged

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 your Quick Start Guide for details on how to set up your computer’s IP address.

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

Figure 74 Configuration Upload Error



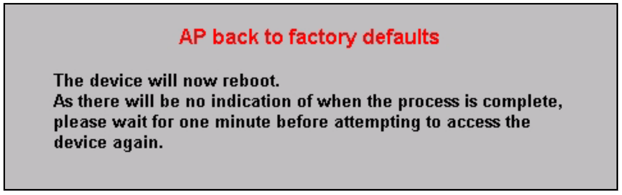
Restore configuration error!

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

15.7.3 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 warning screen will appear.

Figure 75 Reset Warning Message



AP back to factory defaults

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

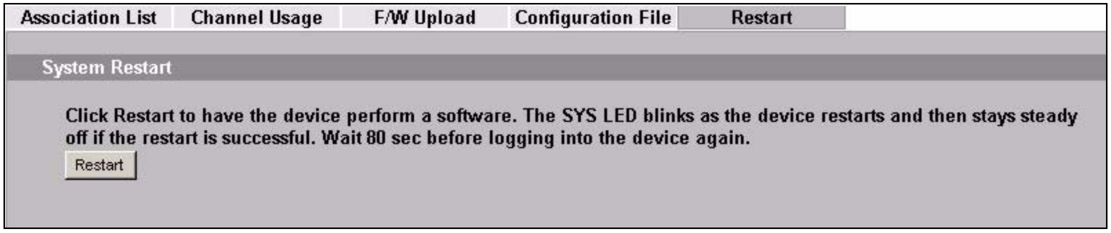
You can also press the **RESET** button to reset your NWA to its factory default settings. Refer to Section 2.2 on page 30 for more information.

15.8 Restart Screen

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

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

Figure 76 Restart Screen



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.

16

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

16.1 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 27.
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.

16.2 NWA Access and Login

I forgot the IP address for the NWA.

1. The default IP address is **192.168.1.2**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the NWA by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter “**cmd**”, and then enter “**ipconfig**”. The IP address of the **Default Gateway** might be the IP address of the NWA (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 30.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 30.

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 11.4 on page 106), 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 27.
3. Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Section 16.1 on page 137.
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 your Quick Start Guide.

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 to the **WAN** port or 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 password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using the Telnet to access the NWA. Log out of the NWA in the other session, or ask the person who is logged in to log out.

3 Disconnect and re-connect the power adaptor or cord to the NWA.

4 If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 30.

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.

16.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 16.1 on page 137.

2 2. Make sure your NWA is connected to a networking device that provides Internet access.

3 If you are trying to access the Internet wirelessly, make sure the wireless settings on the wireless client are the same as the settings on the AP.

4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the 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 27.
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 27. 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.

Product Specifications

The following tables summarize the NWA’s hardware and firmware features.

Table 50 Hardware Specifications

Power Specification	12 V DC, 1.5 A
Reset button	Returns all settings to their factory defaults.
Ethernet Port	• Auto-negotiating: 10/100/1000 Mbps in either half-duplex or full-duplex mode. • Auto-crossover: Use either crossover or straight-through Ethernet cables.
Power over Ethernet (PoE)	IEEE 802.3af compliant.
Antenna	SMA antenna connectors, equipped by default with 3dBi omni antenna, 60°
Operation Temperature	0 ~ 50 º C
Storage Temperature	-30 ~ 60 º C
Operation Humidity	20 ~ 95 % (non-condensing)
Storage Humidity	10 ~ 90 % (non-condensing)
Dimensions	152mm x 92mm x 45mm

Table 51 Firmware Specifications

Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Wireless LAN Standards	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Wireless security	WEP, WPA(2), WPA(2)-PSK, 802.1x
Multiple BSSID (MBSSID)	MBSSID mode allows the NWA to operate up to 4 different wireless networks (BSSs) simultaneously, each with independently-configurable wireless and security settings.
STP (Spanning Tree Protocol) / RSTP (Rapid STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network.
WMM QoS	allows you to prioritize wireless traffic.
Certificates	The NWA can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

Table 51 Firmware Specifications (continued)

SSL Passthrough	SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https” instead of “http”. The NWA allows SSL connections to take place through the NWA.
MAC Address Filter	Your NWA checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.
Wireless Association List	With the wireless association list, you can see the list of the wireless stations that are currently using the NWA to access your wired network.
Logging and Tracing	Built-in message logging and packet tracing.
Embedded FTP and TFTP Servers	The embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.
Auto Configuration	Administrators can use text configuration files to configure the wireless LAN settings for multiple APs. The AP can automatically get a configuration file from a TFTP server at start up or after renewing DHCP client information.
SNMP	SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your NWA supports SNMP agent functionality, which allows a manger station to manage and monitor the NWA through the network. The NWA supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

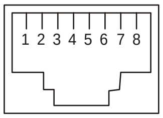
Power over Ethernet (PoE) Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.-7

Table 52 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Table 53 Power over Ethernet Injector RJ-45 Port Pin Assignments

	**PIN NO**	**RJ-45 SIGNAL ASSIGNMENT**
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

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.

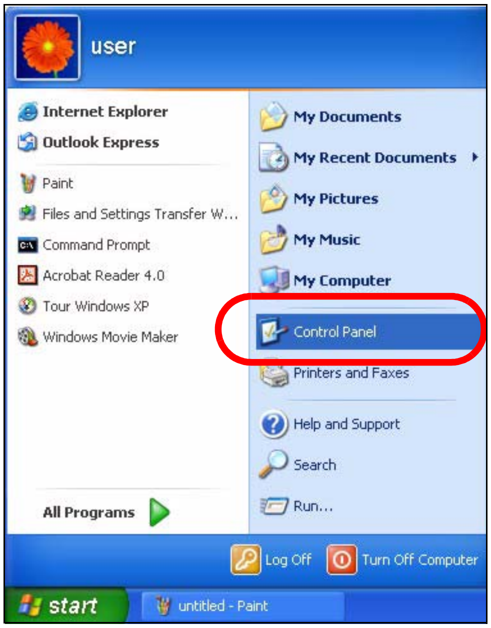
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 143
- Windows Vista on page 147
- Windows 7 on page 151
- Mac OS X: 10.3 and 10.4 on page 155
- Mac OS X: 10.5 and 10.6 on page 158
- Linux: Ubuntu 8 (GNOME) on page 161
- Linux: openSUSE 10.3 (KDE) on page 165

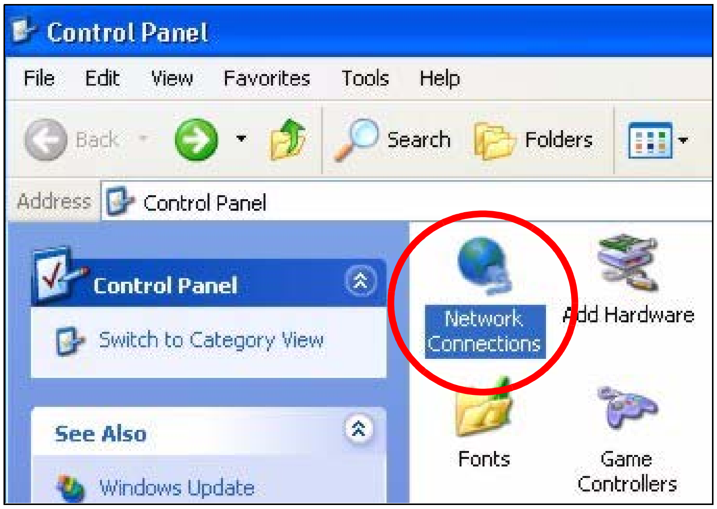
Windows XP/NT/2000

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

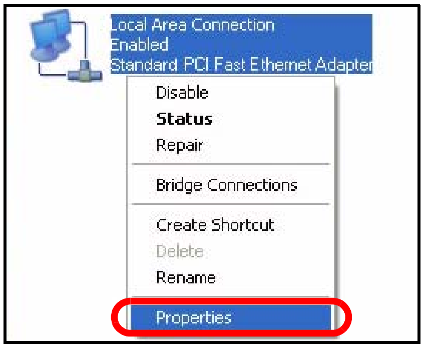
1 Click **Start** > **Control Panel**.



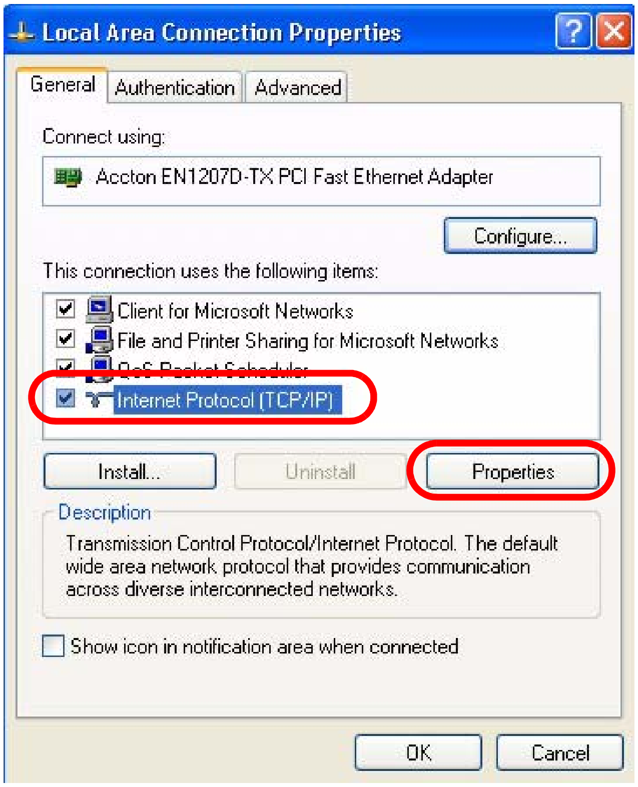
2 In the **Control Panel**, click the **Network Connections** icon.



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



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



Local Area Connection Properties

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

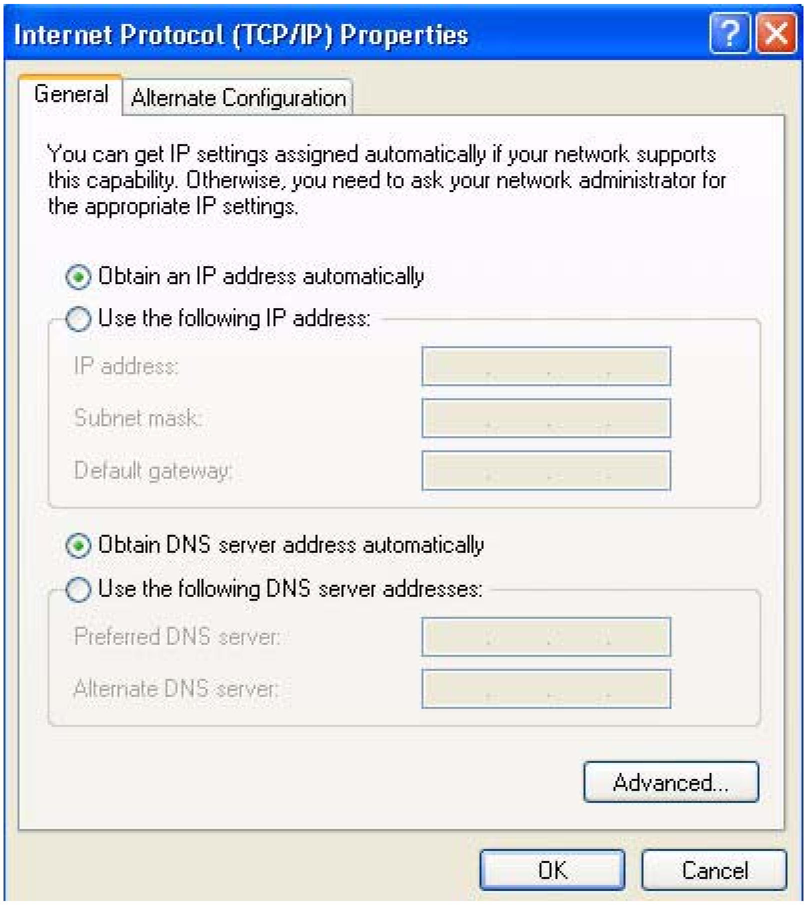
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

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:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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**.

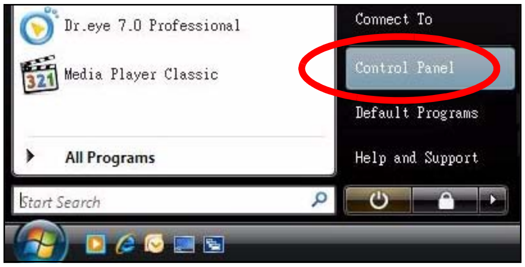
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

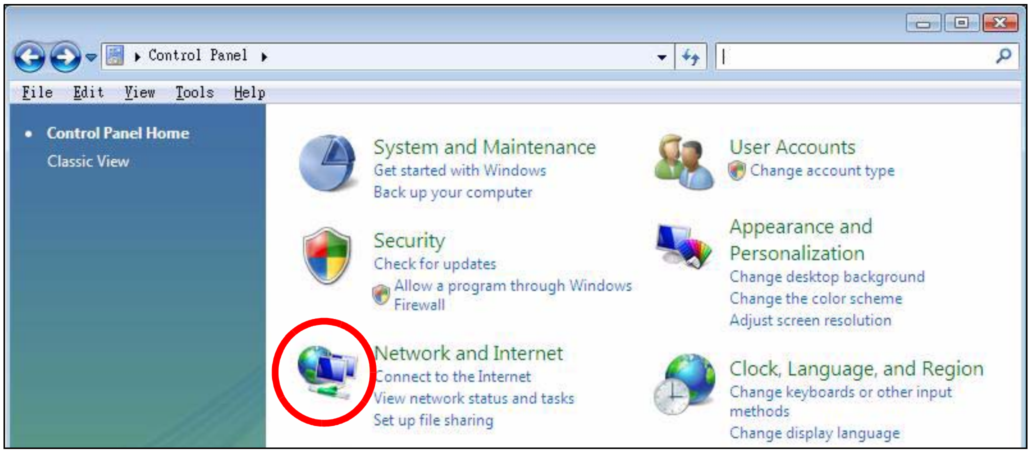
Windows Vista

This section shows screens from Windows Vista Professional.

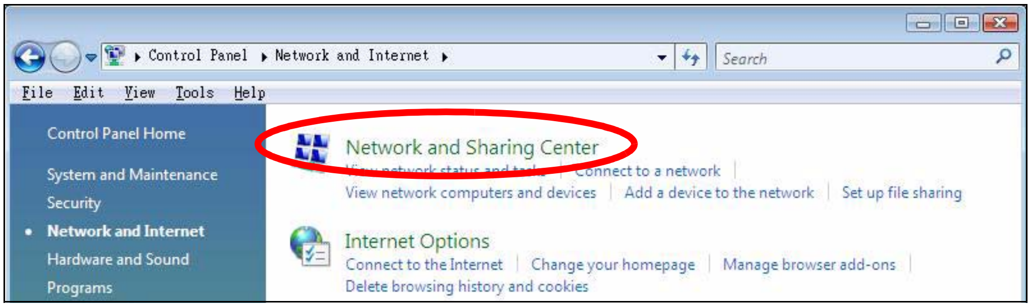
1 Click **Start** > **Control Panel**.



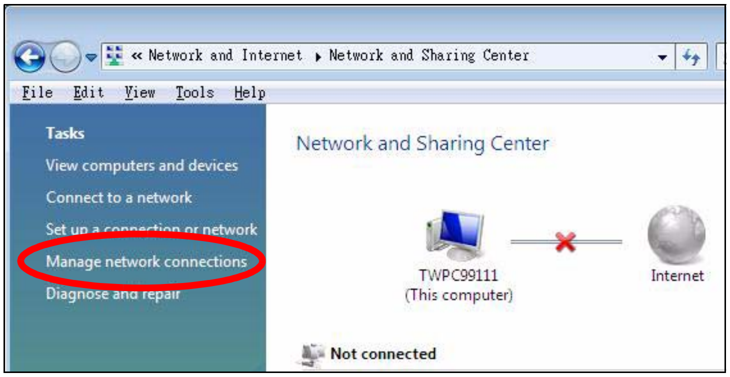
2 In the **Control Panel**, click the **Network and Internet** icon.



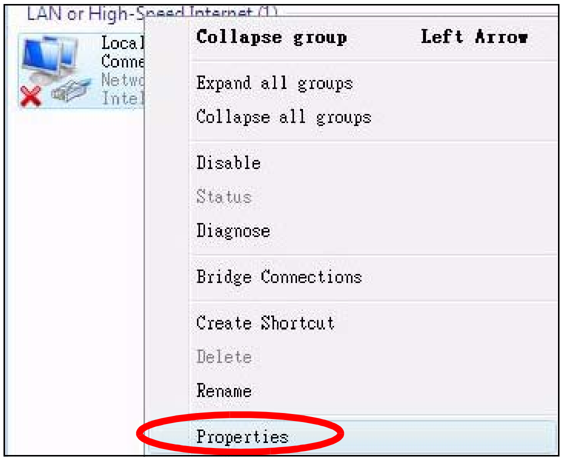
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

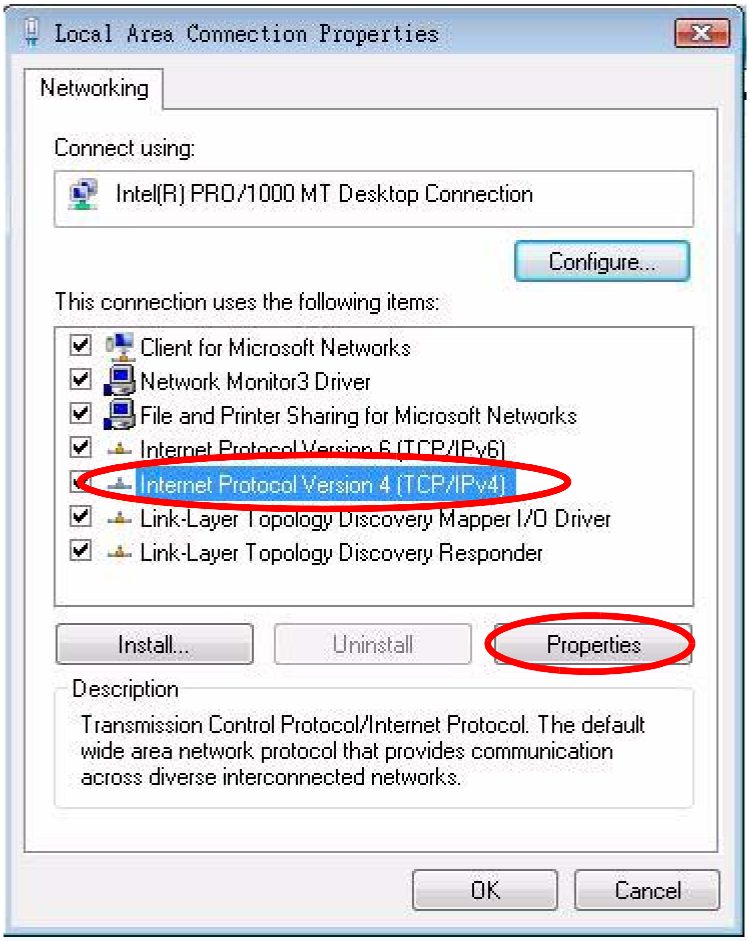

« Network and Internet ▸ Network and Sharing Center
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
TWPC99111
(This computer)
Internet
Not connected

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**.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Connection

Configure...

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

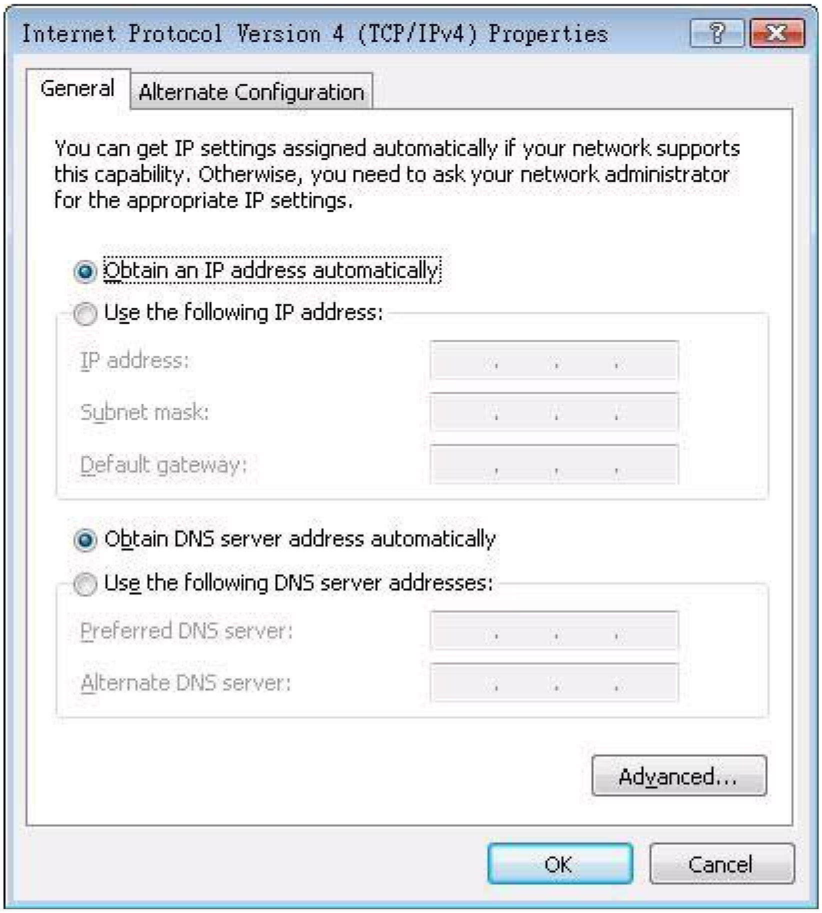
Install... Uninstall Properties

Description

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

OK Cancel

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**.

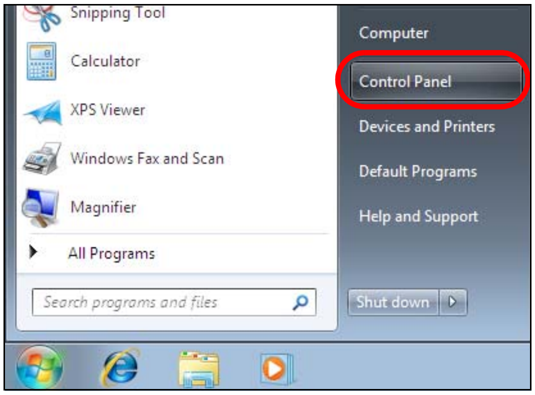
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

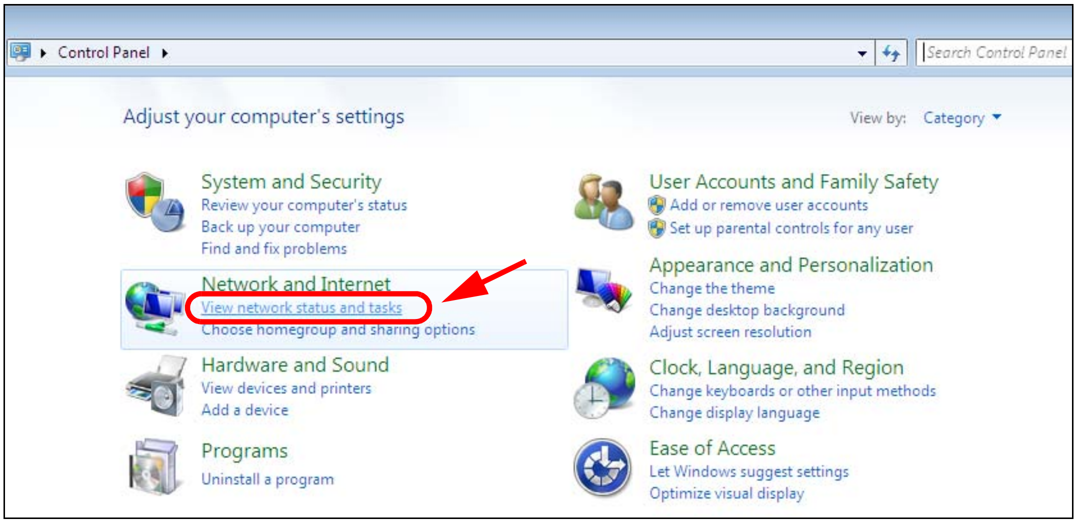
Windows 7

This section shows screens from Windows 7 Enterprise.

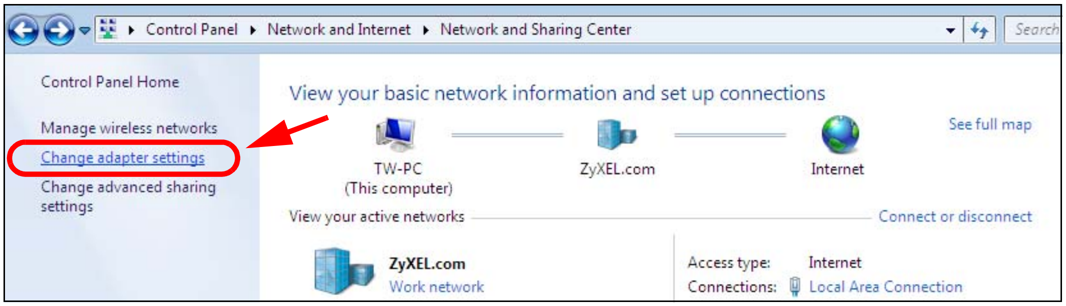
1 Click **Start** > **Control Panel**.



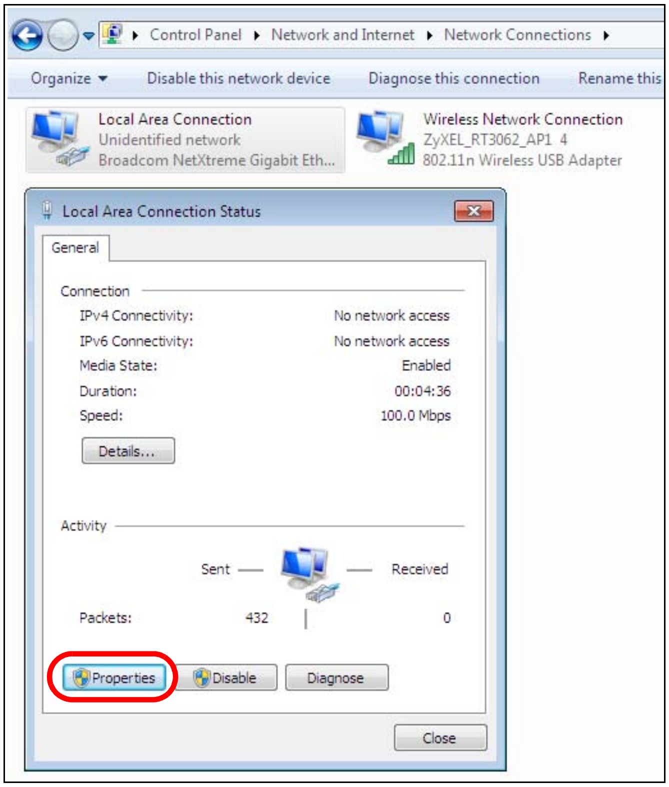
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.


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**.



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

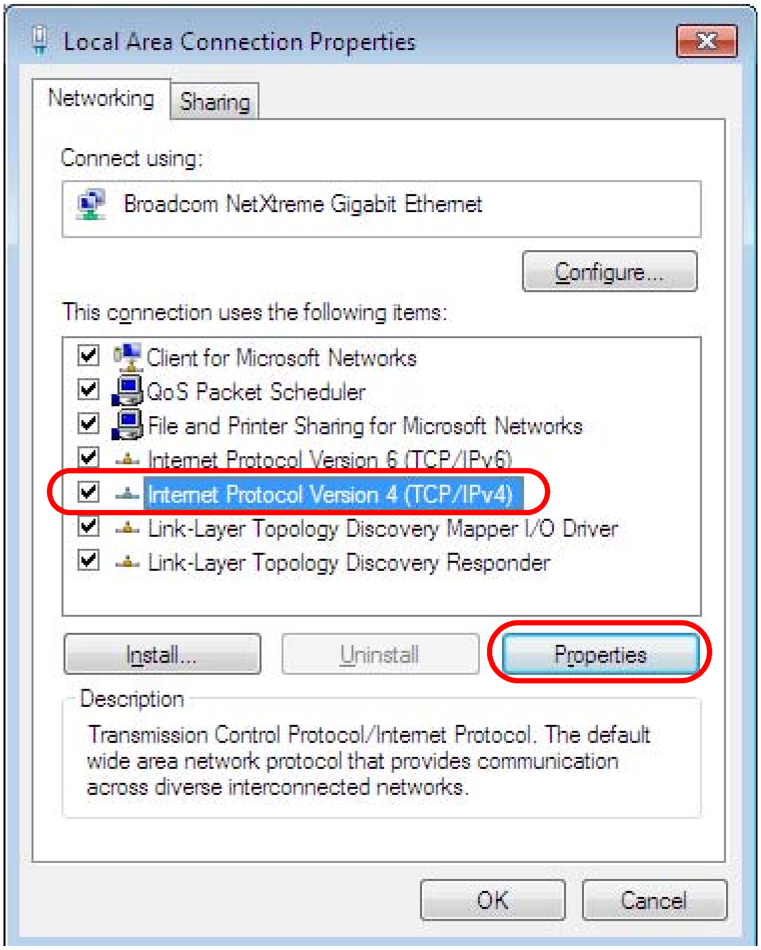
Activity

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**.



Connect using:

Broadcom NetXtreme Gigabit Ethernet

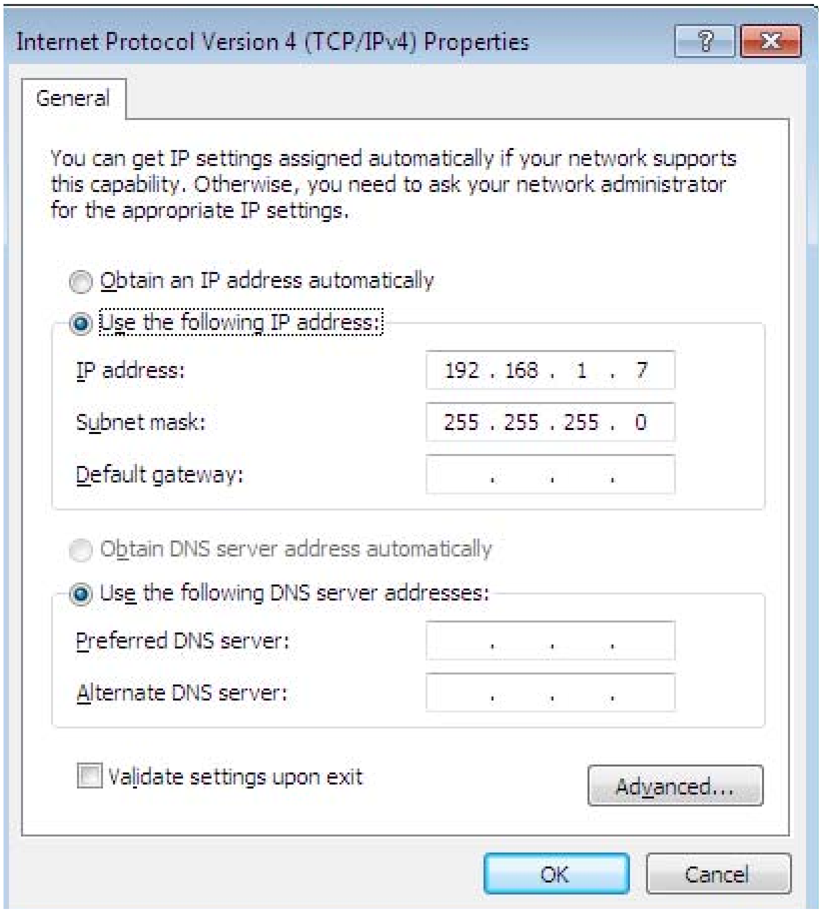
This connection uses the following items:

- ☑ 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)
- ☑ 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.

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.

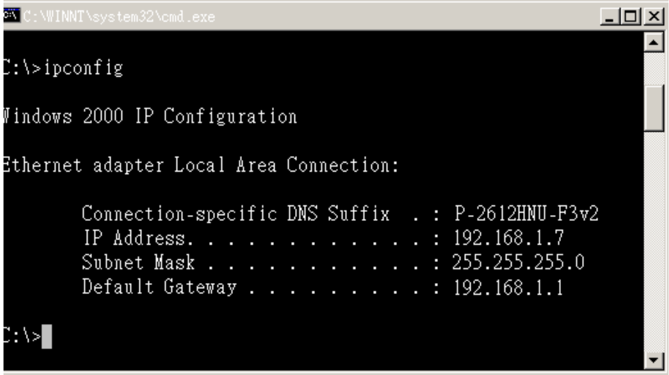
9 Click **OK** to close the **Local Area Connection Properties** window.

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.

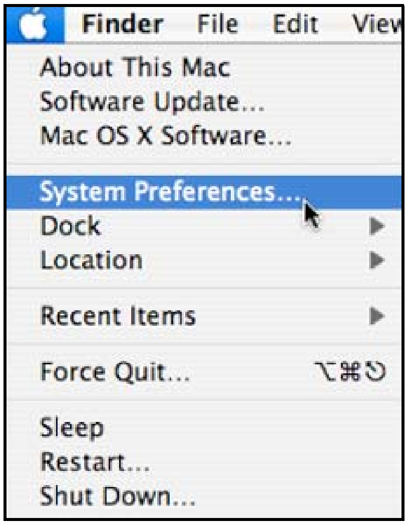


```
C:\>ipconfig

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:\>
```

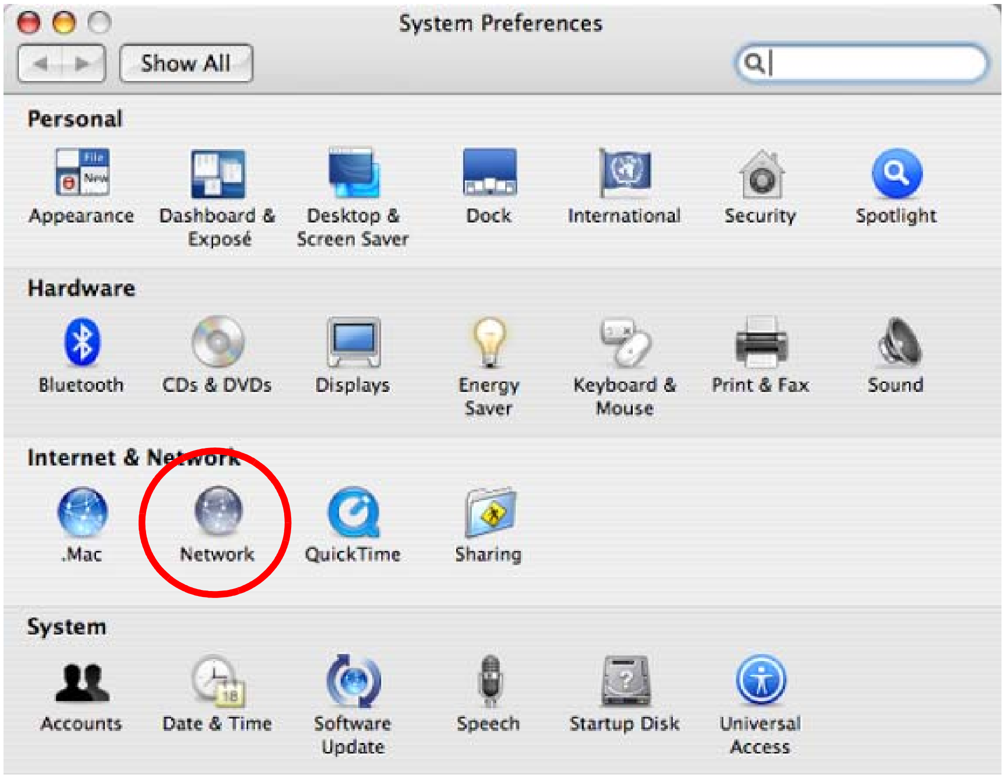
Mac OS X: 10.3 and 10.4

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

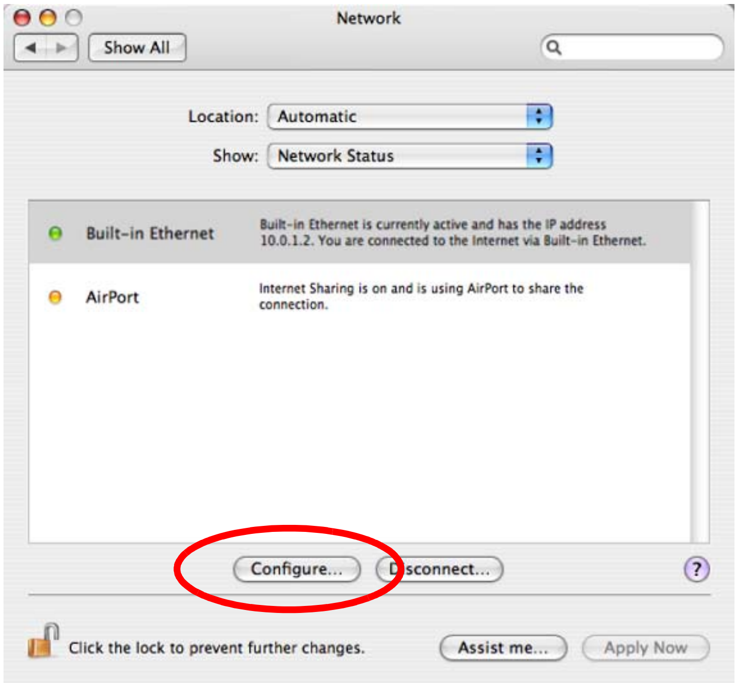
1 Click **Apple** > **System Preferences**.



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.**



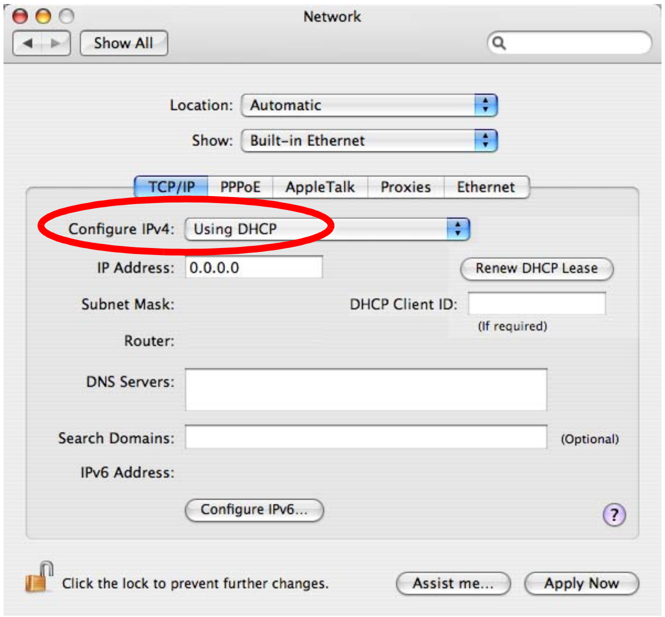
Location: Automatic

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.



Network

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:

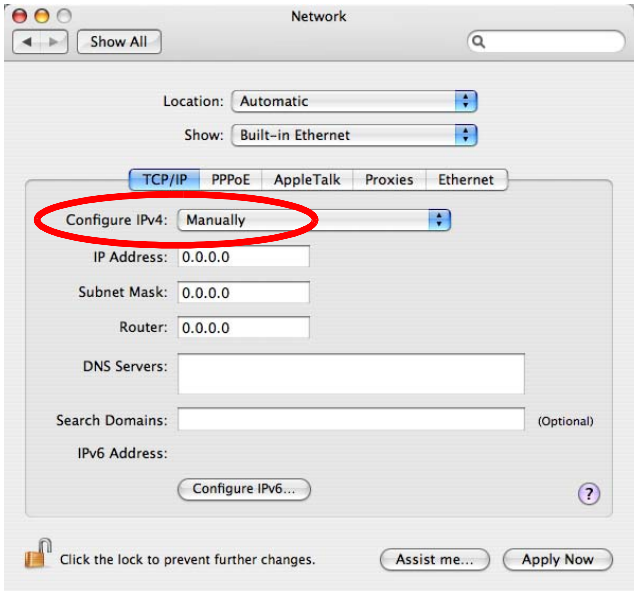
Search Domains: (Optional)

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.



Network

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:

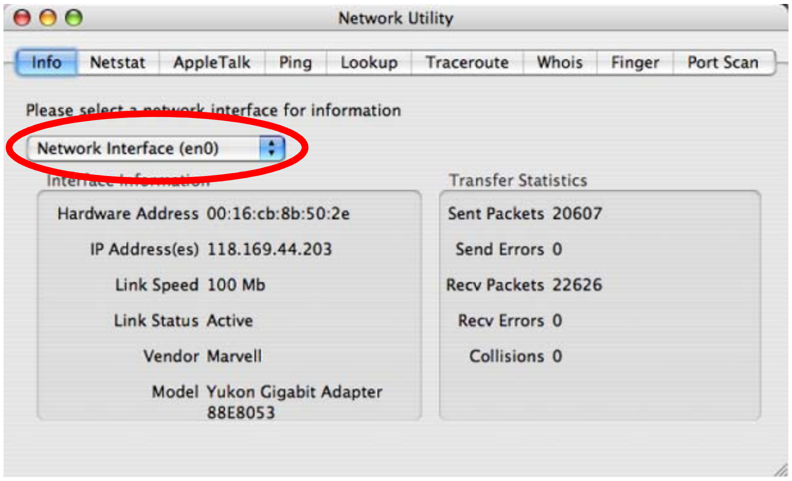
Click the lock to prevent further changes.

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 77 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

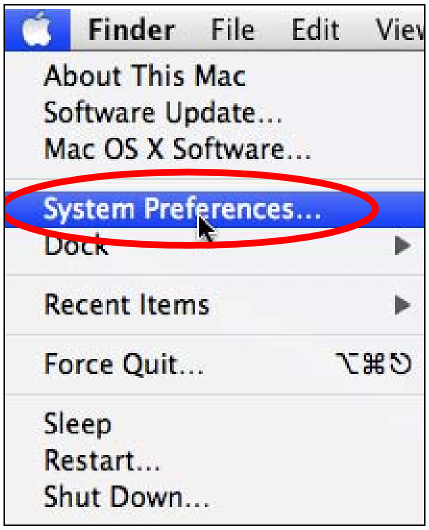
Recv Errors 0

Collisions 0

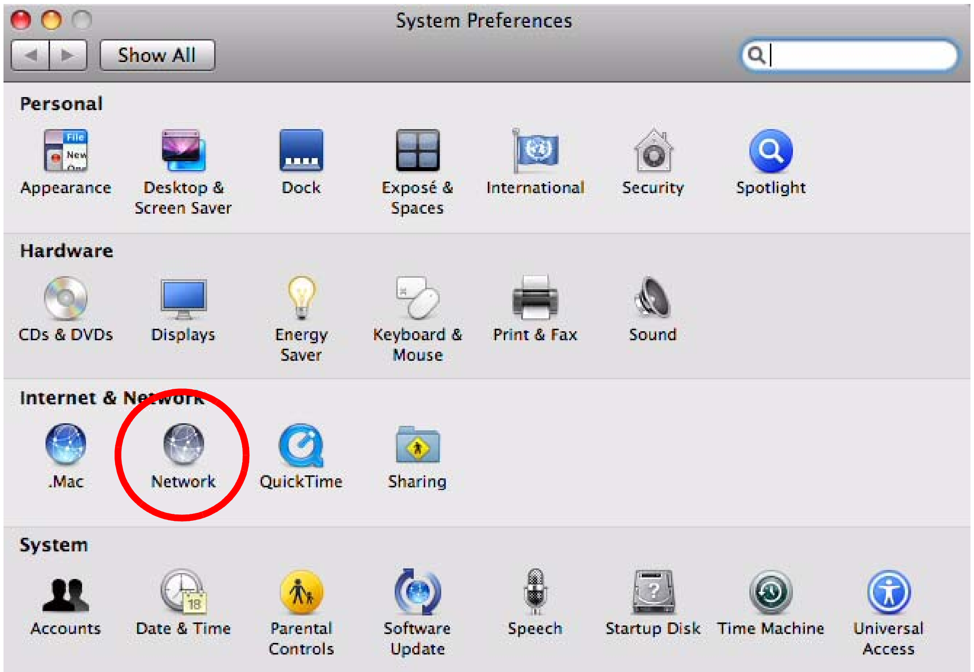
Mac OS X: 10.5 and 10.6

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

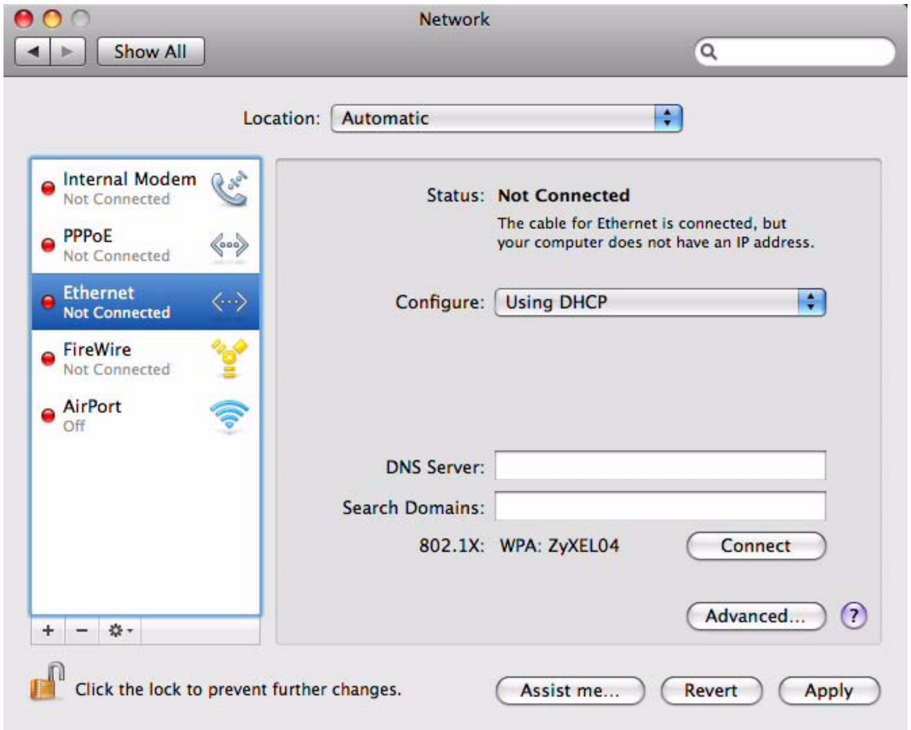
1 Click **Apple** > **System Preferences**.



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:

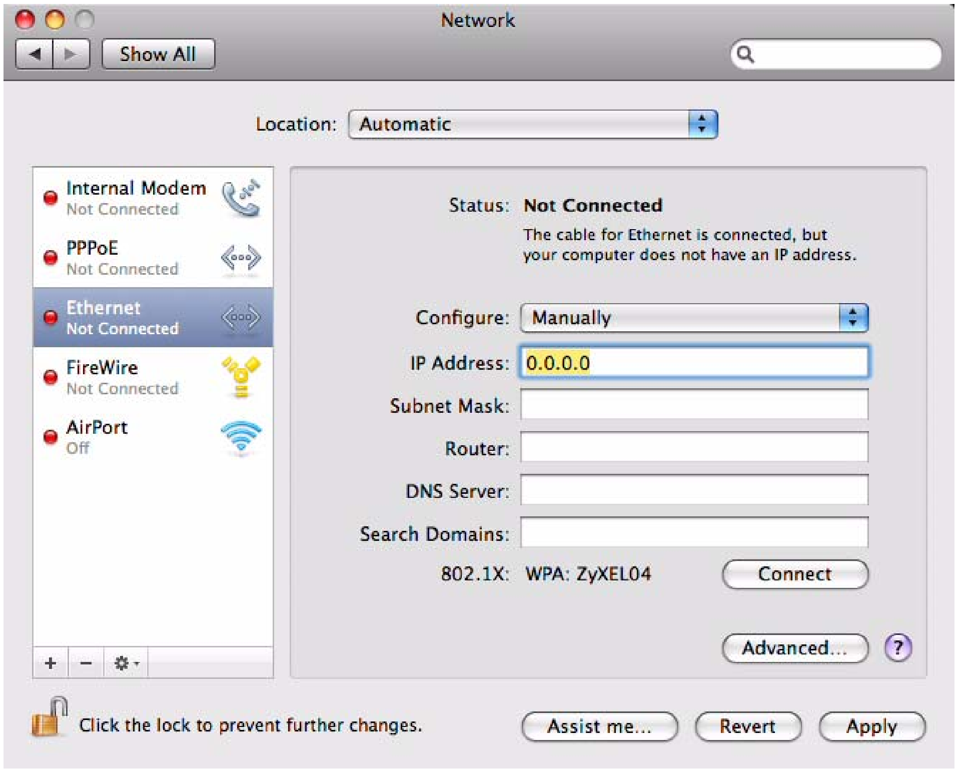
Search Domains:

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

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

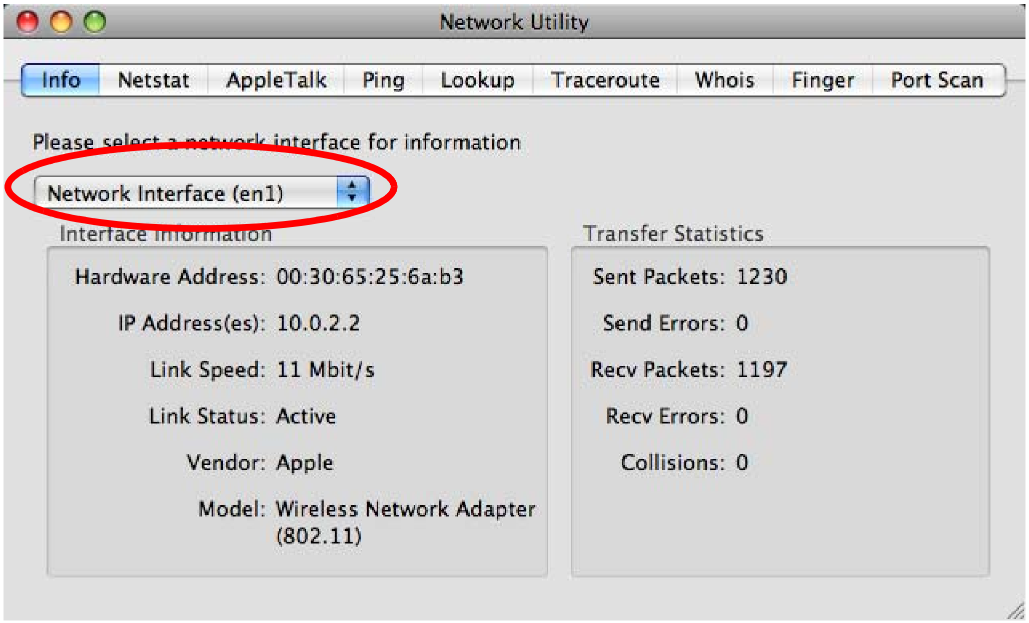
802.1X: WPA: ZyXEL04

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 78 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

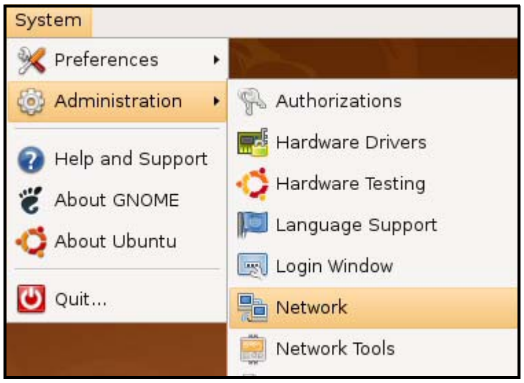
Linux: Ubuntu 8 (GNOME)

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.

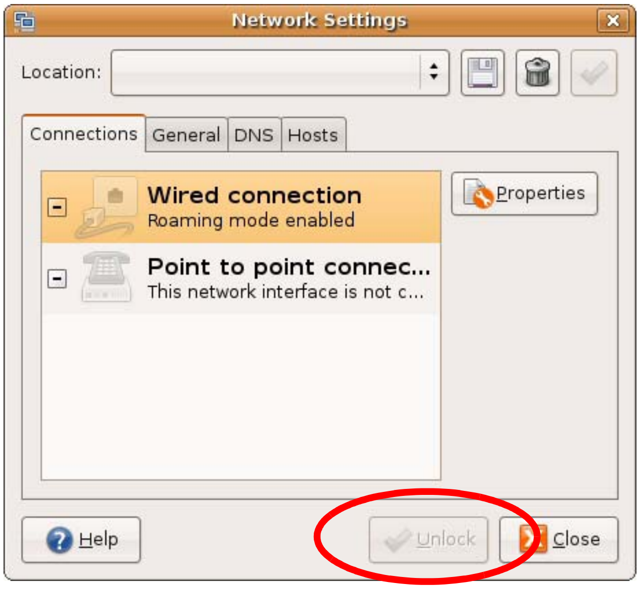
Note: Make sure you are logged in as the root administrator.

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

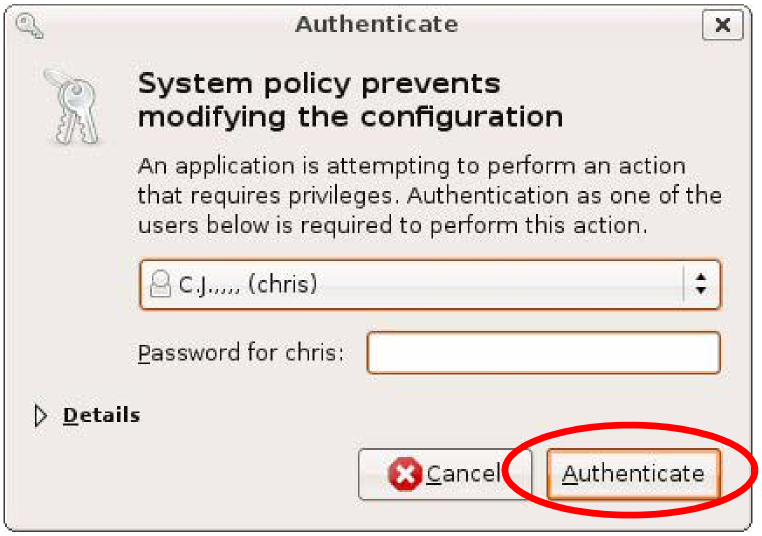
1 Click **System > Administration > Network**.



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.



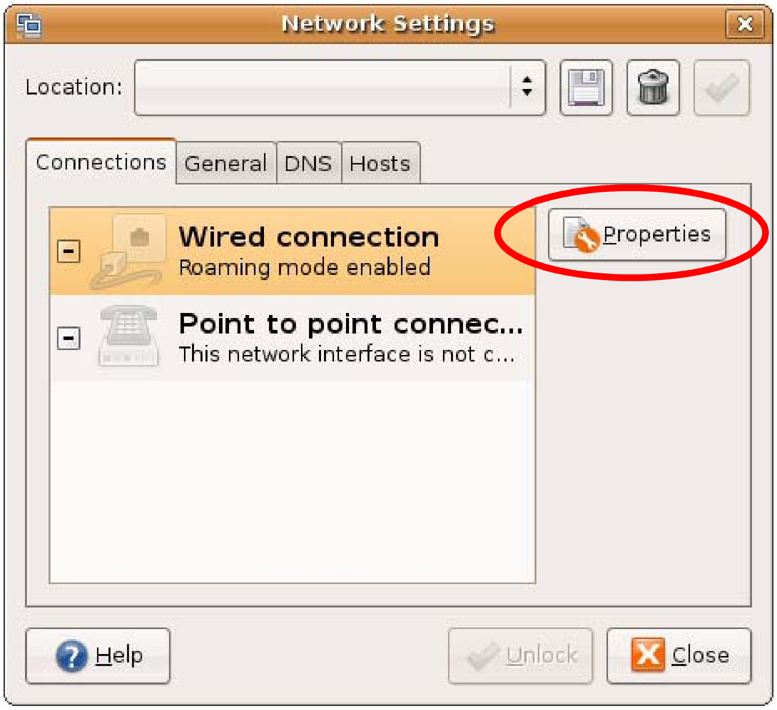
System policy prevents modifying the configuration

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

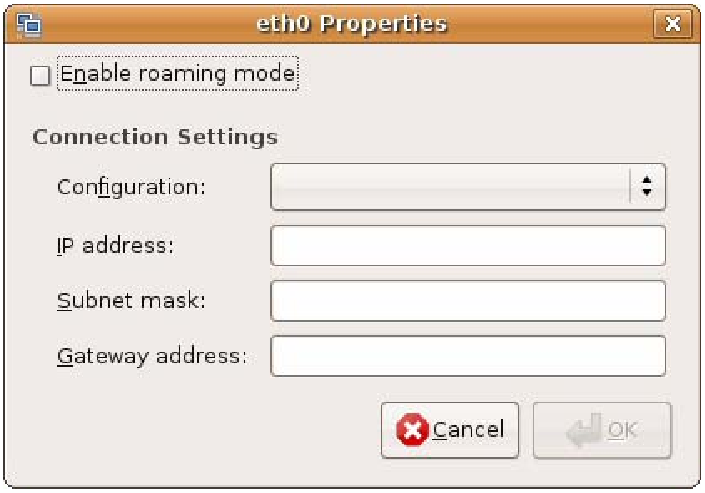
C.J....., (chris)

Password for chris:

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



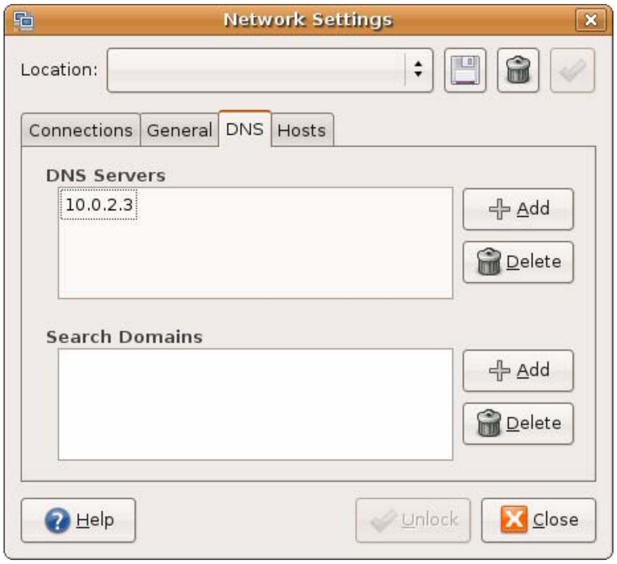
5 The **Properties** dialog box opens.



- 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.



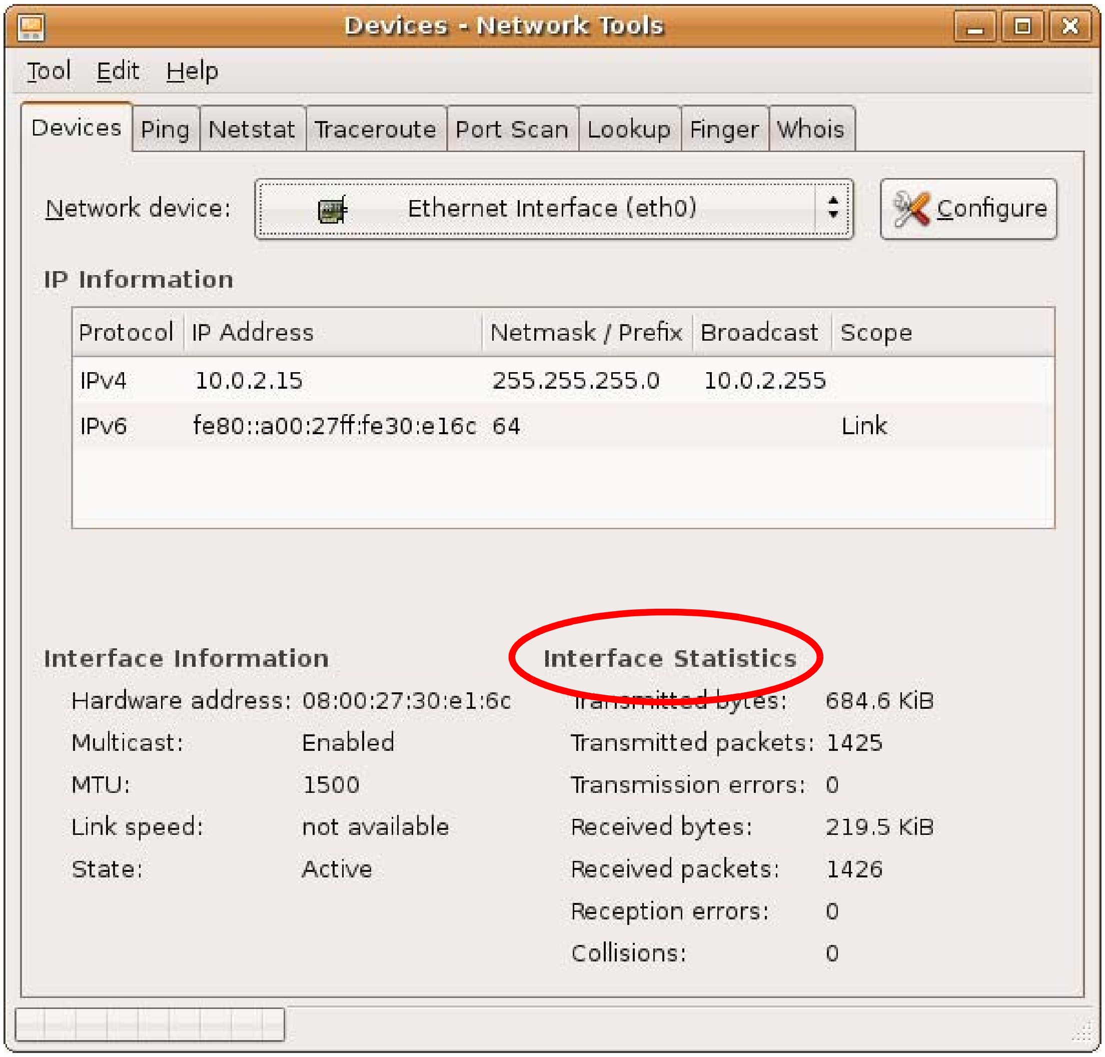
DNS Servers: 10.0.2.3

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 79 Ubuntu 8: Network Tools


Devices - Network Tools
Tool Edit Help
Devices Ping Netstat Traceroute Port Scan Lookup Finger Whois
Configure

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

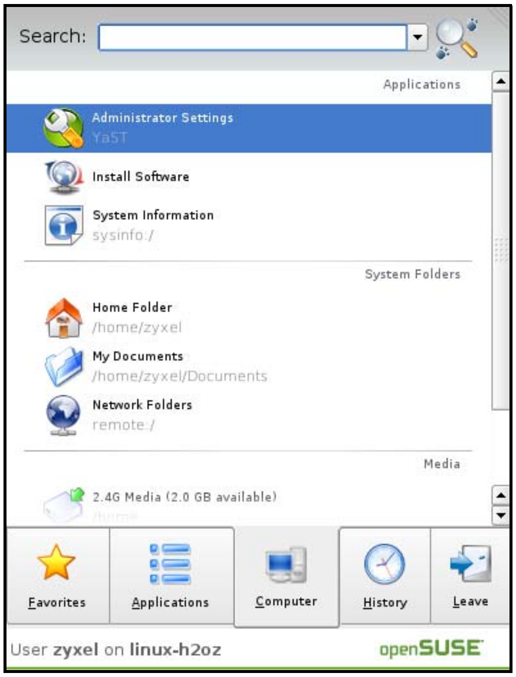
Linux: openSUSE 10.3 (KDE)

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.

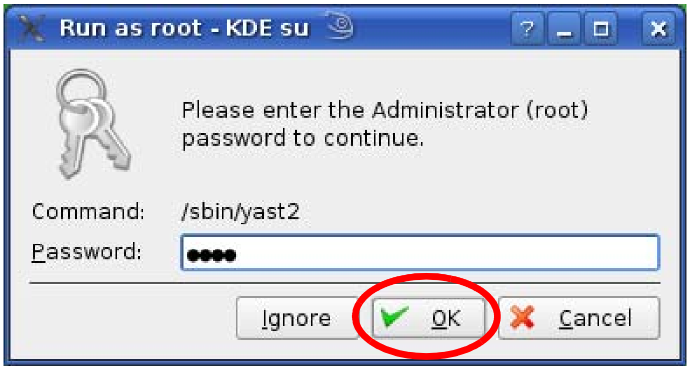
Note: Make sure you are logged in as the root administrator.

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**.

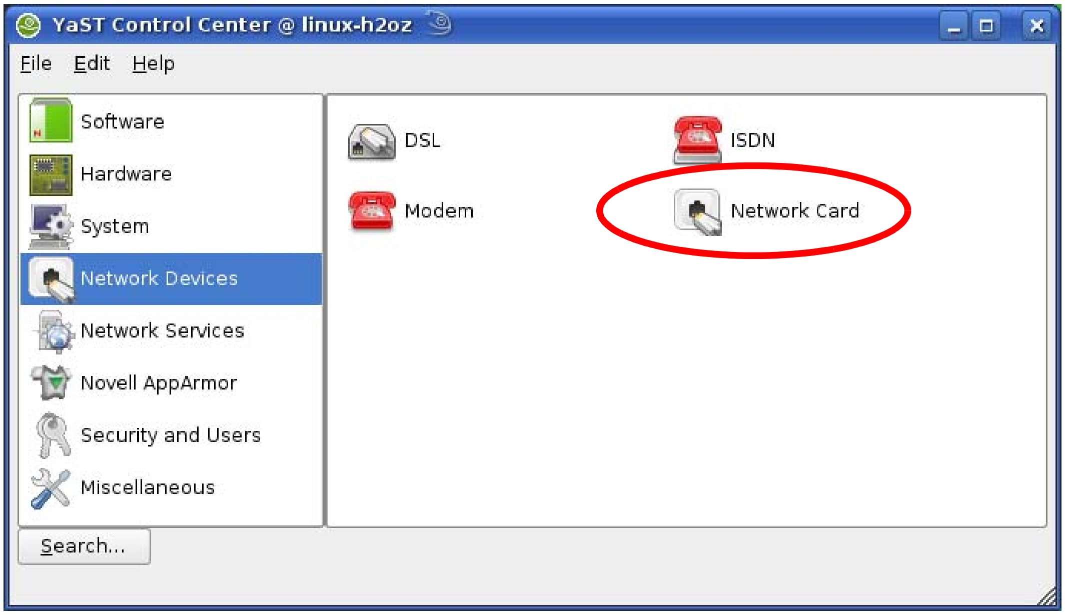


Please enter the Administrator (root) password to continue.

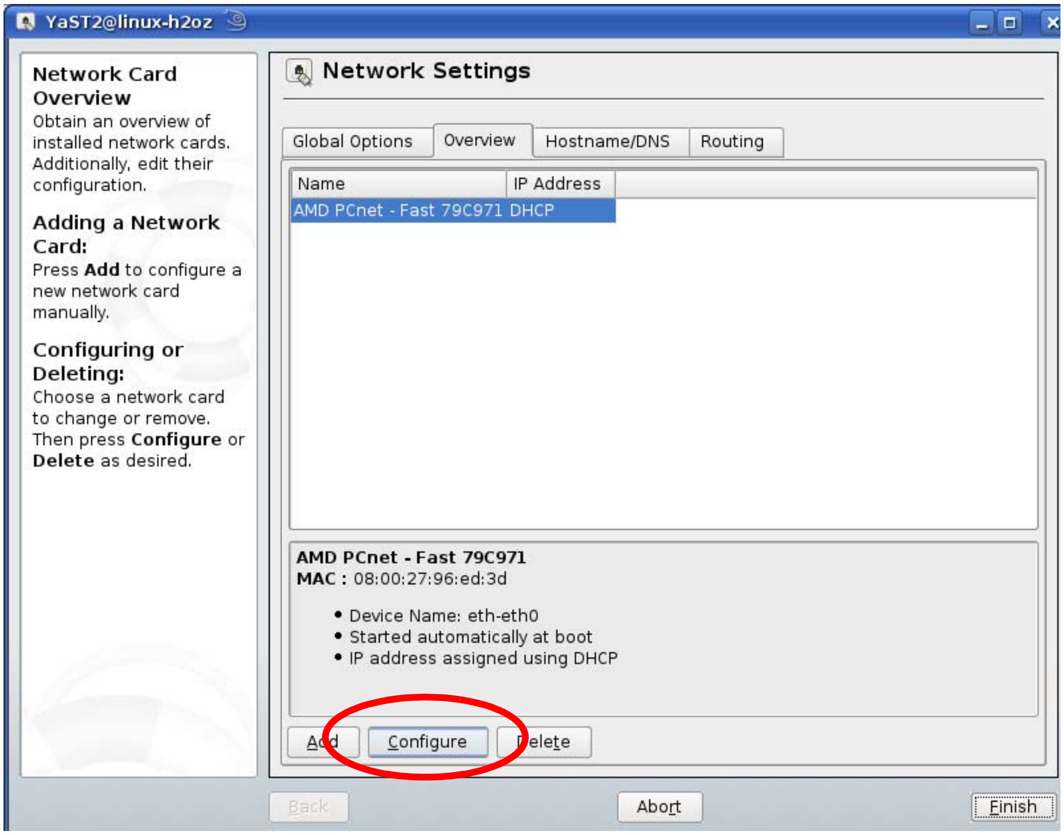
Command: /sbin/yast2

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.

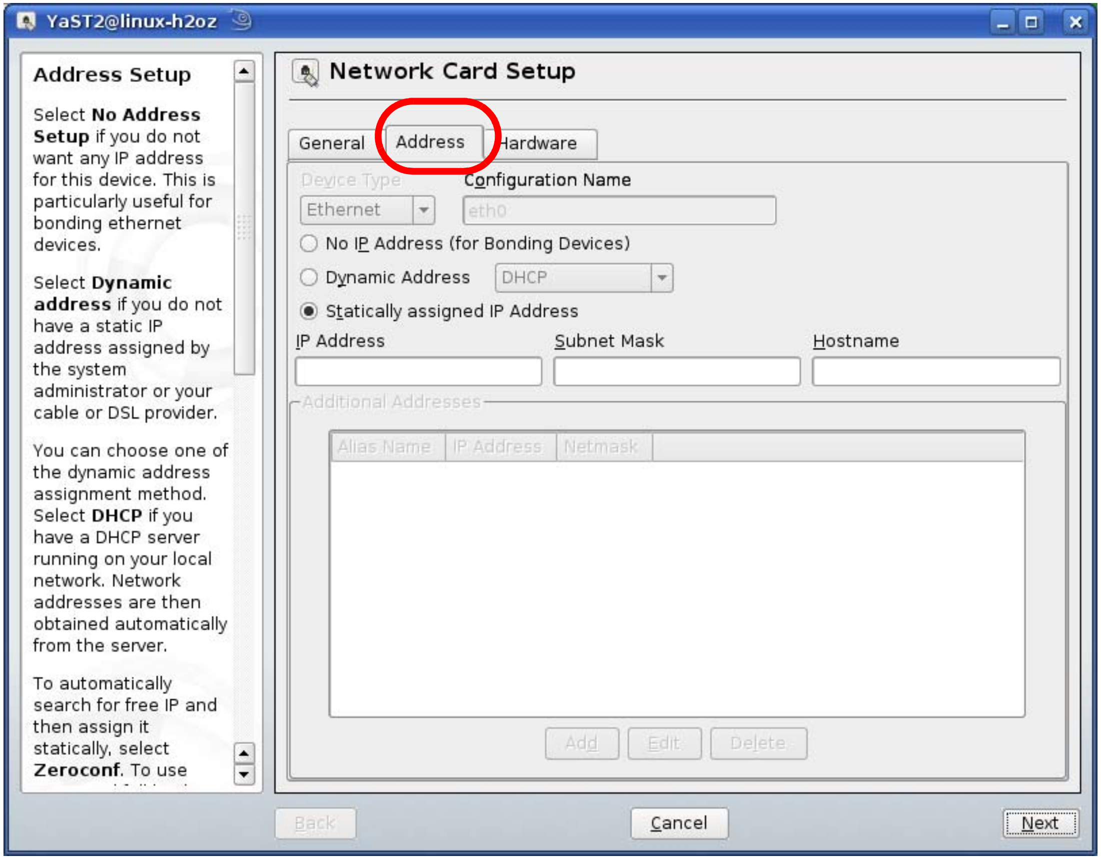
Name	IP Address
AMD PCnet - Fast 79C971	DHCP

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 80 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:

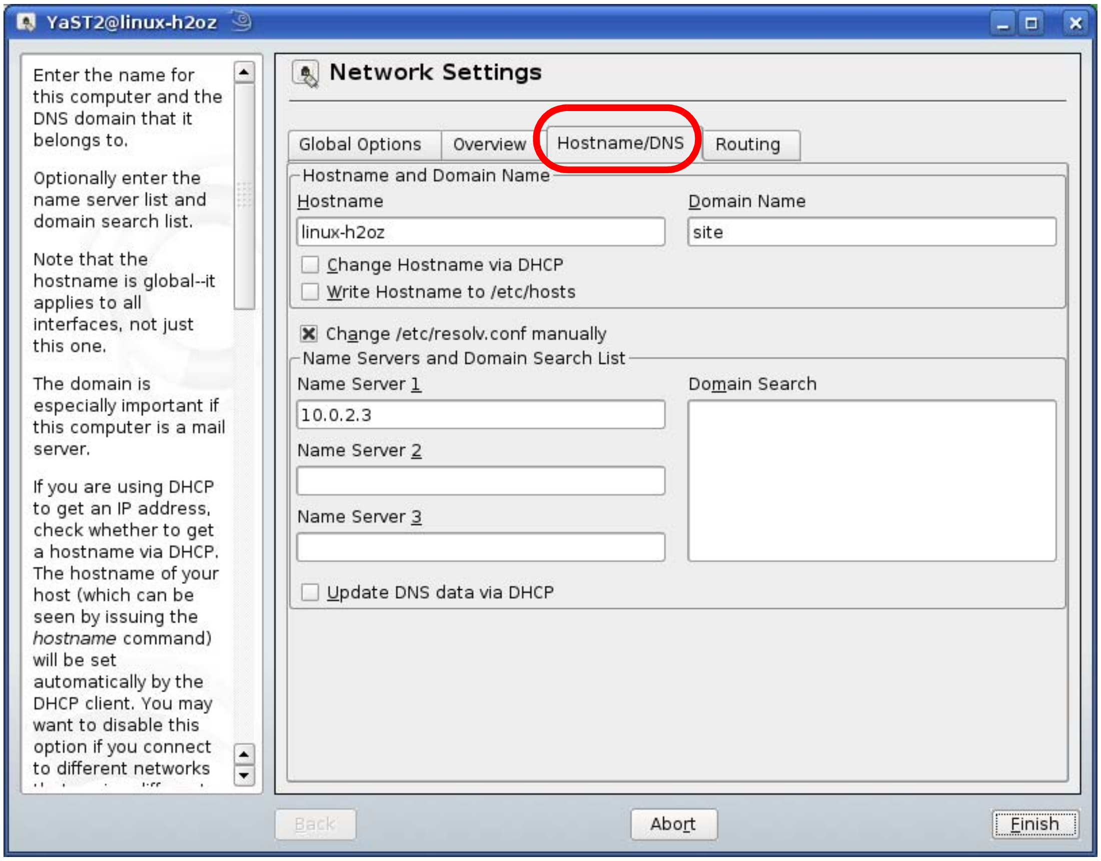
Hostname:

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.



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

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:

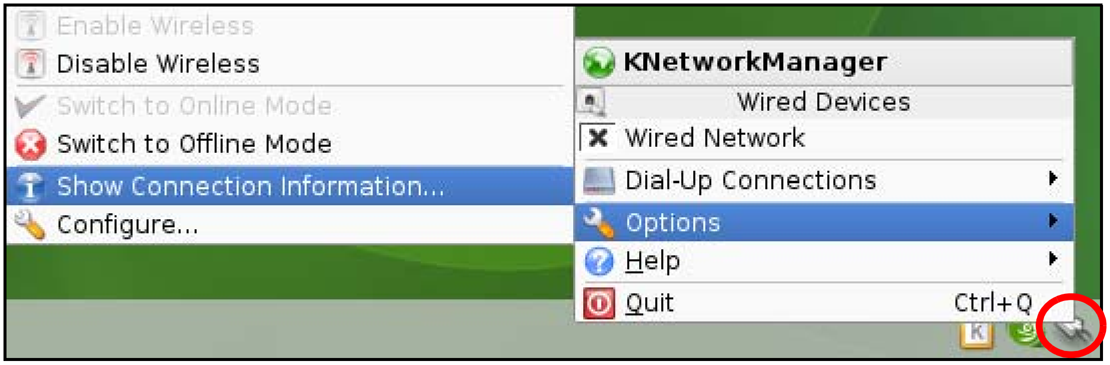
☐ Update DNS data via DHCP

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

Verifying Settings

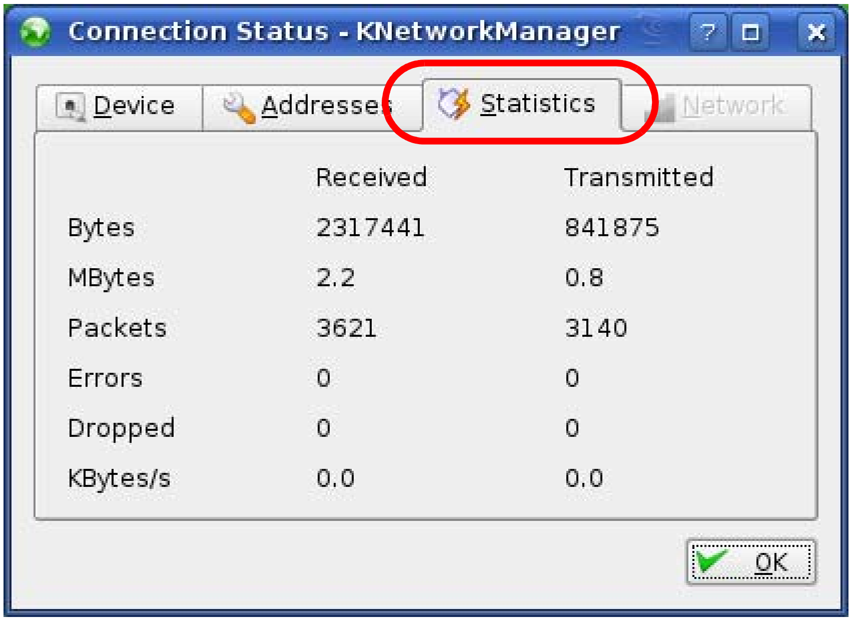
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 81 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 82 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

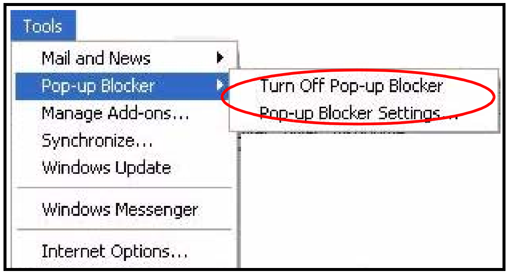
You may have to disable pop-up blocking to log into your device.

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 83 Pop-up Blocker

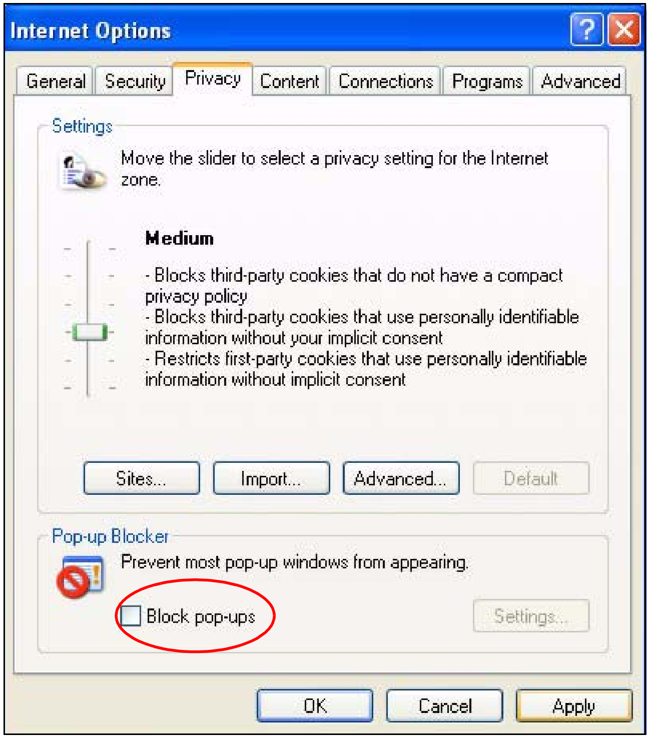


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 84 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.

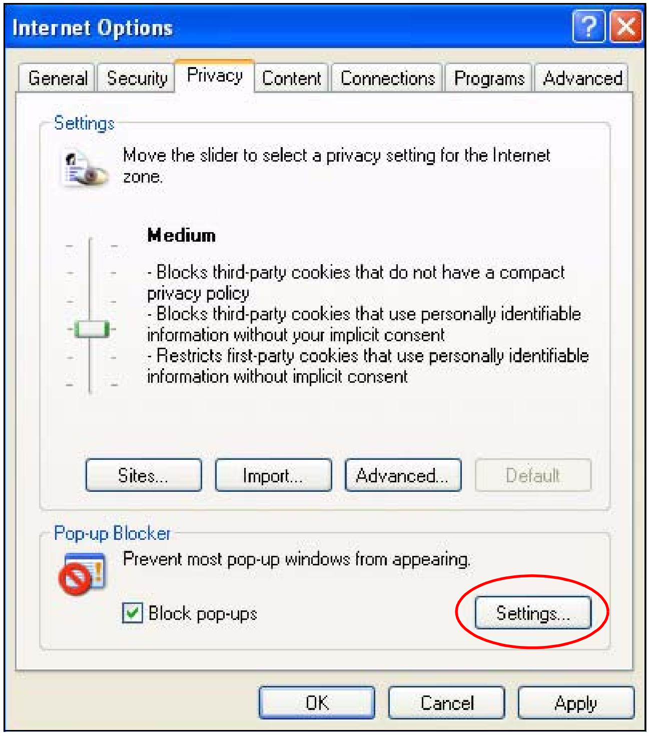
Enable Pop-up Blockers with Exceptions

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 85 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

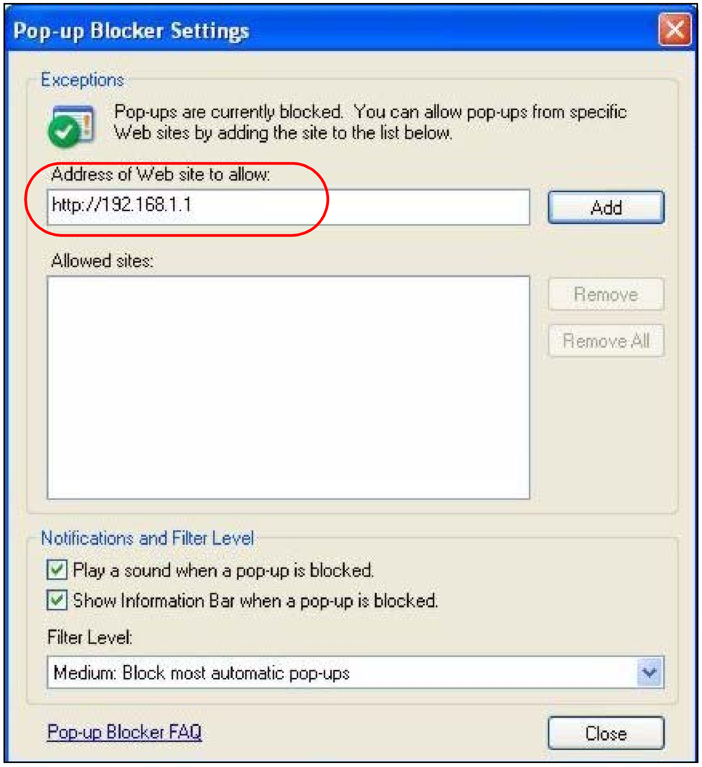
Prevent most pop-up windows from appearing.

☑ 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 86 Pop-up Blocker Settings



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.

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

Allowed sites:

Notifications and Filter Level

☑ 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

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

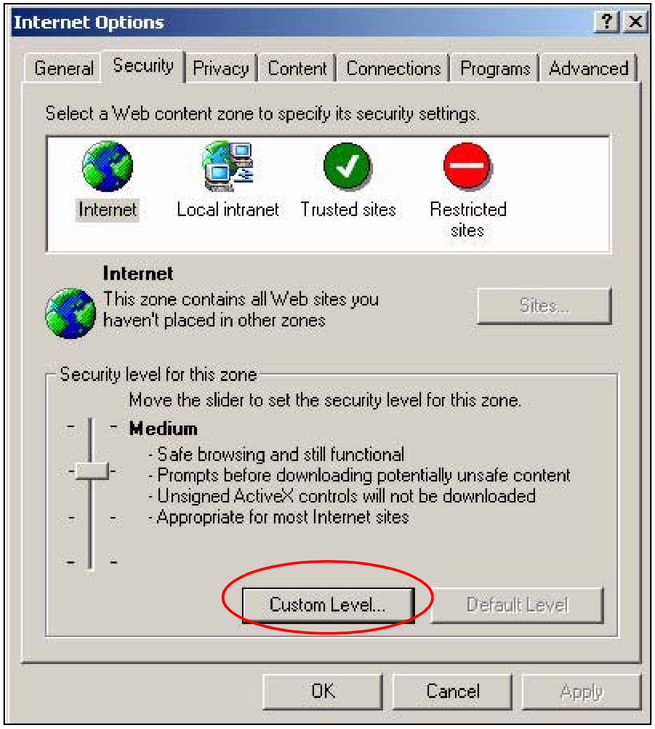
6 Click **Apply** to save this setting.

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 87 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.

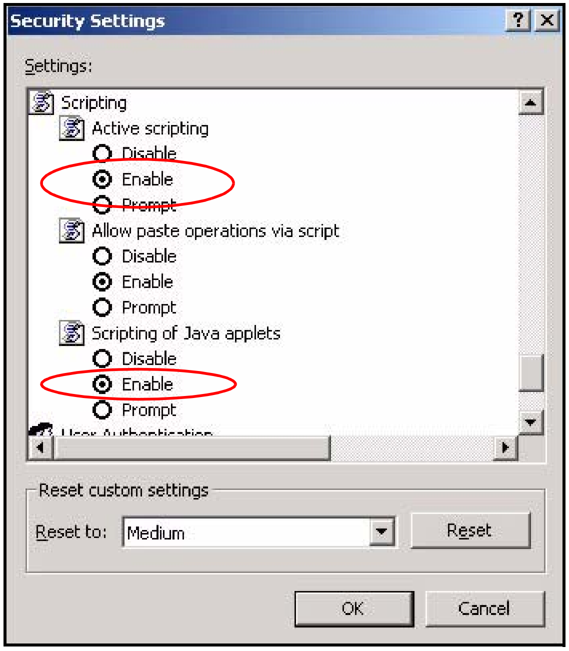
3 Scroll down to **Scripting**.

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 88 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.

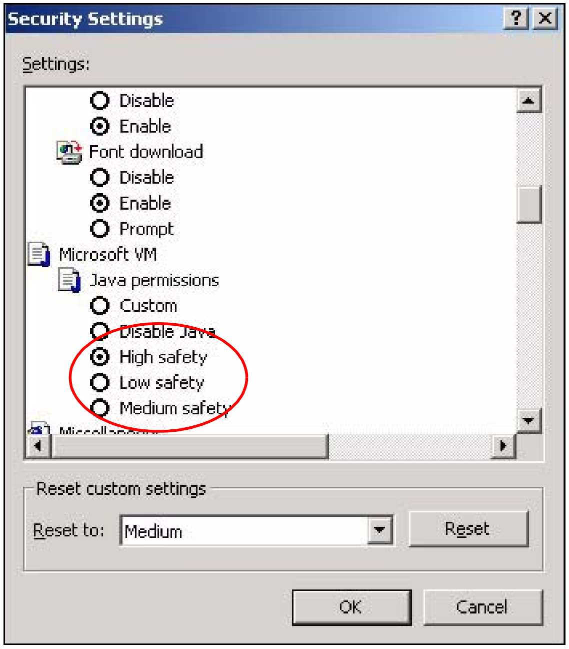
2 Click the **Custom Level...** button.

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 89 Security Settings - Java



Settings:

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

Reset custom settings

Reset to: Medium

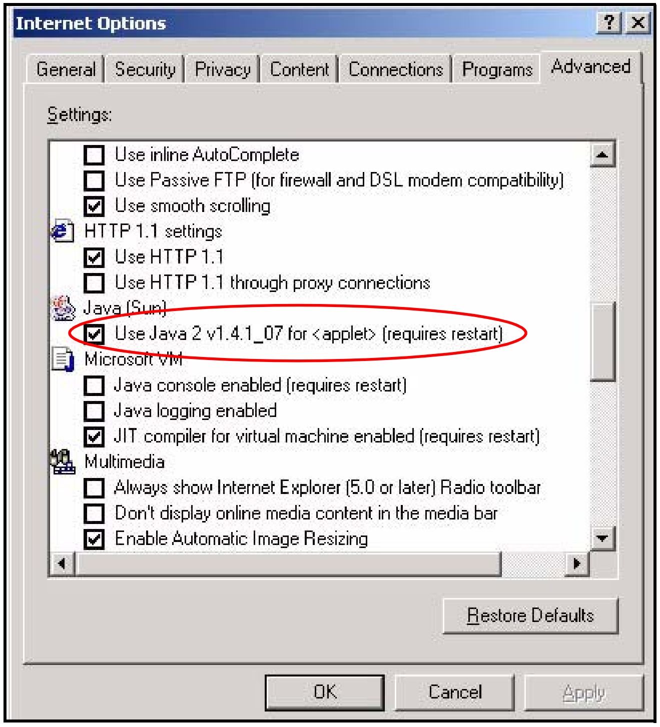
JAVA (Sun)

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 90 Java (Sun)



Internet Options
General | Security | Privacy | Content | Connections | Programs | Advanced
Settings:
Restore Defaults
OK
Cancel
Apply

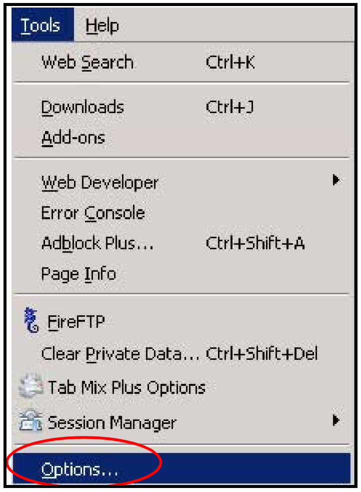
☐ Use inline AutoComplete
☐ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
☐ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
☐ Java console enabled (requires restart)
☐ 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.

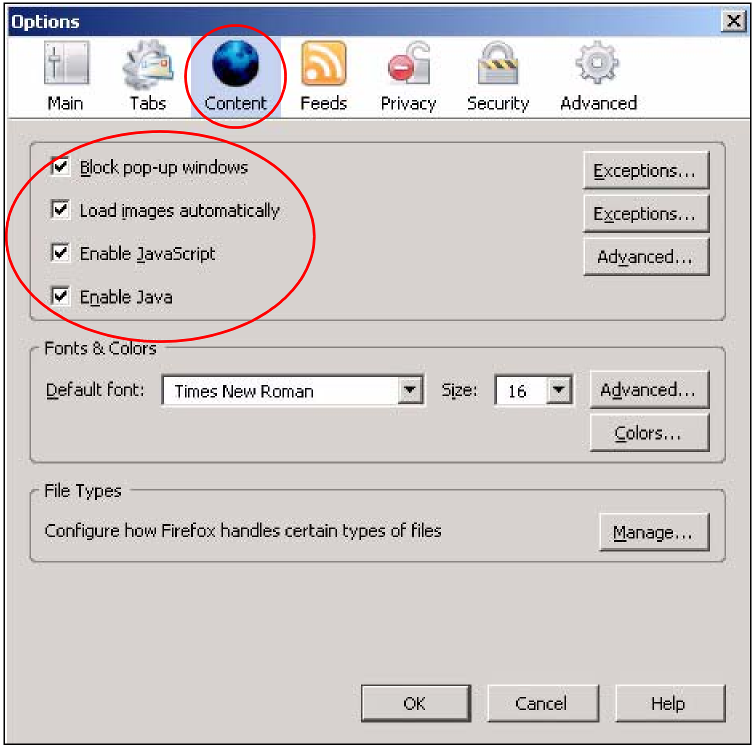
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 91 Mozilla Firefox: TOOLS > Options



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

Figure 92 Mozilla Firefox Content Security



Options

☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman   Size: 16

File Types

Configure how Firefox handles certain types of files

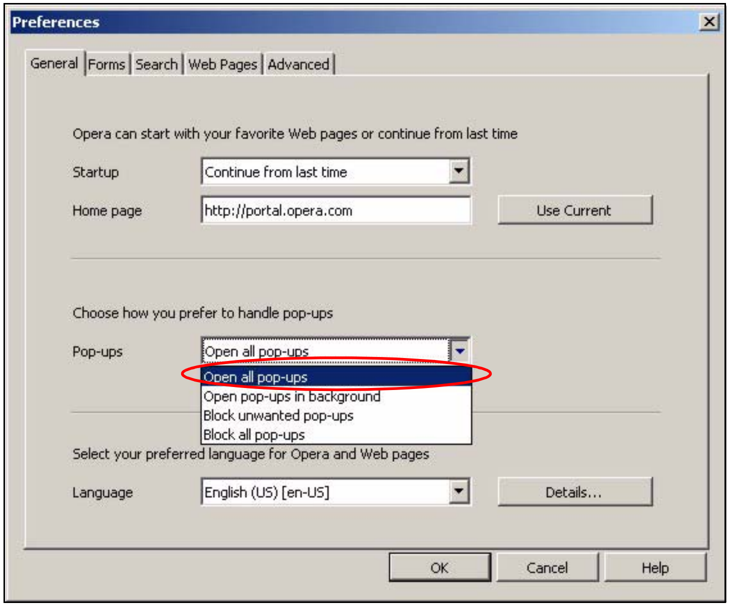
Opera

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 93 Opera: Allowing Pop-Ups



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

Startup: Continue from last time

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

Choose how you prefer to handle pop-ups

Pop-ups: Open all pop-ups

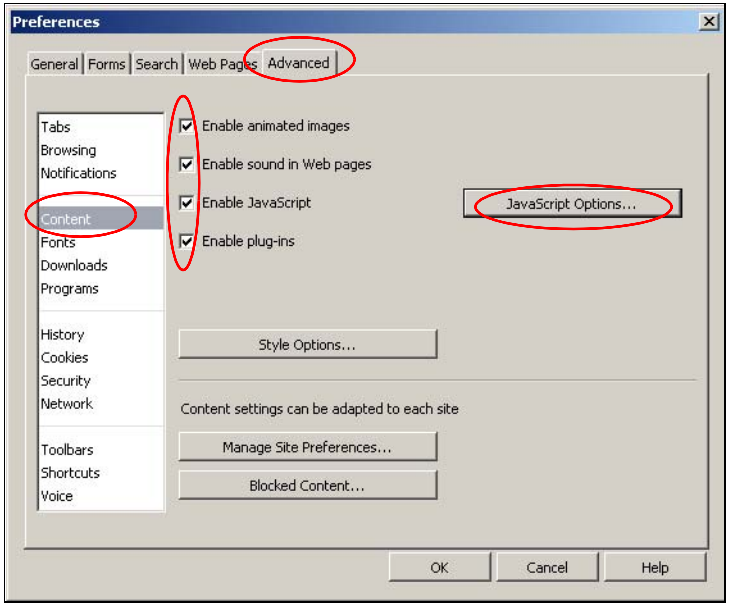
Select your preferred language for Opera and Web pages

Language: English (US) [en-US]

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 94 Opera: Enabling Java



☑ Enable animated images

☑ Enable sound in Web pages

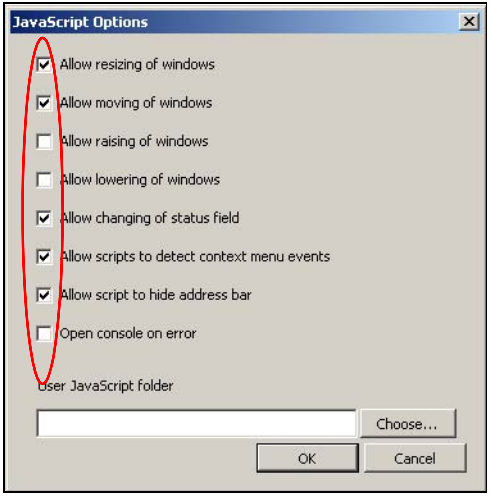
☑ Enable JavaScript

☑ Enable plug-ins

Content settings can be adapted to each site

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

Figure 95 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.

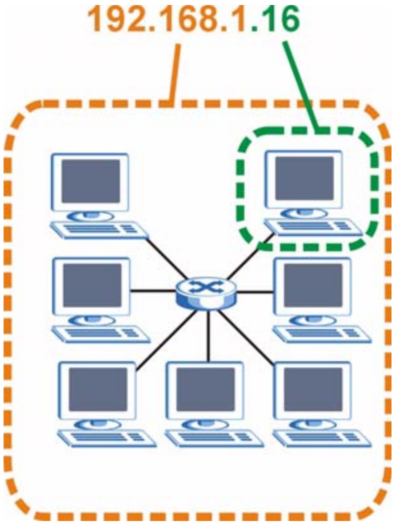
Structure

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 96 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 54 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 55 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 56 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 57 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

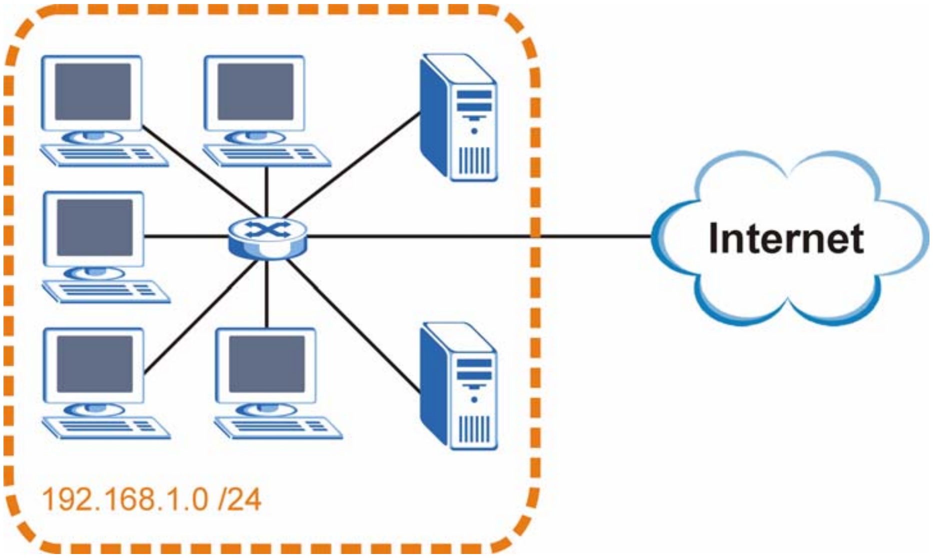
Subnetting

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 97 Subnetting Example: Before Subnetting

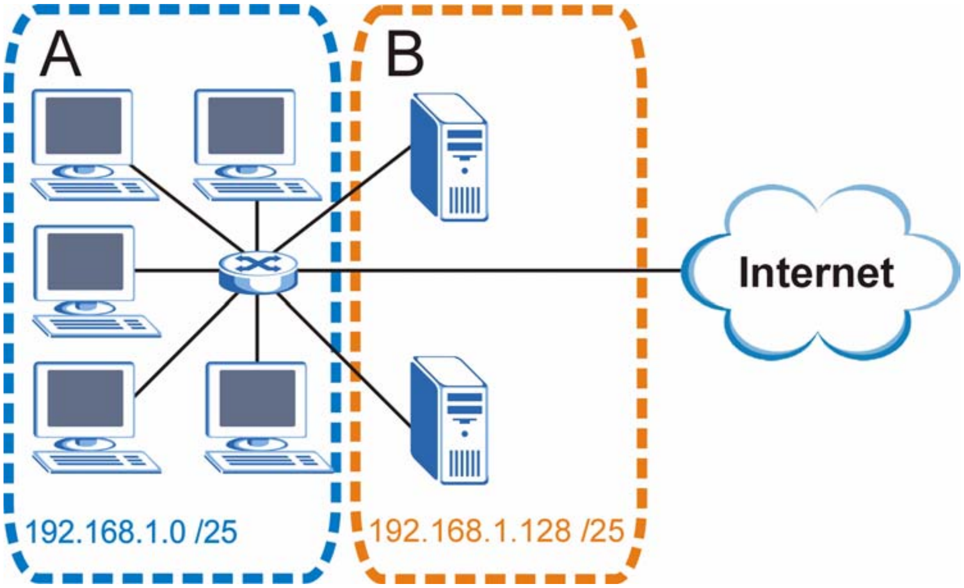


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 98 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 58 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 58 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 59 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 60 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 61 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 62 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 63 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 64 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 64 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.*

Wireless LANs

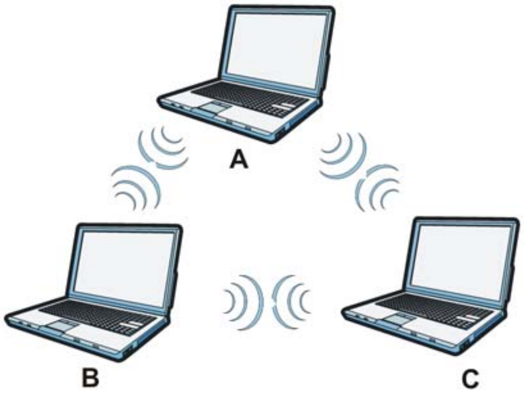
Wireless LAN Topologies

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

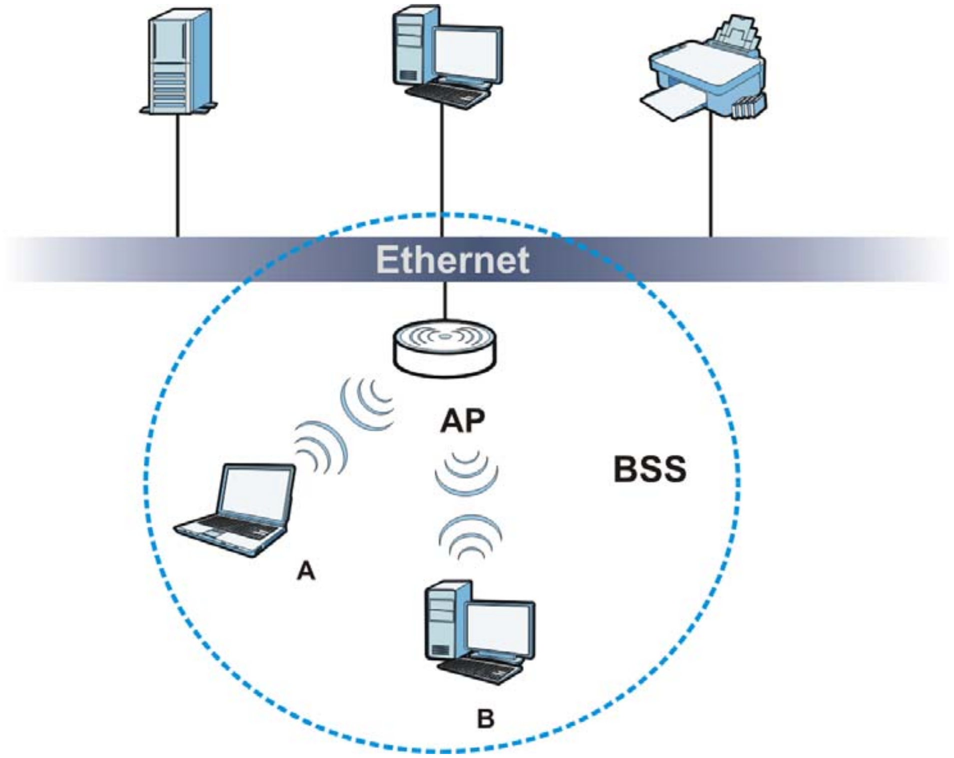


BSS

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 100 Basic Service Set



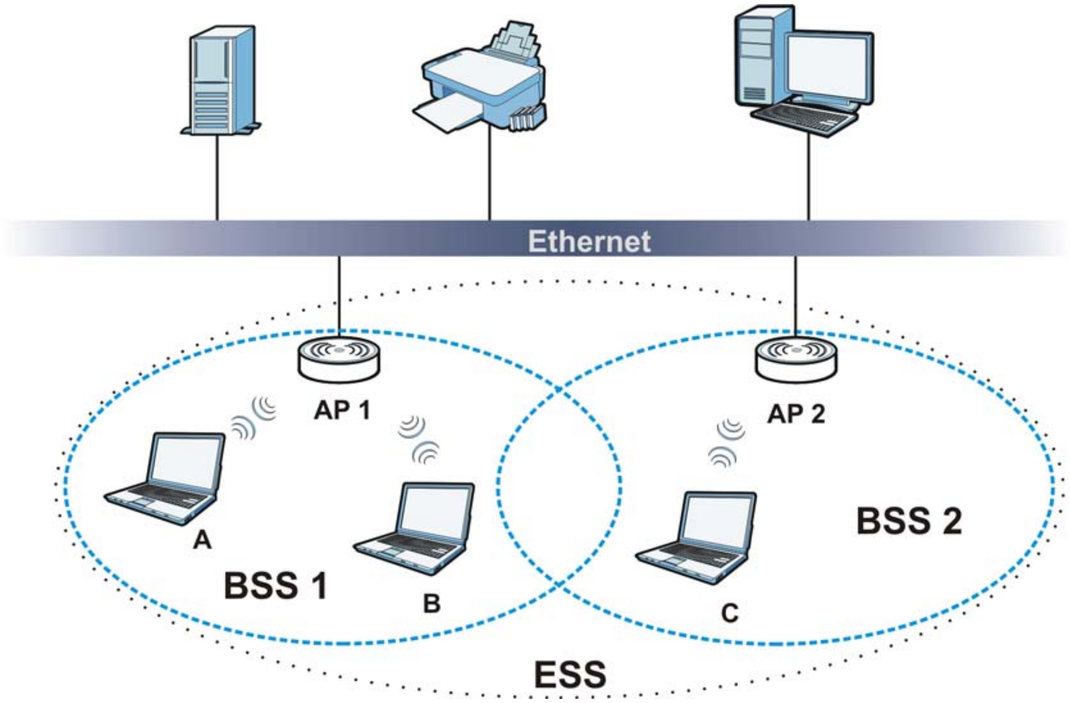
ESS

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 101 Infrastructure WLAN



Channel

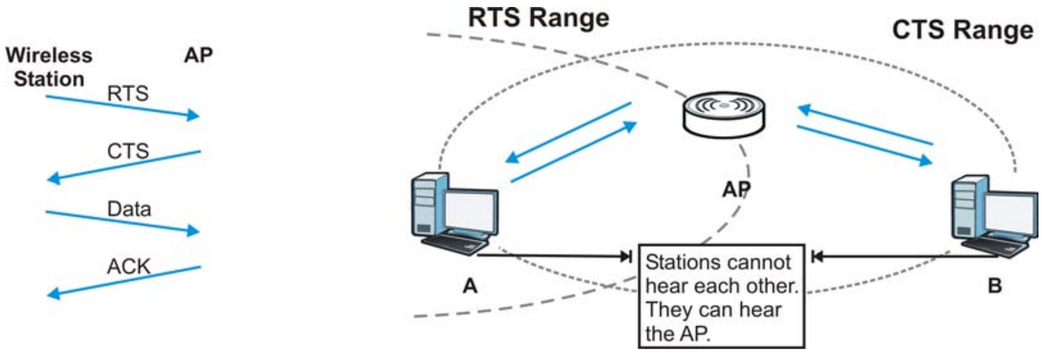
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 102 RTS/CTS



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

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

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

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

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

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

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

Fragmentation Threshold

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

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

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

Preamble Type

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

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

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

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

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

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

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 65 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

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

Wireless security methods available on the 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 66 Wireless Security Levels

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

Note: You must enable the same wireless security settings on the 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 67 Comparison of EAP Authentication Types

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

WPA and WPA2

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

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

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

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

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

Encryption

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

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

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

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

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

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

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

User Authentication

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

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

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

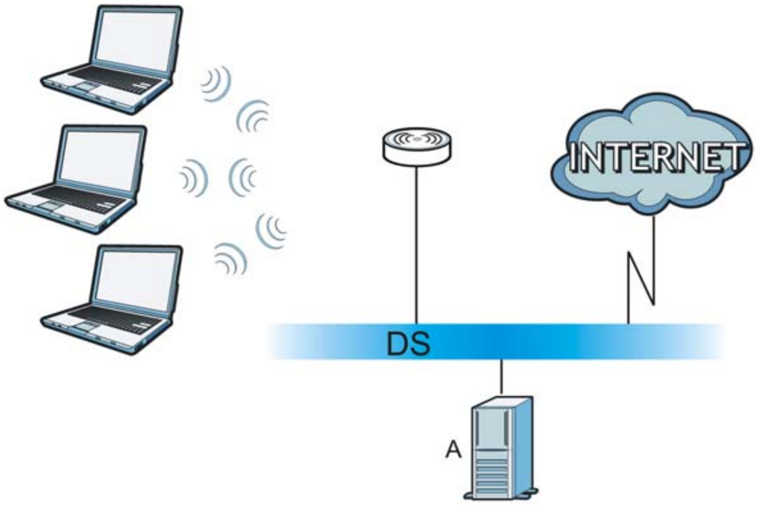
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 103 WPA(2) with RADIUS Application Example



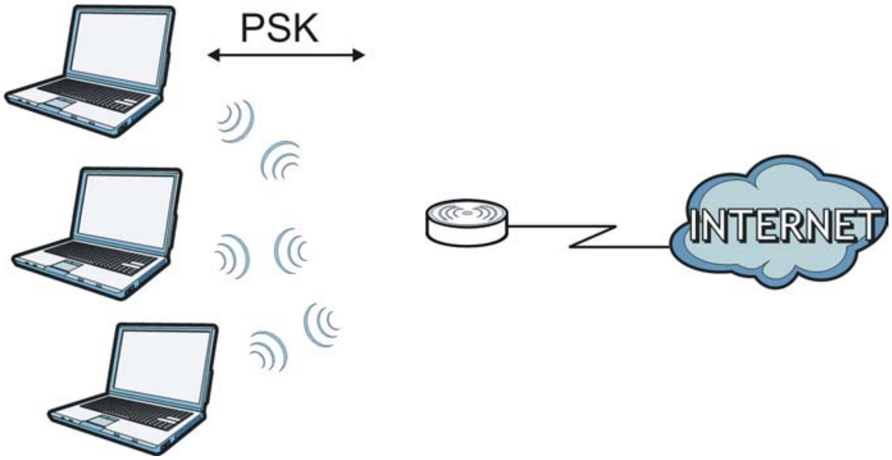
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

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

Figure 104 WPA(2)-PSK Authentication



Security Parameters Summary

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

Table 68 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
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

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

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

Antenna Characteristics

Frequency

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

Radiation Pattern

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

Antenna Gain

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

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

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

Types of Antennas for WLAN

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

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

Positioning Antennas

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

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

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

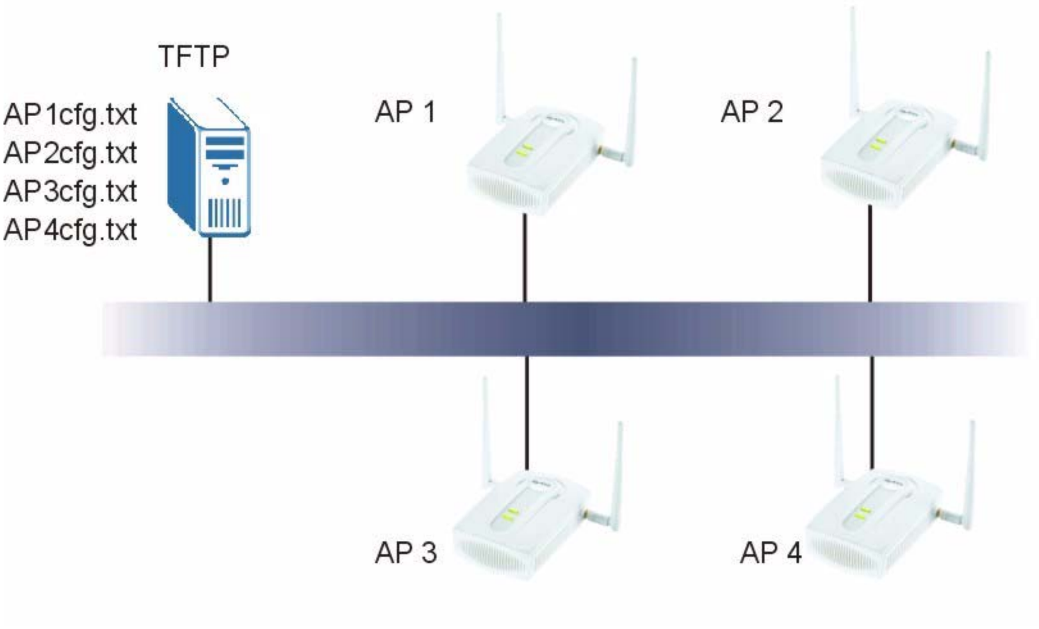
Text File Based Auto Configuration

This chapter describes how administrators can use text configuration files to configure the wireless LAN settings for multiple APs.

Text File Based Auto Configuration Overview

You can use plain text configuration files to configure the wireless LAN settings on multiple APs. The AP can automatically get a configuration file from a TFTP server at startup or after renewing DHCP client information.

Figure 105 Text File Based Auto Configuration



Use one of the following methods to give the AP the IP address of the TFTP server where you store the configuration files and the name of the configuration file that it should download.

You can have a different configuration file for each AP. You can also have multiple APs use the same configuration file.

Note: If adjacent APs use the same configuration file, you should leave out the channel setting since they could interfere with each other's wireless traffic.

Configuration Via SNMP

You can configure and trigger the auto configuration remotely via SNMP.

Use the following procedure to have the AP download the configuration file.

Table 69 Configuration via SNMP

STEPS	MIB VARIABLE	VALUE
Step 1	pwTftpServer	Set the IP address of the TFTP server.
Step 2	pwTftpFileName	Set the file name, for example, g3000hcfg.txt.
Step 3	pwTftpFileType	Set to 3 (text configuration file).
Step 4	pwTftpOpCommand	Set to 2 (download).

Verifying Your Configuration File Upload Via SNMP

You can use SNMP management software to display the configuration file version currently on the device by using the following MIB.

Table 70 Displaying the File Version

ITEM	OBJECT ID	DESCRIPTION
pwCfgVersion	1.3.6.1.4.1.890.1.9.1.2	This displays the current configuration file version.

Troubleshooting Via SNMP

If you have any difficulties with the configuration file upload, you can try using the following MIB 10 to 20 seconds after using SNMP to have the AP download the configuration file.

Table 71 Displaying the File Version

ITEM	OBJECT ID	DESCRIPTION
pwTftpOpStatus	1.3.6.1.4.1.890.1.9.1.6	This displays the current operating status of the TFTP client.

Open Software Announcements

End-User License Agreement for "NWA1100-N

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN-IN PART-SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS"). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Busybox, hostapd, wpa_supplicant, ntpclient, vsftpd, Linux Kernel and u-boot software under GPL 2.0 license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes net-snmp software under below license.

Various copyrights apply to this package, listed in various separate

parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2010, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes SMTPClient software under below license.

```
* Copyright (c) 2008, Stephen Blackheath
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are met:
 *     * Redistributions of source code must retain the above copyright
 *       notice, this list of conditions and the following disclaimer.
 *     * Redistributions in binary form must reproduce the above copyright
 *       notice, this list of conditions and the following disclaimer in the
 *       documentation and/or other materials provided with the distribution.
 *     * Neither the name of the <organization> nor the
 *       names of its contributors may be used to endorse or promote products
 *       derived from this software without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY STEPHEN BLACKHEATH ''AS IS'' AND ANY
 * EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
 * DISCLAIMED. IN NO EVENT SHALL STEPHEN BLACKHEATH BE LIABLE FOR ANY
 * DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
```

This Product includes u-boot software under below license

NOTE! This copyright does *not* cover the so-called "standalone" applications that use U-Boot services by means of the jump table provided by U-Boot exactly for this purpose - this is merely considered normal use of U-Boot, and does *not* fall under the heading of "derived work".

The header files "include/image.h" and "include/asm-*/u-boot.h" define interfaces to U-Boot. Including these (unmodified) header files in another file is considered normal use of U-Boot, and does *not* fall under the heading of "derived work".

Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code that it refers to (the U-Boot source code) is copyrighted by me and others who actually wrote it.

-- Wolfgang Denk

===

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and
you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes

make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Legal Information

Copyright

Disclaimers

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

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

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

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

Trademarks

This item incorporates copy protection technology that is protected by U.S. patents and other intellectual property rights of Rovi Corporation. Reverse engineering and disassembly are prohibited. Use for STBs that need Rovi certification.

Certifications (Class A without wireless)

Federal Communications Commission (FCC) Interference Statement

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

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

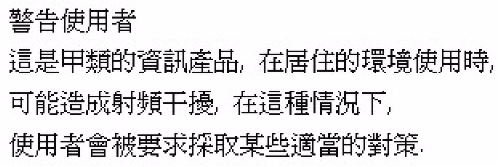
FCC Warning

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

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:



警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Notices

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

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

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

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

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

CLASS 1 LASER PRODUCT (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

APPAREIL À LASER DE CLASS 1 (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

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

Certifications (Class B)

Federal Communications Commission (FCC) Interference Statement

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

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

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

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

(for all wireless devices)

FCC Radiation Exposure Statement

- This device has been tested to the FCC exposure requirements (Specific Absorption Rate). (for USB wireless adapters or CardBus cards)

- This device complies with the requirements of Health Canada Safety Code 6 for Canada. (for USB wireless adapters or CardBus cards)
- Testing was performed on laptop computers with antennas at 0mm spacing. The maximum SAR value is: ??? W/kg. The device must not be collocated with any other antennas or transmitters. (For USB wireless adapters or CardBus cards. The SAR value may differ by model: check before adding this statement.)
- This equipment has been SAR-evaluated for use in laptops (notebooks) with side slot configuration. (for Wireless USB adapters and wireless PCMCIA cards)
- The device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2). End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual. (for USB wireless adapters or CardBus cards)
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. (for all wireless devices)
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment. (for IEEE 802.11a wireless devices)
- IEEE 802.11b, 802.11g or 802.11n(20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n(40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. (for all IEEE 802.11b and 802.11g products)
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons. (for all wireless devices without SAR test, such as an AP or wireless router. the SAR test will be done for wireless USB adapters and CardBus cards)
- Due to the essential high output power natural of WiMAX device, use of this device with other transmitter at the same time may exceed the FCC RF exposure limit and such usage must be prohibited (unless such co-transmission has been approved by FCC in the future). (for WiMAX USB adapters with SAR measurement)
- SAR compliance has been established in typical laptop computer(s) with USB slot, and product could be used in typical laptop computer with USB slot. Other application like handheld PC or similar device has not been verified and may not compliance with related RF exposure rule and such use shall be prohibited. (for WiMAX USB adapters with SAR measurement)

Industry Canada Statement (For all products)

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

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

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

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

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

IMPORTANT NOTE

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

IC Radiation Exposure Statement

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

注意 !(for all products)

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

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現
有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

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

Notices

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

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

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

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

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

CLASS 1 LASER PRODUCT (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

APPAREIL A LASER DE CLASS 1 (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

Viewing Certifications

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

ZyXEL Limited Warranty

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

Note

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

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

Registration

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

Index