

# NWA-3500/NWA-3550

*802.11a/g Dual Radio Wireless Business AP*

*802.11a/g Dual Radio Outdoor WLAN Business AP*

## User's Guide



### Default Login Details

IP Address	http://192.168.1.2
Password	1234

Firmware Version 3.7  
Edition 1, 1/2009

[www.zyxel.com](http://www.zyxel.com)

# ZyXEL



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the NWA using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide

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

Note: It is recommended you use the web configurator to configure the NWA.

- Support Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

Please refer to [www.zyxel.com](http://www.zyxel.com) for additional support documentation and product certifications.

## User's Guide Feedback

Help us help you. Send all User's Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,  
ZyXEL Communications Corp.,  
6 Innovation Road II,  
Science-Based Industrial Park,  
Hsinchu, 300, Taiwan.

E-mail: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

## Customer Support

In the event of problems that cannot be solved by using this manual, 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](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 NWA-3500 or the NWA-3550 may be referred to as the "NWA", the "device", the "system" or the "product" 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 may use the following generic icons. The NWA icon is not an exact representation of your NWA.

**Table 1** Common Icons

NWA 	Computer 	Notebook 
Server 	Printer 	Telephone 
Switch 	Router 	Internet Cloud 
Firewall 	DSLAM 	Wireless Signal 

# 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.
- ONLY qualified service personnel should service or disassemble this device.
- 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 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.
- 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.
- Please select an antenna that conforms with your local radio regulations. ZyXEL bears no responsibility whatsoever for cases of illegal installation.

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

<b>Introduction .....</b>	<b>21</b>
Introducing the NWA .....	23
Introducing the Web Configurator .....	35
Status Screens .....	39
Management Mode .....	47
Controller AP Mode .....	53
Tutorial .....	67
<b>The Web Configurator .....</b>	<b>107</b>
System Screens .....	109
Wireless Configuration .....	119
SSID Screen .....	141
Wireless Security Screen .....	147
RADIUS Screen .....	161
Layer-2 Isolation Screen .....	165
MAC Filter Screen .....	171
IP Screen .....	175
Rogue AP Detection .....	179
Remote Management Screens .....	187
Internal RADIUS Server .....	199
Certificates .....	207
Log Screens .....	227
VLAN .....	235
Load Balancing .....	255
Dynamic Channel Selection .....	261
Maintenance .....	265
<b>Troubleshooting and Specifications .....</b>	<b>277</b>
Troubleshooting .....	279
Product Specifications .....	285
<b>Appendices and Index .....</b>	<b>291</b>



# Table of Contents

<b>About This User's Guide .....</b>	<b>3</b>
<b>Document Conventions.....</b>	<b>5</b>
<b>Safety Warnings.....</b>	<b>7</b>
<b>Contents Overview .....</b>	<b>9</b>
<b>Table of Contents.....</b>	<b>11</b>
<b>Part I: Introduction.....</b>	<b>21</b>
<b>Chapter 1</b>	
<b>Introducing the NWA .....</b>	<b>23</b>
1.1 Introducing the NWA .....	23
1.2 Applications for the NWA .....	23
1.2.1 Access Point .....	24
1.2.2 Bridge / Repeater .....	24
1.2.3 AP + Bridge .....	25
1.2.4 MBSSID .....	26
1.2.5 Pre-Configured SSID Profiles .....	27
1.2.6 Configuring Dual WLAN Adaptors .....	28
1.3 CAPWAP .....	28
1.4 Ways to Manage the NWA .....	29
1.5 Configuring Your NWA's Security Features .....	30
1.5.1 Control Access to Your Device .....	30
1.5.2 Wireless Security .....	30
1.6 Maintaining Your NWA .....	31
1.7 Hardware Connections .....	31
1.8 LEDs .....	32
<b>Chapter 2</b>	
<b>Introducing the Web Configurator .....</b>	<b>35</b>
2.1 Accessing the Web Configurator .....	35
2.2 Resetting the NWA .....	37
2.2.1 Methods of Restoring Factory-Defaults .....	37
2.3 Navigating the Web Configurator .....	37

<b>Chapter 3</b>	
<b>Status Screens .....</b>	<b>39</b>
3.1 The Status Screen .....	40
3.1.1 AP List .....	44
3.1.2 AP Statistics .....	45
3.1.3 SSID Information .....	46
<b>Chapter 4</b>	
<b>Management Mode.....</b>	<b>47</b>
4.1 About CAPWAP .....	47
4.1.1 CAPWAP Discovery and Management .....	48
4.1.2 CAPWAP and DHCP .....	48
4.1.3 CAPWAP and IP Subnets .....	48
4.1.4 Notes on CAPWAP .....	49
4.2 The Management Mode Screen .....	49
<b>Chapter 5</b>	
<b>Controller AP Mode .....</b>	<b>53</b>
5.1 Overview .....	53
5.1.1 What You Can Do in AP Controller Mode .....	53
5.1.2 What You Need to Know .....	53
5.1.3 Before You Begin .....	54
5.2 Controller AP Navigation Menu .....	54
5.3 Controller AP Status Screen .....	55
5.4 AP List Screen .....	57
5.4.1 The AP Lists Edit Screen .....	59
5.5 Configuration Screen .....	60
5.6 Redundancy Screen .....	61
5.7 The Profile Edit Screens .....	62
5.7.1 The Radio Profile Screen .....	62
5.8 The Radio Profile Edit Screen .....	64
<b>Chapter 6</b>	
<b>Tutorial .....</b>	<b>67</b>
6.1 How to Configure the Wireless LAN .....	67
6.1.1 Choosing the Wireless Mode .....	67
6.1.1.1 Configuring Dual WLAN Adaptors .....	68
6.1.2 Wireless LAN Configuration Overview .....	68
6.1.3 Further Reading .....	70
6.2 How to Configure Multiple Wireless Networks .....	70
6.2.1 Change the Operating Mode .....	72
6.2.2 Configure the VoIP Network .....	73
6.2.2.1 Set Up Security for the VoIP Profile .....	75

6.2.2.2 Activate the VoIP Profile .....	77
6.2.3 Configure the Guest Network .....	77
6.2.3.1 Set Up Security for the Guest Profile .....	78
6.2.3.2 Set up Layer 2 Isolation .....	80
6.2.3.3 Activate the Guest Profile .....	82
6.2.4 Testing the Wireless Networks .....	82
6.3 How to Set Up and Use Rogue AP Detection .....	83
6.3.1 Set Up and Save a Friendly AP list .....	85
6.3.2 Activate Periodic Rogue AP Detection .....	88
6.3.3 Set Up E-mail Logs .....	89
6.3.4 Configure Your Other Access Points .....	90
6.3.5 Test the Setup .....	90
6.4 How to Use Multiple MAC Filters and L-2 Isolation Profiles .....	91
6.4.1 Scenario .....	91
6.4.2 Your Requirements .....	92
6.4.3 Setup .....	92
6.4.4 Configure the SERVER_1 Network .....	93
6.4.5 Configure the SERVER_2 Network .....	96
6.4.6 Checking your Settings and Testing the Configuration .....	96
6.4.6.1 Checking Settings .....	96
6.4.6.2 Testing the Configuration .....	98
6.5 How to Configure Management Modes .....	99
6.5.1 Scenario .....	99
6.5.2 Your Requirements .....	99
6.5.3 Setup .....	100
6.5.4 Configure Your NWA in Controller AP Mode .....	101
6.5.4.1 Secondary AP Controller .....	101
6.5.4.2 Primary AP Controller .....	102
6.5.5 Setting Your NWA in Managed AP Mode .....	103
6.5.6 Configuring the Managed Access Points List .....	104
6.5.7 Checking your Settings and Testing the Configuration .....	106
<b>Part II: The Web Configurator .....</b>	<b>107</b>
<b>Chapter 7</b>	
<b>System Screens .....</b>	<b>109</b>
7.1 Overview .....	109
7.2 What You Can Do in the System Screens .....	109
7.3 What You Need To Know .....	110
7.3.1 Administrator Authentication on RADIUS .....	111
7.4 General Setup Screen .....	112

7.5 Configuring the Password .....	113
7.6 Configuring Time Setting .....	116
7.7 Technical Reference .....	118
<b>Chapter 8</b>	
<b>Wireless Configuration.....</b>	<b>119</b>
8.1 Overview .....	119
8.2 What You Can Do in the Wireless Screen .....	119
8.3 What You Need To Know .....	120
8.3.1 Operating Mode .....	121
8.3.2 MBSSID .....	122
8.4 Configuring Wireless Settings .....	123
8.4.1 Access Point Mode .....	123
8.4.2 Bridge / Repeater Mode .....	126
8.4.3 AP + Bridge Mode .....	129
8.4.4 MBSSID Mode .....	130
8.5 Technical Reference .....	131
8.5.1 Spanning Tree Protocol (STP) .....	131
8.5.1.1 Rapid STP .....	131
8.5.1.2 STP Terminology .....	132
8.5.1.3 How STP Works .....	132
8.5.1.4 STP Port States .....	133
8.5.2 DFS .....	133
8.5.3 Roaming .....	133
8.5.3.1 Requirements for Roaming .....	135
8.5.4 Bridge / Repeater Example .....	136
8.5.5 Quality of Service .....	137
8.5.6 WMM QoS .....	137
8.5.6.1 WMM QoS Priorities .....	138
8.5.7 ATC .....	138
8.5.8 ATC+WMM .....	139
8.5.8.1 ATC+WMM from LAN to WLAN .....	139
8.5.8.2 ATC+WMM from WLAN to LAN .....	140
<b>Chapter 9</b>	
<b>SSID Screen.....</b>	<b>141</b>
9.1 Overview .....	141
9.2 What You Can Do in the SSID Screen .....	141
9.3 What You Need To Know .....	142
9.4 The SSID Screen .....	143
9.4.1 Configuring SSID .....	144
<b>Chapter 10</b>	
<b>Wireless Security Screen.....</b>	<b>147</b>

10.1 Overview .....	147
10.2 What You Can Do in the Security Screen .....	147
10.3 What You Need To Know .....	148
10.4 The Security Screen .....	150
10.4.1 Security: WEP .....	151
10.4.2 Security: 802.1x Only .....	153
10.4.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit .....	154
10.4.4 Security: WPA .....	155
10.4.5 Security: WPA2 or WPA2-MIX .....	156
10.4.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX .....	158
10.5 Technical Reference .....	159
<b>Chapter 11</b>	
<b>RADIUS Screen .....</b>	<b>161</b>
11.1 Overview .....	161
11.2 What You Can Do in the RADIUS Screen .....	161
11.3 What You Need To Know .....	162
11.4 The RADIUS Screen .....	163
<b>Chapter 12</b>	
<b>Layer-2 Isolation Screen .....</b>	<b>165</b>
12.1 Overview .....	165
12.2 What You Can Do in the Layer-2 Isolation Screen .....	166
12.3 What You Need To Know .....	166
12.4 The Layer-2 Isolation Screen .....	167
12.4.1 Configuring Layer-2 Isolation .....	167
12.5 Technical Reference .....	169
<b>Chapter 13</b>	
<b>MAC Filter Screen .....</b>	<b>171</b>
13.1 Overview .....	171
13.2 What You Can Do in the MAC Filter Screen .....	171
13.3 What You Should Know About MAC Filter .....	172
13.4 The MAC Filter Screen .....	172
13.4.1 Configuring the MAC Filter .....	173
<b>Chapter 14</b>	
<b>IP Screen .....</b>	<b>175</b>
14.1 Overview .....	175
14.2 What You Can Do in the IP Screen .....	175
14.3 What You Need To Know About IP .....	176
14.4 The IP Screen .....	176
14.5 Technical Reference .....	177

14.5.1 WAN IP Address Assignment .....	177
<b>Chapter 15</b>	
<b>Rogue AP Detection .....</b>	<b>179</b>
15.1 Overview .....	179
15.2 What You Can Do in the Rogue AP Screen .....	180
15.3 What You Need To Know .....	180
15.3.1 Configuration Screen .....	182
15.3.2 Friendly AP Screen .....	183
15.3.3 Rogue AP Screen .....	184
<b>Chapter 16</b>	
<b>Remote Management Screens.....</b>	<b>187</b>
16.1 Overview .....	187
16.2 What You Can Do in the Remote Management Screens .....	188
16.3 What You Need To Know .....	188
16.4 The Telnet Screen .....	190
16.5 The FTP Screen .....	191
16.6 The WWW Screen .....	192
16.7 The SNMP Screen .....	194
16.8 Technical Reference .....	195
16.8.1 MIB .....	195
16.8.2 Supported MIBs .....	196
16.8.3 SNMP Traps .....	196
<b>Chapter 17</b>	
<b>Internal RADIUS Server.....</b>	<b>199</b>
17.1 Overview .....	199
17.2 What You Can Do in the Internal Radius Server Screens .....	200
17.3 What You Need To Know .....	200
17.4 Internal RADIUS Server Setting Screen .....	200
17.5 The Trusted AP Screen .....	202
17.6 The Trusted Users Screen .....	204
17.7 Technical Reference .....	205
<b>Chapter 18</b>	
<b>Certificates .....</b>	<b>207</b>
18.1 Overview .....	207
18.2 What You Can Do in the Certificates Screen .....	207
18.3 What You Need To Know .....	208
18.4 My Certificates Screen .....	208
18.4.1 My Certificates Import Screen .....	210
18.4.2 My Certificates Create Screen .....	211



18.4.3 My Certificates Details Screen .....	214
18.5 Trusted CAs Screen .....	218
18.5.1 Trusted CAs Import Screen .....	219
18.5.2 Trusted CAs Details Screen .....	220
18.6 Technical Reference .....	223
18.6.1 Private-Public Certificates .....	224
18.6.2 Certification Authorities .....	224
18.6.3 Checking the Fingerprint of a Certificate on Your Computer .....	225
<b>Chapter 19</b>	
<b>Log Screens .....</b>	<b>227</b>
19.1 Overview .....	227
19.2 What You Can Do in the Log Screens .....	228
19.3 What You Need To Know .....	228
19.4 The View Log Screen .....	228
19.5 The Log Settings Screen .....	229
19.6 Technical Reference .....	232
19.6.1 Example Log Messages .....	232
19.6.2 Log Commands .....	233
19.6.3 Configuring What You Want the NWA to Log .....	233
19.6.4 Displaying Logs .....	234
19.6.5 Log Command Example .....	234
<b>Chapter 20</b>	
<b>VLAN .....</b>	<b>235</b>
20.1 Overview .....	235
20.2 What You Can Do in the VLAN Screen .....	235
20.3 What You Need To Know About VLAN .....	236
20.4 Wireless VLAN Screen .....	237
20.4.1 RADIUS VLAN Screen .....	239
20.5 Technical Reference .....	240
20.5.1 VLAN Tagging .....	240
20.5.2 Configuring Management VLAN Example .....	240
20.5.3 Configuring Microsoft's IAS Server Example .....	243
20.5.3.1 Configuring VLAN Groups .....	244
20.5.3.2 Configuring Remote Access Policies .....	245
20.5.4 Second Rx VLAN ID Example .....	253
20.5.4.1 Second Rx VLAN Setup Example .....	253
<b>Chapter 21</b>	
<b>Load Balancing .....</b>	<b>255</b>
21.1 Overview .....	255
21.1.1 What You Need to Know About Load Balancing .....	255

21.2 The Load Balancing Screen .....	257
21.2.1 Disassociating and Delaying Connections .....	258
<b>Chapter 22</b>	
<b>Dynamic Channel Selection.....</b>	<b>261</b>
22.1 Overview .....	261
22.2 The DCS Screen .....	262
<b>Chapter 23</b>	
<b>Maintenance .....</b>	<b>265</b>
23.1 Overview .....	265
23.2 What You Can Do in the Maintenance Screens .....	265
23.3 What You Need To Know About the Maintenance Screens .....	266
23.4 System Status Screen .....	266
23.4.1 System Statistics Screen .....	266
23.5 Association List Screen .....	268
23.6 Channel Usage Screen .....	269
23.7 F/W Upload Screen .....	270
23.8 Configuration Screen .....	272
23.8.1 Backup Configuration .....	272
23.8.2 Restore Configuration .....	273
23.8.3 Back to Factory Defaults .....	274
23.9 Restart Screen .....	274
<b>Part III: Troubleshooting and Specifications .....</b>	<b>277</b>
<b>Chapter 24</b>	
<b>Troubleshooting.....</b>	<b>279</b>
24.1 Power and Hardware Connections .....	279
24.2 NWA Access and Login .....	279
24.3 Internet Access .....	281
24.4 Wireless Router/AP Troubleshooting .....	283
<b>Chapter 25</b>	
<b>Product Specifications .....</b>	<b>285</b>
<b>Part IV: Appendices and Index .....</b>	<b>291</b>
Appendix A Setting Up Your Computer's IP Address .....	293
Appendix B Wireless LANs .....	319

Appendix C Pop-up Windows, JavaScripts and Java Permissions ..... 335

Appendix D Importing Certificates ..... 343

Appendix E IP Addresses and Subnetting ..... 369

Appendix F Text File Based Auto Configuration ..... 379

Appendix G Legal Information ..... 387

**Index..... 391**



---

# PART I

# Introduction

---

Introducing the NWA (23)

Introducing the Web Configurator (35)

Status Screens (39)

Management Mode (47)

Tutorial (67)



# Introducing the NWA

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

It is highly versatile, supporting multiple BSSIDs simultaneously. The Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

Multiple security profiles allow you to easily assign different types of security to groups of users. The NWA controls network access with MAC address filtering, rogue AP detection, layer 2 isolation and an internal authentication server. It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access (WPA), WPA2 and WEP data encryption.

At the time of writing, this guide covers the following models.

**Table 2** Models Covered

NWA-3500
NWA-3550

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:

- Access Point (AP)
- Bridge/Repeater
- AP+Bridge
- MBSSID

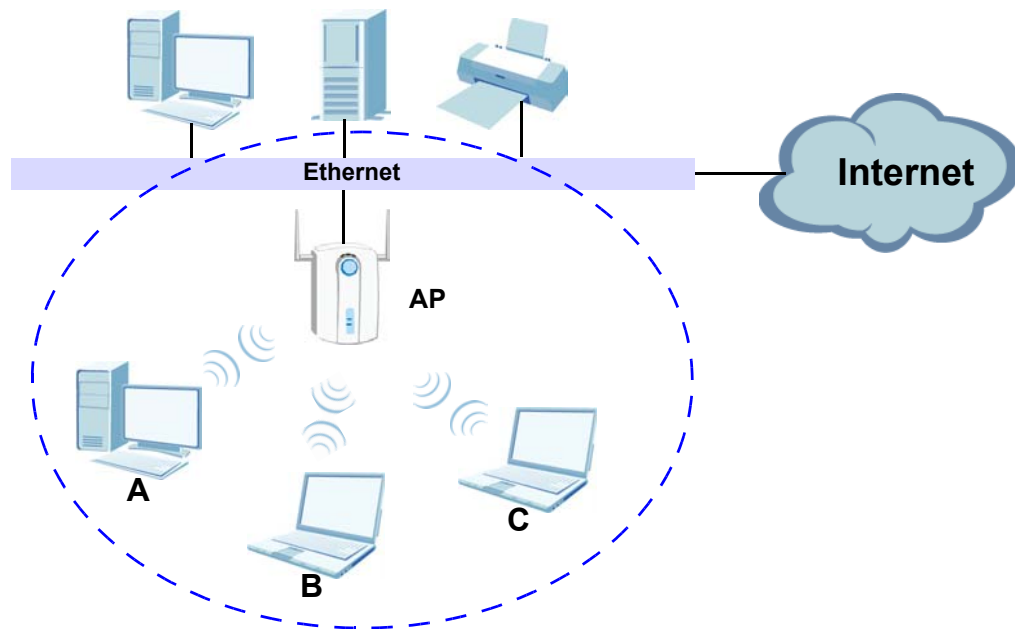
Applications for each operating mode are shown below.

Note: A different channel should be configured for each WLAN interface to reduce the effects of radio interference.

## 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. Clients **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**) has no Ethernet connection. When the NWA is in bridge mode, you should enable STP to prevent bridge loops.

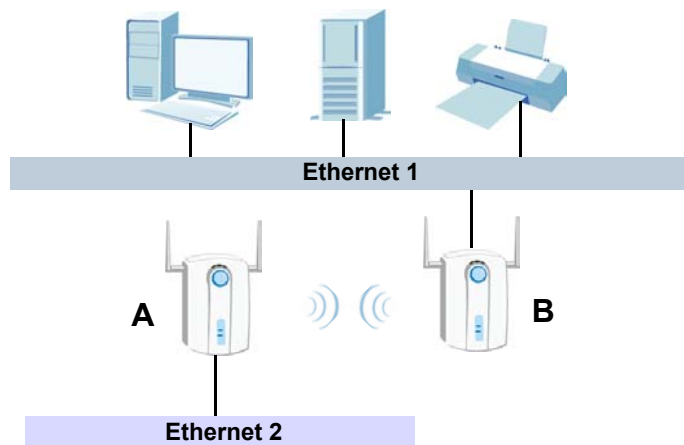


When the NWA is in **Bridge / Repeater** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See [Section 8.4.2 on page 126](#) for more details.

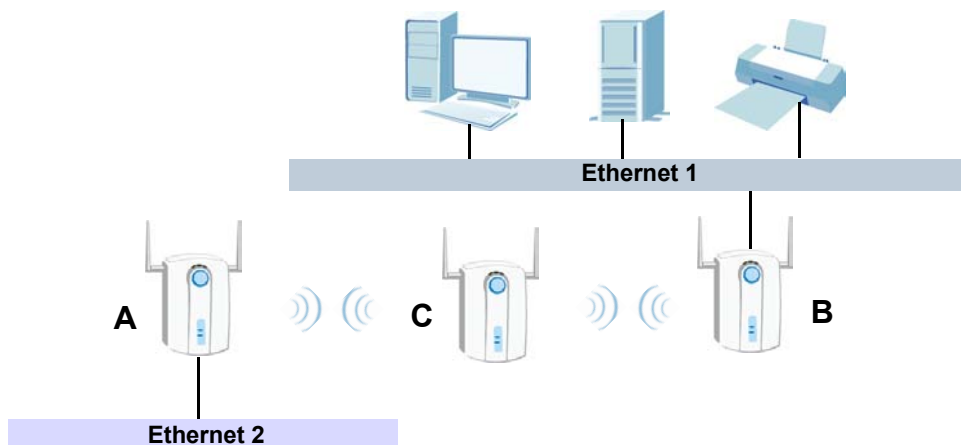
Once the security settings of peer sides match one another, the connection between devices is made.

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

**Figure 2** Bridge Application



**Figure 3** Repeater Application



### 1.2.3 AP + Bridge

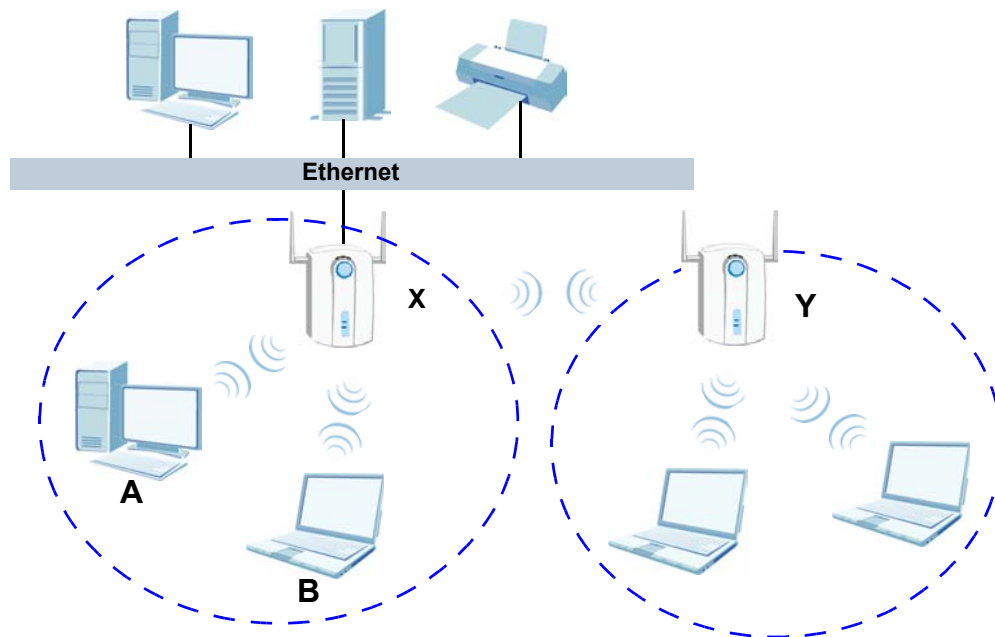
In **AP+Bridge** mode, the NWA supports both AP and bridge connection at the same time.

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.

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 8.4.3 on page 129](#) for more details.

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

**Figure 4** AP+Bridge Application



## 1.2.4 MBSSID

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

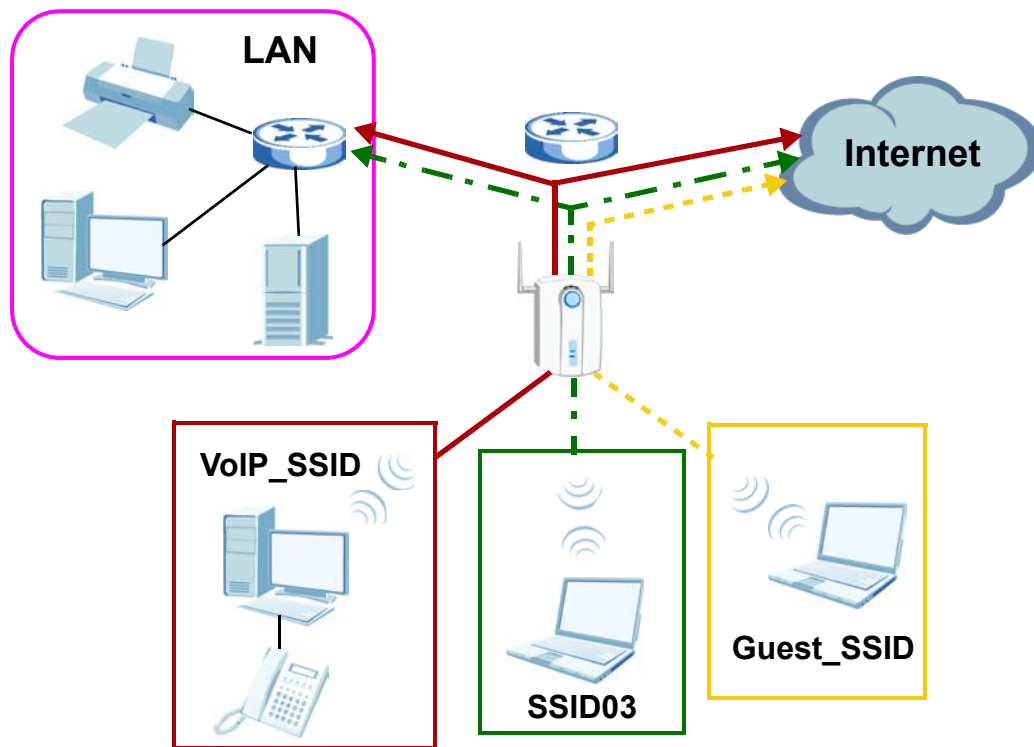
You can configure up to sixteen SSID profiles, and have up to eight active at any one time.

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 (Voice over IP, or 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 Quality of Service (QoS) priority, **SSID03** 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 LAN behind the AP and can access only the Internet.

**Figure 5** Multiple BSSs



## 1.2.5 Pre-Configured SSID Profiles

The NWA has two pre-configured SSID profiles.

- 1 **VoIP\_SSID.** This profile is intended for use by wireless clients requiring the highest QoS (Quality of Service) level for VoIP (Voice over IP) telephony and other applications requiring low latency. The QoS level of this profile is not user-configurable. See [Chapter 8 on page 119](#) for more information on QoS.

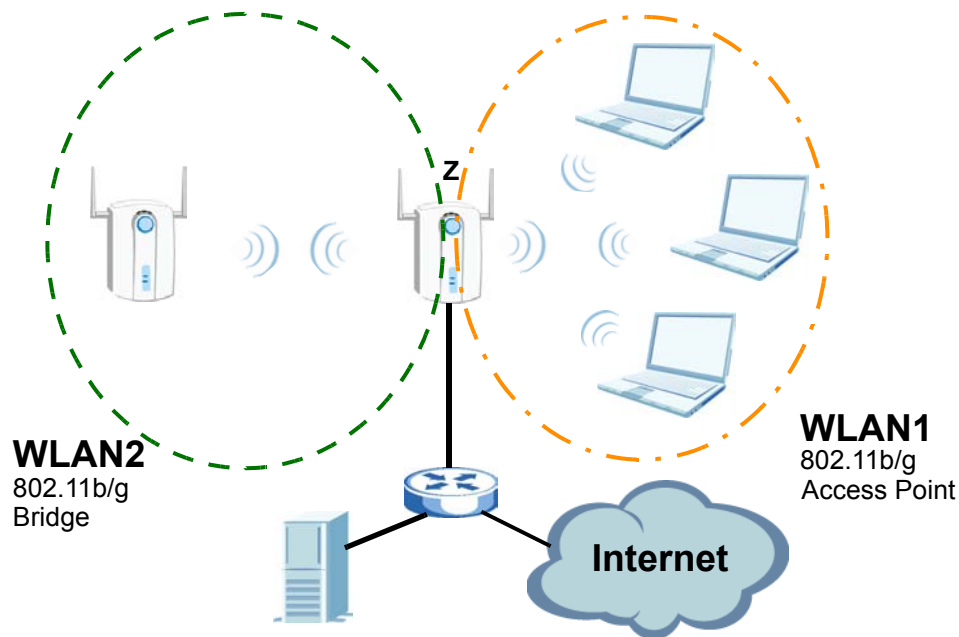
- 2 **Guest\_SSID**. This profile is intended for use by visitors and others who require access to certain resources on the network (an Internet gateway or a network printer, for example) but must not have access to the rest of the network. Layer 2 isolation is enabled (see [Section on page 166](#)), and QoS is set to **NONE**. Intra-BSS traffic blocking is also enabled (see [Section 9.4.1 on page 144](#)). These fields are all user-configurable.

## 1.2.6 Configuring Dual WLAN Adaptors

The NWA is equipped with dual wireless adaptors. This means you can configure two different wireless networks to operate simultaneously.

In the following example, the NWA (**Z**) uses **WLAN1** in **Access Point** mode to allow IEEE 802.11b and IEEE 802.11g clients to access the wired network, and **WLAN2** in **AP+Bridge** mode to allow an IEEE 802.11a AP to communicate with the wired network.

**Figure 6** Dual WLAN Adaptors Example



## 1.3 CAPWAP

The NWA supports CAPWAP (Control And Provisioning of Wireless Access Points). This is ZyXEL's implementation of the IETF's (Internet Engineering Task Force) CAPWAP protocol.

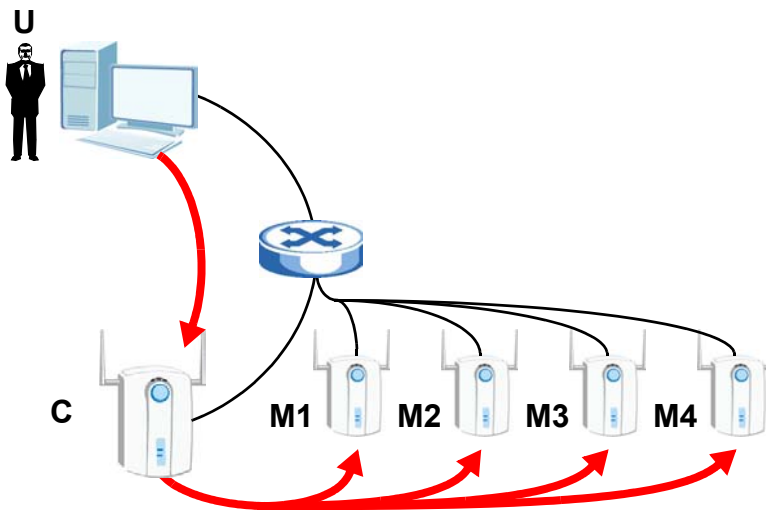
ZyXEL's CAPWAP allows a single access point to manage up to eight other access points. The managed APs receive all their configuration information from the controller AP. The CAPWAP dataflow is protected by DTLS (Datagram Transport Layer Security).

At the time of writing, the following ZyXEL AP models can be CAPWAP managed APs:

- NWA-3160
- NWA-3163
- NWA-3500
- NWA-3550
- NWA-8500

The following figure illustrates a CAPWAP wireless network. The user (**U**) configures the controller AP (**C**), which then automatically updates the configurations of the managed APs (**M1 ~ M4**).

**Figure 7** CAPWAP Network Example



## 1.4 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.

- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device. Use Telnet to access the SMT.
- FTP. File Transfer Protocol for firmware upgrades and configuration backup and restore.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter ([Section 16.7 on page 194](#)) in this User's Guide.

## 1.5 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.

### 1.5.1 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 7 on page 109](#) for instructions on changing your password and setting the timeout period.

- Configure remote management to control who can manage your NWA. See [Chapter 16 on page 187](#) 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.

### 1.5.2 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 10.4 on page 150](#) 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 9.4.1 on page 144](#) 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 Note: on page 174](#) for directions on configuring the MAC filter.

## 1.6 Maintaining Your NWA

Do the following things regularly to keep your NWA running.

- Check the ZyXEL website ([www.zyxel.com.tw](http://www.zyxel.com.tw)) regularly for new firmware for your NWA. Ensure you download the correct firmware for your model.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NWA to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NWA. You could simply restore your last configuration.

## 1.7 Hardware Connections

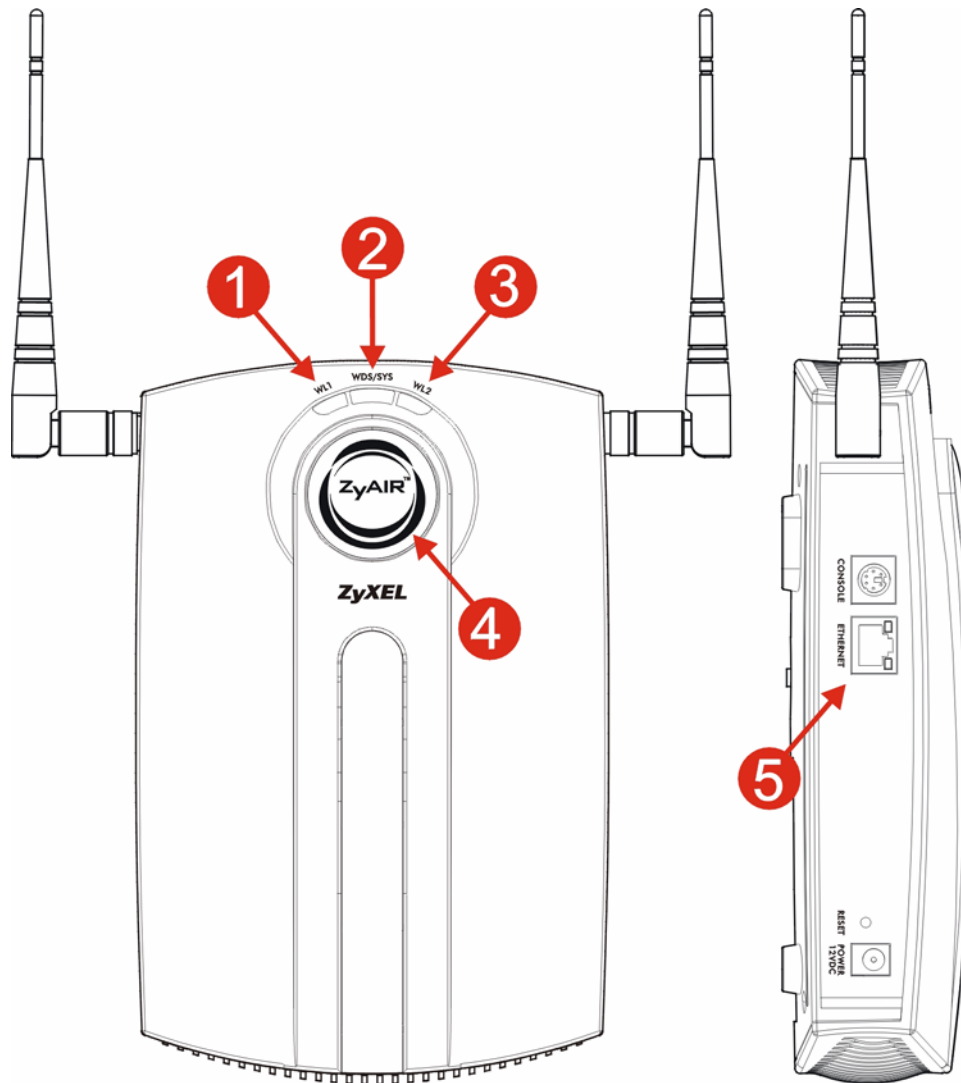
See your Quick Start Guide for information on making hardware connections.

Note: Your NWA has two wireless LAN adaptors, WLAN1 and WLAN2. WLAN1 uses the **RF1** antenna or the antenna on the right (when facing the device) and WLAN2 uses the **RF2** antenna or the antenna on the left. If you connect only one antenna, you can use only the associated wireless LAN adaptor.

## 1.8 LEDs

This section applies to the NWA-3500 only.

**Figure 8** LEDs



**Table 3** LEDs

LABEL	LED	COLOR	STATUS	DESCRIPTION
1	WL1	Green	On	The wireless adaptor WLAN1 is active.
			Blinking	The wireless adaptor WLAN1 is active, and transmitting or receiving data.
			Off	The wireless adaptor WLAN1 is not active.



**Table 3** LEDs (continued)

LABEL	LED	COLOR	STATUS	DESCRIPTION
2	WDS/SYS	Green	On	The NWA is in AP + Bridge or Bridge/ Repeater mode, and has successfully established a Wireless Distribution System (WDS) connection.
		Red	Flashing	The NWA is starting up.
			Off	Either The NWA is in Access Point or MBSSID mode and is functioning normally. The NWA is in AP + Bridge or Bridge/ Repeater mode and has not established a Wireless Distribution System (WDS) connection. or The NWA is not receiving power.
3	WL2	Green	On	The wireless adaptor WLAN2 is active.
			Blinking	The wireless adaptor WLAN2 is active, and transmitting or receiving data.
			Off	The wireless adaptor WLAN2 is not active.
4	ZyAIR	Blue	On	The NWA is receiving power. You can turn the ZyAIR LED off and on using the Web configurator. See <a href="#">Section 8.4 on page 123</a> .
			Blinking	The NWA is receiving power and transmitting data to or receiving data from its wireless stations.
			Off	Either The NWA is not receiving power. or The ZyAIR LED has been disabled. See <a href="#">Section 8.4 on page 123</a> for how to enable the ZyAIR LED.
5	ETHERNET	Green	On	The NWA has a 10 Mbps Ethernet connection.
			Blinking	The NWA has a 10 Mbps Ethernet connection and is sending or receiving data.
		Yellow	On	The NWA has a 100 Mbps Ethernet connection.
			Blinking	The NWA has a 100 Mbps Ethernet connection and is sending/receiving data.
			Off	The NWA does not have an Ethernet connection.



# Introducing the Web Configurator

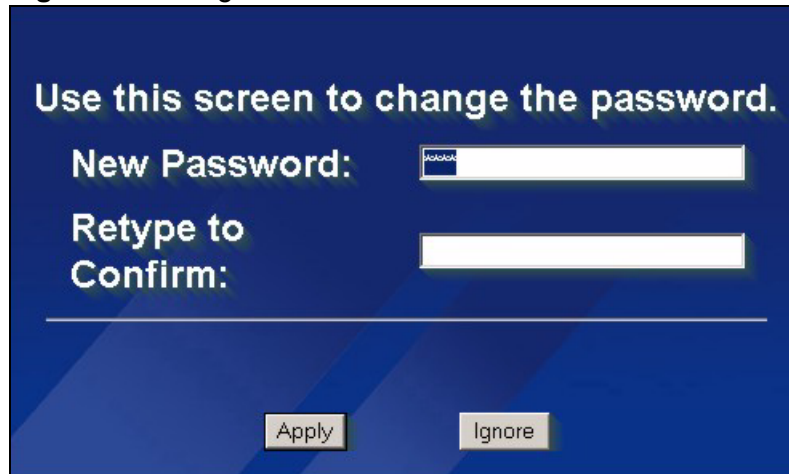
This chapter describes how to access the NWA's web configurator and provides an overview of its screens.

## 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).
- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, 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 9** Change Password Screen



The screenshot shows a dark blue web interface for changing a password. At the top, it says "Use this screen to change the password." Below this, there are two input fields: "New Password:" and "Retype to Confirm:". The "New Password:" field has a small "Password" label on its left. At the bottom of the screen, there are two buttons: "Apply" and "Ignore".

- 6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your NWA's MAC address that will be specific to this device.

**Figure 10** Replace Certificate Screen



The screenshot shows a dark blue web interface titled "Replace Factory Default Certificate". The main text reads: "The factory default certificate is common to all NWA models. Click Apply to create a certificate using your NWA's MAC address that will be specific to this device." At the bottom of the screen, there are two buttons: "Apply" and "Ignore".

You should now see the **Status** screen. See [Chapter 2 on page 35](#) 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

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.

### 2.2.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in the following 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. This applies to the NWA-3500 only.
- Use the web configurator to restore defaults (refer to [Section 23.8.3 on page 274](#)).
- Transfer the configuration file to your NWA using FTP. See the section on SMT configuration for more information.

## 2.3 Navigating the Web Configurator

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

Note: The **Status** screen shown in this section applies to the Standalone AP management mode only.

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

- 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 11** The Status Screen of the Web Configurator

The screenshot displays the ZyXEL Web Configurator Status page. On the left is a navigation menu with options: STATUS, MGNT MODE, SYSTEM, WIRELESS, IP, ROGUE AP, REMOTE MGNT, AUTH. SERVER, CERTIFICATES, LOGS, VLAN, LOAD BALANCING, DCS, MAINTENANCE, and LOGOUT. The main content area is titled 'STATUS' and includes an 'Automatic Refresh Interval' dropdown set to 'None' and a 'Refresh' button. Below this are four sections: 'System Information' (listing details like System Name, Model, Firmware Version, System UP Time, Current Date Time, WLAN1/2 Operating Mode, Management VLAN, IP, LAN MAC, WLAN1/2 MAC), 'System Resources' (with progress bars for Flash, Memory, CPU, WLAN1/2 Associations), 'Interface Status' (a table showing LAN, WLAN1, and WLAN2 status and rates), and 'SSID Status' (a table showing WLAN1 and WLAN2 SSIDs, BSSIDs, Security, and VLAN settings). At the bottom, there are buttons for 'Show Statistics', 'Association List', 'Channel Usage', 'LOGS', and 'Rogue AP List'. A red status bar at the very bottom reads 'Status: Ready'.

- Click the links on the left of the screen to configure advanced features such as **MGNT MODE** (AP Controller, Standalone AP or Managed AP), **SYSTEM** (General, Password and Time Setting), **WIRELESS** (Wireless, SSID, Security, RADIUS, Layer-2 Isolation, MAC Filter), **IP**, **ROGUE AP** (Configuration, Friendly AP, Rogue AP), **REMOTE MGNT** (Telnet, FTP, WWW and SNMP), **AUTH. SERVER** (Setting, Trusted AP, Trusted Users), **CERTIFICATES** (My Certificates, Trusted CAs), **LOGS** (View Log and Log Settings), **VLAN** (Wireless VLAN and RADIUS VLAN), **LOAD BALANCING** and **DCS**.
- Click **MAINTENANCE** to view information about your NWA or upgrade configuration and firmware files. Maintenance features include **Status** (Statistics), **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore and Default) and **Restart**.

# Status Screens

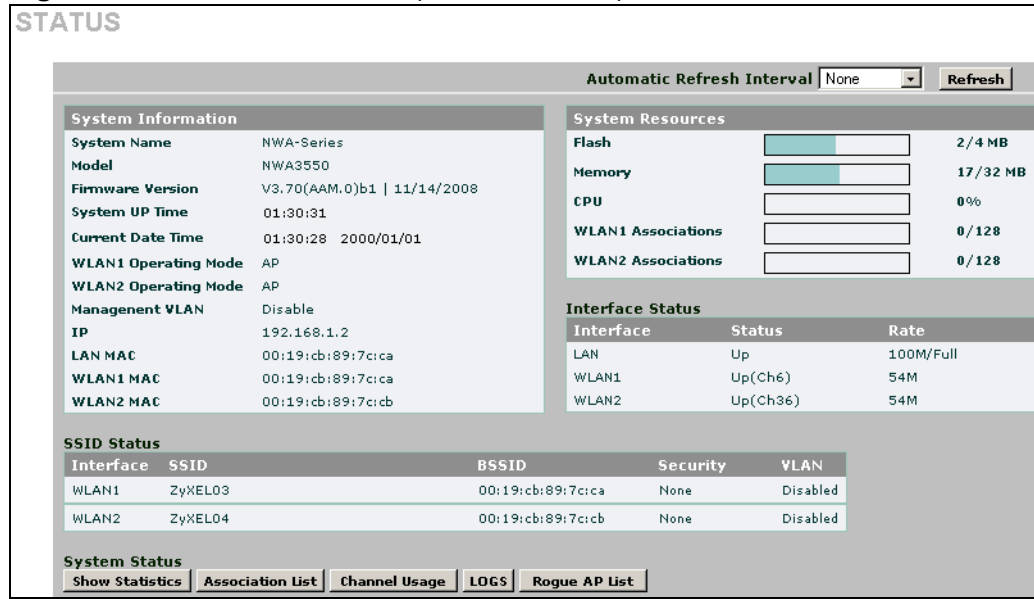
The **Status** screen displays when you log into the NWA, or click **STATUS** in the navigation menu.

Use the **Status** screens to look at the current status of the device, system resources, interfaces and SSID status. The **Status** screen also provides detailed information about associated wireless clients, channel usage, logs and detected rogue APs.

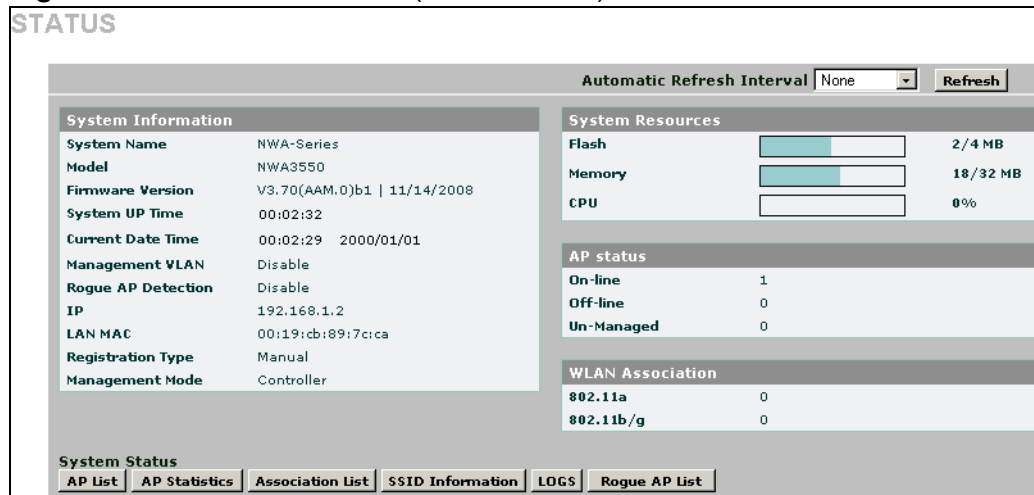
## 3.1 The Status Screen

Click **Status**. The following screen displays. The **Status** screen varies slightly depending on the NWA's management mode you configured in the **MGMT MODE** screen. The NWA works as a standalone AP by default.

**Figure 12** The Status Screen (Standalone AP)



**Figure 13** The Status Screen (AP Controller)



The following table describes the labels in this screen.

**Table 4** The Status Screen

LABEL	DESCRIPTION
Automatic Refresh Interval	Enter how often you want the NWA to update this screen.
Refresh	Click this to update this screen immediately.



**Table 4** The Status Screen

LABEL	DESCRIPTION
System Information	
System Name	This field displays the NWA system name. It is used for identification. You can change this in the <b>System &gt; General</b> screen's <b>System Name</b> field.
Model	This field displays the NWA's exact model name.
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 <b>Maintenance &gt; F/W Upload</b> .
System Up Time	This field displays the elapsed time since the NWA was turned on.
Current Date Time	This field displays the date and time configured on the NWA. You can change this in the <b>System &gt; Time Setting</b> screen.
WLAN1 Operating Mode	This field is not available when the NWA is in AP controller management mode.  This field displays the current operating mode of the first wireless module ( <b>AP, Bridge / Repeater, AP + Bridge</b> or <b>MBSSID</b> ). You can change the operating mode in the <b>Wireless &gt; Wireless</b> screen.
WLAN2 Operating Mode	This field is not available when the NWA is in AP controller management mode.  This field displays the current operating mode of the second wireless module ( <b>AP, Bridge / Repeater, AP + Bridge</b> or <b>MBSSID</b> ). You can change the operating mode in the <b>Wireless &gt; Wireless</b> screen.
Management VLAN	This field displays the management VLAN ID if VLAN is active, or <b>Disabled</b> if it is not active. You can enable or disable VLAN, or change the management VLAN ID, in the <b>VLAN &gt; Wireless VLAN</b> screen.
Rogue AP Detection	This field is available only when the NWA is in AP controller management mode.  This field displays whether rogue AP detection is turned on ( <b>Enable</b> ) or not ( <b>Disable</b> ).
IP	This field displays the current IP address of the NWA on the network.
LAN MAC	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. Your NWA features dual wireless module, and has two MAC addresses. The MAC address of the first wireless module ( <b>WLAN1</b> ) is used on the LAN.
WLAN1 MAC	This field is not available when the NWA is in AP controller management mode.  This displays the MAC address of the first wireless module.
WLAN2 MAC	This field is not available when the NWA is in AP controller management mode.  This displays the MAC address of the second wireless module.

**Table 4** The Status Screen

LABEL	DESCRIPTION
Registration Type	This field is available only when the NWA is in AP controller management mode.  This displays <b>Manual</b> when an access point in managed AP mode needs to register to the NWA manually or <b>Always Accept</b> when the NWA automatically adds any detected access point in managed AP mode to the managed AP list.
Management Mode	This field is available only when the NWA is in AP controller management mode.  This displays <b>Controller</b> when the NWA is in AP controller management mode.
System Resources	
Flash	This field displays the amount of the NWA's flash memory currently in use. The flash memory is used to store firmware and SSID profiles.
Memory	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.
CPU	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.
WLAN1 Associations	This field is not available when the NWA is in AP controller management mode.  This field displays the number of wireless clients currently associated with the first wireless module. Each wireless module supports up to 128 concurrent associations.
WLAN2 Associations	This field is not available when the NWA is in AP controller management mode.  This field displays the number of wireless clients currently associated with the second wireless module. Each wireless module supports up to 128 concurrent associations.
Interface Status	This section is not available when the NWA is in AP controller management mode.
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 <b>Up</b> when the NWA is using the interface and <b>Down</b> when the NWA is not using the interface.
Rate	For the LAN port this displays the port speed and duplex setting.  For the WLAN1 and WLAN2 interfaces, it displays the downstream and upstream transmission rate or <b>N/A</b> if the interface is not in use.
SSID Status	This section is not available when the NWA is in AP controller management mode.
Interface	This column displays each of the NWA's wireless interfaces, <b>WLAN1</b> and <b>WLAN2</b> .

**Table 4** The Status Screen

LABEL	DESCRIPTION
SSID	This field displays the SSID(s) currently used by each wireless module.
BSSID	This field displays the MAC address of the wireless adaptor.
Security	This field displays the type of wireless security used by each SSID.
VLAN	This field displays the VLAN ID of each SSID in use, or <b>Disabled</b> if the SSID does not use VLAN.
AP status	This section is available only when the NWA is in AP controller management mode.
On-line	This field displays how many APs (including the NWA) in the managed AP list are active.
Off-line	This field displays how many APs (including the NWA) in the managed AP list are inactive.
Un-Managed	This field displays how many APs (in managed AP mode) are detected but in the un-managed AP list.
WLAN Association	This section is available only when the NWA is in AP controller management mode.
802.11a	This field displays how many IEEE 802.11a wireless clients connect to the NWA.
802.11b/g	This field displays how many IEEE 802.11b/g wireless clients connect to the NWA.
Redundancy	This section is available only when the NWA is in AP controller management mode. The redundancy feature should be also enabled and the NWA acts as the regular AP controller.
Redundancy Device	This field displays the IP address of the backup AP controller.
Last Synchronization Result	This field displays whether the last synchronization with the backup AP controller is successful ( <b>ENABLED</b> ) or failed ( <b>DISABLED</b> ).
Last Synchronization Time	This field displays the last date and time when the NWA synchronized with the backup AP controller.
Alive Status	This field displays the result ( <b>NO RESPONSE</b> or )when querying for the backup AP controller status.
System Status	
AP List	This link is available only when the NWA is in AP controller management mode.  Click this link to view the MAC address, wireless settings and the number of the connected wireless clients for each wireless module on the AP(s) managed by the NWA.
AP Statistics	This link is available only when the NWA is in AP controller management mode.  Click this link to view wireless mode, channel ID number and packet specific statistics on the AP(s) managed by the NWA.

**Table 4** The Status Screen

LABEL	DESCRIPTION
Show Statistics	This link is not available when the NWA is in AP controller management mode.  Click this link to view port status and packet specific statistics. See <a href="#">Section 23.4.1 on page 266</a> .
Association List	Click this to see a list of wireless clients currently associated to each of the NWA's wireless modules. See <a href="#">Section 23.5 on page 268</a> .
Channel Usage	This link is not available when the NWA is in AP controller management mode.  Click this to see which wireless channels are currently in use in the local area. See <a href="#">Section 23.6 on page 269</a> .
SSID Information	This link is available only when the NWA is in AP controller management mode.  Click this link to view the security mode and the number of the connected wireless clients for the active SSID(s) on the NWA.
Logs	Click this to see a list of logs produced by the NWA. See <a href="#">Section 19.6 on page 232</a> .
Rogue AP List	Click this to see a list of unauthorized access points in the local area. See <a href="#">Section 15.3.3 on page 184</a> .

### 3.1.1 AP List

Click the **AP List** link the **Status** screen when the NWA is in AP controller management mode.

**Figure 14** Status > AP List

AP Description	Model	Radio MAC	802.11 Mode	Channel ID	SSID List	VLAN	Stations
AP-LOCAL	NWA3550	00:19:CB:89:7C:CA	802.11b/g	6	ZyXEL03 (00:19:CB:89:7C:CA)	-	0
		00:19:CB:89:7C:CB	802.11b/g	6	ZyXEL03 (00:19:CB:89:7C:CB)	-	0
AP-001349DF42A8	NWA-3500	00:13:49:DF:42:A8	802.11b/g	6	ZyXEL03 (00:13:49:DF:42:A8)	-	0
		00:13:49:DF:42:A9	-	-	-	-	-

Refresh

The following table describes the labels in this screen.

**Table 5** Status > AP List

LABEL	DESCRIPTION
AP Description	This is the descriptive name configured for this AP in the <b>Controller &gt; AP List</b> .
Model	This is the model name of the AP.
Radio MAC	This is the MAC address of each wireless module.
802.11 Mode	This is the wireless standard supported by each wireless module on the AP.

**Table 5** Status > AP List

LABEL	DESCRIPTION
Channel ID	This is the channel ID number used by each wireless module on the AP.
SSID List	This is the SSID(s) currently used by each wireless module.
VLAN	This is the VLAN ID of each SSID in use. It shows - if the SSID does not use VLAN.
Stations	This is the number of the wireless clients currently associated to each wireless module.
Refresh	Click this button to update the screen statistics immediately.

### 3.1.2 AP Statistics

Click the **AP Statistics** link the **Status** screen when the NWA is in AP controller management mode.

**Figure 15** Status > AP Statistics

AP Description	802.11 Mode	Channel ID	Rx PKT	Tx PKT	Rx FCS Error Count	Tx Retry Count
AP-LOCAL	802.11b/g	6	1528	2220	1708 (53%)	0 (0%)
	802.11b/g	6	3152	2222	3922 (56%)	17 (0%)
AP-001349DF42A8	802.11b/g	6	6144	3618	3058 (33%)	65 (1%)
	-	-	-	-	-	-

Automatic Refresh Interval  Refresh Reset

The following table describes the labels in this screen.

**Table 6** Status > AP Statistics

LABEL	DESCRIPTION
AP Description	This is the descriptive name configured for this AP in the <b>Controller &gt; AP Lists</b> .
802.11 Mode	This is the wireless standard supported by each wireless module on the AP.
Channel ID	This is the channel ID number used by each wireless module on the AP.
Rx PKT	This is the number of received packets on this AP.
Tx PKT	This is the number of transmitted packets on this port.
Rx FCS Error Count	This is the number of received packets with the Frame Check Sequence (FCS) error(s).
Tx Retry Count	This is the number of times for the NWA to resend the packets
Automatic Refresh Interval	Select a number of seconds or <b>None</b> from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen statistics immediately.
Reset	

### 3.1.3 SSID Information

Click the **SSID Information** link the **Status** screen when the NWA is in AP controller management mode.

**Figure 16** Status > SSID Information

SSID	Security Mode	Stations
ZyXEL03	No Security	0
ZyXEL02	No Security	0
ZyXEL04	No Security	0

The following table describes the labels in this screen.

**Table 7** Status > SSID Information

LABEL	DESCRIPTION
SSID	
Security Mode	This is the wireless security mode used by each SSID.
Stations	This is the number of the wireless clients currently associated to each SSID.

# Management Mode

This chapter discusses the **MGNT MODE** (Management Mode) screen. This screen determines whether the NWA is used in its default standalone AP mode or as part of a CAPWAP (Control And Provisioning of Wireless Access Points) network.

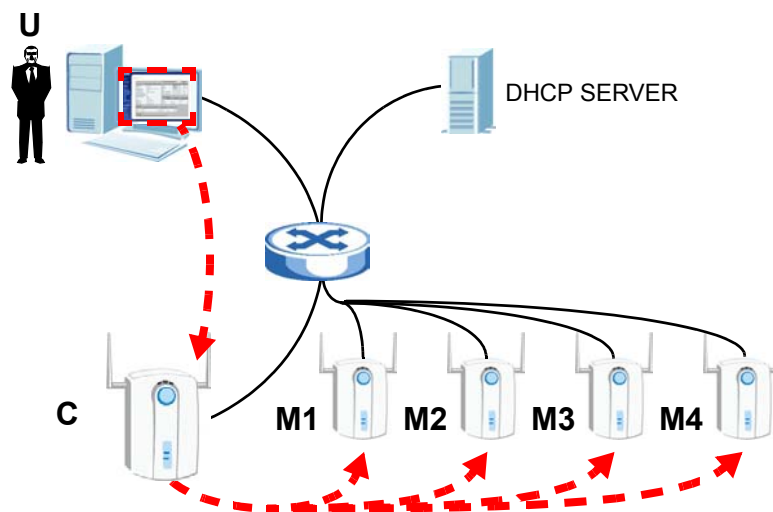
## 4.1 About CAPWAP

The NWA supports CAPWAP (Control And Provisioning of Wireless Access Points). This is ZyXEL's implementation of the IETF's (Internet Engineering Task Force) CAPWAP protocol (RFC 4118).

The CAPWAP dataflow is protected by DTLS (Datagram Transport Layer Security).

The following figure illustrates a CAPWAP wireless network. You (**U**) configure the AP controller (**C**), which then automatically updates the configurations of the managed APs (**M1 ~ M4**).

**Figure 17** CAPWAP Network Example



Note: The NWA can be a standalone AP (default) or a CAPWAP controller AP or a CAPWAP managed AP.

## 4.1.1 CAPWAP Discovery and Management

The link between CAPWAP-enabled access points proceeds as follows:

- 1 An AP in managed AP mode joins a wired network (receives a dynamic IP address).
- 2 The AP sends out a management request, looking for an AP in CAPWAP AP controller mode.
- 3 If there is an AP controller on the network, it receives the management request.

## 4.1.2 CAPWAP and DHCP

CAPWAP managed APs must be DHCP clients, supplied with an IP address by a DHCP server on your network.

Furthermore, the AP controller must have a static IP address; it cannot be a DHCP client.

## 4.1.3 CAPWAP and IP Subnets

By default, CAPWAP works only between devices with IP addresses in the same subnet (see the appendices for information on IP addresses and subnetting).

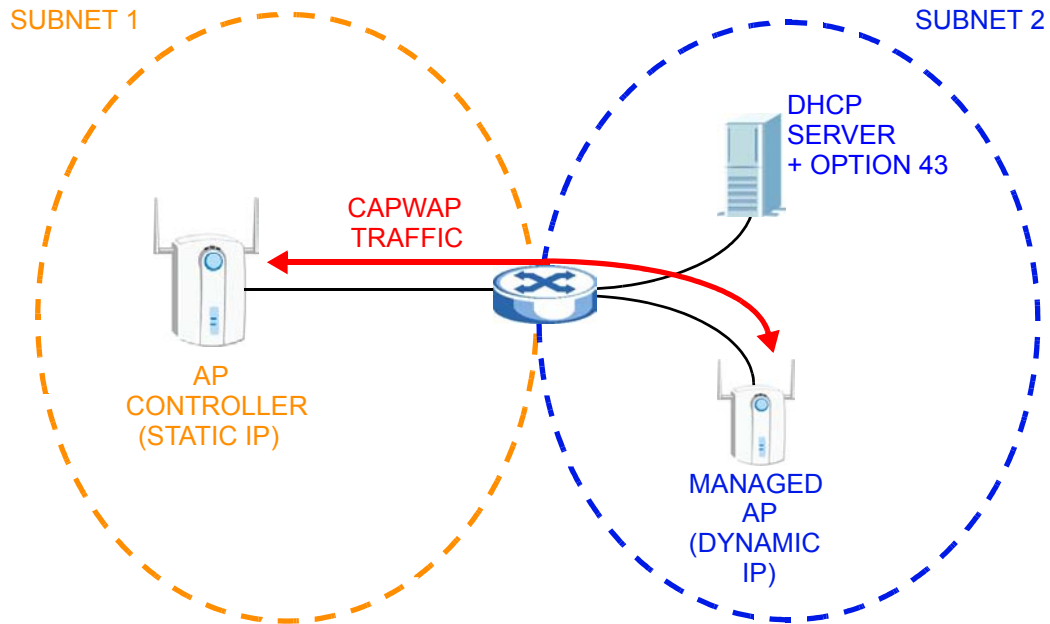
However, you can configure CAPWAP to operate between devices with IP addresses in different subnets by doing the following.

- Activate DHCP option 43 on your network's DHCP server.
- Configure DHCP option 43 with the IP address of the CAPWAP AP controller on your network.



DHCP Option 43 allows the CAPWAP management request (from the AP in managed AP mode) to reach the AP controller in a different subnet, as shown in the following figure.

**Figure 18** CAPWAP and DHCP Option 43



#### 4.1.4 Notes on CAPWAP

This section lists some additional features of ZyXEL's implementation of the CAPWAP protocol.

- When the AP controller uses its internal RADIUS server, managed APs also use the AP controller's authentication server to authenticate wireless clients.
- Only one AP controller can exist in any single broadcast domain.
- If a managed AP's link to the AP controller is broken, the managed AP continues to use the wireless settings with which it was last provided.

## 4.2 The Management Mode Screen

Use this screen to configure the NWA as a CAPWAP controller AP or CAPWAP managed AP or to use it in its default standalone mode.

Click **MGNT MODE** in the NWA's navigation menu. The following screen displays.

**Figure 19** The Management Mode Screen

The following table describes the labels in this screen.

**Table 8** The Management Mode Screen

LABEL	DESCRIPTION
AP Controller	Select this to manage other APs (in Managed AP mode) via this NWA. As of writing, the NWA can manage other ZyXEL APs only.  When you select this and click <b>Apply</b> , you are logged out of the Web Configurator and have to log in again. The screens vary from the default standalone mode to include the controller AP menus.
Standalone AP	Select this to manage the NWA using its own web configurator, neither managing nor managed by other devices.
Managed AP	Select this to have the NWA managed by another NWA on your network.  When you do this, the NWA can be configured <b>ONLY</b> by the management AP.  If you do not have an AP controller on your network and want to return the NWA to standalone mode, you must use its physical <b>RESET</b> button (NWA-3500 only). All settings are returned to their default values.  <b>Note:</b> When you set the NWA to Managed AP mode, it becomes a DHCP client. To discover its new IP address, check the DHCP server on your network. If your network has no DHCP server, the NWA's IP address remains the same. You can also check the <b>Controller &gt; AP Lists</b> screen of the AP controller on your network.
Auto AP Controller IP (DCHP Server Option 43 setting required)	Check this is you want to send a request (to be managed) to any AP controller within broadcast range.

**Table 8** The Management Mode Screen

LABEL	DESCRIPTION
Manual AP Controller IP	<p>Check this is you know the IP address of the controller AP that you want to manage this AP.</p> <ul style="list-style-type: none"><li>• <b>Primary AP Controller IP</b> - Enter the IP address of the primary controller AP.</li><li>• <b>Secondary AP Controller IP</b> - Enter the IP address of the secondary controller AP.</li></ul>
Apply	<p>Click this to save your changes.</p> <p><b>Note:</b> If you change the mode in this screen, the NWA restarts. Wait a short while before you attempt to log in again. If you changed the mode to <b>Managed AP</b>, you cannot log in as the web configurator is disabled; you must manage the NWA through the management AP on your network.</p>
Reset	Click this to return this screen to its previously-saved settings.



# Controller AP Mode

## 5.1 Overview

This chapter discusses the **Controller AP** management mode. When the NWA is used as a CAPWAP (Control And Provisioning of Wireless Access Points) controller AP, the Web Configurator changes to reflect this by including the **Controller** and **Profile Edit** screens.

Refer to [Section 4.1 on page 47](#) for more information on CAPWAP.

### 5.1.1 What You Can Do in AP Controller Mode

- Use the **Navigation Menu** ([Section 5.2 on page 54](#)) to manage settings across all connected APs.
- Use the **Status** screen ([Section 5.3 on page 55](#)) to view information about your managed wireless network.
- Use the **AP Lists** screen ([Section 5.4 on page 57](#)) to manage connected APs.
- Use the **Configuration** screen ([Section 5.5 on page 60](#)) to control the way in which the NWA accepts new APs to manage.
- Use the **Redundancy** screen ([Section 5.6 on page 61](#)) to set the controller AP as a primary or secondary controller.
- Use the **Profile Edit** screens ([Section 5.7 on page 62](#)) to edit an individual AP's Radio, SSID, Security, RADIUS, Layer-2 Isolation, and MAC Address settings.

### 5.1.2 What You Need to Know

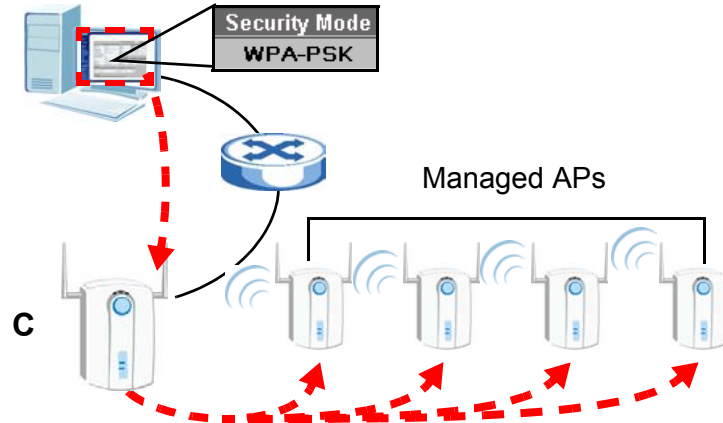
The following terms and concepts may help as you read through this chapter.

#### Controller AP Mode

Your NWA can be a CAPWAP controller AP. In this setup, the NWA can manage the wireless configurations and device settings of several APs at the same time.

In the figure below, an administrator is able to manage the security settings of 5 APs (1 controller AP and 4 managed APs). He changes the security mode to WPA-PSK just by accessing the Web Configurator of the controller AP (C).

**Figure 20** CAPWAP Controller



Note: Be careful when configuring the controller AP as its managed APs automatically inherit some of its settings. Moreover, some of these changes will automatically disconnect the wireless clients of the managed APs.

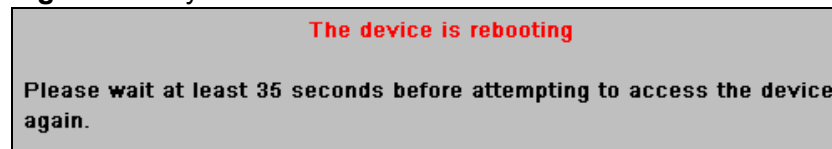
### 5.1.3 Before You Begin

Note: The **Controller AP** options are only available when the NWA is set to function in this mode. Therefore, ensure that you have switched modes first as described in [Section 4.2 on page 49](#) before continuing.

## 5.2 Controller AP Navigation Menu

When you choose **Controller AP** mode in the **MGNT MODE** screen and click **Apply**, you are automatically logged off from the Web Configurator. The NWA reboots and shows the following message.

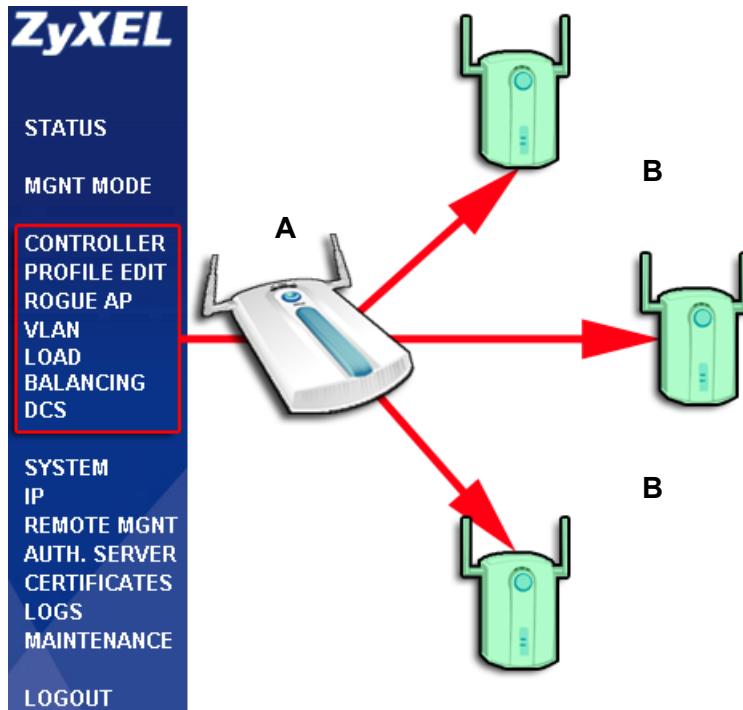
**Figure 21** System Restart



Note: The NWA reboots every time you change mode in the **MGNT MODE** screen. You can switch from **Standalone AP** to **Controller AP** (and vice versa) using the Web Configurator.

After logging in again, the navigation menu changes to include links for the **Controller** and **Profile Edit** screens. The items marked below are screens that can be configured for all APs managed by the NWA.

**Figure 22** Controller AP Navigation Links



In the figure above, changes made in the highlighted screens of the Controller AP (A) are automatically applied to all the Managed APs (B).

Note: A managed AP may potentially be turned off if it is within range of its controller AP while the controller AP updates its settings. The managed AP retains the last settings acquired from the controller AP and is automatically updated once it is detected again by the controller AP.

## 5.3 Controller AP Status Screen

When the NWA is in AP controller mode, the **Status** screen displays some unique fields in the **System Information**, **AP Status**, **WLAN Association** and **System Status** sections. The **System Status** links take you to screens that provide information on the access points managed by the NWA.

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

**Figure 23** AP Controller: the Status Screen

Automatic Refresh Interval: None [Refresh]

System Information		System Resources	
System Name	NWA-Series	Flash	2/4 MB
Model	NWA-3163	Memory	16/32 MB
Firmware Version	V3.70(AAN.0)b1   11/14/2008	CPU	1%
System UP Time	01:15:24		
Current Date Time	01:15:21 2000/01/01		
Management VLAN	Disable		
Rogue AP Detection	Disable		
IP	192.168.1.2		
LAN MAC	00:13:49:31:63:04		
Registration Type	Manual		
Management Mode	Controller		

AP status	
On-line	1
Off-line	0
Un-Managed	0

WLAN Association	
802.11a	0
802.11b/g	0

System Status

AP List | AP Statistics | Association List | SSID Information | LOGS | Rogue AP List

The following table describes the new labels in this screen.

**Table 9** AP Controller: the Status Screen

LABEL	DESCRIPTION
Registration Type	This field displays how the managed APs are registered with the NWA. <ul style="list-style-type: none"> <li><b>Manual</b> displays if you add unmanaged APs to the NWA's list of managed APs manually.</li> <li><b>Always Accept</b> displays if the NWA automatically manages any CAPWAP-enabled AP that transmits a management request over the network.</li> </ul>
Management Mode	When the NWA is in AP controller mode, this displays <b>Controller</b> .
On-line	This field displays the number of access points, managed by the NWA, that are currently active.
Off-line	This field displays the number of access points, managed by the NWA, that are not currently active (turned off or otherwise unreachable on the network).
Un-managed	This field displays the number of access points on the network that are not managed by the NWA, but are transmitting CAPWAP management requests.
802.11a	This field displays the number of wireless clients associated with APs managed by the NWA (including the NWA itself) using IEEE 802.11a.
802.11b/g	This field displays the number of wireless clients associated with APs managed by the NWA (including the NWA itself) using IEEE 802.11b or IEEE 802.11g.
AP List	Click this to see a list of the APs managed by the NWA.
AP Statistics	Click this to see packet statistics related to each of the APs managed by the NWA.
Association List	Click this to see information about each of the wireless clients connected to APs managed by the NWA.
SSID Information	Click this to see details of the security settings used by each SSID, and the number of wireless clients associated with each SSID.



## 5.4 AP List Screen

Use this screen to view and add managed APs. By default, the NWA is always included in this table. Although you cannot remove it, you can edit its settings.

Click **Controller > AP Lists**. The following screen displays.

**Figure 24** The Controller > AP Lists Screen

The screenshot shows the 'AP Lists' screen with three tabs: 'AP Lists', 'Configuration', and 'Redundancy'. The 'AP Lists' tab is active. It contains two main sections: 'Managed Access Points List' and 'Un-Managed Access Points List'. The 'Managed Access Points List' has a table with columns: Index, Select, IP, MAC Address, Model, Description, and Status. It contains one entry with Index 1, IP 127.0.0.1, MAC 00:19:CB:89:7C:CA, Model NWA3550 802.11a/g, Description AP-LOCAL, and a status icon. Below this table are 'Edit' and 'Delete' buttons. The 'Un-Managed Access Points List' has a table with columns: Index, Select, IP, MAC Address, Model, and Description. It contains one entry with Index 1, IP 192.168.1.35, MAC 00:13:49:DF:42:A8, Model NWA-3500 802.11a/g, and Description AP-001349DF42A8. Below this table is an 'Add' button. At the bottom of the screen, there is an 'Automatic Refresh Interval' set to '30 seconds' and a 'Refresh' button.

The following table describes the labels in this screen.

**Table 10** The Controller > AP Lists Screen

LABEL	DESCRIPTION
Managed Access Points List	This section lists the access points currently controlled by the NWA. This always includes the NWA itself.
Index	This is the index number of the managed AP.
Select	Click this then select <b>Edit</b> to configure the managed AP's settings. Click <b>Delete</b> to remove it from the NWA's managed AP list.
IP	This displays the IP address of the managed AP.
MAC Address	This displays the MAC address of the managed AP.
Model	This displays the model name and 802.11 mode of the managed AP.
Description	This displays the description of the managed AP.

**Table 10** The Controller > AP Lists Screen

LABEL	DESCRIPTION
Status	<p>This displays whether the managed AP is active, not active or upgrading its firmware.</p> <ul style="list-style-type: none"> <li>• <b>Red:</b> the AP is not active.</li> <li>• <b>Green:</b> the AP is active.</li> <li>• <b>Yellow:</b> the AP is upgrading its firmware.</li> </ul> <p><b>Note:</b> You can still edit a managed AP's settings even if it is offline. However, the changes only take effect when the NWA detects that the managed AP is online again.</p>
Edit	Select the managed AP from the list and click this to edit the managed AP's settings.
Delete	<p>Select the managed AP from the list and click this to delete the managed AP from the list.</p> <p>When you do this, the managed AP is no longer handled by the NWA until you add it back to the list.</p>
Un-Managed Access Points List	This section lists the CAPWAP-enabled access points in the area that are in managed AP mode but which are not currently controlled by the NWA.
Index	This is the index number of an unmanaged AP that is requesting to be managed by the NWA.
Select	Click this then select <b>Add</b> to include the unmanaged AP in the NWA's managed AP list.
IP	This displays the IP address of the unmanaged AP.
MAC Address	This displays the MAC address of the unmanaged AP.
Model	This displays the model name and 802.11 mode of the unmanaged AP.
Description	This displays the description of the unmanaged AP.
Add	Select the unmanaged AP from the list and click this to include the unmanaged AP in the NWA's managed AP list.
Automatic Refresh Interval	Enter how often you want the NWA to update this screen.
Refresh	Click this to update this screen immediately.

## 5.4.1 The AP Lists Edit Screen

Use this screen to change the description or radio profile of an AP managed by the NWA. Click **Edit** in the **CONTROLLER > AP Lists** screen. The following screen displays.

**Figure 25** The Controller > AP Configuration Screen

The screenshot shows the 'AP Configuration' screen. At the top, there is a tab labeled 'Access Point'. Below this, the following fields are visible:

- Model:** NWA-3500
- MAC Address:** 00:13:49:DF:42:A8
- Description:** AP-001349DF42A8
- Enable Breathing LED:** A checked checkbox.
- WLAN1 Radio Profile:** radio09
- WLAN2 Radio Profile:** radio07

At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Figure 26** The Controller > AP Configuration Screen

LABEL	DESCRIPTION
Model	This is the model number of the managed AP.
MAC Address	This is the MAC address of the managed AP.
Description	Enter a short description of this access point (up to 32 English keyboard characters).
Enable Breathing LED	This field displays only if the managed AP supports this feature. Select this box to disable the WLAN LED (light). Clear this box to enable the WLAN LED.
WLAN1 Radio Profile	Select the radio profile you want to use for this AP. Configure radio profiles in the Profile <b>Edit &gt; Radio</b> screen. Select <b>Disable</b> if you do not want to use a radio profile. The AP's radio is not active when you select <b>Disable</b> .
WLAN2 Radio Profile	This field displays only if the managed AP has dual radios. Select the second radio profile you want to use for this AP. Configure radio profiles in the Profile <b>Edit &gt; Radio</b> screen. Select <b>Disable</b> if you do not want to use a second radio profile. The AP's radio is not active when you select <b>Disable</b> .
Apply	Click this to save the changes in this screen.
Reset	Click this to return the fields in this screen to their previously-saved values.

## 5.5 Configuration Screen

Use this screen to control the way in which the NWA accepts new APs to manage. You can also configure the pre-shared key (PSK) that is use to secure the data transmitted between the NWA and the APs it manages.

When the NWA is in AP controller mode, click **CONTROLLER > Configuration**. The following screen displays.

**Figure 27** The Controller > Configuration Screen

The following table describes the labels in this screen...

**Table 11** The Controller > Configuration Screen

LABEL	DESCRIPTION
Pre-Shared Key	This is the security key used to encrypt communications between the NWA and its managed APs. This key is used to encrypt DTLS (Datagram Transport Layer Security) transmissions. Enter 8~32 English keyboard characters.  The proprietary AutoPSK protocol transfers the DTLS key from the NWA to the managed APs automatically.
Registration Type	This controls whether the NWA manages all CAPWAP-enabled APs that transmit management request packets, or requires the user to select which such APs to manage. <ul style="list-style-type: none"> <li>Select <b>Manual</b> to choose which APs to manage (select the APs you want to manage in the <b>Controller &gt; AP Lists</b> screen).</li> <li>Select <b>Always Accept</b> to manage any AP on your network that transmits a CAPWAP request for management.</li> </ul>
Apply	Click this to save the changes in this screen.
Reset	Click this to return the fields in this screen to their previously-saved values.

## 5.6 Redundancy Screen

Use this screen to set the controller AP as a primary or secondary controller.

If you set your NWA as a primary controller AP, you can have a secondary controller AP to serve as a backup. All configurations are synchronized between the NWA and the secondary controller AP.

When the NWA is in AP controller mode, click **CONTROLLER > Redundancy**. The following screen displays.

**Figure 28** The Controller > Configuration Screen

The following table describes the labels in this screen.

**Table 12** The Controller > Redundancy Screen

LABEL	DESCRIPTION
Redundancy	Select <b>Enable</b> to set the NWA either as a <b>Primary AP Controller</b> or as a <b>Secondary Controller AP</b> .  Select <b>Disable</b> when the NWA acts as a primary AP controller without a backup.
Primary AP Controller	Select this if the NWA has a secondary controller AP. You must give the IP address of this backup in the field below.
Secondary IP	Enter the IP address of the secondary controller AP.
Secondary AP Controller	Select this if the NWA is the secondary controller AP.
Apply	Click this to save the changes in this screen.
Reset	Click this to return the fields in this screen to their previously-saved values.



The following table describes the labels in this screen.

**Table 13** The Profile Edit > Radio Screen

LABEL	DESCRIPTION
Index	This field displays the index number of each radio profile.
Profile Name	This field displays the identification name of each radio profile on the NWA.
802.11 Mode	This field displays the IEEE 802.11 wireless mode the radio profile uses.
Channel ID	This field displays the wireless channel the radio profile uses.
Edit	Click the radio button next to the profile you want to configure and click <b>Edit</b> to go to the radio profile configuration screen.

## 5.8 The Radio Profile Edit Screen

Use this screen to configure a specific radio profile. In the **Profile Edit > Radio** screen, select a profile and click **Edit**. The following screen displays.

**Figure 30** The Profile Edit > Radio > Edit Screen

Radio	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
<b>Profile Name</b> radio01					
<b>802.11 Mode</b> 802.11b+g					
<input type="checkbox"/> <b>Super Mode</b>					
<b>Choose Channel ID</b> Channel-06 2437MHz					
<b>RTS/CTS Threshold</b> 2346 (256 ~ 2346)					
<b>Fragmentation Threshold</b> 2346 (256 ~ 2346) (Fragmentation threshold shall be an even number)					
<b>Beacon Interval</b> 100 (30ms ~ 1000ms)					
<b>DTIM</b> 1 (1 ~ 100)					
<b>Output Power</b> 100%					
<b>Rates Configuration</b>					
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		
<b>Select SSID Profile</b>					
Index	Active	Profile	Index	Active	Profile
1	<input checked="" type="checkbox"/>	SSID03	5	<input type="checkbox"/>	SSID03
2	<input type="checkbox"/>	SSID03	6	<input type="checkbox"/>	SSID03
3	<input type="checkbox"/>	SSID03	7	<input type="checkbox"/>	SSID03
4	<input type="checkbox"/>	SSID03	8	<input type="checkbox"/>	SSID03
<input checked="" type="checkbox"/> <b>Enable Antenna Diversity</b>					
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					



The following table describes the labels in this screen.

**Table 14** The Profile Edit > Radio > Edit Screen

LABEL	DESCRIPTION
Profile Name	Enter a name identifying this profile.
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the NWA.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the NWA.</p> <p>Select <b>802.11b+g</b> 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.</p> <p>Select <b>802.11a</b> (NWA-3160 only) to allow only IEEE 802.11a compliant WLAN devices to associate with the NWA.</p>
Super Mode	Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting.
Choose Channel ID	<p>Set the operating frequency/channel depending on your particular region.</p> <p>To manually set the NWA to use a channel, select a channel from the drop-down list box.</p>
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its smallest value (256) turns on the RTS/CTS handshake. Enter a value between 256 and 2346.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between <b>256</b> and <b>2346</b> .
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 low-power mode before waking up to handle the beacon. This value can be set from 30ms to 1000ms. A high value helps save current consumption of the access point.
DTIM	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. This value can be set from 1 to 100.
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 <b>100%(Full Power)</b> , <b>50%</b> , <b>25%</b> , <b>12.5%</b> or <b>Minimum</b> . See the product specifications for more information on your NWA's output power.

**Table 14** The Profile Edit > Radio > Edit Screen

LABEL	DESCRIPTION
Rates Configuration	<p>This section controls the data rates permitted for clients of an AP using this radio profile.</p> <p>For each <b>Rate</b>, select an option from the <b>Configuration</b> list. The options are:</p> <p><b>Basic</b> (1~11 Mbps only): Clients can always connect to the access point at this speed.</p> <p><b>Optional</b>: Clients can connect to the access point at this speed, when permitted to do so by the AP.</p> <p><b>Disabled</b>: Clients cannot connect to the access point at this speed.</p>
Select SSID Profile	<p>Use this section to choose the SSID profile or profiles you want access points using this radio profile to use. Each AP can use multiple SSID profiles simultaneously.</p> <p>Configure SSID profiles in the <b>Profile Edit &gt; SSID</b> screens.</p>
Index	This is the SSID profile's index number.
Active	Select this to use the SSID profile selected in the <b>Profile</b> field.
Profile	Select the profile you want to use. Ensure that you also select the <b>Active</b> box.
Enable Antenna Diversity	Select this to have access points using this radio profile use antenna diversity, where available. Antenna diversity uses multiple antennas to reduce signal interference.
Apply	Click this to save your changes.
Reset	Click this to reload the previous configuration for this screen.

# 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.

## 6.1 How to Configure the Wireless LAN

This section shows how to choose which wireless operating mode you should use on the NWA, and the steps you should take to set up the wireless LAN in each wireless mode. See [Section 6.1.3 on page 70](#) for links to more information on each step.

Note: This section describes how to use the NWA in standalone mode. For information on using the NWA in a CAPWAP network, see [Chapter 4 on page 47](#).

### 6.1.1 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 24](#) 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 24](#) for details.

The NWA is a bridge when other APs access your wired Ethernet network through the NWA.

The NWA is a repeater when it has no Ethernet connection and allows other APs to communicate with one another through the NWA.

- 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 25](#) for details.
- Use **MBSSID** 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 1.2.4 on page 26](#) for details.

### 6.1.1.1 Configuring Dual WLAN Adaptors

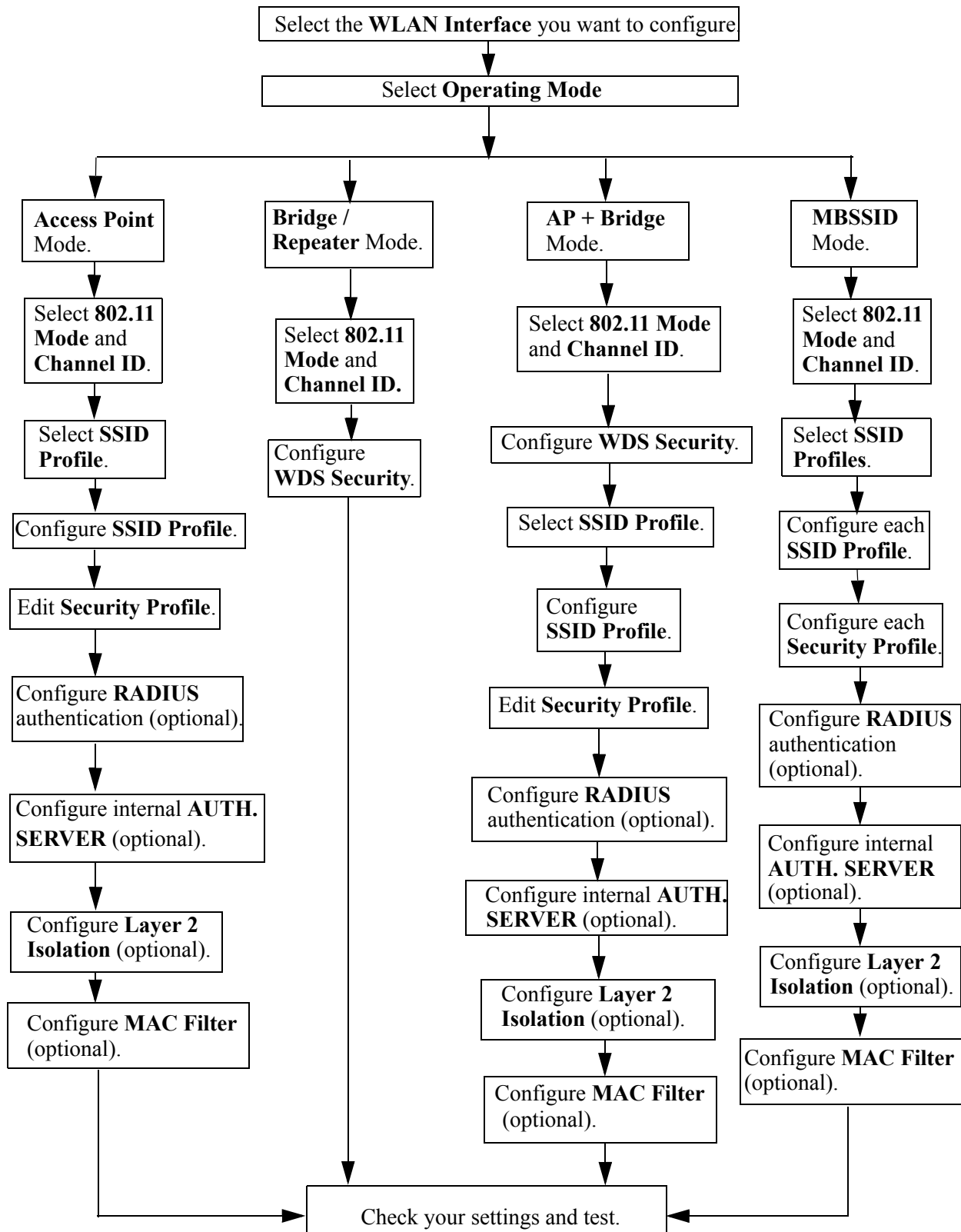
The NWA is equipped with dual wireless adaptors. This means you can configure two different wireless networks to operate simultaneously. See [Section 1.2.6 on page 28](#) for details.

You can configure each wireless adaptor separately in the **WIRELESS > Wireless** screen. To configure the first wireless network, select **WLAN1** in the **WLAN Interface** field and follow the steps in [Section 6.1.2 on page 68](#). Then, select **WLAN2** in the **WLAN Interface** field and follow the same procedure to configure the second network.

### 6.1.2 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).

Figure 31 Configuring Wireless LAN



## 6.1.3 Further Reading

Use these links to find more information on the steps:

- Choosing **802.11 Mode**: see [Section 8.4.1 on page 123](#).
- Choosing a wireless **Channel ID**: see [Section 8.4.1 on page 123](#).
- Selecting and configuring **SSID profile(s)**: see [Section 8.4.1 on page 123](#) and [Section 9.4 on page 143](#).
- Configuring and activating **WDS Security**: see [Section 8.4.2 on page 126](#).
- Editing **Security Profile(s)**: see [Section 10.4 on page 150](#).
- Configuring an external **RADIUS** server: see [Section 11.4 on page 163](#).
- Configuring and activating the internal **AUTH. SERVER**: see [Section 11.4 on page 163](#) and [Chapter 17 on page 199](#).
- Configuring **Layer 2 Isolation**: see [Section 12.4.1 on page 167](#).
- Configuring **MAC Filtering**: see [Section Note: on page 174](#).

## 6.2 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 8.3.2 on page 122](#)) to provide multiple wireless networks. Each wireless network will cater for a different type of user.

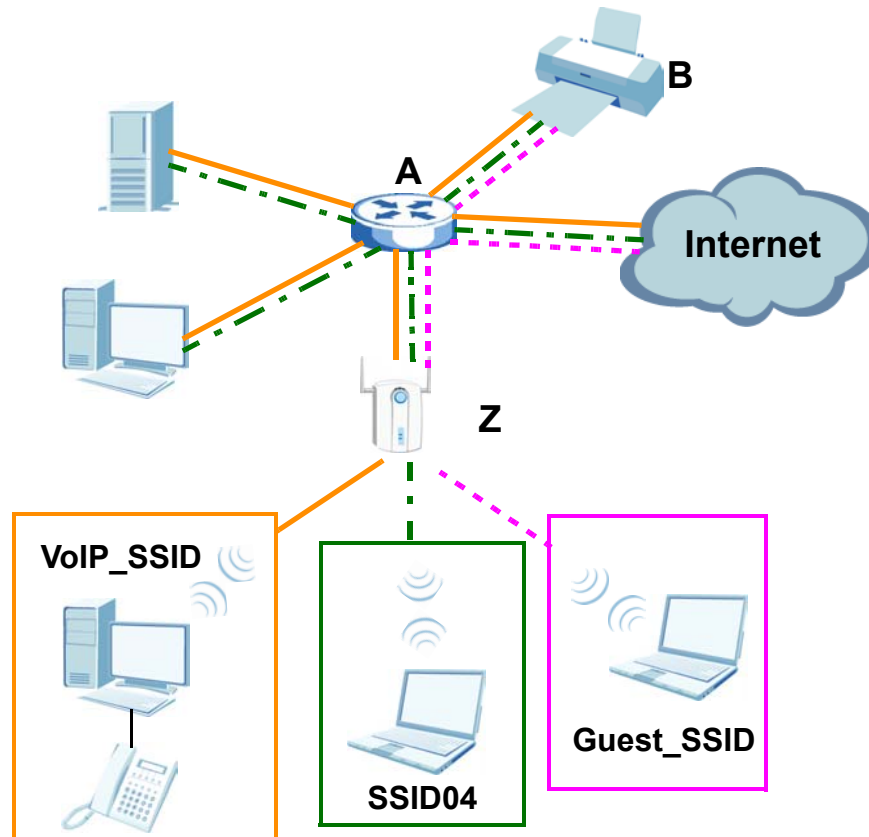
You want to make three wireless networks: one standard office wireless network with all the same settings you already have, another wireless network with high Quality of Service (QoS) settings for Voice over IP users, and a guest network that allows visitors to your office to access only the Internet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

To do this, you will take the following steps:

- 1 Change the operating mode from Access Point to MBSSID and reactivate the standard network.
- 2 Configure a wireless network for Voice over IP users.
- 3 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**.

**Figure 32** Tutorial: Example MBSSID Setup



The standard network (**SSID04**) has access to all resources. The VoIP network (**VoIP\_SSID**) has access to all resources and a high Quality of Service (QoS) setting (see [Chapter 8 on page 119](#) for information on QoS). The guest network (**Guest\_SSID**) has access to the Internet and the network printer only, and a low QoS setting.

To configure these settings, you need to know the MAC (Media Access Control) 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 15** Tutorial: Example Information

Network router ( <b>A</b> ) MAC address	00:AA:00:AA:00:AA
Network printer ( <b>B</b> ) MAC address	AA:00:AA:00:AA:00

## 6.2.1 Change the Operating Mode

Log in to the NWA (see [Section 2.1 on page 35](#)). Click **WIRELESS > Wireless**. The **Wireless** screen appears. In this example, the NWA is using **WLAN Interface 1** in **Access Point** operating mode, and is currently set to use the **SSID04** profile.

**Figure 33** Tutorial: Wireless LAN: Before

The screenshot displays the configuration page for a Wireless LAN interface. The page is divided into several tabs: **Wireless**, **SSID**, **Security**, **RADIUS**, **Layer-2 Isolation**, and **MAC Filter**. The **Wireless** tab is active. The configuration is as follows:

- WLAN Interface:** WLAN1
- Operating Mode:** Access Point
- 802.11 Mode:** 802.11b+g
- Super Mode**
- Choose Channel ID:** Channel-06 2437MHz or **Scan**
- RTS/CTS Threshold:** 2346 (256 ~ 2346)
- Fragmentation Threshold:** 2346 (256 ~ 2346) (Fragmentation threshold shall be an even number)
- Output Power:** 100%
- SSID Profile:** SSID04
- Enable Spanning Tree Protocol (STP)**
- Enable Roaming**

(The STP and Roaming are common settings. The changes are for both WLAN Interfaces.)

Buttons: **Apply** and **Reset**



Select **MBSSID** from the **Operating Mode** drop-down list box. The screen displays as follows.

**Figure 34** Tutorial: Wireless LAN: Change Mode

The screenshot shows the configuration page for a Wireless LAN interface (WLAN1). The **Operating Mode** is set to **MBSSID**. Below this, there is a table for selecting an SSID profile. The table has columns for Index, Active, and Profile. Row 3 is highlighted with a red circle, showing Index 3, Active checked, and Profile SSID04. Other rows show various SSID profiles, some with the Active box unchecked.

Index	Active	Profile	Index	Active	Profile
1	<input type="checkbox"/>	VoIP_SSID	5	<input type="checkbox"/>	SSID03
2	<input type="checkbox"/>	Guest_SSID	6	<input type="checkbox"/>	SSID03
3	<input checked="" type="checkbox"/>	SSID04	7	<input type="checkbox"/>	SSID03
4	<input type="checkbox"/>	SSID03	8	<input type="checkbox"/>	SSID03

This **Select SSID Profile** table allows you to activate or deactivate SSID profiles. Your wireless network was previously using the **SSID04** profile, so select **SSID04** in one of the **Profile** list boxes (number **3** in this example).

Select the **Active** box for the entry and click **Apply** to activate the profile. Your standard wireless network (**SSID04**) is now accessible to your wireless clients as before. You do not need to configure anything else for your standard network.

## 6.2.2 Configure the VoIP Network

Next, click **WIRELESS > SSID**. The following screen displays. Note that the **SSID04** SSID profile (the standard network) is using the **security01** security profile. You cannot change this security profile without changing the standard

network's parameters, so when you set up security for the **VoIP\_SSID** and **Guest\_SSID** profiles you will need to set different security profiles.

**Figure 35** Tutorial: WIRELESS > SSID

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter			
<input checked="" type="radio"/>	1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
<input type="radio"/>	2	Guest_SSID	ZyXEL02	security01	radius01	NONE	I2isolation01	Disable
<input type="radio"/>	3	SSID03	ZyXEL03	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	4	SSID04	ZyXEL04	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	5	SSID05	ZyXEL05	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	8	SSID08	ZyXEL08	security08	radius01	NONE	Disable	Disable
<input type="radio"/>	9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable

The Voice over IP (VoIP) network will use the pre-configured SSID profile, so select **VoIP\_SSID**'s radio button and click **Edit**. The following screen displays.

**Figure 36** Tutorial: VoIP SSID Profile Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
<b>Name :</b>		<b>VoIP_SSID</b>			
<b>SSID :</b>		VoIP_SSID_Example			
<b>Hide Name(SSID) :</b>		Enable			
<b>Security :</b>		security02			
<b>RADIUS :</b>		radius01			
<b>QoS :</b>		VoIP			
<b>L2 Isolation :</b>		Disable			
<b>Intra-BSS Traffic blocking :</b>		Disable			
<b>MAC Filtering :</b>		Disable			

- Choose a new SSID for the VoIP network. In this example, enter **VOIP\_SSID\_Example**. Note that although the SSID changes, the SSID profile name (**VoIP\_SSID**) remains the same as before.
- Select **Enable** from the **Hide Name (SSID)** list box. 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.
- The standard network (**SSID04**) is currently using the **security01** profile, so use a different profile for the VoIP network. If you used the **security01** profile, anyone who could access the standard network could access the VoIP wireless network. Select **security02** from the **Security** field.
- Leave all the other fields at their defaults and click **Apply**.

### 6.2.2.1 Set Up Security for the VoIP Profile

Now you need to configure the security settings to use on the VoIP wireless network. Click the **Security** tab.

**Figure 37** Tutorial: VoIP Security

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
		Index	Profile Name	Security Mode	
<input type="radio"/>		1	security01	WPA2.PSK	
<input checked="" type="radio"/>		2	security02	None	
<input type="radio"/>		3	security03	None	
<input type="radio"/>		4	security04	None	
<input type="radio"/>		5	security05	None	
<input type="radio"/>		6	security06	None	
<input type="radio"/>		7	security07	None	
<input type="radio"/>		8	security08	None	
<input type="radio"/>		9	security09	None	
<input type="radio"/>		10	security10	None	
<input type="radio"/>		11	security11	None	
<input type="radio"/>		12	security12	None	
<input type="radio"/>		13	security13	None	
<input type="radio"/>		14	security14	None	
<input type="radio"/>		15	security15	None	
<input type="radio"/>		16	security16	None	

You already chose to use the **security02** profile for this network, so select the radio button for **security02** and click **Edit**. The following screen appears.

**Figure 38** Tutorial: VoIP Security Profile Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
<p><b>Name :</b> VoIP_Security</p> <p><b>Security Mode :</b> WPA2-PSK</p> <p><b>Pre-Shared Key :</b> ThisismyWPA2-PSKpre-sharedkey</p> <p><b>ReAuthentication Timer :</b> 1800 (in seconds)</p> <p><b>Idle Timeout :</b> 3600 (in seconds)</p> <p><b>Group Key Update Timer :</b> 1800 (in seconds)</p> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Reset"/> </p>					

- Change the **Name** field to "VoIP\_Security" to make it easier to remember and identify.
- In this example, you do not have a RADIUS server for authentication, so select **WPA2-PSK** in the **Security Mode** field. WPA2-PSK provides strong security that anyone with a compatible wireless client can use, once they know the pre-shared key (PSK). Enter the PSK you want to use in your network in the **Pre-Shared Key** field. In this example, the PSK is "ThisismyWPA2-PSKpre-sharedkey".
- Click **Apply**. The **WIRELESS > Security** screen displays. Ensure that the **Profile Name** for entry 2 displays "**VoIP\_Security**" and that the **Security Mode** is **WPA2-PSK**.

**Figure 39** Tutorial: VoIP Security: Updated

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																				
<table border="1"> <thead> <tr> <th></th> <th>Index</th> <th>Profile Name</th> <th>Security Mode</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/></td> <td>1</td> <td>security01</td> <td>None</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td>2</td> <td>VoIP_Security</td> <td>WPA2-PSK</td> </tr> <tr> <td><input type="radio"/></td> <td>3</td> <td>security03</td> <td>None</td> </tr> <tr> <td><input type="radio"/></td> <td>4</td> <td>...</td> <td>...</td> </tr> </tbody> </table>							Index	Profile Name	Security Mode	<input type="radio"/>	1	security01	None	<input checked="" type="radio"/>	2	VoIP_Security	WPA2-PSK	<input type="radio"/>	3	security03	None	<input type="radio"/>	4	...	...
	Index	Profile Name	Security Mode																						
<input type="radio"/>	1	security01	None																						
<input checked="" type="radio"/>	2	VoIP_Security	WPA2-PSK																						
<input type="radio"/>	3	security03	None																						
<input type="radio"/>	4	...	...																						

### 6.2.2.2 Activate the VoIP Profile

You need to activate the **VoIP\_SSID** profile before it can be used. Click the **Wireless** tab. In the **Select SSID Profile** table, select the **VoIP\_SSID** profile's **Active** checkbox and click **Apply**.

**Figure 40** Tutorial: Activate VoIP Profile

Output Power: 100%

Select SSID Profile

Index	Active	Profile	Index	Active	Profile
1	<input checked="" type="checkbox"/>	VoIP_SSID	5	<input type="checkbox"/>	SSID03
2	<input type="checkbox"/>	Guest_SSID	6	<input type="checkbox"/>	SSID03
3	<input checked="" type="checkbox"/>	SSID04	7	<input type="checkbox"/>	SSID03
4	<input type="checkbox"/>	SSID03	8	<input type="checkbox"/>	SSID03

Enable Spanning Tree Protocol (STP)

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.

### 6.2.3 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 layer-2 isolation and intra-BSS traffic blocking enabled by default. "Layer-2 isolation" means that a client accessing the network via the **Guest\_SSID** profile can access only certain pre-defined devices on the network (see [Section on page 166](#)), and "intra-BSS traffic blocking" means that the client cannot access other clients on the same wireless network (see [Section 8.4 on page 123](#)).

Click **WIRELESS > SSID**. Select **Guest\_SSID**'s entry in the list and click **Edit**. The following screen appears.

**Figure 41** Tutorial: Guest Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name :		Guest_SSID			
SSID :		Guest_SSID_Example			
Hide Name(SSID) :		Disable			
Security :		security03			
RADIUS :		radius01			
QoS :		NONE			
L2 Isolation :		l2isolation01			
Intra-BSS Traffic blocking :		Enable			
MAC Filtering :		Disable			
		Apply		Reset	

- Choose a new SSID for the guest network. In this example, enter **Guest\_SSID\_Example**. Note that although the SSID changes, the SSID profile name (**Guest\_SSID**) remains the same as before.
- Select **Disable** from the **Hide Name (SSID)** list box. This makes it easier for guests to configure their own computers' wireless clients to your network's settings.
- The standard network (**SSID04**) is already using the **security01** profile, and the VoIP network is using the **security02** profile (renamed **VoIP\_Security**) so select the **security03** profile from the **Security** field.
- Leave all the other fields at their defaults and click **Apply**.

### 6.2.3.1 Set Up Security for the Guest Profile

Now you need to configure the security settings to use on the guest wireless network. Click the **Security** tab.

You already chose to use the **security03** profile for this network, so select **security03**'s entry in the list and click **Edit**. The following screen appears.

**Figure 42** Tutorial: Guest Security Profile Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
<p><b>Name :</b> <input type="text" value="Guest_Security"/></p> <p><b>Security Mode :</b> <input type="text" value="WPA-PSK"/></p> <p><b>Pre-Shared Key :</b> <input type="text" value="ThisismyGuestWPApre-shared-key"/></p> <p><b>ReAuthentication Timer :</b> <input type="text" value="1800"/> ( in seconds)</p> <p><b>Idle Timeout :</b> <input type="text" value="3600"/> ( in seconds)</p> <p><b>Group Key Update Timer :</b> <input type="text" value="1800"/> ( in seconds)</p> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Reset"/> </p>					

- Change the **Name** field to "Guest\_Security" to make it easier to remember and identify.
- 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.
- 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**. The **WIRELESS > Security** screen displays. Ensure that the **Profile Name** for entry 3 displays "**Guest\_Security**" and that the **Security Mode** is **WPA-PSK**.

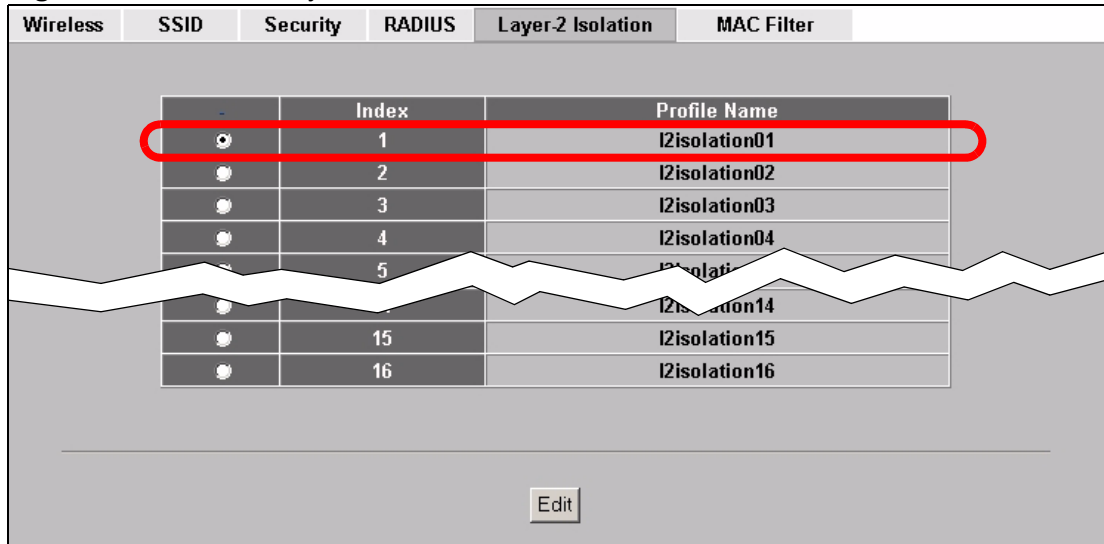
**Figure 43** Tutorial: Guest Security: Updated

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																				
		<table border="1"> <thead> <tr> <th></th> <th>Index</th> <th>Profile Name</th> <th>Security Mode</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/></td> <td>1</td> <td>security01</td> <td>WPA2-PSK</td> </tr> <tr> <td><input type="radio"/></td> <td>2</td> <td>VoIP_Security</td> <td>WPA2-PSK</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td>3</td> <td>Guest_Security</td> <td>WPA-PSK</td> </tr> <tr> <td><input type="radio"/></td> <td>4</td> <td>security04</td> <td>None</td> </tr> </tbody> </table>		Index	Profile Name	Security Mode	<input type="radio"/>	1	security01	WPA2-PSK	<input type="radio"/>	2	VoIP_Security	WPA2-PSK	<input checked="" type="radio"/>	3	Guest_Security	WPA-PSK	<input type="radio"/>	4	security04	None			
	Index	Profile Name	Security Mode																						
<input type="radio"/>	1	security01	WPA2-PSK																						
<input type="radio"/>	2	VoIP_Security	WPA2-PSK																						
<input checked="" type="radio"/>	3	Guest_Security	WPA-PSK																						
<input type="radio"/>	4	security04	None																						

### 6.2.3.2 Set up Layer 2 Isolation

Configure layer 2 isolation to control the specific devices you want the users on your guest network to access. Click **WIRELESS > Layer-2 Isolation**. The following screen appears.

**Figure 44** Tutorial: Layer 2 Isolation



Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
				<input checked="" type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	
				<input type="radio"/>	

Index      Profile Name

1      l2isolation01

2      l2isolation02

3      l2isolation03

4      l2isolation04

5      l2isolation05

6      l2isolation06

7      l2isolation07

8      l2isolation08

9      l2isolation09

10      l2isolation10

11      l2isolation11

12      l2isolation12

13      l2isolation13

14      l2isolation14

15      l2isolation15

16      l2isolation16

Edit



The **Guest\_SSID** network uses the **l2isolation01** profile by default, so select its entry and click **Edit**. The following screen displays.

**Figure 45** Tutorial: Layer 2 Isolation Profile

Wireless | SSID | Security | RADIUS | **Layer-2 Isolation** | MAC Filter

Layer-2 Isolation Configuration

Profile Name:

Allow devices with these MAC addresses

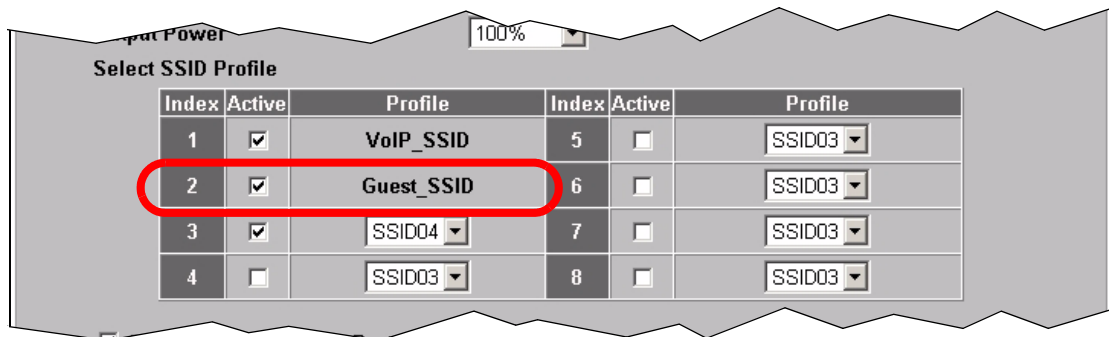
Index	MAC Address	Description	Index	MAC Address	Description
1	00:AA:00:AA:00:AA	network router	17	00:00:00:00:00:00	
2	AA:00:AA:00:AA:00	network printer	18	00:00:00:00:00:00	
3	00:00:00:00:00:00		19	00:00:00:00:00:00	
4	00:00:00:00:00:00		20	00:00:00:00:00:00	
5	00:00:00:00:00:00		21	00:00:00:00:00:00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

Enter the MAC addresses and descriptions of the two network devices you want users on the guest network to be able to access: the main network router (00:AA:00:AA:00:AA) and the network printer (AA:00:AA:00:AA:00). Click **Apply**.

### 6.2.3.3 Activate the Guest Profile

You need to activate the **Guest\_SSID** profile before it can be used. Click the **Wireless** tab. In the **Select SSID Profile** table, select the check box for the **Guest\_SSID** profile and click **Apply**.

**Figure 46** Tutorial: Activate Guest Profile



Your guest wireless network is now ready to use.

### 6.2.4 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 **VoIP\_SSID** network. If you can see the **VoIP\_SSID** network, go to its **SSID Edit** screen and make sure **Hide Name (SSID)** is set to **Enable**.

Whether or not you see the standard network's SSID (**SSID04**) depends on whether "hide SSID" is enabled.

- 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 VoIP 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.
- Access the **Guest\_SSID** network and try to access other resources than those specified in the Layer 2 Isolation (**I2isolation01**) profile screen.

You can use the ping utility to do this. Click **Start > Run...** and enter "cmd" in the **Open:** field. Click **OK**. At the **c:\>** prompt, enter "ping 192.168.1.10" (substitute the IP address of a real device on your network that is not on the layer 2 isolation list). If you receive a reply, check the settings in the **WIRELESS > Layer-2 Isolation > Edit** screen, and ensure that the correct layer 2 isolation profile is enabled in the **Guest\_SSID** profile screen.

## 6.3 How to Set Up and Use Rogue AP Detection

This example shows you how to configure the rogue AP detection feature on the NWA.

A rogue AP is a wireless access point operating in a network's coverage area that is not a sanctioned part of that network. The example also shows how to set the NWA to send out e-mail alerts whenever it detects a rogue wireless access point. See [Chapter 15 on page 179](#) for background information on the rogue AP function and security considerations.

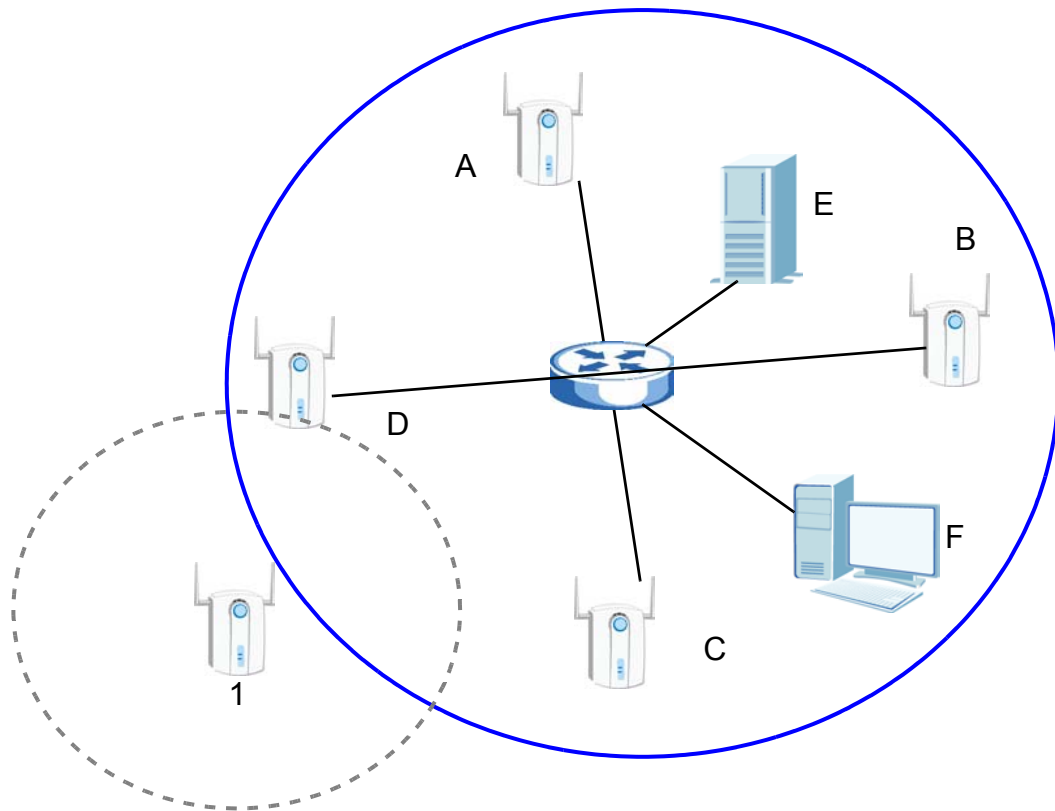
In this example, you want to ensure that your company's data is not accessible to an attacker gaining entry to your wireless network through a rogue AP.

Your wireless network operates in an office building. It consists of four access points (all NWAs) and a variable number of wireless clients. You also know that the coffee shop on the ground floor has a wireless network consisting of a single access point, which can be detected and accessed from your floor of the building. There are no other static wireless networks in your coverage area.

The following diagram shows the wireless networks in your area. Your access points are marked **A**, **B**, **C** and **D**. You also have a network mail/file server, marked

**E**, and a computer, marked **F**, connected to the wired network. The coffee shop's access point is marked **1**.

**Figure 47** Tutorial: Wireless Network Example



In the figure, the solid circle represents the range of your wireless network, and the dashed circle represents the extent of the coffee shop's wireless network. Note that the two networks overlap. This means that one or more of your APs can detect the AP (**1**) in the other wireless network.

When configuring the rogue AP feature on your NWAs in this example, you will need to use the information in the following table. You need the IP addresses of your APs to access their Web configurators, and you need the MAC address of each AP to configure the friendly AP list. You need the IP address of the mail server to set up e-mail alerts.

**Table 16** Tutorial: Rogue AP Example Information

DEVICE	IP ADDRESS	MAC ADDRESS
Access Point <b>A</b>	192.168.1.1	00:AA:00:AA:00:AA
Access Point <b>B</b>	192.168.1.2	AA:00:AA:00:AA:00
Access Point <b>C</b>	192.168.1.3	A0:0A:A0:0A:A0:0A
Access Point <b>D</b>	192.168.1.4	0A:A0:0A:A0:0A:A0
File / Mail Server <b>E</b>	192.168.1.25	N/A
Access Point <b>1</b>	UNKNOWN	AF:AF:AF:FA:FA:FA

Note: The NWA can detect the MAC addresses of APs automatically. However, it is more secure to obtain the correct MAC addresses from another source and add them to the friendly AP list manually. For example, an attacker's AP mimicking the correct SSID could be placed on the friendly AP list by accident, if selected from the list of auto-detected APs. In this example you have spoken to the coffee shop's owner, who has told you the correct MAC address of his AP.

In this example, you will do the following things.

- 1 Set up and save a friendly AP list.
- 2 Activate periodic Rogue AP Detection.
- 3 Set up e-mail alerts.
- 4 Configure your other access points.
- 5 Test the setup.

### 6.3.1 Set Up and Save a Friendly AP list

Take the following steps to set up and save a list of access points you want to allow in your network's coverage area.

- 1 On a computer connected to the wired network (**F** in the previous figure), open your Internet browser and enter the URL of access point **A** (192.168.1.1). Login to the Web configurator and click **ROGUE AP > Friendly AP**. The following screen displays.

**Figure 48** Tutorial: Friendly AP (Before Data Entry)

Configuration	Friendly AP	Rogue AP			
Add Friendly AP					
MAC Address	Description	Add			
Friendly AP List					
#	MAC Address	SSID	Channel	Security	Description

- 2 Fill in the **MAC Address** and **Description** fields as in the following table. Click **Add** after you enter the details of each AP to include it in the list.

Note: You can add APs that are not part of your network to the friendly AP list, as long as you know that they do not pose a threat to your network's security.

**Table 17** Tutorial: Friendly AP Information

MAC ADDRESS	DESCRIPTION
00:AA:00:AA:00:AA	My Access Point _A_
AA:00:AA:00:AA:00	My Access Point _B_
A0:0A:A0:0A:A0:0A	My Access Point _C_
0A:A0:0A:A0:0A:A0	My Access Point _D_
AF:AF:AF:FA:FA:FA	Coffee Shop Access Point _1_

The **Friendly AP** screen now appears as follows.

**Figure 49** Tutorial: Friendly AP (After Data Entry)

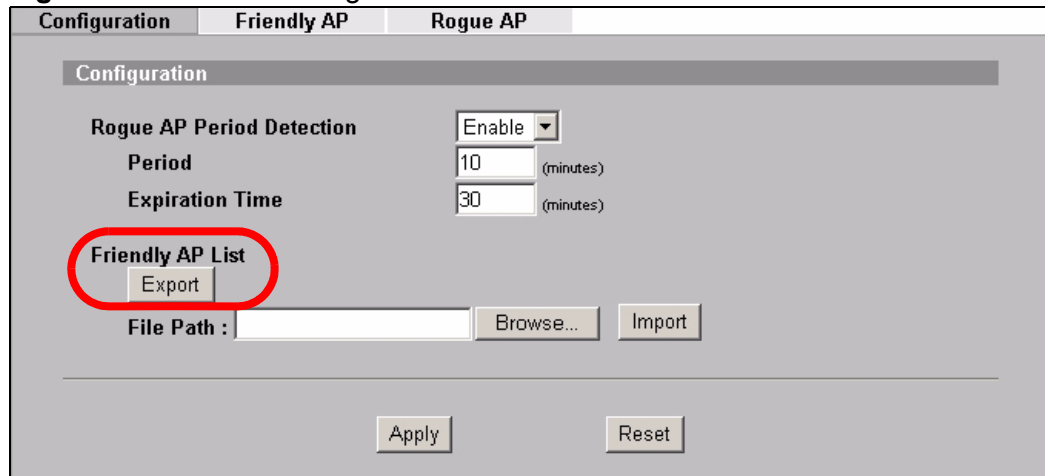
The screenshot shows the 'Friendly AP' configuration screen. At the top, there are three tabs: 'Configuration', 'Friendly AP', and 'Rogue AP'. Below the tabs is a section titled 'Add Friendly AP' which contains a form with two input fields: 'MAC Address' and 'Description', and an 'Add' button. Below this is a section titled 'Friendly AP List' which contains a table with the following data:

#	MAC Address	SSID	Channel	Security	Last Seen	Description	
1	00:aa:00:aa:00:aa	N/A	N/A	N/A	4:00:02	My Access Point _A_	
2	aa:00:aa:00:aa:00	N/A	N/A	N/A	4:00:02	My Access Point _B_	
3	a0:0a:a0:0a:a0:0a	N/A	N/A	N/A	4:00:02	My Access Point _C_	
4	0a:a0:0a:a0:0a:a0	N/A	N/A	N/A	4:00:00	My Access Point _D_	
5	af:af:af:fa:fa:fa	N/A	N/A	N/A	3:50:00	Coffee Shop Access Point _1_	

- 3 Next, you will save the list of friendly APs in order to provide a backup and upload it to your other access points.

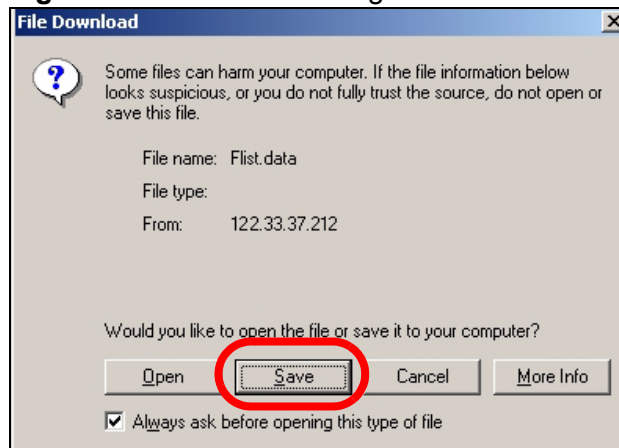
Click the **Configuration** tab. The following screen appears.

**Figure 50** Tutorial: Configuration



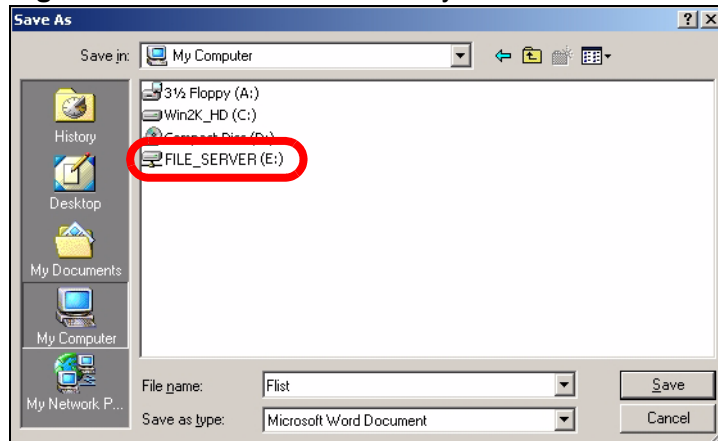
- 4 Click **Export**. If a window similar to the following appears, click **Save**.

**Figure 51** Tutorial: Warning



- 5 Save the friendly AP list somewhere it can be accessed by all the other access points on the network. In this example, save it on the network file server (**E** in [Figure 47 on page 84](#)). The default filename is "Flist".

**Figure 52** Tutorial: Save Friendly AP list

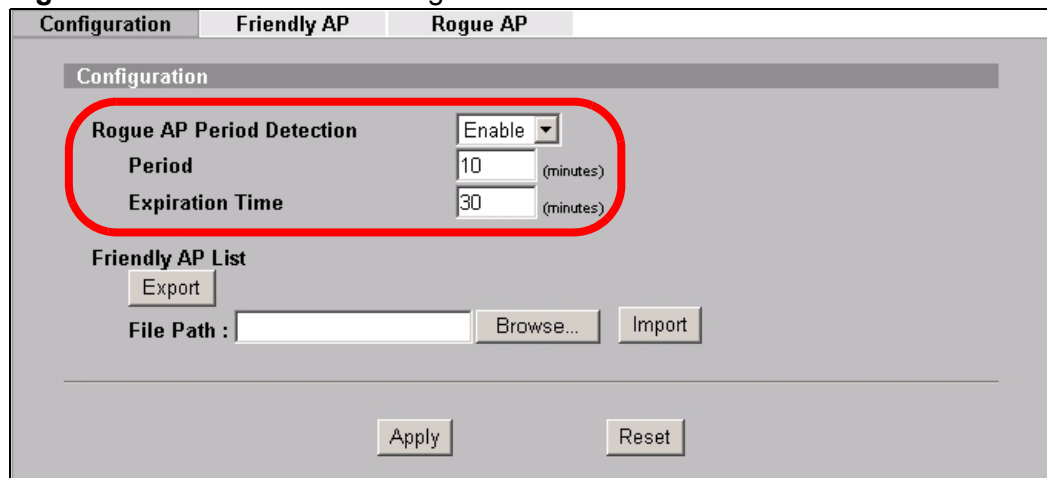


## 6.3.2 Activate Periodic Rogue AP Detection

Take the following steps to activate rogue AP detection on the first of your NWAs.

- 1 In the **ROGUE AP > Configuration** screen, select **Enable** from the **Rogue AP Period Detection** field.

**Figure 53** Tutorial: Periodic Rogue AP Detection



- 2 In the **Period** field, enter how often you want the NWA to scan for rogue APs. You can have the NWA scan anywhere from once every ten minutes to once every hour. In this example, enter "10".
- 3 In the **Expiration Time** field, enter how long an AP's entry can remain in the list before the NWA discards it from the list when the AP is no longer active. In this example, enter "30".



- 4 Click **Apply**.

### 6.3.3 Set Up E-mail Logs

In this section, you will configure the first of your four APs to send a log message to your e-mail inbox whenever a rogue AP is discovered in your wireless network's coverage area.

- 1 Click **LOGS > Log Settings**. The following screen appears.

**Figure 54** Tutorial: Log Settings

The screenshot shows the 'Log Settings' configuration page. It is divided into several sections:

- Address Info:** This section is highlighted with a red box. It contains four input fields:
  - Mail Server:** 192.168.1.25 (Outgoing SMTP Server NAME or IP Address)
  - Mail Subject:** ALERT\_Access\_Point\_A
  - Send log to:** (E-Mail Address)
  - Send alerts to:** mvname@mvfirm.com (E-Mail Address)
- SMTP Authentication:** Includes checkboxes for SMTP Authentication, and input fields for User NAME and Password.
- Syslog Logging:** Includes a checkbox for Active, Syslog IP Address (0.0.0.0), and Log Facility (Local 1).
- Send Log:** Includes a dropdown for Log Schedule (None), Day for Sending Log (Sunday), and Time for Sending Log (0 hour, 0 minutes). It also has a checkbox for Clear log after sending mail.
- Log:** A list of checkboxes for various log categories: System Maintenance, System Errors, PKI, SSL/TLS, 802.1x, Wireless, Internal RADIUS Server, and Rogue AP Detection.
- Send immediate alert:** This section is highlighted with a red box. It includes a checkbox for Send immediate alert, and sub-sections for System Errors (checked), PKI, and Rogue AP Detection (checked).

At the bottom of the page, there are 'Apply' and 'Reset' buttons.

- In this example, your mail server's IP address is **192.168.1.25**. Enter this IP address in the **Mail Server** field.

- Enter a subject line for the alert e-mails in the **Mail Subject** field. Choose a subject that is eye-catching and identifies the access point - in this example, "ALERT\_Access\_Point\_A".
- Enter the email address to which you want alerts to be sent (**myname@myfirm.com**, in this example).
- In the **Send Immediate Alert** section, select the events you want to trigger immediate e-mails. Ensure that **Rogue AP Detection** is selected.
- Click **Apply**.

### 6.3.4 Configure Your Other Access Points

Access point **A** is now configured to do the following.

- Scan for access points in its coverage area every ten minutes.
- Recognize friendly access points from a list.
- Send immediate alerts to your email account if it detects an access point not on the list.

Now you need to configure the other wireless access points on your network to do the same things.

For each access point, take the following steps.

- 1 From a computer on the wired network, enter the access point's IP address and login to its Web configurator. See [Table 16 on page 84](#) for the example IP addresses.
- 2 Import the friendly AP list. Click **ROGUE AP > Configuration > Browse...** Find the "Flist" file where you previously saved it on the network and click **Open**.
- 3 Click **Import**. Check the **ROGUE AP > Friendly AP** screen to ensure that the friendly AP list has been correctly uploaded.
- 4 Activate periodic rogue AP detection. See [Section 6.3.2 on page 88](#).
- 5 Set up e-mail logs as in [Section 6.3.3 on page 89](#), but change the **Mail Subject** field so you can tell which AP the alerts come from ("ALERT\_Access\_Point\_B", etc.)

### 6.3.5 Test the Setup

Next, test your setup to ensure it is correctly configured.

- Log into each AP's Web configurator and click **ROGUE AP > Rogue AP**. Click **Refresh**. If any of the MAC addresses from [Table 17 on page 86](#) appear in the list, the friendly AP function may be incorrectly configured - check the **ROGUE AP > Friendly AP** screen.

If any entries appear in the rogue AP list that are not in [Table 17 on page 86](#), write down the AP's MAC address for future reference and check your e-mail inbox. If you have received a rogue AP alert, email alerts are correctly configured on that NWA.

- If you have another access point that is not used in your network, make a note of its MAC address and set it up next to each of your NWAs in turn while the network is running.

Either wait for at least ten minutes (to ensure the NWA performs a scan in that time) or login to the NWA's Web configurator and click **ROGUE AP > Rogue AP > Refresh** to have the NWA perform a scan immediately.

- Check the **ROGUE AP > Rogue AP** screen. You should see an entry in the list with the same MAC address as your "rogue" AP.
- Check the **LOGS > View Logs** screen. You should see a **Rogue AP Detection** entry in red text, including the MAC address of your "rogue" AP.
- Check your e-mail. You should have received at least one e-mail alert (your other NWAs may also have sent alerts, depending on their proximity and the output power of your "rogue" AP).

## 6.4 How to Use Multiple MAC Filters and L-2 Isolation Profiles

This example shows you how to allow certain users to access only specific parts of your network. You can do this by using multiple MAC filters and layer-2 isolation profiles.

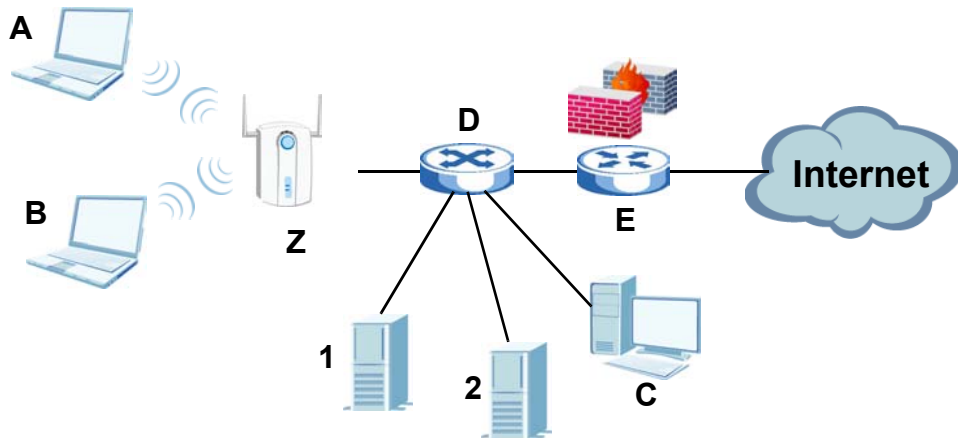
### 6.4.1 Scenario

In this example, you run a company network in which certain employees must wirelessly access secure file servers containing valuable proprietary data.

You have two secure servers (**1** and **2** in the following figure). Wireless user "Alice" (**A**) needs to access server **1** (but should not access server **2**) and wireless user "Bob" (**B**) needs to access server **2** (but should not access server **1**). Your

NWA is marked **Z**. **C** is a workstation on your wired network, **D** is your main network switch, and **E** is the security gateway you use to connect to the Internet.

**Figure 55** Tutorial: Example Network



## 6.4.2 Your Requirements

- 1 You want to set up a wireless network to allow only Alice to access Server **1** and the Internet.
- 2 You want to set up a second wireless network to allow only Bob to access Server **2** and the Internet.

## 6.4.3 Setup

In this example, you have already set up the NWA in MBSSID mode (see [Chapter 12 on page 165](#)). It uses two SSID profiles simultaneously. You have configured each SSID profile as shown in the following table.

**Table 18** Tutorial: SSID Profile Security Settings

SSID Profile Name	<b>SERVER_1</b>	<b>SERVER_2</b>
SSID	<b>SSID_S1</b>	<b>SSID_S2</b>
Security	Security Profile <b>security03</b> : WPA2-PSK Hide SSID	Security Profile <b>security04</b> : WPA2-PSK Hide SSID
Intra-BSS traffic blocking	Enabled	Enabled

Each SSID profile already uses a different pre-shared key.

In this example, you will configure access limitations for each SSID profile. To do this, you will take the following steps.

- 1 Configure the **SERVER\_1** network's SSID profile to use specific MAC filter and layer-2 isolation profiles.
- 2 Configure the **SERVER\_1** network's MAC filter profile.
- 3 Configure the **SERVER\_1** network's layer-2 isolation profile.
- 4 Repeat steps 1 ~ 3 for the **SERVER\_2** network.
- 5 Check your settings and test the configuration.

To configure layer-2 isolation, you need to know the MAC addresses of the devices on your network, which are as follows.

**Table 19** Tutorial: Example Network MAC Addresses

DEVICE	LABEL	MAC ADDRESS
NWA	Z	BB:AA:99:88:77:66
Secure Server 1	1	AA:99:88:77:66:55
Secure Server 2	2	99:88:77:66:55:44
Workstation	C	88:77:66:55:44:33
Switch	D	77:66:55:44:33:22
Security gateway	E	66:55:44:33:22:11

To configure MAC filtering, you need to know the MAC addresses of the devices Alice and Bob use to connect to the network, which are as follows.

**Table 20** Tutorial: Example User MAC Addresses

USER	MAC ADDRESS
Alice	11:22:33:44:55:66
Bob	22:33:44:55:66:77

## 6.4.4 Configure the **SERVER\_1** Network

First, you will set up the **SERVER\_1** network which allows Alice to access secure server **1** via the network switch.

You will configure the MAC filter to restrict access to Alice alone, and then configure layer-2 isolation to allow her to access only the network switch, the file server and the Internet security gateway.

Take the following steps to configure the **SERVER\_1** network.

- 1 Log into the NWA's Web Configurator and click **WIRELESS > SSID**. The following screen displays, showing the SSID profiles you already configured.

**Figure 56** Tutorial: SSID Profile

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter		
SERVER_1							
Index	Profile Name	SSID	Security	RADIUS	QoS	Layer-2 Isolation	MAC Filter
1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
2	Guest_SSID	ZyXEL02	security01	radius01	NONE	I2isolation01	Disable
3	SERVER_1	SSID03	security03	radius01	NONE	Disable	Disable
4	SERVER_2	SSID04	security04	radius01	NONE	Disable	Disable
5	SSID05	ZyXEL05	security03	radius01	NONE	Disable	Disable
6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable
8	SSID08	ZyXEL08	security01	radius01	NONE	Disable	Disable
9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable
10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable
11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable
12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable
13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable
14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable
15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable
16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable

- 2 Select **SERVER\_1**'s entry and click **Edit**. The following screen displays.

**Figure 57** Tutorial: SSID Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name :	<input type="text" value="SERVER_1"/>				
SSID :	<input type="text" value="SSID03"/>				
Hide Name(SSID) :	Enable ▾				
Security :	security03 ▾				
RADIUS :	radius01 ▾				
QoS :	NONE ▾				
L2 Isolation :	I2isolation03 ▾				
Intra-BSS Traffic blocking :	Enable ▾				
MAC Filtering :	macfilter03 ▾				
<input type="button" value="Apply"/>		<input type="button" value="Reset"/>			

Select **I2Isolation03** in the **L2 Isolation** field, and select **macfilter03** in the **MAC Filtering** field. Click **Apply**.

- Click the **Layer-2 Isolation** tab. When the **Layer-2 Isolation** screen appears, select **L2Isolation03**'s entry and click **Edit**. The following screen displays.

**Figure 58** Tutorial: Layer-2 Isolation Edit

Index	MAC Address	Description	Index	MAC Address	Description
1	77:66:55:44:33:22	NET_SWITCH	17	00:00:00:00:00:00	
2	AA:99:88:77:66:55	SERVER_1	18	00:00:00:00:00:00	
3	66:55:44:33:22:11	GATEWAY	19	00:00:00:00:00:00	
4	00:00:00:00:00:00		20	00:00:00:00:00:00	

Enter the network switch's **MAC Address** and add a **Description** ("NET\_SWITCH" in this case) in **Set 1**'s entry.

Enter server 1's **MAC Address** and add a **Description** ("SERVER\_1" in this case) in **Set 2**'s entry.

Change the **Profile Name** to "L-2-ISO\_SERVER\_1" and click **Apply**. You have restricted users on the **SERVER\_1** network to access only the devices with the MAC addresses you entered.

- Click the **MAC Filter** tab. When the **MAC Filter** screen appears, select **macfilter03**'s entry and click **Edit**.

Enter the MAC address of the device Alice uses to connect to the network in **Index 1**'s **MAC Address** field and enter her name in the **Description** field, as shown in the following figure. Change the **Profile Name** to "MacFilter\_SERVER\_1". Select **Allow Association** from the **Filter Action** field and click **Apply**.

**Figure 59** Tutorial: MAC Filter Edit (SERVER\_1)

Index	MAC Address	Description	Index	MAC Address	Description
1	11:22:33:44:55:66	Alice	17	00:00:00:00:00:00	
2	00:00:00:00:00:00		18	00:00:00:00:00:00	
3	00:00:00:00:00:00		19	00:00:00:00:00:00	

You have restricted access to the **SERVER\_1** network to only the networking device whose MAC address you entered. The **SERVER\_1** network is now configured.

## 6.4.5 Configure the SERVER\_2 Network

Next, you will configure the **SERVER\_2** network that allows Bob to access secure server **2** and the Internet.

To do this, repeat the procedure in [Section 6.4.4 on page 93](#), substituting the following information.

**Table 21** Tutorial: SERVER\_2 Network Information

<b>SSID</b> Screen	
Index	4
<b>Profile Name</b>	SERVER_2
<b>SSID Edit (SERVER_2)</b> Screen	
<b>L2 Isolation</b>	L2Isolation04
<b>MAC Filtering</b>	macfilter04
<b>Layer-2 Isolation (L2Isolation04)</b> Screen	
Profile Name	L-2-ISO_SERVER-2
<b>Set 1</b>	MAC Address: 77:66:55:44:33:22 Description: NET_SWITCH
<b>Set 2</b>	MAC Address: 99:88:77:66:55:44 Description: SERVER_2
<b>Set 3</b>	MAC Address: 66:55:44:33:22:11 Description: GATEWAY
<b>MAC Filter (macfilter04)</b> Edit Screen	
Profile Name	MacFilter_SERVER_2
<b>Set 1</b>	MAC Address: 22:33:44:55:66:77 Description: Bob

## 6.4.6 Checking your Settings and Testing the Configuration

Use the following sections to ensure that your wireless networks are set up correctly.

### 6.4.6.1 Checking Settings

Take the following steps to check that the NWA is using the correct SSIDs, MAC filters and layer-2 isolation profiles.



- 1 Click **WIRELESS > Wireless**. Check that the **Operating Mode** is **MBSSID** and that the correct SSID profiles are selected and activated, as shown in the following figure.

**Figure 60** Tutorial: SSID Profiles Activated

The screenshot shows the 'Wireless' configuration page with the 'SSID' tab selected. The 'WLAN Interface' is set to 'WLAN1', 'Operating Mode' is 'MBSSID', and '802.11 Mode' is '802.11b+g'. The 'Super Mode' checkbox is checked. The 'Choose Channel ID' is 'Channel-06 2437MHz'. The 'RTS/CTS Threshold' and 'Fragmentation Threshold' are both set to 2346. The 'Output Power' is set to 100%. Below these settings is a table for 'Select SSID Profile'.

Index	Active	Profile	Index	Active	Profile
1	<input type="checkbox"/>	VoIP_SSID	5	<input type="checkbox"/>	SERVER_1
2	<input type="checkbox"/>	Guest_SSID	6	<input type="checkbox"/>	SERVER_1
3	<input checked="" type="checkbox"/>	SERVER_1	7	<input type="checkbox"/>	SERVER_1
4	<input checked="" type="checkbox"/>	SERVER_2	8	<input type="checkbox"/>	SERVER_1

- 2 Next, click the **SSID** tab. Check that each configured SSID profile uses the correct **Security**, **Layer-2 Isolation** and **MAC Filter** profiles, as shown in the following figure.

**Figure 61** Tutorial: SSID Tab Correct Settings

The screenshot shows the 'SSID' configuration page with a table of SSID profiles. Profiles 3 and 4 are highlighted with a red circle.

Index	Profile Name	SSID	Security	RADIUS	QoS	Layer-2 Isolation	MAC Filter
1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
2	Guest_SSID	ZyXEL02	security01	radius01	NONE	L2-Isolation01	Disable
3	SERVER_1	SSID_S1	security03	radius01	NONE	L2-ISO_SERVER_1	MacFilter_SERVER_1
4	SERVER_2	SSID_S2	security04	radius01	NONE	L2-ISO_SERVER_2	MacFilter_SERVER_2
5	SSID05	ZyXEL05	security01	radius01	NONE	Disable	Disable
6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable

If the settings are not as shown, follow the steps in the relevant section of this tutorial again.

### 6.4.6.2 Testing the Configuration

Before you allow employees to use the network, you need to thoroughly test whether the setup behaves as it should. Take the following steps to do this.

**1** Test the **SERVER\_1** network.

- Using Alice's computer and wireless client, and the correct security settings, do the following.

Attempt to access Server **1**. You should be able to do so.

Attempt to access the Internet. You should be able to do so.

Attempt to access Server **2**. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.

- Using Alice's computer and wireless client, and incorrect security settings, attempt to associate with the **SERVER\_1** network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and wireless client, but with the correct security settings, attempt to associate with the **SERVER\_1** network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

**2** Test the **SERVER\_2** network.

- Using Bob's computer and wireless client, and the correct security settings, do the following.

Attempt to access Server **2**. You should be able to do so.

Attempt to access the Internet. You should be able to do so.

Attempt to access Server **1**. You should be unable to do so. If you can do so, layer-2 isolation is misconfigured.

- Using Bob's computer and wireless client, and incorrect security settings, attempt to associate with the **SERVER\_2** network. You should be unable to do so. If you can do so, security is misconfigured.
- Using another computer and wireless client, but with the correct security settings, attempt to associate with the **SERVER\_2** network. You should be unable to do so. If you can do so, MAC filtering is misconfigured.

If you cannot do something that you should be able to do, check the settings as described in [Section 6.4.6.1 on page 96](#), and in the individual Security, layer-2 isolation and MAC filter profiles for the relevant network. If this does not help, see the Troubleshooting chapter in this User's Guide.

## 6.5 How to Configure Management Modes

This example shows you how to configure the NWA's controller AP and manage AP modes.

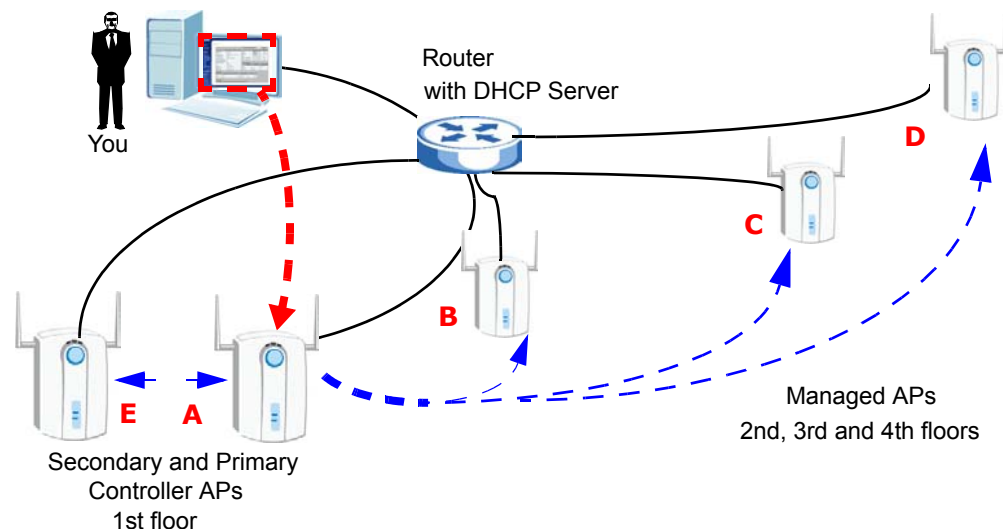
### 6.5.1 Scenario

In this example, you are the administrator of a company network wherein a group of users need stable wireless connection. These users are employees who move around the company building a lot, yet need to connect to network resources at various times of the day.

Currently you have 4 NWA standalone APs (**A**, **B**, **C** and **D**) in each floor of the 4-storey company building. Though the current setup works, it takes a lot of your time to edit profiles in the APs because of their location. You want to convert one of your NWA to a controller AP (**A**) which will allow you to manage all 4 NWA APs using the Web Configurator of this newly transformed NWA controller AP.

Additionally, you want a backup for this controller AP. You add another NWA (**E**) in the first floor of the building, which you will then set as a secondary controller AP.

**Figure 62** Tutorial: Controller AP with Backup and Managed APs Example



### 6.5.2 Your Requirements

- 1 You want to manage the APs in your company using one controller AP's Web Configurator. That is, you only need to know one IP address to edit the settings of the NWAs in your wireless network.
- 2 You want to have a backup of the NWA controller AP configuration.

## 6.5.3 Setup

In this example, each of your NWA standalone AP mirror each other. They all have the same SSID profiles stored. First you need to download the configuration file from one of your NWAs for backup purposes. Refer to [Section 23.8.1 on page 272](#) for information on how to download the configuration file from your NWA.

In case there are various SSID profiles stored in each NWA standalone AP, the administrator will have to copy each SSID profile to just one NWA (which will serve as the NWA controller AP.)

Note: This tutorial covers only the **MGNT MODE** and **Controller** screens.

You will need to do the following steps to configure the management modes of your NWAs.

- 1 Assign one NWA AP (**A**) as the controller AP for your wireless NWA AP network. This will be your primary controller AP. Acquire another NWA with the same model and firmware version as **A**, to serve as the secondary controller AP (**E**). Both controller APs (**A** and **E**) are in the 1st floor of the building (recommended). The NWA APs (**B**, **C** and **D**) from the 2nd, 3rd and 4th floors are going to be your managed APs.

Note: The controllers need to have static IP addresses in the same network. Make sure you set the IP addresses in the **IP** screen (see [Section 14.4 on page 176](#)).

- Configure the newly added NWA (**E**) in **Secondary Controller AP** mode.
  - Configure the 1st floor NWA in **Primary Controller AP (A)** mode and enter the IP address of your **Secondary Controller AP (E)** for synchronization.
- 2 Change the management mode of your 2nd, 3rd and 4th floor NWAs (**B**, **C** and **D**, originally in default standalone mode) to **Managed AP** mode. You can also manually enter the IP addresses of your primary and secondary NWA controller APs.
  - 3 Add the newly converted managed APs (**B**, **C** and **D**, from step 4) to the **Managed Access Points List** of the NWA primary controller AP.
  - 4 Check your settings and test the configuration. This example uses screens from G-302 v3, a wireless client that will try to access one of the managed APs, for this section.

## 6.5.4 Configure Your NWA in Controller AP Mode

The NWA is set to **Standalone AP** mode by default. After you have made sure you have the correct configuration (see [Section 23.8 on page 272](#)) in the NWAs (**A** and **E**) of the 1st floor, you need to set both of them to controller AP mode, one will serve as your main controller while the other works as your backup.

Note: If your NWA is in controller AP mode, it serves as an access point for other APs in managed mode as well as for wireless clients in the network. That is, it still functions like a regular access point on top of being a controller AP. If you enable a SSID profile for it, the controller AP can still appear in the list of available wireless networks for wireless clients. However in case you have both primary and secondary controller APs in the network, the secondary controller AP's WLAN radio is turned off as long as the primary controller AP is turned on.

- 1 Access the Web Configurator of the NWA. Go to **MGNT MODE** to open the following screen.

**Figure 63** Tutorial: MGNT Mode (AP Controller)

The screenshot shows the 'MGNT Mode' web configurator. Under the 'Management Mode' heading, there are four radio button options: 'AP Controller' (which is selected and circled in red), 'Standalone AP', 'Managed AP', and 'Auto AP Controller IP (DHCP Server Option 43 setting required)'. Below the 'Managed AP' option, there is a sub-option for 'Manual AP Controller IP'. This sub-option includes two text input fields: 'Primary AP Controller IP' and 'Secondary AP Controller IP', both containing the value '0.0.0.0'. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

- 2 Select **AP Controller** and click **Apply**.
- 3 The device reboots. You need to log in again to the Web Configurator.

### 6.5.4.1 Secondary AP Controller

The secondary AP controller is simply a backup of the primary AP controller. It takes over the management of APs covered by the primary controller AP as soon as the secondary controller AP fails to detect the primary AP controller's presence. This happens when the primary controller AP is disconnected from the network, rebooting or turned off.

Note: While the primary controller AP is online, the secondary controller AP cannot configure any of the managed APs. However, it still has to be turned on to synchronize with the primary controller AP's latest settings.

- 1 To set your NWA in secondary controller AP mode, open the **Controller > Redundancy** screen (this screen only appears when the NWA is in **Controller AP** mode) in the Web Configurator of the NWA that you want to serve as backup.

**Figure 64** Tutorial: Secondary Controller AP

The screenshot shows the 'Redundancy' configuration page. At the top, there are tabs for 'AP Lists', 'Configuration', and 'Redundancy'. Below the tabs, the 'Redundancy' section is highlighted. A dropdown menu labeled 'Redundancy' is set to 'Enable'. Below this, there are two radio button options: 'Primary AP Controller' (unselected) and 'Secondary AP Controller' (selected). Under the 'Secondary AP Controller' option, there is a text input field for 'Secondary IP' which is currently empty. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

- 2 Enable **Redundancy**. Then select **Secondary AP Controller** and click **Apply**.

### 6.5.4.2 Primary AP Controller

The primary controller AP manages the NWA APs (in managed AP mode) in your network. Changes made in the Web Configurator of the NWA primary AP controller are synchronized automatically with the secondary controller AP (if there is one) and the members of the managed AP list.

- 1 To set your NWA in primary controller AP mode, open the **Controller > Redundancy** screen (this screen only appears when the NWA is in **Controller AP** mode) in the Web Configurator of the NWA that you want to serve as the main controller.

**Figure 65** Tutorial: Primary Controller AP

The screenshot shows the 'Redundancy' configuration page. At the top, there are tabs for 'AP Lists', 'Configuration', and 'Redundancy'. Below the tabs, the 'Redundancy' section is highlighted. A dropdown menu labeled 'Redundancy' is set to 'Enable'. Below this, there are two radio button options: 'Primary AP Controller' (selected) and 'Secondary AP Controller' (unselected). Under the 'Primary AP Controller' option, there is a text input field for 'Secondary IP' which contains the value '192.168.1.27'. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

- 2 Enable **Redundancy**. Then select **Primary AP Controller** and enter the IP address of the secondary controller AP (required). Click **Apply**.

Note: Only NWAs in managed AP mode are visible to the controller AP.

## 6.5.5 Setting Your NWA in Managed AP Mode

After setting the NWAs (**A** and **E**) to controller AP modes, you can now transform the NWAs (**B**, **C** and **D**) in the 2nd, 3rd and 4th floors of your company building to managed APs.

It is very important to note that once an NWA is in managed AP mode, its web configurator cannot be viewed anymore. It cannot be accessed any other way other than through its controller AP's Web Configurator. The same rule applies to its TELNET, FTP and SNMP features. To put it simply, the managed NWA is not directly configurable. This is because its controller AP is continuously managing it.

You can switch the NWA to standalone AP mode by pressing the reset button on the casing (NWA-3500 only). Previous configurations are lost.

- 1 To set your NWA in managed AP mode, open the **MGNT** screen in the Web Configurator of the NWA that you want to serve as a managed AP.

**Figure 66** Tutorial: Managed AP

The screenshot shows the 'MGNT Mode' configuration interface. Under the 'Management Mode' section, three radio buttons are present: 'AP Controller', 'Standalone AP', and 'Managed AP'. The 'Managed AP' option is selected and highlighted with a red rounded rectangle. Below 'Managed AP', there are two sub-options: 'Auto AP Controller IP (DCHP Server Option 43 setting required)' and 'Manual AP Controller IP'. The 'Manual AP Controller IP' option is selected. Under this option, there are two input fields: 'Primary AP Controller IP' with the value '192.168.1.31' and 'Secondary AP Controller IP' with the value '192.168.1.27'. At the bottom of the screen, there are 'Apply' and 'Reset' buttons.

- 2 Select **Managed AP** and enter the IP addresses of the NWA primary and secondary controller AP (recommended). Click **Apply**.

Note: DHCP Server Option 43 enables your managed AP to send a request to be managed to controller APs that are within range, even if the controller AP belongs to another network.

- 3 You are logged out of the Web Configurator and the screen shows a message that the device is rebooting. You lose access to the Web Configurator.

You must now add the NWA managed APs to the controller's managed AP list.

## 6.5.6 Configuring the Managed Access Points List

At this point, you have 3 NWA managed APs (**B**, **C** and **D**) that can now be managed by the primary controller AP.

First in the Web Configurator of your primary controller AP (**A**), go to **Controller > Configuration**.

**Figure 67** Tutorial: Registration Type

The screenshot shows the 'Controller Setting' page with the following details:

- Pre-Shared Key: 12345678 (8-32 characters)
- Registration Type:  Manual  Always Accept
- Buttons: Apply, Reset

If the **Registration Type** is set to **Manual**, the controller AP add managed APs to a queue in the **Un-Managed Access Points List** in the **Controller > AP Lists** screen.

If the **Registration Type** is set to **Always Accept**, the controller AP immediately adds the AP to the **Managed Access Points List** in the **Controller > AP Lists** screen.

For this example, we set the **Registration Type** to **Manual**.

- 1 To add a managed AP to the controller AP's coverage, go to **Controller > AP Lists**.

**Figure 68** Tutorial: AP List (Un-Managed)

The screenshot shows the 'Un-Managed Access Points List' with the following data:

Index	<input type="checkbox"/>	IP	MAC Address	Model	Description	Status	Edit
1	<input checked="" type="checkbox"/>	192.168.1.33	00:13:49:DF:42:A8	NWA-3500 802.11a/g	NWA-Managed AP-1st floor		Edit
2	<input checked="" type="checkbox"/>	192.168.1.35	00:19:27:DF:42:16	NWA-3500 802.11a/g	NWA-Managed AP-2nd floor		

Buttons: Delete, Add

Automatic Refresh Interval: None Refresh



- 2 Select the NWA managed APs from the **Un-Managed Access Points List** as shown in the screen above. You can also identify these managed APs by filling in the **Description** field. Click **Add**.
- 3 The 2nd, 3rd and 4th floor NWA managed APs (**B**, **C** and **D**) should now be in the **Manged Access Points List**. By default, newly added managed APs in the list have their **WLAN Radio Profile** set to disabled. This means that their wireless functions are turned off.

Note: The NWA controller AP uses **WLAN Radio Profile** to categorize different wireless settings present in a managed AP. Each profile contains the SSID, security mode, RADIUS, Layer-2 Isolation and MAC filter configurations.

Turn on a WLAN Radio Profile by selecting the managed AP from the list and clicking **Edit**.

**Figure 69** Tutorial:AP List (Managed)

Index	<input type="checkbox"/>	IP	MAC Address	Model	Description	Status	Edit
1	<input type="checkbox"/>	127.0.0.1	00:19:CB:08:81:03	NWA-3160 802.11a/g	NWA-Primary Controller		Edit
2	<input checked="" type="checkbox"/>	192.168.1.33	00:13:49:DF:42:A8	NWA-3500 802.11a/q	NWA-Managed AP-1st floor		Edit
3	<input checked="" type="checkbox"/>	192.168.1.35	00:19:27:DF:42:16	NWA-3500 802.11a/g	NWA-Managed AP-2nd floor		Edit

Un-Managed Access Points List

Index	<input type="checkbox"/>	IP	MAC Address	Model	Description
Add					

Automatic Refresh Interval: None Refresh

- 4 In the screen that opens, choose the radio profile for each WLAN radio and click **Apply**.

**Figure 70** Tutorial: Managed AP WLAN Radio Profile

AP Configuration

Access Point

Model: NWA-3500  
 MAC Address: 00:13:49:DF:42:A8  
 Description: NWA-Managed AP-1st floor

Enable Breathing LED

WLAN1 Radio Profile: radio06  
 WLAN2 Radio Profile: Disable

Apply Reset

In this example, the 1st floor NWA managed AP uses **radio06** for its **WLAN1 Radio Profile**.

The WLAN2 radio is disabled. Refer to [Section 5.7.1 on page 62](#) for instructions on how to set up WLAN radio profiles in the NWA controller APs.

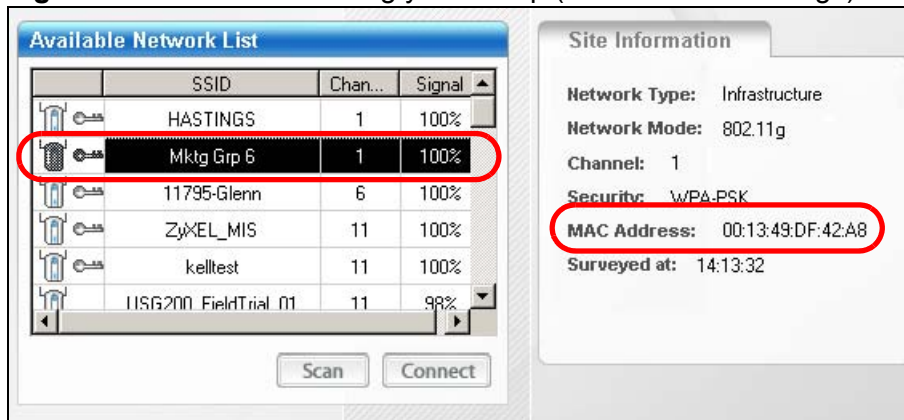
## 6.5.7 Checking your Settings and Testing the Configuration

The NWAs should be working at this point. You can configure the settings of each NWA unit by just opening the Web Configurator of the primary controller AP.

One way to test if the setup is working is to use a wireless client to check if all the profiles you have set up in the managed APs and the controller APs are available for wireless connection.

For this example, we use the G-302 v3 wireless client utility screen to check if **radio6** (SSID: **Mktg Grp 6**) is in the list of wireless networks available.

**Figure 71** Tutorial: Checking your Setup (MGNT Mode Settings)



Open the wireless client's screen that list the available networks within range. In the image above, we can see Mktg Grp 6 which is the SSID in the WLAN1 radio profile enabled for the 1st floor NWA managed AP.

Do the same for the other WLAN radio profiles of the remaining NWA APs (both controller and managed APs) and check if all the security configurations and device settings are in place. Do the proper modifications in the primary controller AP's Web Configurator if necessary.

**Note:** Be sure you update the primary controller AP and not the secondary controller AP when setting the configuration for the managed APs. If you accidentally set up the secondary controller AP instead, the changes you made will not take effect. They are overridden by the configurations of the primary controller AP.

---

# PART II

## The Web Configurator

---

System Screens (109)

Wireless Configuration (119)

SSID Screen (141)

Wireless Security Screen (147)

RADIUS Screen (161)

Layer-2 Isolation Screen (165)

MAC Filter Screen (171)

IP Screen (175)

Rogue AP Detection (179)

Remote Management Screens (187)

Internal RADIUS Server (199)

Certificates (207)

Log Screens (227)

VLAN (235)

Maintenance (265)

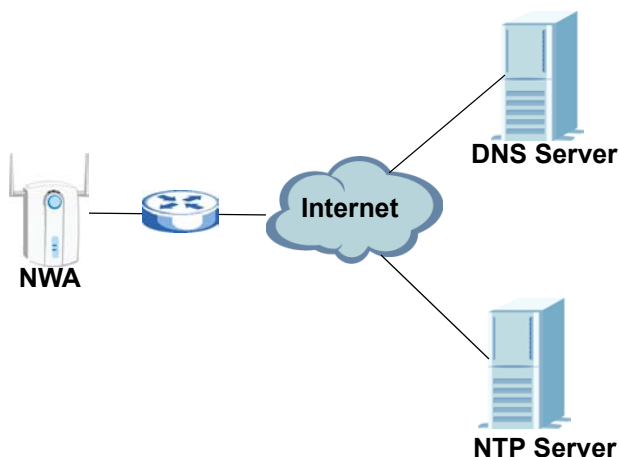


# System Screens

## 7.1 Overview

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

**Figure 72** 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.

## 7.2 What You Can Do in the System Screens

- Use the **General** screen (see [Section 7.4 on page 112](#)) to specify the **System name**, **Domain name** and Web Configurator timeout limit. You can also configure your **System DNS Servers** in this screen.
- Use the **Password** screen (see [Section 7.5 on page 113](#)) to manage the password for your ZyXEL Device and have a RADIUS server authenticate management logins to the ZyXEL Device.

- Use the **Time Setting** screen (see [Section 7.6 on page 116](#)) to change your NWA's time and date. This screen allows you to configure the NWA's time based on your local time zone.

## 7.3 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 22** 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.

### **7.3.1 Administrator Authentication on RADIUS**

The administrator authentication on RADIUS feature lets a (external or internal) RADIUS server authenticate management logins to the NWA. This is useful if you need to regularly change a password that you use to manage several NWAs.

Activate administrator authentication on RADIUS in the SYSTEM > Password screen and configure the same user name, password and RADIUS server information on each NWA. Then, whenever you want to change the password, just change it on the RADIUS server.

## 7.4 General Setup Screen

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

**Figure 73** System > General

The following table describes the labels in this screen.

**Table 23** System > General

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



**Table 23** System > General

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

## 7.5 Configuring the Password

It is strongly recommended that you change your NWA's password. Click **SYSTEM > Password**. The screen appears as shown.

If you forget your NWA's password (or IP address), you will need to reset the device. See the section on resetting the NWA for details

Note: Regardless of how you configure this screen, you still use the local system password to log in via the console port (for internal use only).

**Figure 74** System > Password.

The following table describes the labels in this screen.

**Table 24** System > Password

LABEL	DESCRIPTIONS
Enable Admin at Local	Select this check box to have the device authenticate management logins to the device.
Use old setting	Select this to have the NWA use the local management password already configured on the device ("1234" is the default).
Use new setting	Select this if you want to change the local management password.
Old Password	Type in your existing system password ("1234" is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.
Enable Admin on RADIUS	Select this (and configure the other fields in this section) to have a RADIUS server authenticate management logins to the NWA.
Use old setting	Select this to have a RADIUS server authenticate management logins to the NWA using the RADIUS username and password already configured on the device.
Use new setting	Select this if you want to change the RADIUS username and password the NWA uses to authenticate management logon.
User Name	Enter the username for this user account. This name can be up to 31 ASCII characters long, including spaces.

**Table 24** System > Password

LABEL	DESCRIPTIONS
Password	<p>Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. Spaces are allowed.</p> <p>Note: If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.</p>
RADIUS	<p>Select the RADIUS server profile of the RADIUS server that is to authenticate management logins to the NWA.</p> <p>The NWA tests the user name and password against the RADIUS server when you apply your settings.</p> <ul style="list-style-type: none"> <li>• The user name and password must already be configured in the RADIUS server.</li> <li>• You must already have a RADIUS profile configured for the RADIUS server (see <a href="#">Section 11.4 on page 163</a>).</li> <li>• The server must be set to <b>Active</b> in the profile.</li> </ul>
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.6 Configuring Time Setting

To change your NWA's time and date, click **SYSTEM > Time Setting**. The screen appears as shown. Use this screen to configure the NWA's time based on your local time zone.

**Figure 75** System > Time Setting

The following table describes the labels in this screen.

**Table 25** System > Time Setting

LABEL	DESCRIPTION
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).
Current Date	This field displays the last updated date from the time server.
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .

**Table 25** System > Time Setting

LABEL	DESCRIPTION
New Date (yyyy:mm:dd)	This field displays the last updated date from the time server or the last date configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .
Get from Time Server	Select this radio button to have the NWA get the time and date from the time server you specify below.
Auto	Select this to have the NWA use the predefined list of time servers.
User Defined Time Server Address	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	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Daylight Savings</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Second, Sunday, March</b> and type 2 in the <b>o'clock</b> field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Mar., Last, Sun</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type "02" because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Daylight Savings</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, November</b> and type 2 in the <b>o'clock</b> field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Oct., Last, Sun</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to reload the previous configuration for this screen.

## 7.7 Technical Reference

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

### 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 26** 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

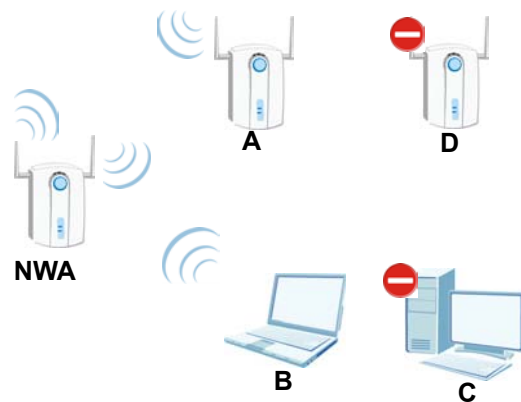
When the NWA uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the NWA goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers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

# Wireless Configuration

## 8.1 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 76** 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.

## 8.2 What You Can Do in the Wireless Screen

Use the **Wireless > Wireless** screen (see [Section 8.4 on page 123](#)) to configure the NWA to use a WLAN interface and operate in **AP** (Access Point), **AP + Bridge**, **Bridge / Repeater** or **MBSSID** mode.

## 8.3 What You Need To Know

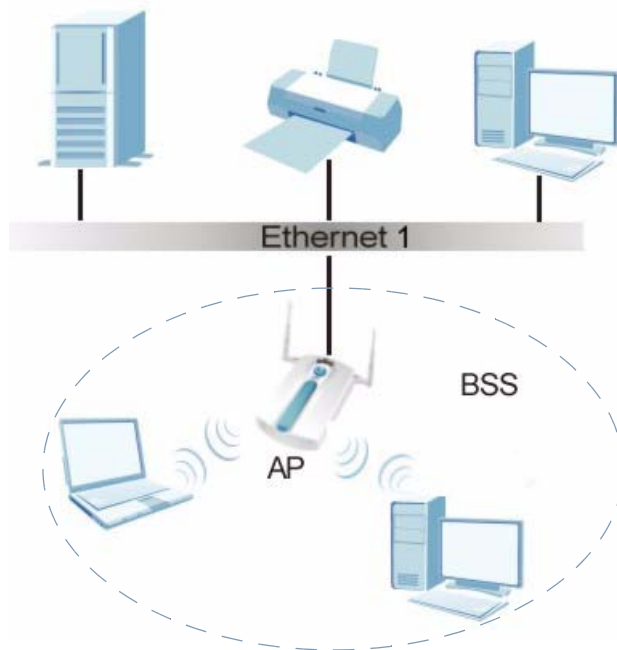
The following are wireless network terminologies that are relevant to this chapter.

### BSS

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

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

**Figure 77** Basic Service set



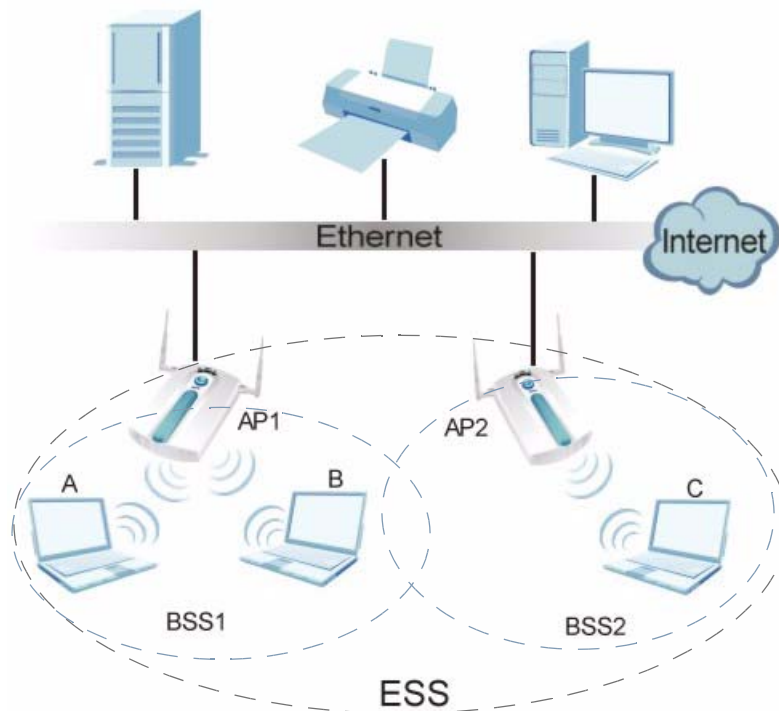
### ESS

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). An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and



their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

**Figure 78** Extended Service Set



### 8.3.1 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 Mode.** The NWA functions as a bridge and access point simultaneously.
- **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 31](#) for illustrations of these wireless applications. The following are terms used for the wireless screens.

## 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 ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device 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 **802.11a**, **802.11b Only**, **802.11g Only** and **802.11b+g**.

### 8.3.2 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 eight 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.

## 8.4 Configuring Wireless Settings

Click **WIRELESS > Wireless**. The screen varies depending upon the operating mode you select.

### 8.4.1 Access Point Mode

Select **Access Point** as the **Operating Mode** to display the screen shown next.

**Figure 79** Wireless: Access Point

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																				
<p><b>WLAN Interface</b> <span style="float: right;">WLAN1 ▾</span></p> <p><b>Operating Mode</b> <span style="float: right;">Access Point ▾</span></p> <p><b>802.11 Mode</b> <span style="float: right;">802.11a ▾</span></p> <p><input checked="" type="checkbox"/> Super Mode</p> <p><input type="checkbox"/> Disable channel switching for DFS</p> <p><b>Choose Channel ID</b> <span style="float: right;">Channel-036 5180MHz ▾</span></p> <p><b>RTS/CTS Threshold</b> <span style="float: right;">2346 (256 ~ 2346)</span></p> <p><b>Fragmentation Threshold</b> <span style="float: right;">2346 (256 ~ 2346) (Fragmentation threshold shall be an even number)</span></p> <p><b>Beacon Interval</b> <span style="float: right;">100 (30ms ~ 1000ms)</span></p> <p><b>DTIM</b> <span style="float: right;">1 (1 ~ 100)</span></p> <p><b>Output Power</b> <span style="float: right;">100% ▾</span></p> <p><b>SSID Profile</b> <span style="float: right;">SSID03 ▾</span></p>																									
<p><b>Rates Configuration</b></p> <table border="1"> <thead> <tr> <th>Rate</th> <th>Configuration</th> <th>Rate</th> <th>Configuration</th> </tr> </thead> <tbody> <tr> <td>6 Mbps</td> <td>Basic ▾</td> <td>9 Mbps</td> <td>Optional ▾</td> </tr> <tr> <td>12 Mbps</td> <td>Basic ▾</td> <td>18 Mbps</td> <td>Optional ▾</td> </tr> <tr> <td>24 Mbps</td> <td>Basic ▾</td> <td>36 Mbps</td> <td>Optional ▾</td> </tr> <tr> <td>48 Mbps</td> <td>Optional ▾</td> <td>54 Mbps</td> <td>Optional ▾</td> </tr> </tbody> </table>						Rate	Configuration	Rate	Configuration	6 Mbps	Basic ▾	9 Mbps	Optional ▾	12 Mbps	Basic ▾	18 Mbps	Optional ▾	24 Mbps	Basic ▾	36 Mbps	Optional ▾	48 Mbps	Optional ▾	54 Mbps	Optional ▾
Rate	Configuration	Rate	Configuration																						
6 Mbps	Basic ▾	9 Mbps	Optional ▾																						
12 Mbps	Basic ▾	18 Mbps	Optional ▾																						
24 Mbps	Basic ▾	36 Mbps	Optional ▾																						
48 Mbps	Optional ▾	54 Mbps	Optional ▾																						
<p><input checked="" type="checkbox"/> Enable Antenna Diversity</p> <p><input checked="" type="checkbox"/> Enable Breathing LED</p> <p><input checked="" type="checkbox"/> Enable Spanning Tree Protocol (STP)</p> <p><input checked="" type="checkbox"/> Enable Roaming</p> <p><small>(The Breathing LED, STP and Roaming are common settings. The changes are for both WLAN Interfaces.)</small></p>																									
<p>Apply      Reset</p>																									

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

**Table 27** Wireless: Access Point

LABEL	DESCRIPTION
WLAN Interface	<p>Select which WLAN adapter you want to configure.</p> <p>It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.</p>
Operating Mode	<p>Select <b>Access Point</b> from the drop-down list.</p>
802.11 Mode	<p>Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the NWA.</p> <p>Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the NWA.</p> <p>Select <b>802.11b+g</b> 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.</p> <p>Select <b>802.11a</b> to allow only IEEE 802.11a compliant WLAN devices to associate with the NWA.</p>
Super Mode	<p>Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting.</p>
Disable channel switching for DFS	<p>This field displays only when you select <b>802.11a</b> in the <b>802.11 Mode</b> field. Select this if you do not want to use DFS (Dynamic Frequency Selection).</p>
Choose Channel ID	<p>Set the operating frequency/channel depending on your particular region.</p> <p>To manually set the NWA to use a channel, select a channel from the drop-down list box.</p> <p>Click <b>MAINTENANCE</b> and then the <b>Channel Usage</b> tab to open the <b>Channel Usage</b> screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.</p> <p>To have the NWA automatically select a channel, click <b>Scan</b> instead.</p>
Scan	<p>Click this button to have the NWA automatically scan for and select the channel with the least interference.</p>
Disable channel switching for DFS	<p>This field is available when you select <b>802.11a</b> in the <b>802.11 Mode</b> field.</p> <p>DFS (dynamic frequency selection) allows an AP to detect other devices in the same channel. If there is another device using the same channel, the AP changes to a different channel, so that it can avoid interference with radar systems or other wireless networks.</p> <p>Select this option to disable DFS on the NWA when <b>802.11 Mode</b> is set to <b>802.11a</b>.</p>

**Table 27** Wireless: Access Point

LABEL	DESCRIPTION
RTS/CTS Threshold	<p>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 (256) turns on the RTS/CTS handshake. Enter a value between <b>256</b> and <b>2346</b>.</p> <p>This field is not available when <b>Super Mode</b> is selected.</p>
Beacon Interval	<p>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 low-power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.</p>
DTIM	<p>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. This value can be set from 1 to 100.</p>
Fragmentation Threshold	<p>The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between <b>256</b> and <b>2346</b>.</p> <p>This field is not available when <b>Super Mode</b> is selected.</p>
Output Power	<p>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 <b>100%</b>, <b>50%</b>, <b>25%</b>, <b>12.5%</b> or <b>Minimum</b>. See the product specifications for more information on your NWA's output power.</p> <p>This field is not available when you select <b>802.11a</b> in the <b>802.11 Mode</b> field.</p>
SSID Profile	<p>The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Select an <b>SSID Profile</b> from the drop-down list box.</p> <p>Configure SSID profiles in the <b>SSID</b> screen (see <a href="#">Section 9.4 on page 143</a> for information on configuring SSID).</p> <p><b>Note:</b> 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 <b>Apply</b> to confirm. You must then change the wireless settings of your computer to match the NWA's new settings.</p>

**Table 27** Wireless: Access Point

LABEL	DESCRIPTION
Rates Configuration	<p>This section controls the data rates permitted for clients.</p> <p>For each <b>Rate</b>, select an option from the <b>Configuration</b> list. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Basic</b> (1~11 Mbps only): Clients can always connect to the access point at this speed.</li> <li>• <b>Optional</b>: Clients can connect to the access point at this speed, when permitted to do so by the AP.</li> <li>• <b>Disabled</b>: Clients cannot connect to the access point at this speed.</li> </ul>
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Breathing LED	<p>Select this check box to enable the blue “breathing” LED, also known as the NWA LED.</p> <p>Clear the check box to turn this LED off even when the NWA is on and data is being transmitted and received.</p>
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select this to activate STP on the NWA.
Enable Roaming	<p>Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this to enable roaming on the NWA if you have two or more NWAs on the same subnet.</p> <p>Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.</p>
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.4.2 Bridge / Repeater Mode

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

The NWA can establish up to five wireless links with other APs.

To have the NWA act as a wireless bridge only, click **WIRELESS > Wireless** and select **Bridge / Repeater** as the **Operating Mode**.

**Figure 80** Wireless: Bridge / Repeater

**Wireless**

**WLAN Interface**

**Operating Mode**

**802.11 Mode**

**Disable channel switching for DFS**

**Choose Channel ID**

**RTS/CTS Threshold**  (256 ~ 2346)

**Fragmentation Threshold**  (256 ~ 2346) (Fragmentation threshold shall be an even number)

**Output Power**

**Rates Configuration**

Rate	Configuration	Rate	Configuration
6 Mbps	<input type="text" value="Basic"/>	9 Mbps	<input type="text" value="Optional"/>
12 Mbps	<input type="text" value="Basic"/>	18 Mbps	<input type="text" value="Optional"/>
24 Mbps	<input type="text" value="Basic"/>	36 Mbps	<input type="text" value="Optional"/>
48 Mbps	<input type="text" value="Optional"/>	54 Mbps	<input type="text" value="Optional"/>

**Enable WDS Security**

**TKIP (ZyAIR Series Compatible)**

**AES**

Index	Active	Remote Bridge MAC	PSK
1	<input type="checkbox"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>

**Enable Antenna Diversity**

**Enable Breathing LED**

**Enable Spanning Tree Protocol (STP)**

(The Breathing LED, STP and Roaming are common settings. The changes are for both WLAN Interfaces.)

The following table describes the bridge labels in this screen.

**Table 28** Wireless: Bridge / Repeater

LABEL	DESCRIPTIONS
Operating Mode	Select <b>Bridge / Repeater</b> in this field.
Enable WDS Security	<p>Select this to turn on security for the NWA's Wireless Distribution System (WDS). A Wireless Distribution System is a wireless connection between two or more APs. If you do not select the check box, traffic between APs is not encrypted.</p> <p><b>Note:</b> WDS security is independent of the security settings between the NWA and any wireless clients.</p> <p>When you enable WDS security, also do the following:</p> <ul style="list-style-type: none"> <li>• Select the type of security you want to use (<b>TKIP</b> or <b>AES</b>) to secure traffic on your WDS.</li> <li>• Enter a pre-shared key in the <b>PSK</b> field for each access point in your WDS. Each access point can use a different pre-shared key.</li> <li>• Configure WDS security and the relevant PSK in each of your other access point(s).</li> </ul> <p><b>Note:</b> Other APs must use the same encryption method to enable WDS security.</p>
TKIP (ZyAIR Series Compatible)	<p>Select this to enable Temporal Key Integrity Protocol (TKIP) security on your WDS. This option is compatible with other ZyXEL access points including that support WDS security. Use this if the other access points on your network support WDS security but do not have an AES option.</p> <p><b>Note:</b> Check your other AP's documentation to make sure it supports WDS security.</p> <p><b>Note:</b> At the time of writing, this option is compatible with other ZyXEL NWA Series and G-3000/G-3000H access points only.</p>
AES	<p>Select this to enable Advanced Encryption System (AES) security on your WDS. AES provides superior security to TKIP. Use AES if the other access points on your network support it for the WDS.</p> <p><b>Note:</b> At the time of writing, this option is compatible with other ZyXEL NWA Series access points only.</p>
Index	This is the index number of the bridge connection.
Active	Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.
Remote Bridge MAC	Type the MAC address of the peer device in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
PSK	Type a pre-shared key (PSK) from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). You must also set the peer device to use the same pre-shared key. Each peer device can use a different pre-shared key.



See [Table 27 on page 124](#) for information on the other labels in this screen.

### 8.4.3 AP + Bridge Mode

Select **AP + Bridge** as the **Operating Mode** in the **WIRELESS > Wireless** screen to have the NWA function as a bridge and access point simultaneously. See the section on applications for more information.

**Figure 81** Wireless: AP + Bridge

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																								
<b>WLAN Interface</b> <span style="float: right;">WLAN1 ▾</span> <b>Operating Mode</b> <span style="float: right;">AP+Bridge ▾</span> <b>802.11 Mode</b> <span style="float: right;">802.11a ▾</span> <input checked="" type="checkbox"/> <b>Super Mode</b> <input type="checkbox"/> <b>Disable channel switching for DFS</b> <b>Choose Channel ID</b> <span style="float: right;">Channel-036 5180MHz ▾</span> <b>RTS/CTS Threshold</b> <span style="float: right;">2346 (256 ~ 2346)</span> <b>Fragmentation Threshold</b> <span style="float: right;">2346 (256 ~ 2346) (Fragmentation threshold shall be an even number)</span> <b>Beacon Interval</b> <span style="float: right;">100 (30ms ~ 1000ms)</span> <b>DTIM</b> <span style="float: right;">1 (1 ~ 100)</span> <b>Output Power</b> <span style="float: right;">100% ▾</span> <b>SSID Profile</b> <span style="float: right;">SSID03 ▾</span>																													
<b>Rates Configuration</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Rate</th> <th>Configuration</th> <th>Rate</th> <th>Configuration</th> </tr> </thead> <tbody> <tr> <td>6 Mbps</td> <td>Basic ▾</td> <td>9 Mbps</td> <td>Optional ▾</td> </tr> <tr> <td>12 Mbps</td> <td>Basic ▾</td> <td>18 Mbps</td> <td>Optional ▾</td> </tr> <tr> <td>24 Mbps</td> <td>Basic ▾</td> <td>36 Mbps</td> <td>Optional ▾</td> </tr> <tr> <td>48 Mbps</td> <td>Optional ▾</td> <td>54 Mbps</td> <td>Optional ▾</td> </tr> </tbody> </table>						Rate	Configuration	Rate	Configuration	6 Mbps	Basic ▾	9 Mbps	Optional ▾	12 Mbps	Basic ▾	18 Mbps	Optional ▾	24 Mbps	Basic ▾	36 Mbps	Optional ▾	48 Mbps	Optional ▾	54 Mbps	Optional ▾				
Rate	Configuration	Rate	Configuration																										
6 Mbps	Basic ▾	9 Mbps	Optional ▾																										
12 Mbps	Basic ▾	18 Mbps	Optional ▾																										
24 Mbps	Basic ▾	36 Mbps	Optional ▾																										
48 Mbps	Optional ▾	54 Mbps	Optional ▾																										
<input type="checkbox"/> <b>Enable WDS Security</b> <input checked="" type="radio"/> <b>TKIP (ZyAIR Series Compatible)</b> <input type="radio"/> <b>AES</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Index</th> <th>Active</th> <th>Remote Bridge MAC</th> <th>PSK</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> <td></td> </tr> <tr> <td>2</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> <td></td> </tr> <tr> <td>3</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> <td></td> </tr> <tr> <td>4</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> <td></td> </tr> <tr> <td>5</td> <td><input type="checkbox"/></td> <td>00:00:00:00:00:00</td> <td></td> </tr> </tbody> </table>						Index	Active	Remote Bridge MAC	PSK	1	<input type="checkbox"/>	00:00:00:00:00:00		2	<input type="checkbox"/>	00:00:00:00:00:00		3	<input type="checkbox"/>	00:00:00:00:00:00		4	<input type="checkbox"/>	00:00:00:00:00:00		5	<input type="checkbox"/>	00:00:00:00:00:00	
Index	Active	Remote Bridge MAC	PSK																										
1	<input type="checkbox"/>	00:00:00:00:00:00																											
2	<input type="checkbox"/>	00:00:00:00:00:00																											
3	<input type="checkbox"/>	00:00:00:00:00:00																											
4	<input type="checkbox"/>	00:00:00:00:00:00																											
5	<input type="checkbox"/>	00:00:00:00:00:00																											
<input checked="" type="checkbox"/> <b>Enable Antenna Diversity</b> <input checked="" type="checkbox"/> <b>Enable Breathing LED</b> <input checked="" type="checkbox"/> <b>Enable Spanning Tree Protocol (STP)</b> <input checked="" type="checkbox"/> <b>Enable Roaming</b> <small>(The Breathing LED, STP and Roaming are common settings. The changes are for both WLAN Interfaces.)</small>																													
<span style="margin: 0 20px;">Apply</span> <span>Reset</span>																													

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

## 8.4.4 MBSSID Mode

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

**Figure 82** Wireless: MBSSID

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
<b>WLAN Interface</b>		WLAN1			
<b>Operating Mode</b>		MBSSID			
<b>802.11 Mode</b>		802.11a			
<input checked="" type="checkbox"/> Super Mode					
<input type="checkbox"/> Disable channel switching for DFS					
<b>Choose Channel ID</b>		Channel-036 5180MHz			
<b>RTS/CTS Threshold</b>		2346 (256 ~ 2346)			
<b>Fragmentation Threshold</b>		2346 (256 ~ 2346) (Fragmentation threshold shall be an even number)			
<b>Beacon Interval</b>		100 (30ms ~ 1000ms)			
<b>DTIM</b>		1 (1 ~ 100)			
<b>Output Power</b>		100%			
<b>Rates Configuration</b>					
Rate	Configuration	Rate	Configuration		
6 Mbps	Basic	9 Mbps	Optional		
12 Mbps	Basic	18 Mbps	Optional		
24 Mbps	Basic	36 Mbps	Optional		
48 Mbps	Optional	54 Mbps	Optional		
<b>Select SSID Profile</b>					
Index	Active	Profile	Index	Active	Profile
1	<input type="checkbox"/>	VoIP_SSID	5	<input type="checkbox"/>	SSID03
2	<input type="checkbox"/>	Guest_SSID	6	<input type="checkbox"/>	SSID03
3	<input type="checkbox"/>	SSID03	7	<input type="checkbox"/>	SSID03
4	<input type="checkbox"/>	SSID03	8	<input type="checkbox"/>	SSID03
<input checked="" type="checkbox"/> Enable Antenna Diversity <input checked="" type="checkbox"/> Enable Breathing LED <input checked="" type="checkbox"/> Enable Spanning Tree Protocol (STP) <input checked="" type="checkbox"/> Enable Roaming <small>(The Breathing LED, STP and Roaming are common settings. The changes are for both WLAN Interfaces.)</small>					
Apply			Reset		

The following table describes the labels in this screen.

**Table 29** Wireless: MBSSID

LABEL	DESCRIPTION
Operating Mode	Select <b>MBSSID</b> in this field to display the screen as shown
Select SSID Profile	<p>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.</p> <p>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.</p>
Index	This is the index number of the SSID profile.
Active	Select the check box to enable an SSID profile.
Profile	<p>Select the profile(s) of the SSIDs you want to use in your wireless network. You can have up to eight BSSs running on the NWA simultaneously, one of which is always the pre-configured VoIP_SSID profile and another of which is always the pre-configured Guest_SSID profile.</p> <p>Configure SSID profiles in the <b>SSID</b> screen.</p>

See [Table 27 on page 124](#) for information on the other labels in this screen.

## 8.5 Technical Reference

This section provides technical background information about the topics covered in this chapter. Refer to [Appendix B on page 319](#) for further readings on Wireless LAN.

### 8.5.1 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.

#### 8.5.1.1 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.

### 8.5.1.2 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 30** 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.

### 8.5.1.3 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.

### 8.5.1.4 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 31** 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.

### 8.5.2 DFS

When you choose **802.11a** in **Access Point** mode, the NWA uses DFS (Dynamic Frequency Selection) to give you a wider choice of wireless channels.

DFS allows you to use channels in the frequency range normally reserved for radar systems. Radar uses radio signals to detect the location of objects for military, meteorological or air traffic control purposes. As long as your NWA detects no radar activity on the channel you select, you can use the channel to communicate. However, a wireless LAN operating on the same frequency as an active radar system could disrupt the radar system. Therefore, if the NWA detects radar activity on the channel you select, it automatically instructs the wireless clients to move to another channel, then resumes communications on the new channel.

### 8.5.3 Roaming

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

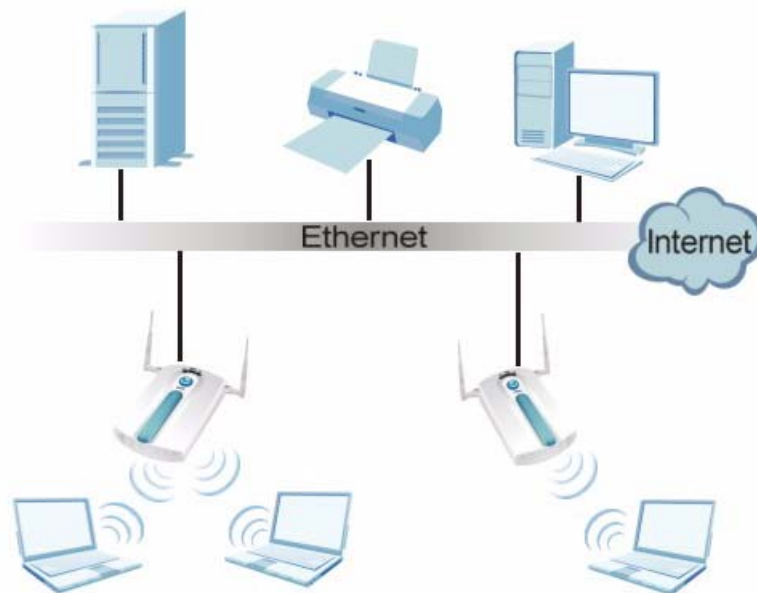
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is known as roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access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

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the other access points on the LAN about the change. An example is shown in [Figure 83 on page 134](#).

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

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

**Figure 83** Roaming Example



The steps below describe the roaming process.

- 1 Wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**.
- 2 Wireless station **Y** scans and detects the signal of access point **AP 2**.
- 3 Wireless station **Y** sends an association request to access point **AP 2**.
- 4 Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.

- 5 Access point **AP 1** updates the new position of wireless station **Y**.

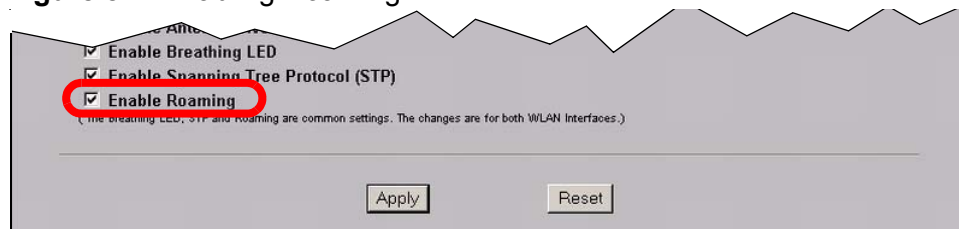
### 8.5.3.1 Requirements for Roaming

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

- All the access points must be on the same subnet and configured with the same ESSID.
- If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
- The adjacent access points should use different radio channels when their coverage areas overlap.
- All access points must use the same port number to relay roaming information.
- The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

To enable roaming on your NWA, click **WIRELESS > Wireless**. The screen appears as shown.

**Figure 84** Enabling Roaming



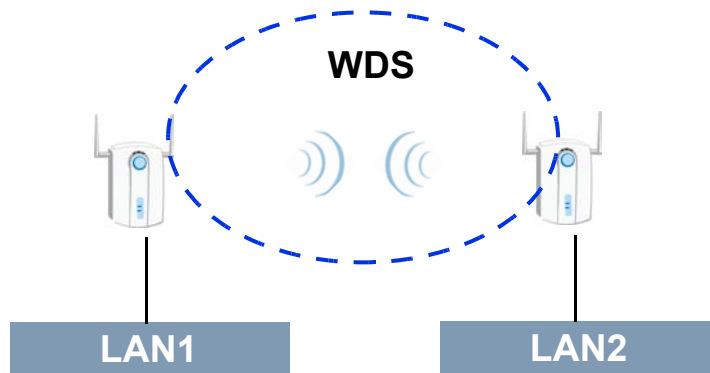
Select the **Enable Roaming** check box and click **Apply**.

Note: Roaming cannot be enabled in Bridge / Repeater mode.

## 8.5.4 Bridge / Repeater Example

This section shows an example of two NWAs in **Bridge/Repeater** mode forming a WDS (Wireless Distribution System) and allowing the computers in **LAN 1** to connect to the computers in **LAN 2**. This is shown in the following figure.

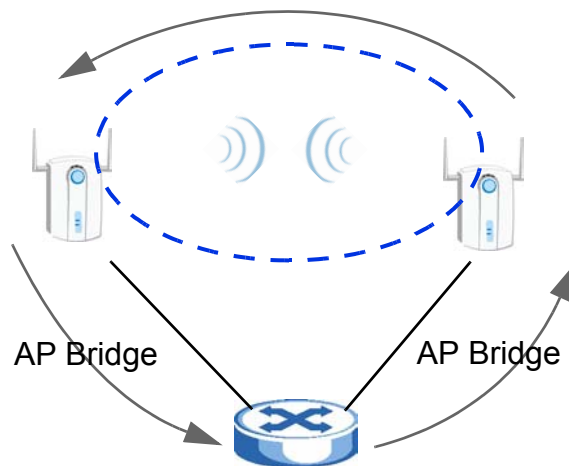
**Figure 85** Bridging Example



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.

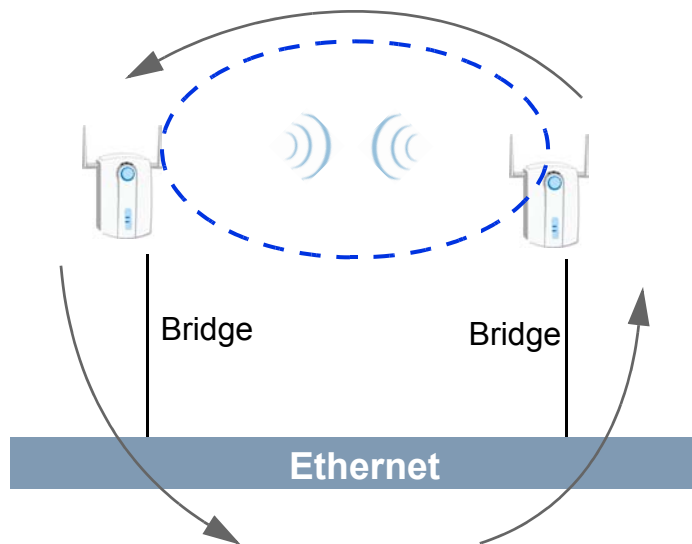
**Figure 86** Bridge Loop: Two Bridges Connected to Hub





- 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 87** 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.

## 8.5.5 Quality of Service

This section discusses the Quality of Service (QoS) features available on the NWA.

### 8.5.6 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 delivery requirements. 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 tag 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 (delay) and jitter (variations in delay).

### 8.5.6.1 WMM QoS Priorities

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

**Table 32** 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.

### 8.5.7 ATC

Automatic Traffic Classifier (ATC) is a bandwidth management tool that prioritizes data packets sent across the network. ATC assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency and a low level of jitter such as Voice over IP or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

ATC assigns priority based on packet size, since time-sensitive applications such as Internet telephony (Voice over IP or VoIP) tend to have smaller packet sizes than non-time sensitive applications such as FTP (File Transfer Protocol). The following table shows some common applications, their time sensitivity, and their typical data packet sizes. Note that the figures given are merely examples - sizes may differ according to application and circumstances.

**Table 33** Typical Packet Sizes

APPLICATION	TIME SENSITIVITY	TYPICAL PACKET SIZE (BYTES)
Voice over IP (SIP)	High	< 250
Online Gaming	High	60 ~ 90

**Table 33** Typical Packet Sizes

APPLICATION	TIME SENSITIVITY	TYPICAL PACKET SIZE (BYTES)
Web browsing (http)	Medium	300 ~ 600
FTP	Low	1500

When ATC is activated, the device sends traffic with smaller packets before traffic with larger packets if the network is congested.

ATC assigns priority to packets as shown in the following table.

**Table 34** Automatic Traffic Classifier Priorities

PACKET SIZE (BYTES)	ATC PRIORITY
1 ~ 250	ATC_High
250 ~ 1100	ATC_Medium
1100 +	ATC_Low

You should activate ATC on the NWA if your wireless network includes networking devices that do not support WMM QoS, or if you want to prioritize traffic but do not want to configure WMM QoS settings.

## 8.5.8 ATC+WMM

The NWA can use a mapping mechanism to use both ATC and WMM QoS. The ATC+WMM function prioritizes all packets transmitted onto the wireless network using WMM QoS, and prioritizes all packets transmitted onto the wired network using ATC. See [Section 9.4.1 on page 144](#) for details of how to configure ATC+WMM.

Use the ATC+WMM function if you want to do the following:

- enable WMM QoS on your wireless network and automatically assign a WMM priority to packets that do not already have one (see [Section 8.5.8.1 on page 139](#)).
- automatically prioritize all packets going from your wireless network to the wired network (see [Section 8.5.8.2 on page 140](#)).

### 8.5.8.1 ATC+WMM from LAN to WLAN

ATC+WMM from LAN (the wired Local Area Network) to WLAN (the Wireless Local Area Network) allows WMM prioritization of packets that do not already have WMM QoS priorities assigned. The NWA automatically classifies data packets using ATC and then assigns WMM priorities based on that ATC classification.

The following table shows how priorities are assigned for packets coming from the LAN to the WLAN.

**Table 35** ATC + WMM Priority Assignment (LAN to WLAN)

PACKET SIZE (BYTES)	→	ATC VALUE	→	WMM VALUE
1 ~ 250		ATC_High		WMM_VIDEO
250 ~ 1100		ATC_Medium		WMM_BEST_EFFORT
1100 +		ATC_Low		WMM_BACKGROUND

### 8.5.8.2 ATC+WMM from WLAN to LAN

ATC+WMM from WLAN to LAN automatically prioritizes (assigns an ATC value to) all packets coming from the WLAN. Packets are assigned an ATC value based on their WMM value, not their size.

The following table shows how priorities are assigned for packets coming from the WLAN to the LAN when using ATC+WMM.

**Table 36** ATC + WMM Priority Assignment (WLAN to LAN)

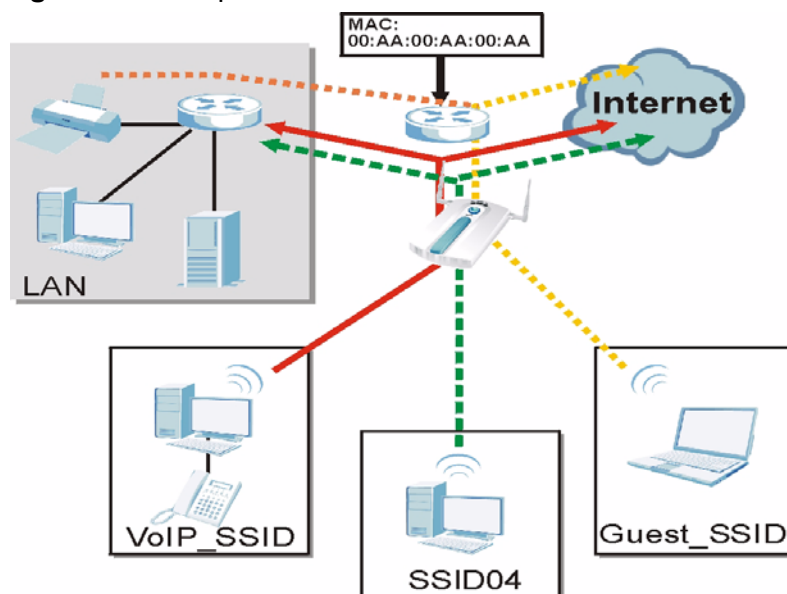
WMM VALUE	→	ATC VALUE
WMM_VOICE		ATC_High
WMM_VIDEO		ATC_High
WMM_BEST_EFFORT		ATC_Medium
WMM_BACKGROUND		ATC_Low
NONE		ATC_Medium

# SSID Screen

## 9.1 Overview

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

**Figure 88** Sample SSID Profiles



In the figure above, the NWA has three SSID profiles configured: a standard profile (**SSID04**), 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**).

## 9.2 What You Can Do in the SSID Screen

Use the **Wireless > SSID** screen (see [Section 9.4 on page 143](#)) to configure up to 16 SSID profiles for your NWA.

## 9.3 What You Need To Know

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 [Chapter 1 on page 31](#) 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).
- **Wireless > Layer 2 Isolation** (the layer 2 isolation 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.

Refer to [Section 8.3 on page 120](#) for pertinent information related to the screens in this chapter.

## 9.4 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 89** Wireless > SSID

Wireless > SSID								
Wireless								
SSID								
Security								
RADIUS								
Layer-2 Isolation								
MAC Filter								
	Index	Profile Name	SSID	Security	RADIUS	QoS	Layer-2 Isolation	MAC Filter
<input type="radio"/>	1	VoIP_SSID	ZyXEL01	security01	radius01	VoIP	Disable	Disable
<input type="radio"/>	2	Guest_SSID	ZyXEL02	security01	radius01	NONE	Isolation01	Disable
<input type="radio"/>	3	SSID03	ZyXEL03	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	4	SSID04	ZyXEL04	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	5	SSID05	ZyXEL05	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	6	SSID06	ZyXEL06	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	7	SSID07	ZyXEL07	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	8	SSID08	ZyXEL08	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	9	SSID09	ZyXEL09	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	10	SSID10	ZyXEL10	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	11	SSID11	ZyXEL11	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	12	SSID12	ZyXEL12	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	13	SSID13	ZyXEL13	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	14	SSID14	ZyXEL14	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	15	SSID15	ZyXEL15	security01	radius01	NONE	Disable	Disable
<input type="radio"/>	16	SSID16	ZyXEL16	security01	radius01	NONE	Disable	Disable

The following table describes the labels in this screen.

**Table 37** Wireless > SSID

LABEL	DESCRIPTION
Index	This field displays the index number of each SSID profile.
Profile Name	This field displays the identification name of each SSID profile on the NWA.
SSID	This field displays the 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 <a href="#">Section 10.4 on page 150</a> 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 <b>NONE</b> if QoS is not configured on a profile.

**Table 37** Wireless > SSID

LABEL	DESCRIPTION
Layer 2 Isolation	This field displays which layer 2 isolation profile is currently associated with each SSID profile, or <b>Disable</b> if Layer 2 Isolation is not configured on an SSID profile.
MAC Filter	This field displays which MAC filter profile is currently associated with each SSID profile, or <b>Disable</b> 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 <b>Edit</b> to go to the SSID configuration screen.

## 9.4.1 Configuring SSID

Use this screen to configure an SSID profile. Select an SSID profile in **Wireless > SSID** and click **Edit** to display the following screen.

**Figure 90** Wireless > SSID > Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name	SSID07				
SSID	ZyXEL07				
Hide Name(SSID)	Disable				
Security	security01				
RADIUS	radius01				
QoS	NONE				
Layer-2 Isolation	Disable				
Intra-BSS Traffic blocking	Disable				
MAC Filtering	Disable				
		Apply	Reset		

The following table describes the labels in this screen.

**Table 38** Wireless > SSID > Edit

LABEL	DESCRIPTION
Profile Name	Enter a name 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.
Hide Name (SSID)	Select <b>Disable</b> if you want the NWA to broadcast this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, select <b>Enable</b> to have the NWA hide this SSID (a wireless client scanning for an AP will not find this SSID).
Security	Select a security profile to use with this SSID profile. See <a href="#">Section 10.4 on page 150</a> 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 <a href="#">Section 11.4 on page 163</a> for more information.



**Table 38** Wireless > SSID > Edi

LABEL	DESCRIPTION
QoS	<p>Select the Quality of Service priority for this BSS's traffic.</p> <ul style="list-style-type: none"> <li>In the pre-configured <b>VoIP_SSID</b> profile, the QoS setting is <b>VoIP</b>. This is not user-configurable. The <b>VoIP</b> setting is available only on the <b>VoIP_SSID</b> profile, and provides the highest level of QoS.</li> <li>If you select <b>WMM</b> from the QoS list, the priority of a data packet depends on the packet's IEEE 802.1q or DSCP header. See <a href="#">Section 8.5.6 on page 137</a> for more information on WMM and WMM priorities. If a packet has no WMM value assigned to it, it is assigned the default priority.</li> <li>If you select <b>ATC</b> from the QoS list, the NWA automatically assigns priority based on packet size. See <a href="#">Section 8.5.7 on page 138</a> for more information on ATC.</li> <li>If you select <b>ATC+WMM</b> from the QoS list, the NWA uses WMM on the wireless network and ATC on the wired network. See <a href="#">Section 8.5.8 on page 139</a> for more information on ATC+WMM.</li> <li>If you select <b>WMM_VOICE</b>, <b>WMM_VIDEO</b>, <b>WMM_BEST_EFFORT</b> or <b>WMM_BACKGROUND</b>, the NWA applies that QoS setting to all of that SSID's traffic.</li> <li>If you select <b>NONE</b>, the NWA applies no priority to traffic on this SSID.</li> </ul> <p>Note: When you configure an SSID profile's QoS settings, the NWA applies the same QoS setting to all of the profile's traffic.</p>
L2 Isolation	<p>Select a layer 2 isolation profile from the drop-down list box. If you do not want to use layer 2 isolation on this profile, select <b>Disable</b>. See <a href="#">Section on page 166</a> for more information.</p>
Intra-BSS Traffic blocking	<p>Select <b>Enable</b> from the drop-down list box to prevent wireless clients in this profile's BSS from communicating with one another.</p>
MAC Filtering	<p>Select a MAC filter profile from the drop-down list box. If you do not want to use MAC filtering on this profile, select <b>Disable</b>. See <a href="#">Section Note: on page 174</a> for more information.</p>
Apply	<p>Click <b>Apply</b> to save your changes.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>



# Wireless Security Screen

## 10.1 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 91** 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.

## 10.2 What You Can Do in the Security Screen

Use the **Wireless > Security** screen (see [Section 10.4 on page 150](#)) to choose the security mode for your NWA.

## 10.3 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.

You can configure up to 16 security profiles in your NWA. The following table shows the relative effectiveness of wireless security methods:.

**Table 39** 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)
	WPA2
Most Secure	

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.
- **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.

## 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

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 B on page 233](#).

## 10.4 The Security Screen

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

Use this screen to choose and edit a security profile. Click **Wireless > Security**. The following screen displays.

**Figure 92** Wireless > Security

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																																																																				
<table border="1"> <thead> <tr> <th></th> <th>Index</th> <th>Profile Name</th> <th>Security Mode</th> </tr> </thead> <tbody> <tr><td><input type="radio"/></td><td>1</td><td>security01</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>2</td><td>security02</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>3</td><td>security03</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>4</td><td>security04</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>5</td><td>security05</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>6</td><td>security06</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>7</td><td>security07</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>8</td><td>security08</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>9</td><td>security09</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>10</td><td>security10</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>11</td><td>security11</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>12</td><td>security12</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>13</td><td>security13</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>14</td><td>security14</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>15</td><td>security15</td><td>None</td></tr> <tr><td><input type="radio"/></td><td>16</td><td>security16</td><td>None</td></tr> </tbody> </table>							Index	Profile Name	Security Mode	<input type="radio"/>	1	security01	None	<input type="radio"/>	2	security02	None	<input type="radio"/>	3	security03	None	<input type="radio"/>	4	security04	None	<input type="radio"/>	5	security05	None	<input type="radio"/>	6	security06	None	<input type="radio"/>	7	security07	None	<input type="radio"/>	8	security08	None	<input type="radio"/>	9	security09	None	<input type="radio"/>	10	security10	None	<input type="radio"/>	11	security11	None	<input type="radio"/>	12	security12	None	<input type="radio"/>	13	security13	None	<input type="radio"/>	14	security14	None	<input type="radio"/>	15	security15	None	<input type="radio"/>	16	security16	None
	Index	Profile Name	Security Mode																																																																						
<input type="radio"/>	1	security01	None																																																																						
<input type="radio"/>	2	security02	None																																																																						
<input type="radio"/>	3	security03	None																																																																						
<input type="radio"/>	4	security04	None																																																																						
<input type="radio"/>	5	security05	None																																																																						
<input type="radio"/>	6	security06	None																																																																						
<input type="radio"/>	7	security07	None																																																																						
<input type="radio"/>	8	security08	None																																																																						
<input type="radio"/>	9	security09	None																																																																						
<input type="radio"/>	10	security10	None																																																																						
<input type="radio"/>	11	security11	None																																																																						
<input type="radio"/>	12	security12	None																																																																						
<input type="radio"/>	13	security13	None																																																																						
<input type="radio"/>	14	security14	None																																																																						
<input type="radio"/>	15	security15	None																																																																						
<input type="radio"/>	16	security16	None																																																																						
<input type="button" value="Edit"/>																																																																									

The following table describes the labels in this screen.

**Table 40** Wireless > Security

LABEL	DESCRIPTION
Index	This is the index number of the security profile.
Profile Name	This field displays a name given to a security profile in the <b>Security</b> configuration screen.

**Table 40** Wireless > Security

LABEL	DESCRIPTION
Security Mode	This field displays the security mode this security profile uses.
Edit	Select an entry from the list and click <b>Edit</b> to configure security settings for that profile.

After selecting the security profile you want to edit, the following screen appears. Enter the name you want to call this security profile in the **Profile Name** field.

**Figure 93** Security: Profile Name

The screenshot shows a configuration interface with tabs for Wireless, SSID, Security, RADIUS, Layer-2 Isolation, and MAC Filter. The Security tab is active. It features a text input for 'Profile Name' with the value 'security01' and a dropdown menu for 'Security Mode' currently set to 'None'. At the bottom, there are 'Apply' and 'Reset' buttons.

The next screen varies according to the **Security Mode** you select.

## 10.4.1 Security: WEP

Use this screen to set the selected profile to Wired Equivalent Privacy (WEP) security mode. Select **WEP** in the **Security Mode** field to display the following screen.

**Figure 94** Wireless > Security: WEP

The screenshot shows the configuration screen for WEP security. The Security tab is active. Fields include 'Profile Name' (security01), 'Security Mode' (WEP), 'WEP Encryption' (64-bit WEP), and 'Authentication Method' (Auto). Below these are instructions for key lengths and a choice between ASCII and Hex. Four radio buttons labeled 'Key 1' through 'Key 4' are followed by four empty text input fields. 'Apply' and 'Reset' buttons are at the bottom.

The following table describes the labels in this screen.

**Table 41** Wireless > Security: WEP

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose <b>WEP</b> in this field.
WEP Encryption	Select <b>Disable</b> to allow wireless stations to communicate with the access points without any data encryption.  Select <b>64-bit WEP</b> , <b>128-bit WEP</b> or <b>152-bit WEP</b> to enable data encryption.
Authentication Method	Select <b>Auto</b> , <b>Open System</b> or <b>Shared Key</b> from the drop-down list box.  The default setting is <b>Auto</b> .
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys.  The preceding "0x" is entered automatically.
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 <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").  If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").  If you chose <b>152-bit WEP</b> , 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. The default key is key 1.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



## 10.4.2 Security: 802.1x Only

Use this screen to set the selected profile to 802.1x Only security mode. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

**Figure 95** Wireless > Security: 802.1x Only

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name		<input type="text" value="security01"/>			
Security Mode		8021x-Only ▾			
ReAuthentication Timer		<input type="text" value="0"/> (seconds, 0 means no ReAuthentication)			
Idle Timeout		<input type="text" value="3600"/> (seconds)			
		<input type="button" value="Apply"/>		<input type="button" value="Reset"/>	

The following table describes the labels in this screen.

**Table 42** Wireless > Security: 802.1x Only

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose <b>802.1x Only</b> in this field.
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. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.  <b>Note:</b> If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	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.  The default time interval is <b>3600</b> seconds (or 1 hour).
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 10.4.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

Use this screen to set the selected profile to 802.1x Static 64 or 802.1x Static 128 security mode. Select **802.1x Static 64** or **802.1x Static 128** in the **Security Mode** field to display the following screen.

**Figure 96** Wireless > Security: 802.1x Static 64-bit, 802.1x Static 128-bit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name : <input type="text" value="security04"/>					
Security Mode : <input type="text" value="8021x-Static128"/>					
Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4). <input checked="" type="radio"/> ASCII <input type="radio"/> Hex					
<input checked="" type="radio"/> Key 1 <input type="text"/>					
<input type="radio"/> Key 2 <input type="text"/>					
<input type="radio"/> Key 3 <input type="text"/>					
<input type="radio"/> Key 4 <input type="text"/>					
ReAuthentication Timer : <input type="text" value="1800"/> ( in seconds, 0 mean no ReAuthentication)					
Idle Timeout : <input type="text" value="3600"/> ( in seconds)					
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

The following table describes the labels in this screen.

**Table 43** Wireless > Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose <b>802.1x Static 64</b> or <b>802.1x Static 128</b> in this field.
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	Select this option to enter hexadecimal characters as the WEP keys. The preceding "0x" is entered automatically.
Key 1 to Key 4	<p>If you chose <b>802.1x Static 64</b>, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>If you chose <b>802.1x Static 128-bit</b>, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>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.</p> <p>The preceding "0x" is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p>

**Table 43** Wireless > Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
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. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.  <b>Note:</b> If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	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.  The default time interval is <b>3600</b> seconds (or 1 hour).
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 10.4.4 Security: WPA

Use this screen to set the selected profile to Wi-Fi Protected Access (WPA) security mode. Select **WPA** in the **Security Mode** field to display the following screen.

**Figure 97** Wireless > Security: WPA

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name		security01			
Security Mode		WPA			
ReAuthentication Timer		0 (seconds, 0 means no ReAuthentication)			
Idle Timeout		3600 (seconds)			
Group Key Update Timer		1800 (seconds)			
		<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

The following table describes the labels in this screen.

**Table 44** Wireless > Security: WPA

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose <b>WPA</b> in this field.

**Table 44** Wireless > Security: WPA

LABEL	DESCRIPTION
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. The default time interval is <b>1800</b> seconds (30 minutes). 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.
Idle Timeout	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.  The default time interval is <b>3600</b> seconds (or 1 hour).
Group Key Update Timer	The <b>Group Key Update Timer</b> 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 <b>Group Key Update Timer</b> is also supported in WPA-PSK mode. The NWA default is 1800 seconds (30 minutes).
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 10.4.5 Security: WPA2 or WPA2-MIX

Use this screen to set the selected profile to WPA2 or WPA2-MIX security mode. Select **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

**Figure 98** Wireless > Security:WPA2 or WPA2-MIX

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name	security01				
Security Mode	WPA2-MIX				
ReAuthentication Timer	0 (seconds, 0 means no ReAuthentication)				
Idle Timeout	3600 (seconds)				
Group Key Update Timer	1800 (seconds)				
PMK Cache	Enable				
Pre-Authentication	Disable				
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

The following table describes the labels not previously discussed

**Table 45** Wireless > Security: WPA2 or WPA2-MIX

LABEL	DESCRIPTIONS
Profile Name	Type a name to identify this security profile.
Security Mode	Choose <b>WPA2</b> or <b>WPA2-MIX</b> in this field.
ReAuthentication Timer	<p>Specify how often wireless stations have to resend usernames and passwords in order to stay connected.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.</p> <p><b>Note:</b> If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Idle Timeout	<p>The NWA automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.</p> <p>The default time interval is <b>3600</b> seconds (or 1 hour).</p>
Group Key Update Timer	<p>The <b>Group Key Update Timer</b> 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 <b>Group Key Update Timer</b> is also supported in WPA-PSK mode. The NWA's default is 1800 seconds (30 minutes).</p>
PMK Cache	<p>When a wireless client moves from one AP's coverage area to another, it performs an authentication procedure (exchanging security information) with the new AP. Instead of re-authenticating a client each time it returns to the AP's coverage area, which can cause delays to time-sensitive applications, the AP and the client can store (or "cache") and use information about their previous authentication. Select <b>Enable</b> to allow PMK caching, or <b>Disable</b> to switch this feature off.</p>
Pre-Authentication	<p>Pre-authentication allows a wireless client to perform authentication with a different AP from the one to which it is currently connected, before moving into the new AP's coverage area. This speeds up roaming. Select <b>Enable</b> to allow pre-authentication, or <b>Disable</b> to switch it off.</p>
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 10.4.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Use this screen to set the selected profile to WPA-PSK, WPA2-PSK or WPA2-PSK-MIX security mode. Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in the **Security Mode** field to display the following screen.

**Figure 99** Wireless > Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name	<input type="text" value="security01"/>				
Security Mode	WPA2-PSK-MIX ▾				
Pre-Shared Key	<input type="text"/>				
ReAuthentication Timer	<input type="text" value="0"/>	(seconds, 0 means no ReAuthentication)			
Idle Timeout	<input type="text" value="3600"/>	(seconds)			
Group Key Update Timer	<input type="text" value="1800"/>	(seconds)			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

The following table describes the labels not previously discussed

**Table 46** Wireless > Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose <b>WPA-PSK</b> , <b>WPA2-PSK</b> or <b>WPA2-PSK-MIX</b> in this field.
Pre-Shared Key	<p>The encryption mechanisms used for <b>WPA</b> and <b>WPA-PSK</b> are the same. The only difference between the two is that <b>WPA-PSK</b> uses a simple common password, instead of user-specific credentials.</p> <p>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).</p>
ReAuthentication Timer	<p>Specify how often wireless stations have to resend usernames and passwords in order to stay connected.</p> <p>Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off.</p> <p>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Idle Timeout	<p>The NWA automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.</p> <p>The default time interval is <b>3600</b> seconds (or 1 hour).</p>

**Table 46** Wireless > Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Group Key Update Timer	The <b>Group Key Update Timer</b> 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 <b>Group Key Update Timer</b> is also supported in WPA-PSK mode. The NWA's default is 1800 seconds (30 minutes).
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 10.5 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) 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 B on page 233](#).





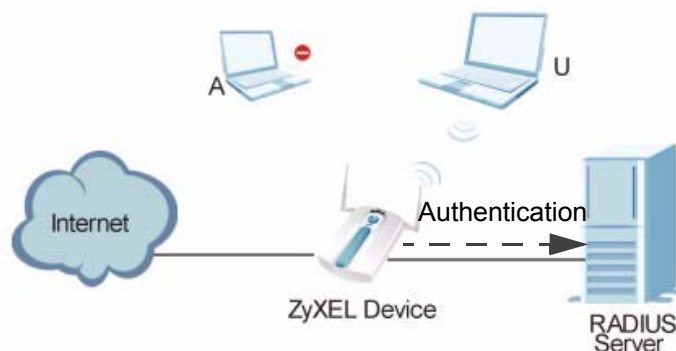
# RADIUS Screen

## 11.1 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 100** 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.

## 11.2 What You Can Do in the RADIUS Screen

Use the **Security > RADIUS** screen (see [Section 11.4 on page 163](#)) if you want to authenticate wireless users using a RADIUS Server and/or Accounting Server.

## 11.3 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.

You can configure up to four RADIUS server profiles. Each profile also has one backup authentication server and a backup accounting server. These profiles can be assigned to an SSID profile in the **Wireless > SSID** configuration screen.

## 11.4 The RADIUS Screen

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

**Figure 101** Wireless > RADIUS

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Index : <input type="text" value="1"/>					
Profile Name : <input type="text" value="radius01"/>					
			<b>Primary</b>		<b>Backup</b>
RADIUS Option			<input type="radio"/> Internal <input checked="" type="radio"/> External		<input type="radio"/> Internal <input checked="" type="radio"/> External
			<input type="checkbox"/> Active		<input type="checkbox"/> Active
RADIUS Server IP Address			<input type="text" value="0.0.0.0"/>		<input type="text" value="0.0.0.0"/>
RADIUS Server Port			<input type="text" value="1812"/>		<input type="text" value="1812"/>
Share Secret			<input type="text"/>		<input type="text"/>
			<input type="checkbox"/> Active		<input type="checkbox"/> Active
Accounting Server IP Address			<input type="text" value="0.0.0.0"/>		<input type="text" value="0.0.0.0"/>
Accounting Server Port			<input type="text" value="1813"/>		<input type="text" value="1813"/>
Share Secret			<input type="text"/>		<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

The following table describes the labels in this screen.

**Table 47** Wireless > RADIUS

LABEL	DESCRIPTION
Index	Select the RADIUS profile you want to configure from the drop-down list box.
Profile Name	Type a name for the RADIUS profile associated with the <b>Index</b> number above.
Primary	Configure the fields below to set up user authentication and accounting.
Backup	<p>If the NWA cannot communicate with the <b>Primary</b> accounting server, you can have the NWA use a <b>Backup</b> RADIUS server. Make sure the <b>Active</b> check boxes are selected if you want to use backup servers.</p> <p>The NWA will attempt to communicate three times before using the <b>Backup</b> 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 <b>ReAuthentication Timer</b> field in the <b>Security</b> screen.</p>
RADIUS Option	

**Table 47** Wireless > RADIUS

LABEL	DESCRIPTION
Internal	Select this check box to use the NWA's internal authentication server. The <b>Active</b> , <b>RADIUS Server IP Address</b> , <b>RADIUS Server Port</b> and <b>Share Secret</b> fields are not available when you use the internal authentication server.
External	Select this check box to use an external authentication server. The NWA does not use the internal authentication server when this check box is enabled.
Active	Select the check box to enable user authentication through an external authentication server. This check box is not available when you select <b>Internal</b> .
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 <b>Internal</b> .
RADIUS Server Port	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so. This field is not available when you select <b>Internal</b> .
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 <b>Internal</b> .
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. The default port number is 1813. You need not 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 <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# Layer-2 Isolation Screen

## 12.1 Overview

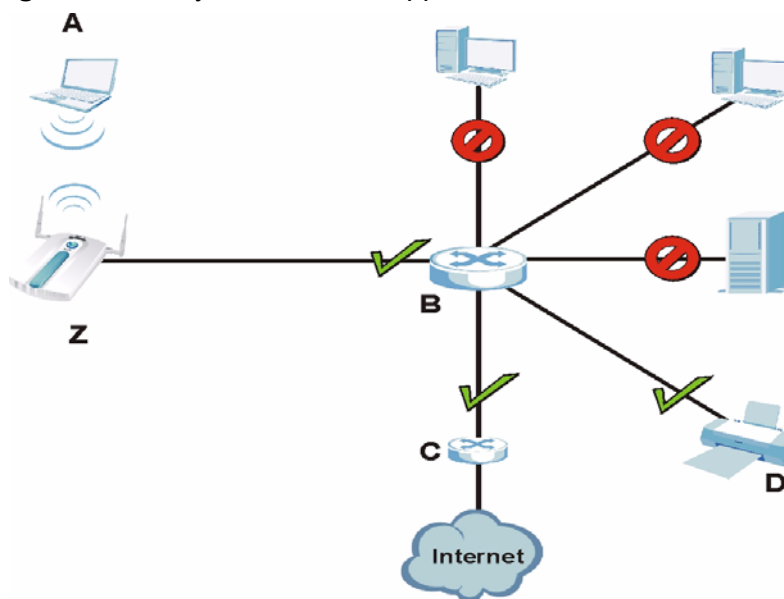
This chapter describes how you can configure the **Layer-2 Isolation** screen on your NWA.

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

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

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

**Figure 102** Layer-2 Isolation Application



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

## 12.2 What You Can Do in the Layer-2 Isolation Screen

Use the **Wireless > Layer-2 Isolation** screen (see [Section 12.4 on page 167](#)) to configure the MAC addresses of the wireless client, AP, computer or router that you want to allow the associated wireless clients to have access to.

## 12.3 What You Need To Know

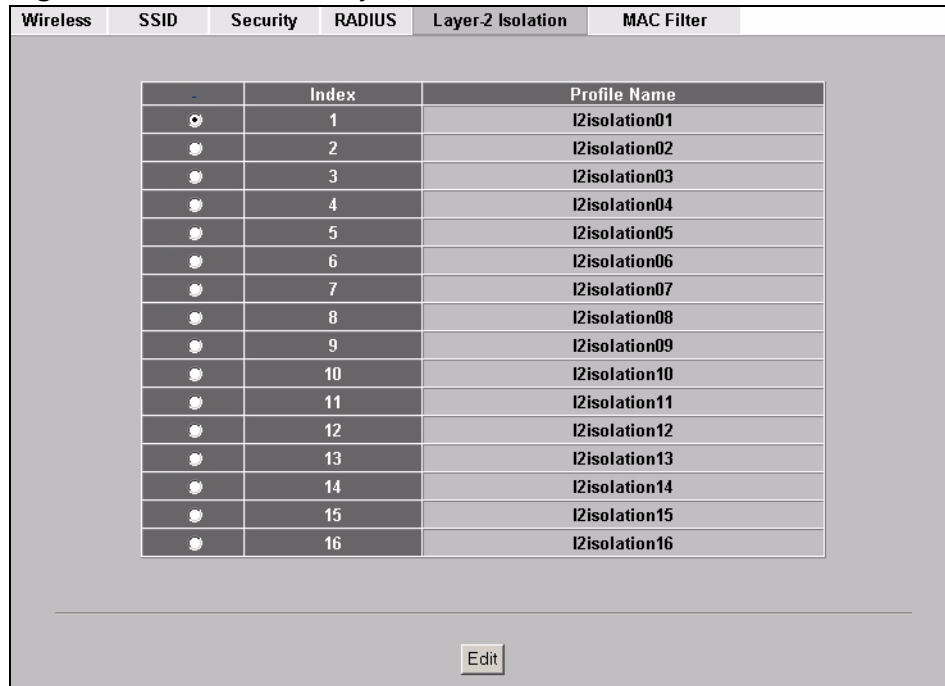
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of each device to configure MAC filtering on the NWA.

If layer-2 isolation is enabled, you need to know the MAC address of each wireless client, AP, computer or router that you want to allow to communicate with the ZyXEL Device's wireless clients.

## 12.4 The Layer-2 Isolation Screen

Use this screen to select and configure a layer-2 isolation profile. Click **Wireless** > **Layer-2 Isolation**. The screen appears as shown next.

**Figure 103** Wireless > Layer 2 Isolation



The following table describes the labels in this screen.

**Table 48** Wireless > Layer-2 Isolation

LABEL	DESCRIPTION
Index	This is the index number of the profile.
Profile Name	This field displays the name given to a layer-2 isolation profile in the <b>Layer-2 Isolation Configuration</b> screen.
Edit	Select an entry from the list and click <b>Edit</b> to configure settings for that profile.

### 12.4.1 Configuring Layer-2 Isolation

Use this screen to specify the configuration for your layer-2 isolation profile. Select a layer-2 isolation profile in **Wireless** > **Layer-2 Isolation** and click **Edit** to display the following screen.

Note: When configuring this screen, remember to select the correct layer-2 isolation profile in the Wireless> SSID > Edit screen of the relevant SSID profile.

**Figure 104** Wireless > Layer-2 Isolation > Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Layer-2 Isolation Configuration					
Profile Name		<input type="text" value="l2isolation01"/>			
Allow devices with these MAC addresses					
Index	MAC Address	Description	Index	MAC Address	Description
1	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	17	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
2	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	18	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
3	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	19	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
4	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	20	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
5	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	21	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
6	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	22	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
7	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	23	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
8	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	24	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
9	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	25	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
10	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	26	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
11	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	27	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
12	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	28	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
13	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	29	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
14	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	30	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
15	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	31	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
16	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>	32	<input type="text" value="00:00:00:00:00:00"/>	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

The following table describes the labels in this screen.

**Table 49** Wireless> Layer-2 Isolation > Edit

LABEL	DESCRIPTION
Profile Name	Type a name to identify this layer-2 isolation profile.
Allow devices with these MAC addresses	These are the MAC address of a wireless client, AP, computer or router. A wireless client associated with the NWA can communicate with another wireless client, AP, computer or router only if the MAC addresses of those devices are listed in this table.
Index	This is the index number of the MAC address.
MAC Address	Type the MAC addresses of the wireless client, AP, computer or router that you want to allow the associated wireless clients to have access to in these address fields. Type the MAC address in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).
Description	Type a name to identify this device.



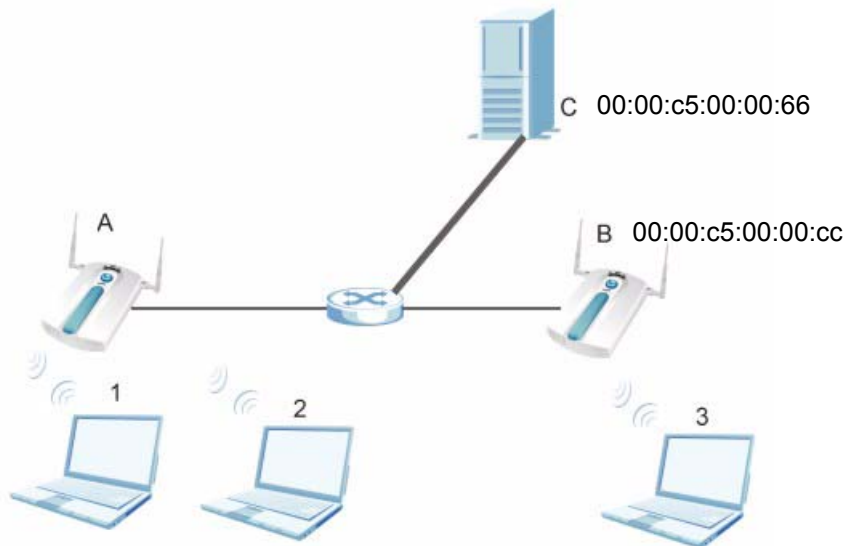
**Table 49** Wireless> Layer-2 Isolation > Edit

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 12.5 Technical Reference

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

The figure that follows illustrates two example layer-2 isolation configurations on your NWA (**A**).

**Figure 105** Layer-2 Isolation Example Configuration

### Example 1: Restricting Access to Server

In the following example wireless clients **1** and **2** can communicate with file server **C**, but not access point **B** or wireless client **3**.

- Enter **C**'s MAC address in the **MAC Address** field, and enter "File Server C" in the **Description** field.

**Figure 106** Layer-2 Isolation Example 1

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Layer-2 Isolation Configuration					
Profile Name <input type="text" value="l2isolation01"/>					
Allow devices with these MAC addresses					
Set	MAC Address	Description	Set	MAC Address	Description
1	00:00:c5:00:00:66	File Server C	17	00:00:00:00:00:00	
2	00:00:00:00:00:00		18	00:00:00:00:00:00	
3	00:00:00:00:00:00		19	00:00:00:00:00:00	

### Example 2: Restricting Access to Client

In the following example wireless clients **1** and **2** can communicate with access point **B** and file server **C** but not wireless client **3**.

- Enter the server's and your NWA's MAC addresses in the **MAC Address** fields. Enter "File Server C" in **C**'s **Description** field, and enter "Access Point B" in **B**'s **Description** field.

**Figure 107** Layer-2 Isolation Example 2

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Layer-2 Isolation Configuration					
Profile Name <input type="text" value="l2isolation01"/>					
Allow devices with these MAC addresses					
Set	MAC Address	Description	Set	MAC Address	Description
1	00:00:c5:00:00:66	File Server C	17	00:00:00:00:00:00	
2	00:00:c5:00:00:cc	Access Point B	18	00:00:00:00:00:00	
3	00:00:00:00:00:00		19	00:00:00:00:00:00	

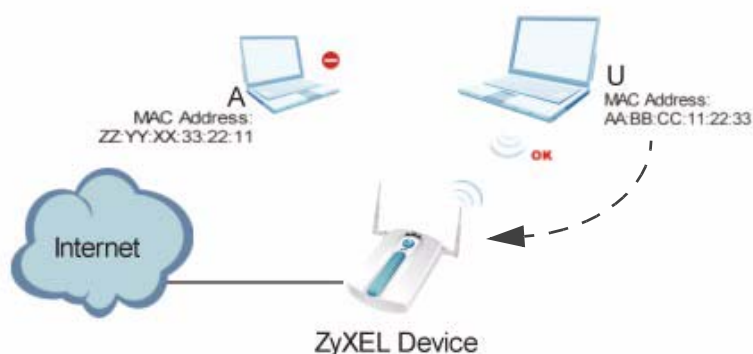
# MAC Filter Screen

## 13.1 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 devices (Allow Association) or exclude devices from accessing the NWA (Deny Association).

**Figure 108** 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.

## 13.2 What You Can Do in the MAC Filter Screen

Use the **Wireless > MAC Filter** screen (see [Section 13.4 on page 172](#)) to specify which wireless station is allowed or denied access to the ZyXEL Device.

## 13.3 What You Should Know About MAC Filter

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.

## 13.4 The MAC Filter Screen

The MAC filter profile is a user-configured list of MAC addresses. Each SSID profile can reference one MAC filter profile. The NWA provides 16 MAC Filter profiles, each of which can hold up to 32 MAC addresses.

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

**Figure 109** Wireless> MAC Filter

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																																																																				
					<table border="1"> <thead> <tr> <th></th> <th>Index</th> <th>Profile Name</th> <th>Filter Action</th> </tr> </thead> <tbody> <tr><td><input type="radio"/></td><td>1</td><td>macfilter01</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>2</td><td>macfilter02</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>3</td><td>macfilter03</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>4</td><td>macfilter04</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>5</td><td>macfilter05</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>6</td><td>macfilter06</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>7</td><td>macfilter07</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>8</td><td>macfilter08</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>9</td><td>macfilter09</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>10</td><td>macfilter10</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>11</td><td>macfilter11</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>12</td><td>macfilter12</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>13</td><td>macfilter13</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>14</td><td>macfilter14</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>15</td><td>macfilter15</td><td>Deny Association</td></tr> <tr><td><input type="radio"/></td><td>16</td><td>macfilter16</td><td>Deny Association</td></tr> </tbody> </table>		Index	Profile Name	Filter Action	<input type="radio"/>	1	macfilter01	Deny Association	<input type="radio"/>	2	macfilter02	Deny Association	<input type="radio"/>	3	macfilter03	Deny Association	<input type="radio"/>	4	macfilter04	Deny Association	<input type="radio"/>	5	macfilter05	Deny Association	<input type="radio"/>	6	macfilter06	Deny Association	<input type="radio"/>	7	macfilter07	Deny Association	<input type="radio"/>	8	macfilter08	Deny Association	<input type="radio"/>	9	macfilter09	Deny Association	<input type="radio"/>	10	macfilter10	Deny Association	<input type="radio"/>	11	macfilter11	Deny Association	<input type="radio"/>	12	macfilter12	Deny Association	<input type="radio"/>	13	macfilter13	Deny Association	<input type="radio"/>	14	macfilter14	Deny Association	<input type="radio"/>	15	macfilter15	Deny Association	<input type="radio"/>	16	macfilter16	Deny Association
	Index	Profile Name	Filter Action																																																																						
<input type="radio"/>	1	macfilter01	Deny Association																																																																						
<input type="radio"/>	2	macfilter02	Deny Association																																																																						
<input type="radio"/>	3	macfilter03	Deny Association																																																																						
<input type="radio"/>	4	macfilter04	Deny Association																																																																						
<input type="radio"/>	5	macfilter05	Deny Association																																																																						
<input type="radio"/>	6	macfilter06	Deny Association																																																																						
<input type="radio"/>	7	macfilter07	Deny Association																																																																						
<input type="radio"/>	8	macfilter08	Deny Association																																																																						
<input type="radio"/>	9	macfilter09	Deny Association																																																																						
<input type="radio"/>	10	macfilter10	Deny Association																																																																						
<input type="radio"/>	11	macfilter11	Deny Association																																																																						
<input type="radio"/>	12	macfilter12	Deny Association																																																																						
<input type="radio"/>	13	macfilter13	Deny Association																																																																						
<input type="radio"/>	14	macfilter14	Deny Association																																																																						
<input type="radio"/>	15	macfilter15	Deny Association																																																																						
<input type="radio"/>	16	macfilter16	Deny Association																																																																						
					Edit																																																																				

The following table describes the labels in this screen.

**Table 50** Wireless > MAC Filter

LABEL	DESCRIPTION
Index	This is the index number of the profile.
Profile Name	This field displays the name given to a MAC filter profile in the <b>MAC Filter Configuration</b> screen.
Edit	Select an entry from the list and click <b>Edit</b> to configure settings for that profile.

## 13.4.1 Configuring the MAC Filter

To change your NWA's MAC filter settings, click **WIRELESS > MAC Filter > Edit**. The screen appears as shown.

**Figure 110** Wireless > MAC Filter > Edit

The screenshot shows the 'MAC Address Filter' configuration interface. At the top, there are navigation tabs: Wireless, SSID, Security, RADIUS, Layer-2 Isolation, and MAC Filter. The 'MAC Filter' tab is selected. Below the tabs, the 'MAC Address Filter' section is visible. It contains a 'Profile Name' field with the text 'macfilter01' and a 'Filter Action' dropdown menu currently set to 'Deny Association'. Below these fields is a table with 6 columns: Index, MAC Address, Description, Index, MAC Address, and Description. The table has 16 rows, with the first 8 rows visible. At the bottom of the screen, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 51** Wireless > MAC Filter > Edit

LABEL	DESCRIPTION
Profile Name	Type a name to identify this profile.
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table.  Select <b>Deny Association</b> to block access to the router. MAC addresses not listed will be allowed to access the router.  Select <b>Allow Association</b> to permit access to the router. MAC addresses not listed will be denied access to the router.

**Table 51** Wireless > MAC Filter > Edit

LABEL	DESCRIPTION
Index	This is the index number of the MAC address.
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.
Description	Type a name to identify this wireless station.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

Note: To activate MAC filtering on an SSID profile, select **the correct filter** from the **Enable MAC Filtering** drop-down list box in the **Wireless > SSID > Edit** screen and click **Apply**

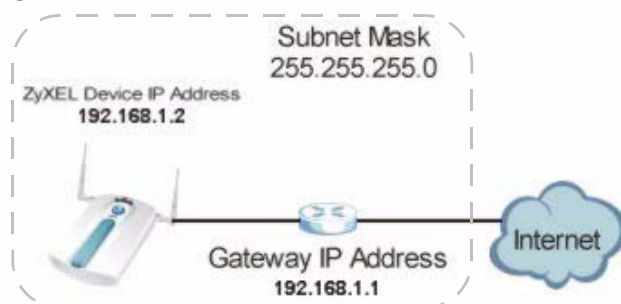
# IP Screen

## 14.1 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 111** IP Setup



The figure above illustrates one possible setup of your NWA. The gateway IP address is 192.168.1.1 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.

## 14.2 What You Can Do in the IP Screen

Use the **IP Screen** (see [Section 14.4 on page 176](#)) to configure the IP address of your NWA.

## 14.3 What You Need To Know About IP

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)

These parameters should work for the majority of installations.

## 14.4 The IP Screen

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

**Figure 112** IP Setup

The following table describes the labels in this screen.

**Table 52** IP Setup

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	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.



**Table 52** IP Setup

LABEL	DESCRIPTION
IP Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your 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.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 14.5 Technical Reference

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

### 14.5.1 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 53** 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.

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.



# Rogue AP Detection

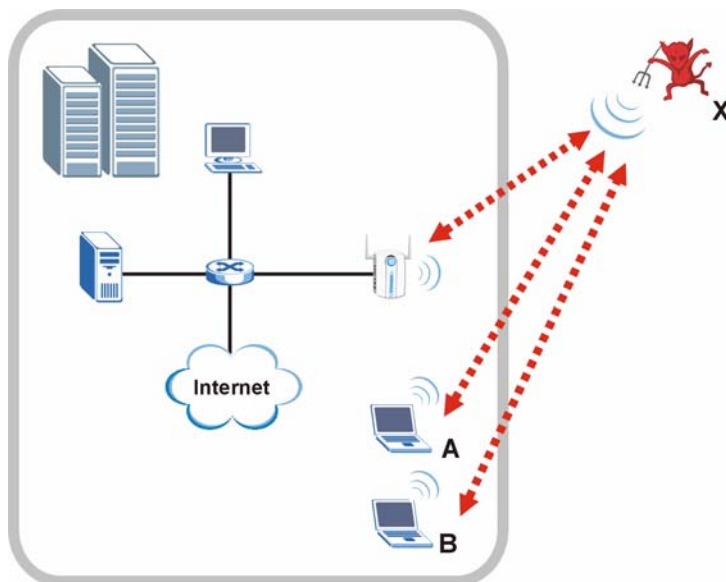
## 15.1 Overview

This chapter discusses rogue wireless access points and how to configure the NWA's rogue AP detection feature.

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can open up holes in a network's security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain access to the network, or set up their own rogue APs in order to capture information from wireless clients. If a scan reveals a rogue AP, you can use commercially-available software to physically locate it.

Note that it is not necessary for a network to have a legitimate wireless LAN component for rogue APs to open the network to an attacker. In this case, any AP detected can be classified as rogue.

**Figure 113** Rogue AP Example



In the example above, a corporate network's security is compromised by a rogue AP (**R**) set up by an employee at his workstation in order to allow him to connect his notebook computer wirelessly (**A**). The company's legitimate wireless network

(the dashed ellipse **B**) is well-secured, but the rogue AP uses inferior security that is easily broken by an attacker (**X**) running readily available encryption-cracking software. In this example, the attacker now has access to the company network, including sensitive data stored on the file server (**C**).

## 15.2 What You Can Do in the Rogue AP Screen

- Use the **Rogue AP > Configuration** screen (see [Section 15.3.1 on page 182](#)) to enable your NWA's Rogue AP detection settings. You can choose to scan for rogue APs manually, or to have the NWA scan automatically at pre-defined intervals.
- Use the **Rogue AP > Friendly AP** screen (see [Section 15.3.2 on page 183](#)) to specify APs as trusted.
- Use the **Rogue AP > Rogue AP** screen (see [Section 15.3.3 on page 184](#)) to display details of all IEEE 802.11a/b/g wireless access points within the NWA's coverage area, except for the NWA itself and the access points included in the friendly AP list.

## 15.3 What You Need To Know

You can configure the NWA to detect rogue IEEE 802.11a (5 GHz) and IEEE 802.11b/g (2.4 GHz) APs.

You can also set the NWA to e-mail you immediately when a rogue AP is detected (see [Chapter 19 on page 229](#) for information on how to set up e-mail logs).

You can set how often you want the NWA to scan for rogue APs in the **Rogue AP > Configuration** screen (see [Section 15.3.1 on page 182](#)).

### Friendly APs

If you have more than one AP in your wireless network, you must also configure the list of "friendly" APs. Friendly APs are other wireless access points, aside from the NWA, that are detected in your network, as well as any others that you know are not a threat (those from neighboring networks, for example). It is recommended that you export (save) your list of friendly APs often, especially if you have a network with a large number of access points. If you do not add them to the friendly AP list, these access points will appear in the **Rogue AP** list each time the NWA scans.

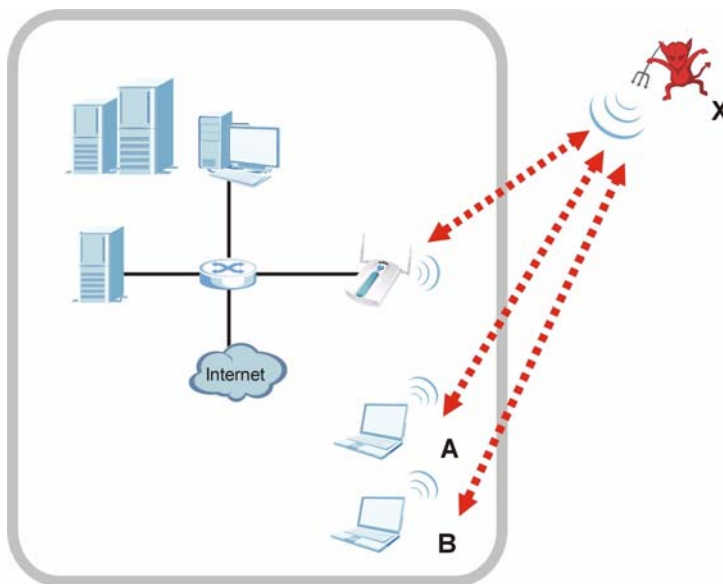
The friendly AP list displays details of all the access points in your area that you know are not a threat. If you have more than one AP in your network, you need to configure this list to include your other APs. If your wireless network overlaps with

that of a neighbor (for example) you should also add these APs to the list, as they do not compromise your own network's security. If you do not add them to the friendly AP list, these access points will appear in the **Rogue AP** list each time the NWA scans.

### “Honeypot” Attack

Rogue APs need not be connected to the legitimate network to pose a severe security threat. In the following example, an attacker (**X**) is stationed in a vehicle outside a company building, using a rogue access point equipped with a powerful antenna. By mimicking a legitimate (company network) AP, the attacker tries to capture usernames, passwords, and other sensitive information from unsuspecting clients (**A** and **B**) who attempt to connect. This is known as a “honeypot” attack.

**Figure 114** “Honeypot” Attack



If a rogue AP in this scenario has sufficient power and is broadcasting the correct SSID (Service Set Identifier) clients have no way of knowing that they are not associating with a legitimate company AP. The attacker can forward network traffic from associated clients to a legitimate AP, creating the impression of normal service. This is a variety of “man-in-the-middle” attack.

This scenario can also be part of a wireless denial of service (DoS) attack, in which associated wireless clients are deprived of network access. Other opportunities for the attacker include the introduction of malware (malicious software) into the network.

## 15.3.1 Configuration Screen

Use this screen to enable your NWA's Rogue AP detection settings. Click **Rogue AP > Configuration**. The following screen appears:

**Figure 115** Rogue AP > Configuration

The following table describes the labels in this screen.

**Table 54** Rogue AP > Configuration

LABEL	DESCRIPTION
Rogue AP Period Detection	Select <b>Enable</b> to turn rogue AP detection on. You must also enter a time value in the <b>Period</b> field.  Select <b>No</b> to turn rogue AP detection off.
Period (minutes)	Enter the period you want the NWA to wait between scanning for rogue APs (between 10 and 60 minutes). You must also select <b>Enable</b> in the <b>Active Rogue AP Period Detection</b> field.
Expiration Time (minutes)	Specify how long (between 30 and 180 minutes) an AP's entry can remain in the <b>Rogue AP List</b> before the NWA removes it from the list if the AP is no longer active.
Friendly AP List	
Export	Click this button to save the current list of friendly APs' MAC addresses and descriptions (as displayed in the <b>ROGUE AP &gt; Friendly AP</b> screen) to your computer.
File Path	Enter the location of a previously-saved friendly AP list to upload to the NWA. Alternatively, click the <b>Browse</b> button to locate a list.
Browse	Click this button to locate a previously-saved list of friendly APs to upload to the NWA.
Import	Click this button to upload the previously-saved list of friendly APs displayed in the <b>File Path</b> field to the NWA.
Apply	Click <b>Apply</b> to save your settings.
Reset	Click <b>Reset</b> to return all fields in this screen to their previously-saved values.

## 15.3.2 Friendly AP Screen

Use this screen to specify APs as trusted. Click **Rogue AP > Friendly AP**. The following screen appears:

**Figure 116** Rogue AP > Friendly AP

Index	MAC Address	SSID	Channel	Radio Mode	Security	Last Seen	Description
1	00:13:49:f5:18:c5	ZyXEL	6	BGN	None	3:10:59	N/A

The following table describes the labels in this screen.

**Table 55** Rogue AP > Friendly AP

LABEL	DESCRIPTION
Add Friendly AP	Use this section to manually add a wireless access point to the list. You must know the device's MAC address.
MAC Address	Enter the MAC address of the AP you wish to add to the list.
Description	Enter a short, explanatory description identifying the AP with a maximum of 32 alphanumeric characters. Spaces, underscores ( _ ) and dashes ( - ) are allowed.
Add	Click this button to include the AP in the list.
Friendly AP List	This is the list of safe wireless access points you have already configured.
Index	This is the index number of the AP's entry in the list.
MAC Address	This field displays the Media Access Control (MAC) address of the AP. All wireless devices have a MAC address that uniquely identifies them.
SSID	This field displays the Service Set Identifier (also known as the network name) of the AP.
Channel	This field displays the wireless channel the AP is currently using.
Radio Mode	This is the 802.11 Mode of the AP.
Security	This field displays the type of wireless encryption the AP is currently using.
Last Seen	This field displays the last time the NWA scanned for the AP.
Description	This is the description you entered when adding the AP to the list.
Delete	Click this button to remove an AP's entry from the list.

### 15.3.3 Rogue AP Screen

Use this screen to display details of all wireless access points within the NWA's coverage area. Click **Rogue AP** > **Rogue AP**. The following screen displays.

**Figure 117** Rogue AP > Rogue AP

Index	Select	MAC Address	SSID	Channel	Radio Mode	Security	Last Seen	Description
1	<input type="checkbox"/>	00:19:cb:13:36:33	WLAN-1190lvt	1	BGN	WPA2-PSK-MIX	3:16:32	
2	<input type="checkbox"/>	00:02:cf:dd:b7:8c	WLAN-7496fqz	1	BGN	WPA2-PSK-MIX	3:16:32	
3	<input type="checkbox"/>	00:02:cf:dd:b7:ac	WLAN-9471myf	1	BGN	WPA2-PSK-MIX	3:16:32	
4	<input type="checkbox"/>	00:00:00:00:00:00	N/A	1	B	WEP	3:16:32	
5	<input type="checkbox"/>	0a:19:cb:4b:22:0f	ZyXEL_Guest	1	BG	WPA2-MIX	3:16:32	
6	<input type="checkbox"/>	00:19:cb:30:22:10	6812-wifi	3	BG	WPA-PSK	3:16:32	
7	<input type="checkbox"/>	00:19:70:14:6e:ac	ZyXEL01_13708	3	BG	None	3:16:32	

The following table describes the labels in this screen.

**Table 56** Rogue AP > Rogue AP

LABEL	DESCRIPTION
Rogue AP List	This displays details of access points in the NWA's coverage area that are not listed in the friendly AP list (see <a href="#">Section 15.3.2 on page 183</a> )
Refresh	Click this button to have the NWA scan for rogue APs.
Index	This is the index number of the AP's entry in the list.
Select	Use this check box to select the APs you want to move to the friendly AP list (see <a href="#">Section 15.3.2 on page 183</a> )
MAC Address	This field displays the Media Access Control (MAC) address of the AP. All wireless devices have a MAC address that uniquely identifies them.
SSID	This field displays the Service Set Identifier (also known as the network name) of the AP.
Channel	This field displays the wireless channel the AP is currently using.
Radio Mode	This is the 802.11 Mode of the AP.
Security	This field displays the type of wireless encryption the AP is currently using.
Last Seen	This field displays the last time the NWA scanned for the AP.



**Table 56** Rogue AP > Rogue AP

LABEL	DESCRIPTION
Description	If you want to move the AP's entry to the friendly AP list, enter a short, explanatory description identifying the AP before you click <b>Add to Friendly AP List</b> . A maximum of 32 alphanumeric characters are allowed in this field. Spaces, underscores (_) and dashes (-) are allowed.
Add to Friendly AP List	If you know that the AP described in an entry is not a threat, select the <b>Active</b> check box, enter a short description in the <b>Description</b> field and click this button to add the entry to the friendly AP list (see <a href="#">Section 15.3.2 on page 183</a> ). When the NWA next scans for rogue APs, the selected AP does not appear in the rogue AP list.
Reset	Click <b>Reset</b> to return all fields in this screen to their default values.



# Remote Management Screens

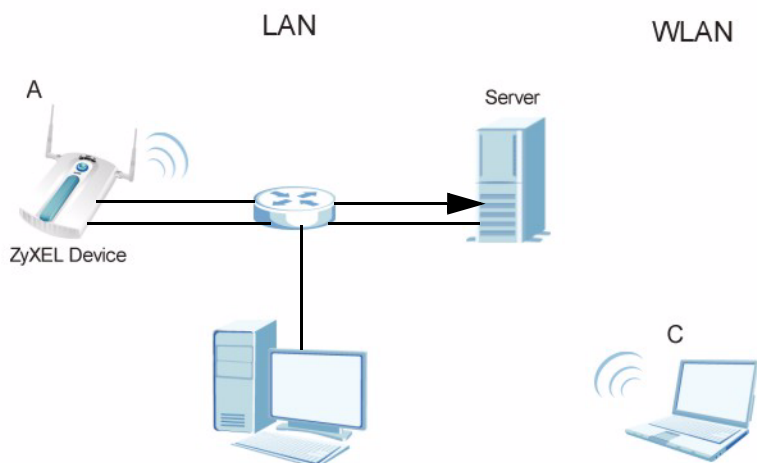
## 16.1 Overview

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 118** 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).

## 16.2 What You Can Do in the Remote Management Screens

- Use the **Telnet** screen (see [Section 16.4 on page 190](#)) to configure through which interface(s) and from which IP address(es) you can use Telnet to manage the ZyXEL Device. A Telnet connection is prioritized by the NWA over other remote management sessions.
- Use the **FTP** screen (see [Section 16.5 on page 191](#)) to configure through which interface(s) and from which IP address(es) you can use File Transfer Protocol (FTP) to manage the ZyXEL Device. You can use FTP to upload the latest firmware for example.
- Use the **WWW** screen (see [Section 16.6 on page 192](#)) to configure through which interface(s) and from which IP address(es) you can use the Web Browser to manage the ZyXEL Device.
- Use the **SNMP** screen (see [Section 16.7 on page 194](#)) to configure through which interface(s) and from which IP address(es) a network systems manager can access the ZyXEL Device.

## 16.3 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

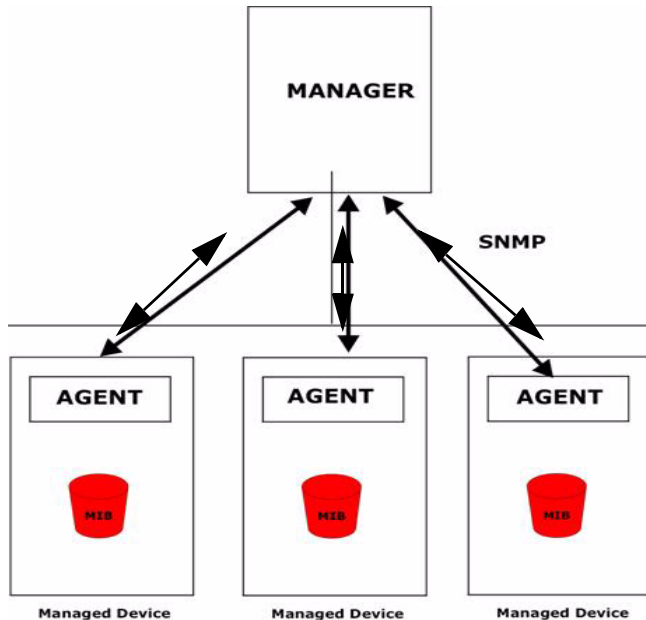
Simple Network Management Protocol (SNMP) is a member of the TCP/IP protocol suite used for exchanging management information between network devices.

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 119** 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.

## 16.4 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 (CLS).

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

**Figure 120** Remote MGNT > Telnet

The following table describes the labels in this screen.

**Table 57** Remote MGNT > 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.

**Table 57** Remote MGNT > Telnet

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 <b>All</b> to allow any computer to access the NWA using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the NWA using this service.
SSH	
Server Certificate	Select the certificate whose corresponding private key is to be used to identify the NWA for SSH connections. You must have certificates already configured in the <b>Certificates &gt; My Certificates</b> screen.
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 SSH.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the NWA using this service.  Select <b>All</b> to allow any computer to access the NWA using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the NWA using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.5 The FTP Screen

You can upload and download the NWA’s firmware and configuration files 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 121** Remote MGNT> FTP

The screenshot shows the configuration interface for the FTP service. At the top, there are four tabs: TELNET, FTP, WWW, and SNMP. The FTP tab is selected. Below the tabs, the word 'FTP' is displayed in a grey bar. The configuration area includes three main settings: 'Server Port' with a text box containing '21'; 'Server Access' with a dropdown menu showing 'WLAN & LAN'; and 'Secured Client IP Address' with radio buttons for 'All' (which is selected) and 'Selected', followed by a text box containing '0.0.0.0'. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 58** Remote MGNT > FTP

LABEL	DESCRIPTION
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 <b>All</b> to allow any computer to access the NWA using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the NWA using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.6 The WWW Screen

You can choose 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 122** Remote MGNT > WWW

The screenshot shows the configuration interface for the WWW service. It includes the following elements:

- Navigation Tabs:** TELNET, FTP, **WWW** (active), SNMP.
- WWW Section:**
  - Server Port: 80
  - Server Access: WLAN & LAN
  - Secured Client IP Address:  All  Selected, 0.0.0.0
- HTTPS Section:**
  - Server Certificate: auto\_generated\_self\_signed\_cert (See [My Certificates](#))
  - Authenticate Client Certificates (See [Trusted CAs](#))
  - Server Port: 443
  - Server Access: WLAN & LAN
  - Secured Client IP Address:  All  Selected, 0.0.0.0
- Buttons:** Apply, Reset



The following table describes the labels in this screen.

**Table 59** Remote MGNT > 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 <b>All</b> to allow any computer to access the NWA using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the NWA using this service.
HTTPS	
Server Certificate	Select the <b>Server Certificate</b> that the NWA will use to identify itself. The NWA is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the NWA).
Authenticate Client Certificates	Select <b>Authenticate Client Certificates</b> (optional) to require the SSL client to authenticate itself with the NWA by sending the NWA a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the NWA (see the appendix on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the NWA, for example 8443, then you must notify people who need to access the NWA web configurator to use "https://NWA IP Address: <b>8443</b> " as the URL.
Server Access	Select a NWA interface from <b>Server Access</b> on which incoming HTTPS access is allowed.  You can allow only secure web configurator access by setting the <b>HTTP Server Access</b> field to <b>Disable</b> and setting the <b>HTTPS Server Access</b> field to an interface(s).
Secured Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the NWA using this service.  Select <b>All</b> to allow any computer to access the NWA using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the NWA using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.7 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 123** Remote MGNT > SNMP

The following table describes the labels in this screen.

**Table 60** Remote MGNT > SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
SNMP Version	Select the SNMP version for the NWA. The SNMP version on the NWA must match the version on the SNMP manager. Choose SNMP version 1 ( <b>SNMPv1</b> ), SNMP version 2 ( <b>SNMPv2</b> ) or SNMP version 3 ( <b>SNMPv3</b> ).
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is "public" and allows all requests.  This field is available only when <b>SNMPv1</b> or <b>SNMPv2</b> is selected in the <b>SNMP Version</b> field.

**Table 60** Remote MGNT > SNMP

LABEL	DESCRIPTION
User Profile	<p>This field is available only when you select <b>SNMPv3</b> in the <b>SNMP Version</b> field.</p> <p>When sending SNMP v3 traps (messages sent independently by the SNMP agent) the agent must authenticate the SNMP manager. If the SNMP manager does not provide the correct security details, the agent does not send the traps.</p> <p>The NWA has two SNMP version 3 login accounts, <b>User</b> and <b>Admin</b>. Each account has different security settings. You can use either account's security settings for authenticating SNMP traps.</p> <p>Select <b>User</b> to have the NWA use the <b>User</b> account's security settings, or select <b>Admin</b> to have the NWA use the <b>Admin</b> account's security settings.</p> <p>Use the <b>Configure SNNMPv3 User Profile</b> link to set up each account's security settings.</p>
Configure SNMPv3 User Profile	Click this to go to the <b>SNMPv3 User Profile</b> 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.
Secured Client IP Address	<p>A secured client is a "trusted" computer that is allowed to communicate with the NWA using this service.</p> <p>Select <b>All</b> to allow any computer to access the NWA using this service.</p> <p>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the NWA using this service.</p>
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.8 Technical Reference

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

### 16.8.1 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.

## 16.8.2 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.

## 16.8.3 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 61** 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.

**Table 61** SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
authenticationFailure (defined in <i>RFC-1215</i> )	1.3.6.1.6.3.1.1.5.5	The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password).  Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps.
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.1 3.0.1	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 62** 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



# Internal RADIUS Server

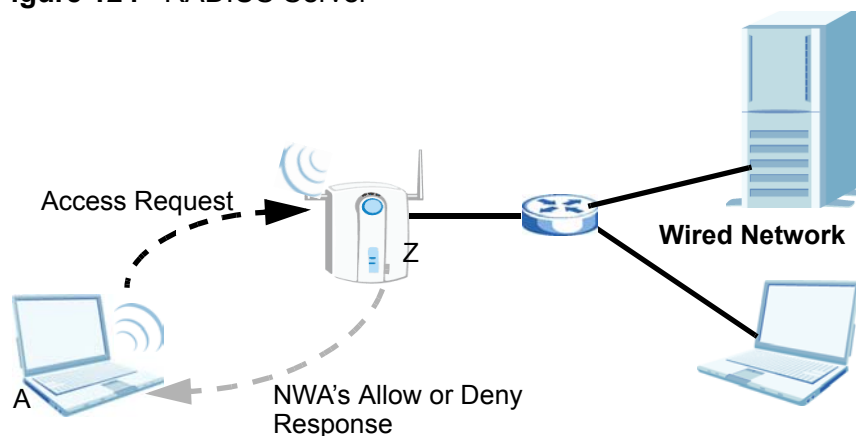
## 17.1 Overview

This chapter describes how the NWA can use its internal RADIUS server to authenticate wireless clients.

Remote Authentication Dial In User Service (RADIUS) is a protocol that enables you to control access to a network by authenticating user credentials.

The following figure shows the NWA (**Z**) using its internal RADIUS server to control access to a wired network. A wireless notebook (**A**) requests access by sending its credentials. The NWA consults its internal RADIUS server's list of user names and passwords. If the credentials of the wireless notebook match an entry, the NWA allows the client to access the network.

**Figure 124** RADIUS Server



The NWA can also serve as a RADIUS server to authenticate other APs and their wireless clients. For more background information on RADIUS, see [Section 11.3 on page 162](#).

## 17.2 What You Can Do in the Internal Radius Server Screens

- Use the **AUTH. SERVER > Setting** screen (see [Section 17.4 on page 200](#)) to turn the NWA's internal RADIUS server off or on and to view information about the NWA's certificates.
- Use the **AUTH. SERVER > Trusted AP** screen (see [Section 17.5 on page 202](#)) to specify APs as trusted. Trusted APs can use the NWA's internal RADIUS server to authenticate wireless clients.
- Use the **AUTH. SERVER > Trusted Users** screen (see [Section 17.6 on page 204](#)) to configure a list of wireless client user names and passwords.

## 17.3 What You Need To Know

The NWA has a built-in RADIUS server that can authenticate wireless clients or other trusted APs. Certificates are used by wireless clients to authenticate the RADIUS server. These are "digital signatures" that identify network devices. Certificates ensure that the clients supply their login details to the correct device. Information matching the certificate is held on the wireless client's utility. A password and user name on the utility must match the **Trusted Users** list so that the RADIUS server can be authenticated.

Note: The NWA can function as an AP and as a RADIUS server at the same time.

## 17.4 Internal RADIUS Server Setting Screen

Use this screen to turn the NWA's internal RADIUS server off or on and to view information about the NWA's certificates.



Click **AUTH. SERVER > Setting**. The following screen displays.

**Figure 125** Setting Screen

Setting	Trusted AP	Trusted Users				
<input checked="" type="checkbox"/> Active						
#	Name	Type	Subject	Issuer	Valid From	Valid To
1	auto_generated_self_signed_cert	*SELF	CN=NWA-3500 001349DF42A8	CN=NWA-3500 001349DF42A8	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT
<input type="button" value="Apply"/>			<input type="button" value="Reset"/>			

The following table describes the labels in this screen.

**Table 63** Internal RADIUS Server Setting Screen

LABEL	DESCRIPTION
Active	Select the <b>Active</b> check box to have the NWA use its internal RADIUS server to authenticate wireless clients or other APs.
#	This field displays the certificate index number. The certificates are listed in alphabetical order. Use the <b>CERTIFICATES</b> screens to manage certificates. The internal RADIUS server uses one of the certificates listed in this screen for authentication with each wireless client. The exact certificate used depends on the certificate information configured on the wireless client.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.  <b>auto_generated_self_signed_cert</b> is the factory default certificate common to all NWAs that use certificates.  Note: It is recommended that you replace the factory default certificate with one that uses your NWA's MAC address. Do this when you first log in to the NWA or in the <b>CERTIFICATES &gt; My Certificates</b> screen.
Type	This field displays what kind of certificate this is.  <b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request.  <b>SELF</b> represents a self-signed certificate.  <b>*SELF</b> represents the default self-signed certificate, which the NWA uses to sign imported trusted remote host certificates.  <b>CERT</b> represents a certificate issued by a certification authority.

**Table 63** Internal RADIUS Server Setting Screen (continued)

LABEL	DESCRIPTION
Subject	This field displays identifying information about the certificate's owner, such as <b>CN</b> (Common Name), <b>OU</b> (Organizational Unit or department), <b>O</b> (Organization or company) and <b>C</b> (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a <b>Not Yet Valid!</b> message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an <b>Expiring!</b> or <b>Expired!</b> message if the certificate is about to expire or has already expired.
Apply	Click <b>Apply</b> to have the NWA use certificates to authenticate wireless clients.
Reset	Click <b>Reset</b> to start configuring this screen afresh.

## 17.5 The Trusted AP Screen

Use this screen to specify APs as trusted. Click **AUTH. SERVER > Trusted AP**. The following screen displays:

**Figure 126** Trusted AP Screen

#	Active	IP Address	Shared Secret
1	<input checked="" type="checkbox"/>	127.0.0.1	
2	<input type="checkbox"/>	0.0.0.0	
3	<input type="checkbox"/>	0.0.0.0	
4	<input type="checkbox"/>	0.0.0.0	
5	<input type="checkbox"/>	0.0.0.0	
...			
29	<input type="checkbox"/>	0.0.0.0	
30	<input type="checkbox"/>	0.0.0.0	
31	<input type="checkbox"/>	0.0.0.0	
32	<input type="checkbox"/>	0.0.0.0	

The following table describes the labels in this screen.

**Table 64** Trusted AP Screen

LABEL	DESCRIPTION
#	This field displays the trusted AP index number.
Active	Select this check box to have the NWA use the <b>IP Address</b> and <b>Shared Secret</b> to authenticate a trusted AP.
IP Address	Type the IP address of the trusted AP in dotted decimal notation.
Shared Secret	<p>Enter a password (up to 31 alphanumeric characters, no spaces) as the key for encrypting communications between the AP and the NWA. The key is not sent over the network. This key must be the same on the AP and the NWA.</p> <p>Both the NWA's IP address and this shared secret must also be configured in the "external RADIUS" server fields of the trusted AP.</p> <p><b>Note:</b> The first trusted AP fields are for the NWA itself.</p>
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 17.6 The Trusted Users Screen

Use this screen to configure trusted user entries. Click **AUTH. SERVER > Trusted Users**. The following screen displays.

**Figure 127** Trusted Users Screen

#	Active	User Name	Password
1	<input type="checkbox"/>		
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
...			
125	<input type="checkbox"/>		
126	<input type="checkbox"/>		
127	<input type="checkbox"/>		
128	<input type="checkbox"/>		

Note. Password: Maximum 14 ASCII characters with PEAP

Apply      Reset

The following table describes the labels in this screen.

**Table 65** Trusted Users

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

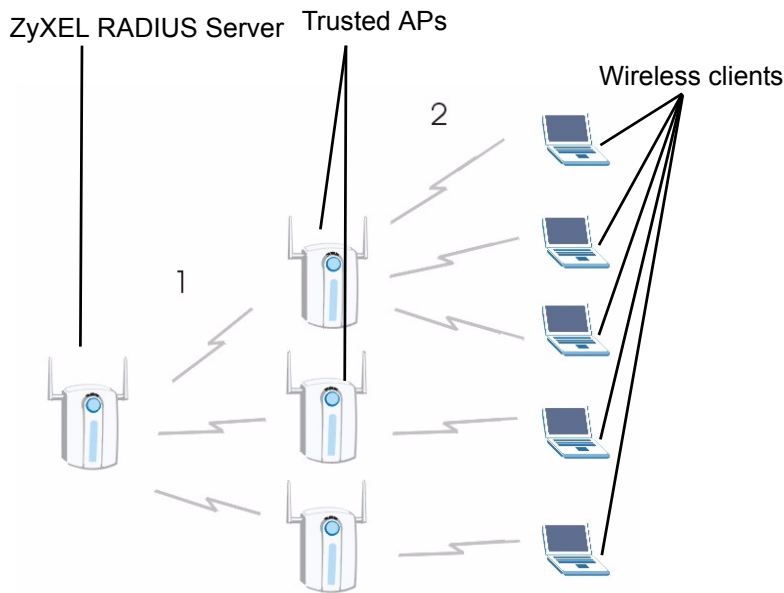
## 17.7 Technical Reference

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

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

The following figure shows how this is done. Wireless clients make access requests to trusted APs, which relay the requests to the NWA.

**Figure 128** Trusted APs Overview



Take the following steps to set up trusted APs and trusted users.

- 1 Configure an IP address and shared secret in the **Trusted AP** database to specify an AP as trusted.
- 2 Configure wireless client user names and passwords in the **Trusted Users** database to use a trusted AP as a relay between the NWA's internal RADIUS server and the wireless clients.

The wireless clients can then be authenticated by the NWA's internal RADIUS server.

PEAP (Protected EAP) and MD5 authentication is implemented on the internal RADIUS server using simple username and password methods over a secure TLS connection. See [Appendix B on page 319](#) for more information on the types of EAP authentication and the internal RADIUS authentication method used in your NWA.

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

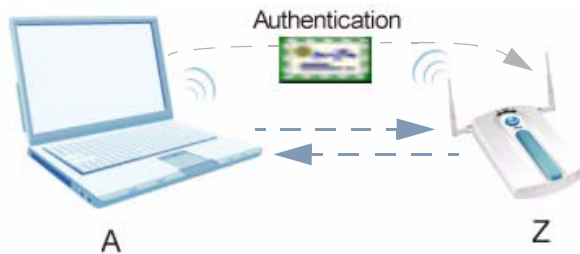
# Certificates

## 18.1 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 129** Certificates Example



In the figure above, the NWA (**Z**) checks the identity of the notebook (**A**) using a certificate before granting it access to the network.

## 18.2 What You Can Do in the Certificates Screen

- Use the **Certificates > My Certificate** (see [Chapter 18 on page 214](#)) screens to view details of certificates storage space and settings. This screen also allows you to import or create a new certificate.
- Use the **Certificates > Trusted CAs** (see [Chapter 18 on page 219](#)) screens to save CA certificates to the NWA. This screen displays a summary list of certificates of the certification authorities that you have set the NWA to accept as trusted.

## 18.3 What You Need To Know

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. Note that the NWA also trusts any valid certificate signed by any of the imported trusted CA certificates. 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.

The NWA only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.

Certificates are based on public-private key pairs. Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

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

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

You can have the NWA act as a certification authority and sign its own certificates. See [Section 18.4.2 on page 211](#) for details on how to apply this.

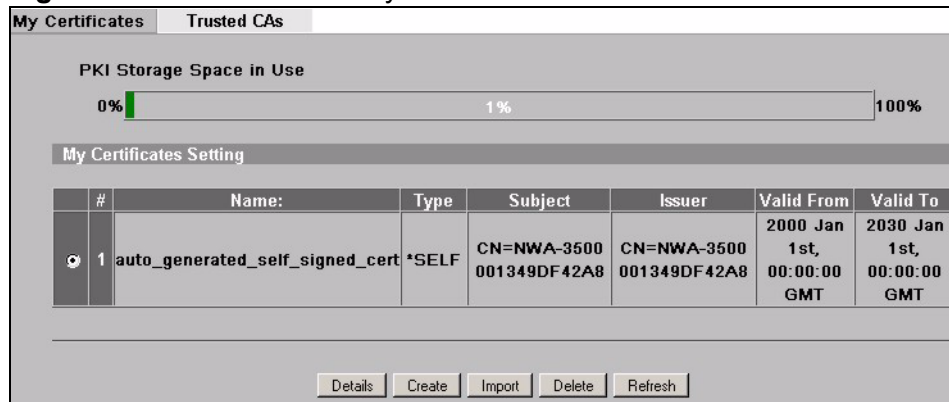
## 18.4 My Certificates Screen

Use this screen to view the NWA's summary of certificates and certification requests. Click **Certificates** > **My Certificates**. The following screen displays.



Note: Certificates display in black and certification requests display in gray.

**Figure 130** Certificates > My Certificates



The following table describes the labels in this screen.

**Table 66** Certificates > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the NWA's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
My Certificates Setting	
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is.  <b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request.  <b>SELF</b> represents a self-signed certificate.  <b>*SELF</b> represents the default self-signed certificate, which the NWA uses to sign imported trusted remote host certificates.  <b>CERT</b> represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.

**Table 66** Certificates > My Certificates (continued)

LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Details	<p>Click the details icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features is configured to use.</p> <p>Do the following to delete a certificate that shows <b>*SELF</b> in the <b>Type</b> field.</p> <ol style="list-style-type: none"> <li>1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the <b>*SELF</b> certificate.</li> <li>2. Click the details icon next to another self-signed certificate (see the description on the <b>Create</b> button if you need to create a self-signed certificate).</li> <li>3. Select the <b>Default self-signed certificate which signs the imported remote host certificates</b> check box.</li> <li>4. Click <b>Apply</b> to save the changes and return to the <b>My Certificates</b> screen.</li> <li>5. The certificate that originally showed <b>*SELF</b> displays <b>SELF</b> and you can delete it now.</li> </ol> <p>Note that subsequent certificates move up by one when you take this action</p>
Create	Click <b>Create</b> to go to the screen where you can have the NWA generate a certificate or a certification request.
Import	Click <b>Import</b> to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the NWA.
Delete	Click <b>Delete</b> to delete an existing certificate. A window display asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Refresh	Click <b>Refresh</b> to display the current validity status of the certificates.

### 18.4.1 My Certificates Import Screen

Use this screen if you have an existing CA-issued certificate you want to use for authentication. Follow the instructions in this screen to save it to the NWA. Click **Certificates > My Certificates** and then **Import** to open the **My Certificate Import** screen.

Note: You can import only a certificate that matches a corresponding certification request that was generated by the NWA.

Note: The certificate you import replaces the corresponding request in the My Certificates screen.

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

**Figure 131** Certificates > My Certificates Import

The following table describes the labels in this screen.

**Table 67** Certificates > My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the NWA.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

## 18.4.2 My Certificates Create Screen

Use this screen if you do not have an existing or issued certificate and want to have the NWA create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Click **Certificates > My Certificates** and then **Create** to open the **My Certificate Create** screen. The following figure displays.

**Figure 132** Certificates > My Certificate Create

The following table describes the labels in this screen.

**Table 68** Certificates > My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the <b>Common Name</b> is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the NWA drops trailing spaces.

**Table 68** Certificates > My Certificate Create (continued)

LABEL	DESCRIPTION
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the NWA drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the NWA drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select <b>Create a self-signed certificate</b> to have the NWA generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	<p>Select <b>Create a certification request and save it locally for later manual enrollment</b> to have the NWA generate and store a request for a certificate. Use the <b>My Certificate Details</b> screen to view the certification request and copy it to send to the certification authority.</p> <p>Copy the certification request from the <b>My Certificate Details</b> screen (<a href="#">Section 18.4.3 on page 214</a>) and then send it to the certification authority.</p>
Create a certification request and enroll for a certificate immediately online	<p>Select <b>Create a certification request and enroll for a certificate immediately online</b> to have the NWA generate a request for a certificate and apply to a certification authority for a certificate.</p> <p>You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen.</p> <p>When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the <b>Reference Number</b> and <b>Key</b> if the certification authority requires them.</p>
Enrollment Protocol	<p>Select the certification authority's enrollment protocol from the drop-down list box.</p> <p><b>Simple Certificate Enrollment Protocol (SCEP)</b> is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.</p> <p><b>Certificate Management Protocol (CMP)</b> is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.</p>
CA Server Address	Enter the IP address (or URL) of the certification authority server.

**Table 68** Certificates > My Certificate Create (continued)

LABEL	DESCRIPTION
CA Certificate	Select the certification authority's certificate from the <b>CA Certificate</b> drop-down list box.  You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen. Click <b>Trusted CAs</b> to go to the <b>Trusted CAs</b> screen where you can view (and manage) the NWA's list of certificates of trusted certification authorities.
Request Authentication	When you select <b>Create a certification request and enroll for a certificate immediately online</b> , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the <b>Reference Number</b> and the <b>Key</b> fields if your certification authority uses CMP enrollment protocol. Just fill in the <b>Key</b> field if your certification authority uses the SECP enrollment protocol.
Key	Type the key that the certification authority gave you.
Apply	Click <b>Apply</b> to begin certificate or certification request generation.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

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

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

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

### 18.4.3 My Certificates Details Screen

Use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the NWA uses to sign the trusted remote host certificates that you import to the NWA.

Click **Certificates > My Certificates** to open the **My Certificates** screen (Figure 130 on page 209). Click the details button to open the **My Certificate Details** screen.

**Figure 133** Certificates > My Certificate Details

The screenshot displays the 'My Certificate Details' interface. At the top, the 'Name' field is set to 'auto\_generated\_self\_signed\_cert'. Below it, a 'Property' section contains a checked checkbox for 'Default self-signed certificate which signs the imported remote host certificates.' The 'Certificate Path' section features a search box with 'Searching...' and a 'Refresh' button. The 'Certificate Information' section lists various attributes:

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946685120
Subject	CN=NWA-3160 0019CB000001
Issuer	CN=NWA-3160 0019CB000001
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=0019CB000001@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	2b:d5:da:d5:cf:ae:b7:96:06:72:c2:24:0c:49:e0:2d
SHA1 Fingerprint	af:f6:db:ac:fe:ab:13:d1:43:24:bf:4f:43:e2:4d:4f:d7:f2:18:aa

The 'Certificate in PEM (Base-64) Encoded Format' section shows a text area with the following content:

```

eUFJUiBHLTEwMDBQIEZHY3RvcnkgRGVmYXVsdCBDZXJOaWZpY2FOZTAeFwOwMDAx
MDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBaMDQxMjAwBgNVBAMTKVp5QU1SIEctMTAw
MFAgRmFjdG9yeSBEZlZhdWx0IEN1cnRpZmljYXR1MFwwDQYJKoZIhvcNAQEBBQAD
SwAwSAJBANB1YebOCBx9tjUjVL2VoIFv1WBrQM613TF1UQoHKQtSFywWdFNnXX5L
qXfX1YHFgoO8MnC6cJGUGGhd5pWau8MCAwEAAN7MHKwDgYDVROPAQEABAQDAGKk
HCAGA1UdEQQ2MBeBFwZHY3Rvcn1AYXV0by5nZW4uY2VydDASBgNVHRMBAQAECDAG
AQH/AgEBMDEGA1UdJQqMCgGCCeGAQUFCAICBggrBgEFBQcDAQYIKwYBBQUHAwQG
CCsGAQUFBwMCAOGCSqGSIb3DQEBBQUAAOEAK/6Za1/UjL+WZkiE+h6UmGJYT/gG
D0yeDwtMQzydQ2Rn3dDLGI9QJtZwJrD8njPGv3oR7AZrcw1T2VQkA9FA9g==
-----END CERTIFICATE-----

```

At the bottom of the screen, there are three buttons: 'Export', 'Apply', and 'Cancel'.

The following table describes the labels in this screen.

**Table 69** Certificates > My Certificate Details

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



**Table 69** Certificates > My Certificate Details (continued)

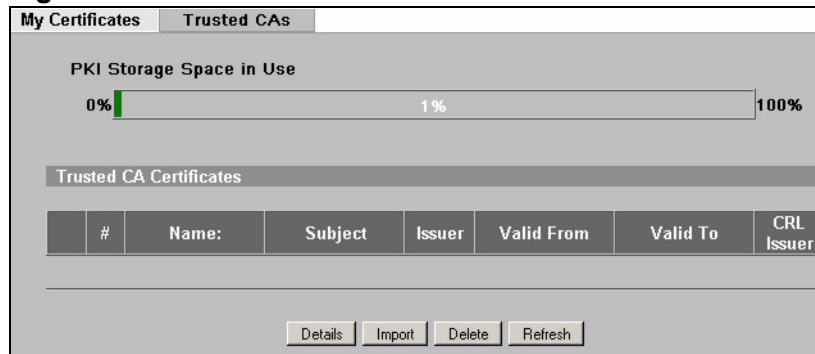
LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the NWA uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the NWA calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the NWA calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Export	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

## 18.5 Trusted CAs Screen

Use this screen to view the list of trusted certificates. The NWA accepts any valid certificate signed by a certification authority on this list as being trustworthy. You do not need to import any certificate that is signed by any certification authority on this list.

Click **Certificates > Trusted CAs** to open the **Trusted CAs** screen. The following figure displays.

**Figure 134** Certificates > Trusted CAs



The following table describes the labels in this screen.

**Table 70** Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the NWA's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Trusted CA Certificates	
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

**Table 70** Trusted CAs (continued)

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

## 18.5.1 Trusted CAs Import Screen

Use this screen to save a trusted certification authority's certificate to the NWA. Click **Certificates > Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CAs Import** screen. The following figure displays.

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

**Figure 135** Certificates > Trusted CAs Import

**Import**

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

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

File Path:

The following table describes the labels in this screen.

**Table 71** Certificates > Trusted CA Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the NWA.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.

## 18.5.2 Trusted CAs Details Screen

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the NWA to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Click **Certificates > Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CAs Details** screen.

**Figure 136** Certificates > Trusted CAs Details

**Name:** VeriSign.cer

**Property**

Check incoming certificates issued by this CA against a CRL

**Certificate Path**

Searching...

Refresh

**Certificate Information**

<b>Type</b>	Self-signed X.509 Certificate
<b>Version</b>	V1
<b>Serial Number</b>	3658802160848854062232407011527417280
<b>Subject</b>	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US
<b>Issuer</b>	OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US
<b>Signature Algorithm</b>	rsa-pkcs1-md2
<b>Valid From</b>	1994 Nov 9th, 00:00:00 GMT
<b>Valid To</b>	2010 Jan 7th, 23:59:59 GMT
<b>Key Algorithm</b>	rsaEncryption (1000 bits)
<b>MD5 Fingerprint</b>	74:7b:82:03:43:f0:00:9e:6b:b3:ec:47:bf:85:a5:93
<b>SHA1 Fingerprint</b>	44:63:c5:31:d7:cc:c1:00:67:94:61:2b:b6:56:d3:bf:82:57:84:6f

**Certificate in PEM (Base-64) Encoded Format**

```
-----BEGIN CERTIFICATE-----
MIICNDCCAECAktZnSORf5eV288mB1e3cAwDQYJKoZIhvcNAQEFBQAwXzELMakG
A1UEBhMVCVVMxIDAeBgNVBaoTF1JTSBZEYXRhIFN1Y3VyaXR5L0JmMUMS4wLAYD
VQQLZyVTZW1cmUgU2VydMvYIEN1cnRpZm1jYXRpb24gQXV0aG9yaXR5MB4XDk0
MTEwOTAwMDAwMFOXDTEwMDEwNzIzNTk1OVowXzELMakGA1UEBhMVCVVMxIDAeBgNV
BAoTF1JTSBZEYXRhIFN1Y3VyaXR5L0JmMUMS4wLAYDVQQLZyVTZW1cmUgU2VydMvYI
EN1cnRpZm1jYXRpb24gQXV0aG9yaXR5MIGbMAOGCSqGSIb3DQEBAQUAA4GJ
ADCBhQJ+AJLOesGugz5aqomDV6wLAXYMr a6OLDf06zV4ZFQD5YR&Ucm/ jwjiioII
OhaGN1XpsSECrXZogZofokvJSyVmI1ZsiAeP94FZbYQHZZATcXY+m3dM41CJVphI
uR2nKR0TLkoRWZweFdVJVCxzOmmCs2c5nG1wZ0j13S3WYB57AgMBAAEwDQYJKoZI
```

Export Apply Cancel

The following table describes the labels in this screen.

**Table 72** Certificates > Trusted CAs Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the NWA check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).  Clear this check box to have the NWA not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).

**Table 72** Certificates > Trusted CAs Details (continued)

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

**Table 72** Certificates > Trusted CAs Details (continued)

LABEL	DESCRIPTION
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the NWA calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the NWA has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See <a href="#">Section 18.3 on page 208</a> for how to verify a remote host's certificate before you import it into the NWA.
SHA1 Fingerprint	This is the certificate's message digest that the NWA calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the NWA has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See <a href="#">Section 18.3 on page 208</a> for how to verify a remote host's certificate before you import it into the NWA.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Export	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes. You can only change the name and/or set whether or not you want the NWA to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.

## 18.6 Technical Reference

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

## 18.6.1 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.

## 18.6.2 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.



## 18.6.3 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.

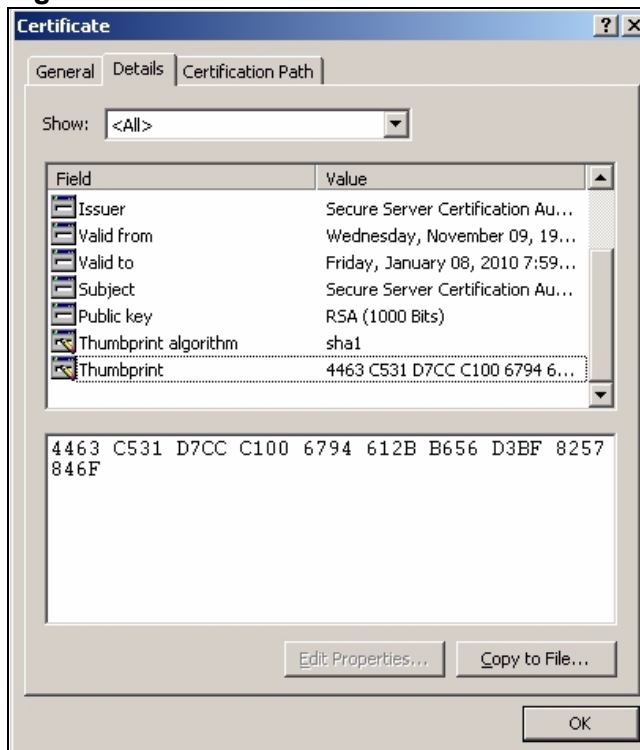
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 137** 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 138** Certificate Details



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

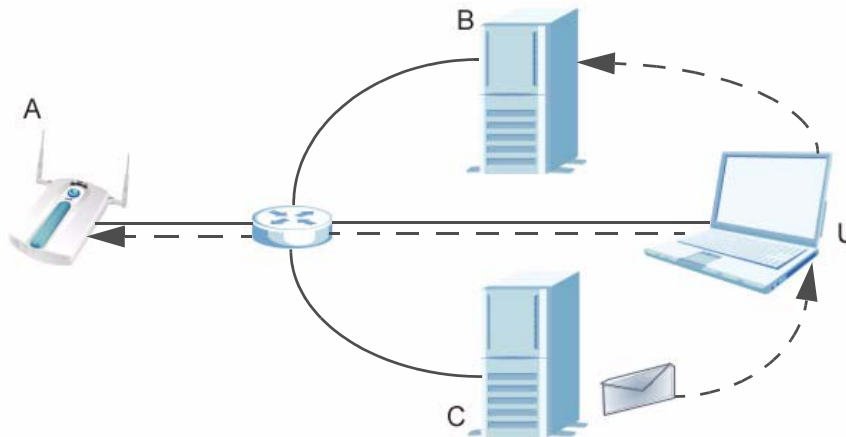
# Log Screens

## 19.1 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 computer 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 139** 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.

## 19.2 What You Can Do in the Log Screens

- Use the **View Log** screen ([Section 19.4 on page 228](#)) 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.
- Use the **Log Settings** screen ([Section 19.5 on page 229](#)) to configure where and when the NWA will send the logs, and which logs and/or immediate alerts it will send.

## 19.3 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 Email

If you want to receive logs in your email account, you need to have the necessary details ready, such as the Server Name or SMPT Address of your email account. Ensure that you have a valid email address.

### Enabling Syslog Logging

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

## 19.4 The View Log Screen

Use this screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Figure 141 on page 230](#)). Options include logs about system maintenance, system errors and access control.

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.

Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Click **Logs > View Log**. The following screen displays.

**Figure 140** Logs > View Log

Index	Time	Message	Source	Destination	Notes
1	01/01/2000 21:34:51	Rogue AP Detection.			MAC:00:13:a6:10:1b:c1, Channel:01, Security:None, SSID:testonly
2	01/01/2000 21:24:24	Cert trusted: CN=NWA3550 001349000001			CERT MANAGER
3	01/01/2000 20:37:24	Successful HTTPS login	192.168.1.33		User:admin

The following table describes the labels in this screen.

**Table 73** Logs > View Log

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

## 19.5 The Log Settings Screen

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

Click **Logs > Log Settings**. The following screen displays.

**Figure 141** Logs > Log Settings

The following table describes the labels in this screen.

**Table 74** Logs > 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.

**Table 74** Logs > Log Settings

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

## 19.6 Technical Reference

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

### 19.6.1 Example Log Messages

This section provides descriptions of some example log messages.

**Table 75** System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The NWA has adjusted its time based on information from the time server.
Time calibration failed	The NWA failed to get information from the time server.
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
SMT Login Successfully	Someone has logged on to the NWA's SMT interface.
SMT Login Fail	Someone has failed to log on to the NWA's SMT interface.
WEB Login Successfully	Someone has logged on to the NWA's web configurator interface.
WEB Login Fail	Someone has failed to log on to the NWA's web configurator interface.
TELNET Login Successfully	Someone has logged on to the NWA via telnet.
TELNET Login Fail	Someone has failed to log on to the NWA via telnet.
FTP Login Successfully	Someone has logged on to the NWA via FTP.
FTP Login Fail	Someone has failed to log on to the NWA via FTP.

**Table 76** ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench



**Table 76** ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

**Table 77** Sys log

LOG MESSAGE	DESCRIPTION
<pre>Mon dd hr:mm:ss hostname src="&lt;srcIP:srcPort&gt;" dst="&lt;dstIP:dstPort&gt;" msg="&lt;msg&gt;" note="&lt;note&gt;"</pre>	This message is sent by the "RAS" when this syslog is generated. The messages and notes are defined in this appendix's other charts.

## 19.6.2 Log Commands

Go to the command interpreter interface (refer to [Appendix F on page 379](#) for a discussion on how to access and use the commands).

## 19.6.3 Configuring What You Want the NWA to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the NWA is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

**Table 78** Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
error	0, 1, 2, 3
mten	0, 1
Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category.	

Use the `sys logs save` command to store the settings in the NWA (you must do this in order to record logs).

## 19.6.4 Displaying Logs

Use the `sys logs display` command to show all of the logs in the NWA's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual NWA log category.

Use the `sys logs clear` command to erase all of the NWA's logs.

## 19.6.5 Log Command Example

This example shows how to set the NWA to record the error logs and alerts and then view the results.

```

ras> sys logs load
ras> sys logs category error 3
ras> sys logs save
ras> sys logs display access

#.      time                source                destination          notes
message
0 | 11/11/2002 15:10:12 | 172.22.3.80:137 | 172.22.255.255:137 | ACCESS
BLOCK

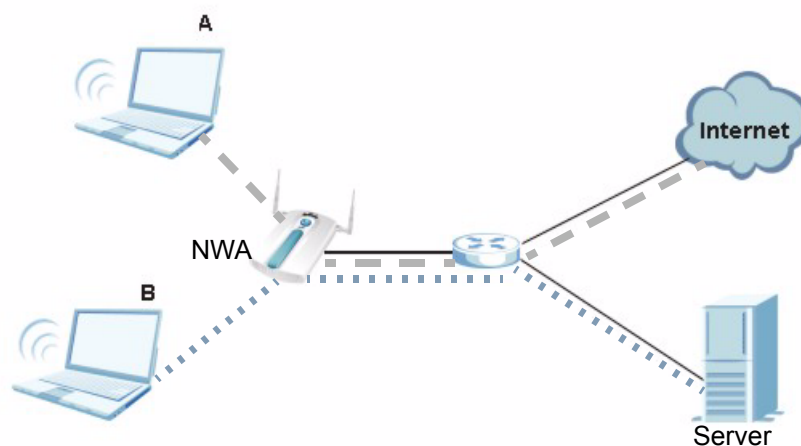
```

## 20.1 Overview

This chapter discusses how to configure VLAN on the NWA.

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

**Figure 142** VLAN Example



In the figure above, the NWA allows station A to connect to the internet but not to the server. It allows station B to connect to the server but not to the Internet.

## 20.2 What You Can Do in the VLAN Screen

- Use the **Wireless VLAN** screen ([Section 20.4 on page 237](#)) to enable and configure your Wireless Virtual LAN setup. The NWA tags all packets from an SSID with the VLAN ID you set in this screen.
- Use the **Radius VLAN** screen ([Section 20.4.1 on page 239](#)) to configure your RADIUS Virtual LAN setup. Your RADIUS server assigns VLAN IDs to a user or user group's traffic based on what you set in this screen.

## 20.3 What You Need To Know About VLAN

When you use wireless VLAN and RADIUS VLAN together, the NWA first tries to assign VLAN IDs based on RADIUS VLAN configuration. If a client's user name does not match an entry in the **RADIUS VLAN** screen, the NWA assigns a VLAN ID based on the settings in the **Wireless VLAN** screen. See [Section 20.5.3 on page 243](#) for more information.

Note: To use RADIUS VLAN, you must first select **Enable VIRTUAL LAN** and configure the **Management VLAN ID** in the VLAN > Wireless VLAN screen.

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

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

## 20.4 Wireless VLAN Screen

Use this screen to enable and configure your Wireless Virtual LAN setup. Click **VLAN > Wireless VLAN**. The following screen appears.

**Figure 143** VLAN > Wireless VLAN

Wireless VLAN
RADIUS VLAN

VIRTUAL LAN Setup

Enable VIRTUAL LAN

Wireless VIRTUAL LAN Setup

Management VLAN ID  (1 - 4094)

**VLAN Mapping Table**

Index	Name	SSID	VLAN ID	Second Rx VLAN ID
1	VoIP_SSID	ZyXEL01	<input style="width: 30px;" type="text" value="1"/>	<input style="width: 30px;" type="text" value="0"/>
2	Guest_SSID	ZyXEL02	<input style="width: 30px;" type="text" value="2"/>	<input style="width: 30px;" type="text" value="0"/>
3	SSID03	ZyXEL03	<input style="width: 30px;" type="text" value="3"/>	<input style="width: 30px;" type="text" value="0"/>
4	SSID04	ZyXEL04	<input style="width: 30px;" type="text" value="4"/>	<input style="width: 30px;" type="text" value="0"/>
5	SSID05	ZyXEL05	<input style="width: 30px;" type="text" value="5"/>	<input style="width: 30px;" type="text" value="0"/>
6	SSID06	ZyXEL06	<input style="width: 30px;" type="text" value="6"/>	<input style="width: 30px;" type="text" value="0"/>
7	SSID07	ZyXEL07	<input style="width: 30px;" type="text" value="7"/>	<input style="width: 30px;" type="text" value="0"/>
8	SSID08	ZyXEL08	<input style="width: 30px;" type="text" value="8"/>	<input style="width: 30px;" type="text" value="0"/>
9	SSID09	ZyXEL09	<input style="width: 30px;" type="text" value="9"/>	<input style="width: 30px;" type="text" value="0"/>
10	SSID10	ZyXEL10	<input style="width: 30px;" type="text" value="10"/>	<input style="width: 30px;" type="text" value="0"/>
11	SSID11	ZyXEL11	<input style="width: 30px;" type="text" value="11"/>	<input style="width: 30px;" type="text" value="0"/>
12	SSID12	ZyXEL12	<input style="width: 30px;" type="text" value="12"/>	<input style="width: 30px;" type="text" value="0"/>
13	SSID13	ZyXEL13	<input style="width: 30px;" type="text" value="13"/>	<input style="width: 30px;" type="text" value="0"/>
14	SSID14	ZyXEL14	<input style="width: 30px;" type="text" value="14"/>	<input style="width: 30px;" type="text" value="0"/>
15	SSID15	ZyXEL15	<input style="width: 30px;" type="text" value="15"/>	<input style="width: 30px;" type="text" value="0"/>
16	SSID16	ZyXEL16	<input style="width: 30px;" type="text" value="16"/>	<input style="width: 30px;" type="text" value="0"/>

The following table describes the labels in this screen

**Table 79** VLAN > Wireless VLAN

FIELD	DESCRIPTION
Enable VIRTUAL LAN	Select this box to enable VLAN tagging.
Management VLAN ID	<p>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.</p> <p>Note: Mail and FTP servers must have the same management VLAN ID to communicate with the NWA.</p> <p>See <a href="#">Section 20.5.2 on page 240</a> for more information.</p>
VLAN Mapping Table	Use this table to have the NWA assign VLAN tags to packets from wireless clients based on the SSID they use to connect to the NWA.
Index	This is the index number of the SSID profile.
Name	This is the name of the SSID profile.
SSID	This is the SSID the profile uses.
VLAN ID	Enter a VLAN ID number from 1 to 4094. Packets coming from the WLAN using this SSID profile are tagged with the VLAN ID number by the NWA. Different SSID profiles can use the same or different VLAN IDs. This allows you to split wireless stations into groups using similar VLAN IDs.
Second Rx VLAN ID	Enter a number from 1 to 4094, but different from the <b>VLAN ID</b> . Traffic received from the LAN that is tagged with this VLAN ID is sent to all SSIDs with this VLAN ID configured in the <b>VLAN ID</b> or <b>Second Rx VLAN ID</b> fields. See <a href="#">Section 20.5.4 on page 253</a> for more information.
Apply	Click this to save your changes to the NWA.
Reset	Click this to return this screen to its last-saved settings.

## 20.4.1 RADIUS VLAN Screen

Use this screen to configure your RADIUS Virtual LAN setup. Click **VLAN > RADIUS VLAN**. The following screen appears.

**Figure 144** VLAN > RADIUS VLAN

Wireless VLAN RADIUS VLAN

RADIUS VIRTUAL LAN Setup

Block station if RADIUS server assign VLAN name error!

VLAN Mapping Table

	Index	ID	Name
<input type="checkbox"/>	1	(1 ~ 4094)	zyxel
<input type="checkbox"/>	2	(1 ~ 4094)	zyxel
<input type="checkbox"/>	3	(1 ~ 4094)	zyxel
<input type="checkbox"/>	4	(1 ~ 4094)	zyxel
<input type="checkbox"/>	5	(1 ~ 4094)	zyxel
<input type="checkbox"/>	6	(1 ~ 4094)	zyxel
<input type="checkbox"/>	7	(1 ~ 4094)	zyxel
<input type="checkbox"/>	8	(1 ~ 4094)	zyxel
<input type="checkbox"/>	9	(1 ~ 4094)	zyxel
<input type="checkbox"/>	10	(1 ~ 4094)	zyxel
<input type="checkbox"/>	11	(1 ~ 4094)	zyxel
<input type="checkbox"/>	12	(1 ~ 4094)	zyxel
<input type="checkbox"/>	13	(1 ~ 4094)	zyxel
<input type="checkbox"/>	14	(1 ~ 4094)	zyxel
<input type="checkbox"/>	15	(1 ~ 4094)	zyxel
<input type="checkbox"/>	16	(1 ~ 4094)	zyxel

Apply Reset

The following table describes the labels in this screen.

**Table 80** VLAN > RADIUS VLAN

LABEL	DESCRIPTION
Block station if RADIUS server assign VLAN name error!	Select this to have the NWA forbid access to wireless clients when the VLAN attributes sent from the RADIUS server do not match a configured <b>Name</b> field. When you select this check box, only users with names configured in this screen can access the network through the NWA.
VLAN Mapping Table	Use this table to map names to VLAN IDs so that the RADIUS server can assign each user or user group a mapped VLAN ID. See your RADIUS server documentation for more information on configuring VLAN ID attributes. See <a href="#">Section 20.5.3 on page 243</a> for more information.
	Select a check box to enable the VLAN mapping profile.
ID	Type a VLAN ID. Incoming traffic from the WLAN is authorized and assigned a VLAN ID before it is sent to the LAN.

**Table 80** VLAN > RADIUS VLAN

LABEL	DESCRIPTION
Name	Type a name to have the NWA check for specific VLAN attributes on incoming messages from the RADIUS server. Access-accept packets sent by the RADIUS server contain VLAN related attributes. The configured <b>Name</b> fields are checked against these attributes. If a configured <b>Name</b> field matches these attributes, the corresponding VLAN ID is added to packets sent from this user to the LAN.  If the VLAN-related attributes sent by the RADIUS server do not match a configured <b>Name</b> field, a wireless station is assigned the wireless VLAN ID associated with its SSID (unless the <b>Block station if RADIUS server assign VLAN error!</b> check box is selected).
Apply	Click <b>Apply</b> to save your changes to the NWA.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 20.5 Technical Reference

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

### 20.5.1 VLAN Tagging

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

Note: You must connect the NWA to a VLAN-aware device that is a member of the management VLAN in order to perform management. See the **Configuring Management VLAN example** BEFORE you configure the VLAN screens.

### 20.5.2 Configuring Management VLAN Example

This section shows you how to create a VLAN on an Ethernet switch.

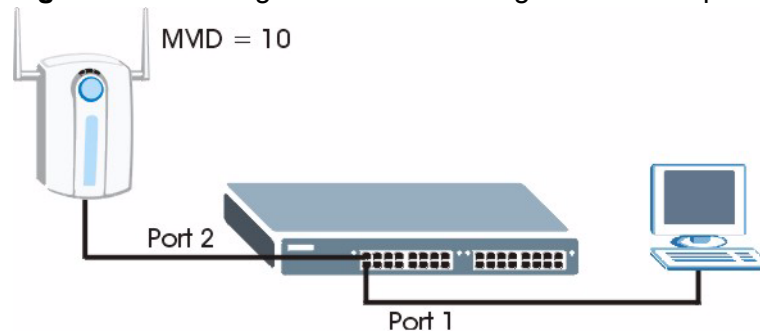
By default, the port on the NWA is a member of the management VLAN (VLAN ID 1). The following procedure shows you how to configure a tagged VLAN.

Note: Use the out-of-band management port or console port to configure the switch if you misconfigure the management VLAN and lock yourself out from performing in-band management.



On an Ethernet switch, create a VLAN that has the same management VLAN ID as the NWA. The following figure has the NWA connected to port 2 of the switch and your computer connected to port 1. The management VLAN ID is ten.

**Figure 145** Management VLAN Configuration Example



Perform the following steps in the switch web configurator:

- 1 Click **VLAN** under **Advanced Application**.
- 2 Click **Static VLAN**.
- 3 Select the **ACTIVE** check box.
- 4 Type a **Name** for the VLAN ID.
- 5 Type a **VLAN Group ID**. This should be the same as the management VLAN ID on the NWA.
- 6 Enable **Transmitted Packets (Tx) Tagging** on the port which you want to connect to the NWA. Disable **Tx Tagging** on the port you are using to connect to your computer.
- 7 Under **Control**, select **Fixed** to set the port as a member of the VLAN.

**Figure 146** VLAN-Aware Switch - Static VLAN

Port		Control		Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="radio"/> Forbidden	<input checked="" type="checkbox"/> Tx Tagging

Static VLAN		VLAN Status
ACTIVE	<input checked="" type="checkbox"/>	
Name	MD1	
VLAN Group ID	10	

- Click **Apply**. The following screen displays.

**Figure 147** VLAN-Aware Switch

VID	Active	Name	Delete
10	Yes	VID1	<input type="checkbox"/>
2	Yes	2	<input type="checkbox"/>
3	Yes	3	<input type="checkbox"/>
4	Yes	VLAN4	<input type="checkbox"/>
5	Yes	cth-test	<input type="checkbox"/>

- Click **VLAN Status** to display the following screen.

**Figure 148** VLAN-Aware Switch - VLAN Status

VLAN Status		Port Number																Elapsed Time	Status
Index	VID	2	4	6	8	10	12	14	16	18	20	22	24	26	S2				
		1	3	5	7	9	11	13	15	17	19	21	23	25	S1				
1	10	T	-	-	-	T	U	-	-	-	-	-	-	-	-	0:08:28	Static		
2	2	T	U	-	-	-	-	-	-	-	-	-	-	-	-	0:08:28	Static		
3	3	T	U	-	-	-	-	-	-	-	-	-	-	-	-	0:08:28	Static		
4	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:08:27	Static		
5	5	-	-	-	-	-	U	-	-	-	-	-	-	-	-	0:08:27	Static		

Follow the instructions in the Quick Start Guide to set up your NWA for configuration. The NWA should be connected to the VLAN-aware switch. In the above example, the switch is using port 1 to connect to your computer and port 2 to connect to the NWA: [Figure 145 on page 241](#).

- In the NWA web configurator click **VLAN** to open the VLAN setup screen.
- Select the **Enable VLAN Tagging** check box and type a **Management VLAN ID** (10 in this example) in the field provided.

- 3 Click **Apply**.

**Figure 149** VLAN Setup

WIRELESS VLAN
RADIUS VLAN

VIRTUAL LAN Setup

Enable VIRTUAL LAN

Wireless VIRTUAL LAN Setup

Management VLAN ID  (1 - 4094)

**VLAN Mapping Table**

Index	Name	SSID	VLAN ID	Second Rx VLAN ID
1	VoIP_SSID	ZyXEL01	<input type="text" value="1"/>	<input type="text" value="0"/>
2	Guest_SSID	ZyXEL02	<input type="text" value="2"/>	<input type="text" value="0"/>
3	SSID03	ZyXEL03	<input type="text" value="3"/>	<input type="text" value="0"/>
4	SSID04	ZyXEL04	<input type="text" value="4"/>	<input type="text" value="0"/>
5	SSID05	ZyXEL05	<input type="text" value="5"/>	<input type="text" value="0"/>
6	SSID06	ZyXEL06	<input type="text" value="6"/>	<input type="text" value="0"/>
7	SSID07	ZyXEL07	<input type="text" value="7"/>	<input type="text" value="0"/>
8	SSID08	ZyXEL08	<input type="text" value="8"/>	<input type="text" value="0"/>
9	SSID09	ZyXEL09	<input type="text" value="9"/>	<input type="text" value="0"/>
10	SSID10	ZyXEL10	<input type="text" value="10"/>	<input type="text" value="0"/>
11	SSID11	ZyXEL11	<input type="text" value="11"/>	<input type="text" value="0"/>
12	SSID12	ZyXEL12	<input type="text" value="12"/>	<input type="text" value="0"/>
13	SSID13	ZyXEL13	<input type="text" value="13"/>	<input type="text" value="0"/>
14	SSID14	ZyXEL14	<input type="text" value="14"/>	<input type="text" value="0"/>
15	SSID15	ZyXEL15	<input type="text" value="15"/>	<input type="text" value="0"/>
16	SSID16	ZyXEL16	<input type="text" value="16"/>	<input type="text" value="0"/>

- 4 The NWA attempts to connect with a VLAN-aware device. You can now access and manage the NWA through the Ethernet switch.

Note: If you do not connect the NWA to a correctly configured VLAN-aware device, you will lock yourself out of the NWA. If this happens, you must reset the NWA to access it again.

### 20.5.3 Configuring Microsoft's IAS Server Example

Dynamic VLAN assignment can be used with the NWA. Dynamic VLAN assignment allows network administrators to assign a specific VLAN (configured on the NWA) to an individual's Windows User Account. When a wireless station is successfully authenticated to the network, it is automatically placed into its respective VLAN.

ZyXEL uses the following standard RADIUS attributes returned from Microsoft's IAS RADIUS service to place the wireless station into the correct VLAN:

**Table 81** Standard RADIUS Attributes

ATTRIBUTE NAME	TYPE	VALUE
Tunnel-Type	064	13 (decimal) – VLAN
Tunnel-Medium-Type	065	6 (decimal) – 802
Tunnel-Private-Group-ID	081	<vlan-name> (string) – either the <b>Name</b> you enter in the NWA's <b>VLAN &gt; RADIUS VLAN</b> screen or the number. See <a href="#">Figure 161 on page 251</a> .

The following occurs under Dynamic VLAN Assignment:

- 1 When you configure your wireless credentials, the NWA sends the information to the IAS server using RADIUS protocol.
- 2 Authentication by the RADIUS server is successful.
- 3 The RADIUS server sends three attributes related to this feature.
- 4 The NWA compares these attributes with the VLAN screen mapping table.
  - 4a If the **Name**, for example "VLAN 20" is found, the mapped VLAN ID is used.
  - 4b If the **Name** is not found in the mapping table, the string in the **Tunnel-Private-Group-ID** attribute is considered as a number ID format, for example 2493. The range of the number ID (Name:string) is between 1 and 4094.
  - 4c If **a** or **b** are not matched, the NWA uses the VLAN ID configured in the **WIRELESS VLAN** screen and the wireless station. This **VLAN ID** is independent and hence different to the **ID** in the VLAN screen.

### 20.5.3.1 Configuring VLAN Groups

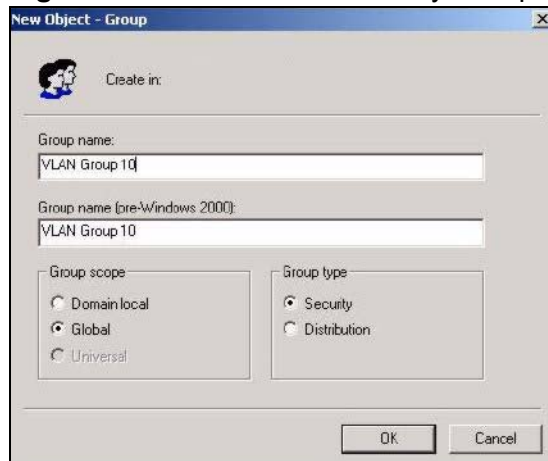
To configure a VLAN group you must first define the VLAN Groups on the Active Directory server and assign the user accounts to each VLAN Group.

1 Using the Active Directory Users and Computers administrative tool, create the VLAN Groups that will be used for each VLAN ID. One VLAN Group must be created for each VLAN defined on the NWA. The VLAN Groups must be created as Global/Security groups.

- 1a Type a name for the **VLAN Group** that describes the VLAN Group's function.
- 1b Select the **Global** Group scope parameter check box.
- 1c Select the **Security** Group type parameter check box.

1d Click **OK**.

**Figure 150** New Global Security Group

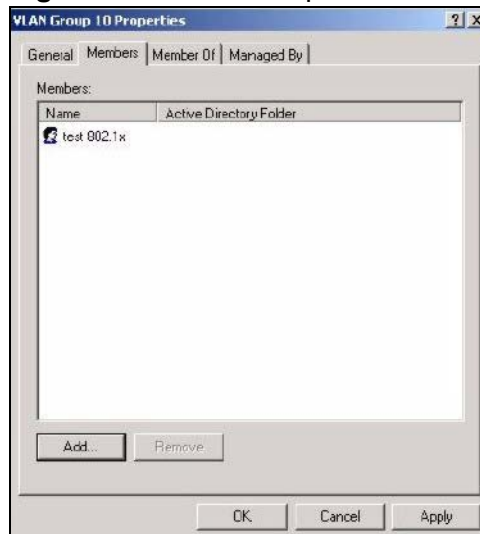


2 In **VLAN Group ID Properties**, click the **Members** tab.

- The IAS uses group memberships to determine which user accounts belong to which VLAN groups. Click the **Add** button and configure the VLAN group details.

3 Repeat the previous step to add each VLAN group required.

**Figure 151** Add Group Members



### 20.5.3.2 Configuring Remote Access Policies

Once the VLAN Groups have been created, the IAS Remote Access Policy needs to be defined. This allows the IAS to compare the user account being authenticated against the group memberships of each VLAN Group.

1 Using the **Remote Access Policy** option on the Internet Authentication Service management interface, create a new VLAN Policy for each VLAN Group defined in the previous section. The order of the remote access policies is important. The most specific policies should be placed at the top of the policy list and the most general at the bottom. For example, if the Day-And-Time Restriction policy is still present, it should be moved to the bottom or deleted to allow the VLAN Group policies to take precedence.

- 1a 1. Right click **Remote Access Policy** and select **New Remote Access Policy**.
- 1b Enter a **Policy friendly name** that describes the policy. Each Remote Access Policy will be matched to one VLAN Group. An example may be, **Allow - VLAN 10 Policy**.
- 1c Click **Next**.

**Figure 152** New Remote Access Policy for VLAN Group

**Add Remote Access Policy**

Policy Name  
Specify a friendly name for the policy.

A Remote Access Policy is a set of actions which can be applied to a group of users meeting certain conditions.

Analogous to rules you can apply to incoming mail in an e-mail application, you can specify a set of conditions that must be matched for the Remote Access Policy to apply. You can then specify actions to be taken when the conditions are met.

Policy friendly name:  
Allow - VLAN 10 Policy

< Back    Next >    Cancel

- 2 The **Conditions** window displays. Select **Add** to add a condition for this policy to act on.
- 3 In the **Select Attribute** screen, click **Windows-Groups** and the **Add** button.

**Figure 153** Specifying Windows-Group Condition

**Add Remote Access Policy**

Conditions:  
Determine the conditions to match

Specify the conditions to match

Conditions:

Add...    Remove

**Select Attribute**

Select the type of attribute to add, and then click the Add button

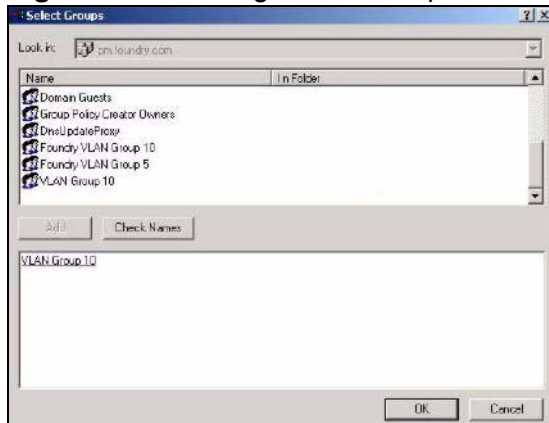
Attribute types:

Name	Description
Called-Station-Id	Phone number dialed by user
Calling-Station-Id	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client. (RAS only)
Client-IP-Address	IP address of RADIUS client. (RAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS. (RAS only)
Day-And-Time-Restrict...	Time periods and days of week during which user is allowed access
Framed-Protocol	The protocol to be used
NAS-Identifier	String identifying the NAS originating the request
NAS-IP-Address	IP address of the NAS originating the request (RAS only)
NAS-Port-Type	Type of physical port used by the NAS originating the request
Service-Type	Type of service user has requested
Tunnel-Type	Tunneling protocols to be used
<b>Windows-Groups</b>	Windows groups that user belongs to

Add...    Cancel

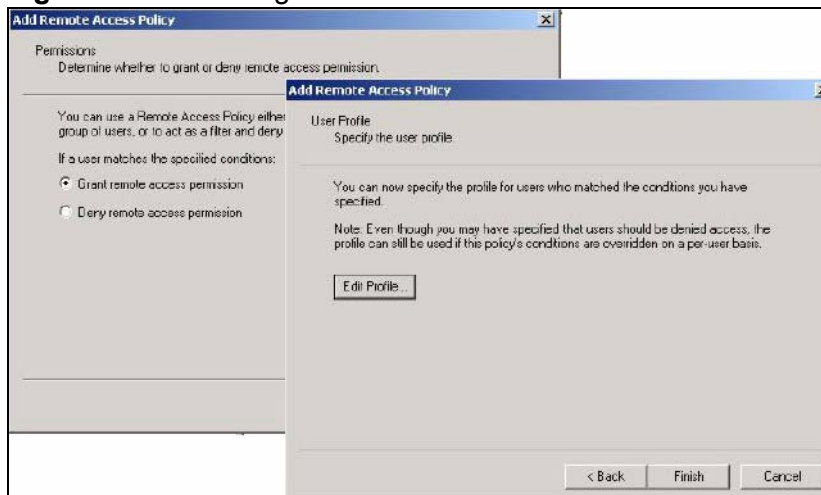
- 4 The **Select Groups** window displays. Select a remote access policy and click the **Add** button. The policy is added to the field below. Only one VLAN Group should be associated with each policy.
- 5 Click **OK** and **Next** in the next few screens to accept the group value.

**Figure 154** Adding VLAN Group



- 6 When the **Permissions** options screen displays, select **Grant remote access permission**.
  - 6a Click **Next** to grant access based on group membership.
  - 6b Click the **Edit Profile** button.

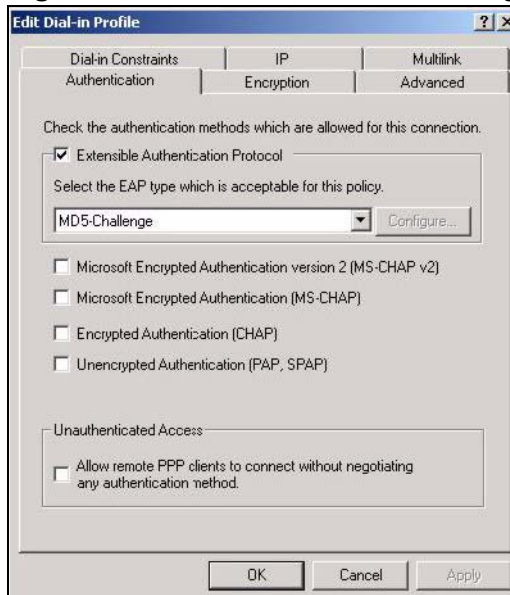
**Figure 155** Granting Permissions and User Profile Screens



- 7 The **Edit Dial-in Profile** screen displays. Click the **Authentication** tab and select the **Extensible Authentication Protocol** check box.
  - 7a Select an EAP type depending on your authentication needs from the drop-down list box.

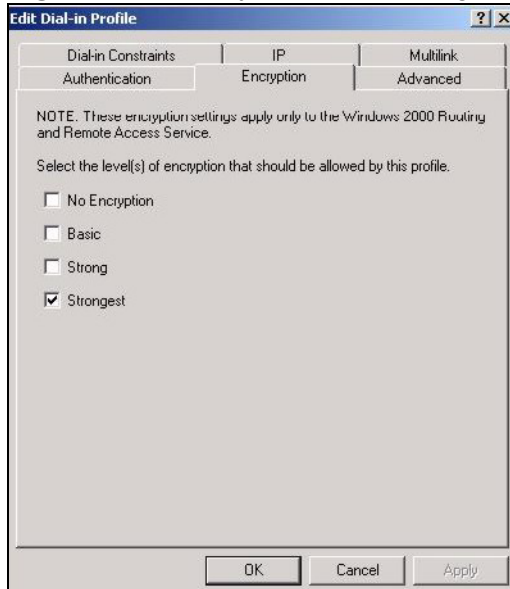
- 7b Clear the check boxes for all other authentication types listed below the drop-down list box.

**Figure 156** Authentication Tab Settings



- 8 Click the **Encryption** tab. Select the **Strongest** encryption option. This step is not required for EAP-MD5, but is performed as a safeguard.

**Figure 157** Encryption Tab Settings

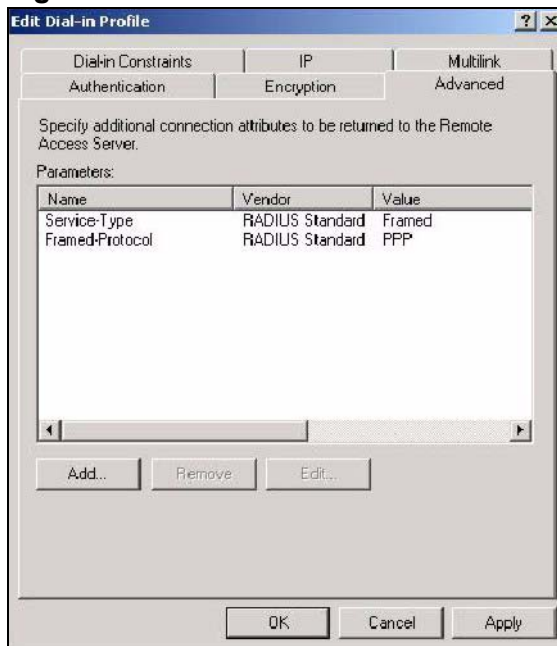


- 9 Click the **IP** tab and select the **Client may request an IP address** check box for DHCP support.
- 10 Click the **Advanced** tab. The current default parameters returned to the NWA should be **Service-Type** and **Framed-Protocol**.



- Click the **Add** button to add an additional three RADIUS VLAN attributes required for 802.1X Dynamic VLAN Assignment.

**Figure 158** Connection Attributes Screen



- 11 The RADIUS Attribute screen displays. From the list, three RADIUS attributes will be added:

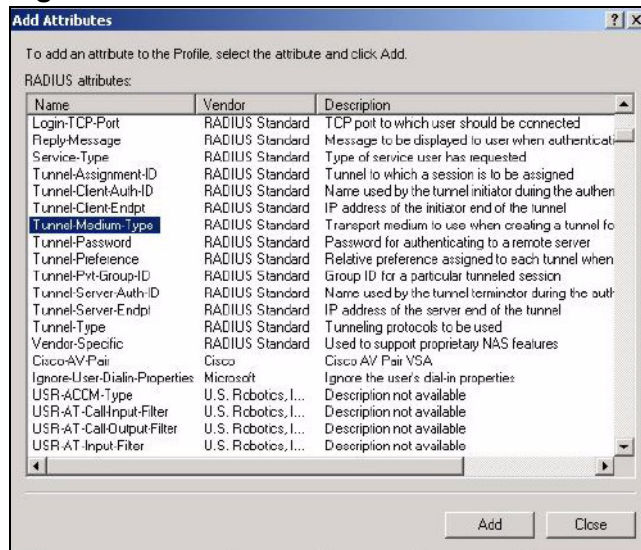
- Tunnel-Medium-Type
- Tunnel-Pvt-Group-ID
- Tunnel-Type

11a Click the **Add** button

11b Select **Tunnel-Medium-Type**

11c Click the **Add** button.

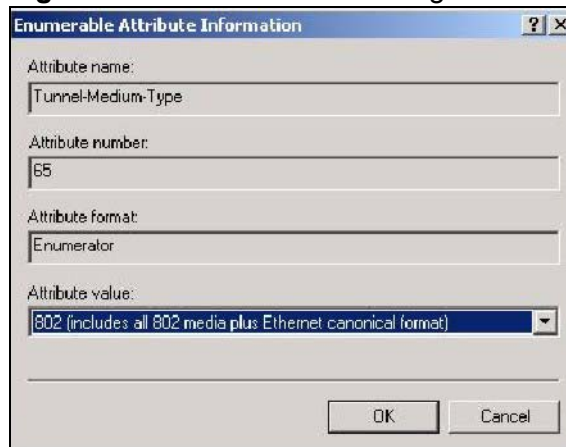
**Figure 159** RADIUS Attribute Screen



12 The **Enumerable Attribute Information** screen displays. Select the **802** value from the **Attribute value** drop-down list box.

- Click **OK**.

**Figure 160** 802 Attribute Setting for Tunnel-Medium-Type



13 Return to the **RADIUS Attribute Screen** shown as [Figure 159 on page 250](#).

13a Select **Tunnel-Pvt-Group-ID**.

13b Click **Add**.

14 The **Attribute Information** screen displays.

14a In the **Enter the attribute value in:** field select **String** and type a number in the range 1 to 4094 or a **Name** for this policy. This **Name** should match a name in the VLAN mapping table on the NWA. Wireless stations belonging to

the VLAN Group specified in this policy will be given a VLAN **ID** specified in the NWA VLAN table.

**14b** Click **OK**.

**Figure 161** VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID

The screenshot shows a dialog box titled "Attribute Information" with the following fields and options:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: DotelString
- Enter the attribute value in:  String  Hexadecimal
- Value field: 10
- Buttons: OK, Cancel

**15** Return to the **RADIUS Attribute Screen** shown as [Figure 159 on page 250](#).

**15a** Select **Tunnel-Type**.

**15b** Click **Add**.

**16** The **Enumerable Attribute Information** screen displays.

**16a** Select **Virtual LANs (VLAN)** from the attribute value drop-down list box.

**16b** Click **OK**.

**Figure 162** VLAN Attribute Setting for Tunnel-Type

The screenshot shows a dialog box titled "Enumerable Attribute Information" with the following fields and options:

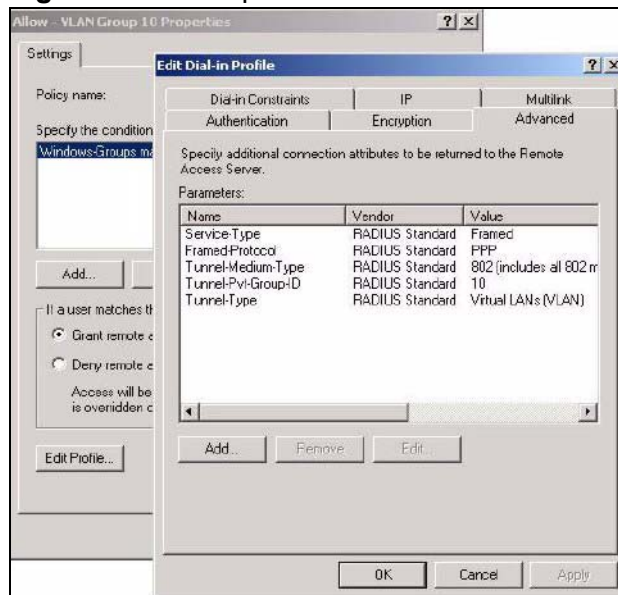
- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute value: Virtual LANs (VLAN) (selected in a drop-down menu)
- Buttons: OK, Cancel

**17** Return to the **RADIUS Attribute Screen** shown as [Figure 159 on page 250](#).

**17a** Click the **Close** button.

**17b** The completed **Advanced** tab configuration should resemble the following screen.

**Figure 163** Completed Advanced Tab

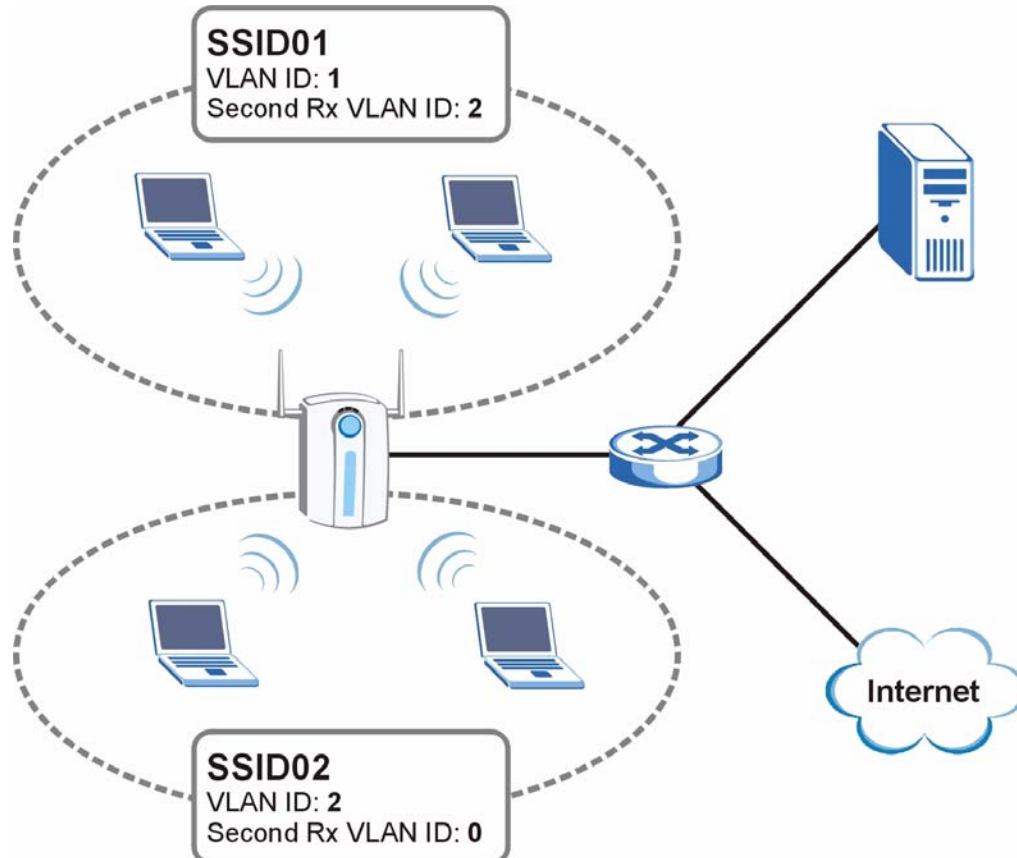


**Note:** Repeat the Configuring Remote Access Policies procedure for each VLAN Group defined in the Active Directory. Remember to place the most general Remote Access Policies at the bottom of the list and the most specific at the top of the list.

## 20.5.4 Second Rx VLAN ID Example

In this example, the NWA is configured to tag packets from **SSID01** with VLAN ID 1 and tag packets from **SSID02** with VLAN ID 2. **VLAN 1** and **VLAN 2** have access to a server, **S**, and the Internet, as shown in the following figure.

**Figure 164** Second Rx VLAN ID Example



Packets sent from the server **S** back to the switch are tagged with a VLAN ID (incoming VLAN ID). These incoming VLAN packets are forwarded to the NWA. The NWA compares the VLAN ID in the packet header with each SSID's configured VLAN ID and second Rx VLAN ID settings.

In this example, **SSID01**'s second Rx VLAN ID is set to **2**. All incoming packets tagged with VLAN ID **2** are forwarded to **SSID02**, and also to **SSID01**. However, **SSID02** has no second Rx VLAN ID configured, and the NWA forwards only packets tagged with VLAN ID **2** to it.

### 20.5.4.1 Second Rx VLAN Setup Example

The following steps show you how to setup a second Rx VLAN ID on the NWA.

- 1 Log into the Web Configurator.

- 2 Click **VLAN > Wireless VLAN**.
- 3 If VLAN is not already enabled, click **Enable Virtual LAN** and set up the **Management VLAN ID** (see [Section 20.5.2 on page 240](#)).

Note: If no devices are in the management VLAN, then no one will be able to access the NWA and you will have to restore the default configuration file.

- 4 Select the SSID profile you want to configure (**SSID03** in this example), and enter the **VLAN ID** number (between 1 and 4094).
- 5 Enter a **Second Rx VLAN ID**. The following screen shows **SSID03** tagged with a **VLAN ID** of **3** and a **Second Rx VLAN ID** of **4**.

**Figure 165** Configuring SSID: Second Rx VLAN ID Example

WIRELESS VLAN
RADIUS VLAN

**VIRTUAL LAN Setup**

Enable VIRTUAL LAN

**Wireless VIRTUAL LAN Setup**

Management VLAN ID  (1 ~ 4094)

**VLAN Mapping Table**

Index	Name	SSID	VLAN ID	Second Rx VLAN ID
1	VoIP_SSID	ZyXEL01	<input type="text" value="1"/>	<input type="text" value="0"/>
2	Guest_SSID	ZyXEL02	<input type="text" value="2"/>	<input type="text" value="0"/>
3	SSID03	ZyXEL03	<input type="text" value="3"/>	<input type="text" value="4"/>
4	SSID04	ZyXEL04	<input type="text" value="4"/>	<input type="text" value="0"/>
5	SSID05	ZyXEL05	<input type="text" value="5"/>	<input type="text" value="0"/>
6	SSID06	ZyXEL06	<input type="text" value="6"/>	<input type="text" value="0"/>
7	SSID07	ZyXEL07	<input type="text" value="7"/>	<input type="text" value="0"/>
8	SSID08	ZyXEL08	<input type="text" value="8"/>	<input type="text" value="0"/>
9	SSID09	ZyXEL09	<input type="text" value="9"/>	<input type="text" value="0"/>
10	SSID10	ZyXEL10	<input type="text" value="10"/>	<input type="text" value="0"/>
11	SSID11	ZyXEL11	<input type="text" value="11"/>	<input type="text" value="0"/>
12	SSID12	ZyXEL12	<input type="text" value="12"/>	<input type="text" value="0"/>
13	SSID13	ZyXEL13	<input type="text" value="13"/>	<input type="text" value="0"/>
14	SSID14	ZyXEL14	<input type="text" value="14"/>	<input type="text" value="0"/>
15	SSID15	ZyXEL15	<input type="text" value="15"/>	<input type="text" value="0"/>
16	SSID16	ZyXEL16	<input type="text" value="16"/>	<input type="text" value="0"/>

- 6 Click **Apply** to save these settings. Outgoing packets from clients in **SSID03** are tagged with a **VLAN ID** of **3**, and incoming packets with a **VLAN ID** of **3** or **4** are forwarded to **SSID03**.

# Load Balancing

## 21.1 Overview

Wireless load balancing is the process whereby you limit the number of connections allowed on an wireless access point or you limit the amount of wireless traffic transmitted and received on it. Because there is a hard upper limit on the AP's wireless bandwidth, this can be a crucial function in areas crowded with wireless users. Rather than let every user connect and subsequently dilute the available bandwidth to the point where each connecting device receives a meager trickle, the load balanced AP instead limits the incoming connections as a means to maintain bandwidth integrity.

### 21.1.1 What You Need to Know About Load Balancing

There are two kinds of load balancing available on the NWA:

**Load balancing by station number** limits the number of devices allowed to connect to your AP. If you know exactly how many stations you want to let connect, choose this option.

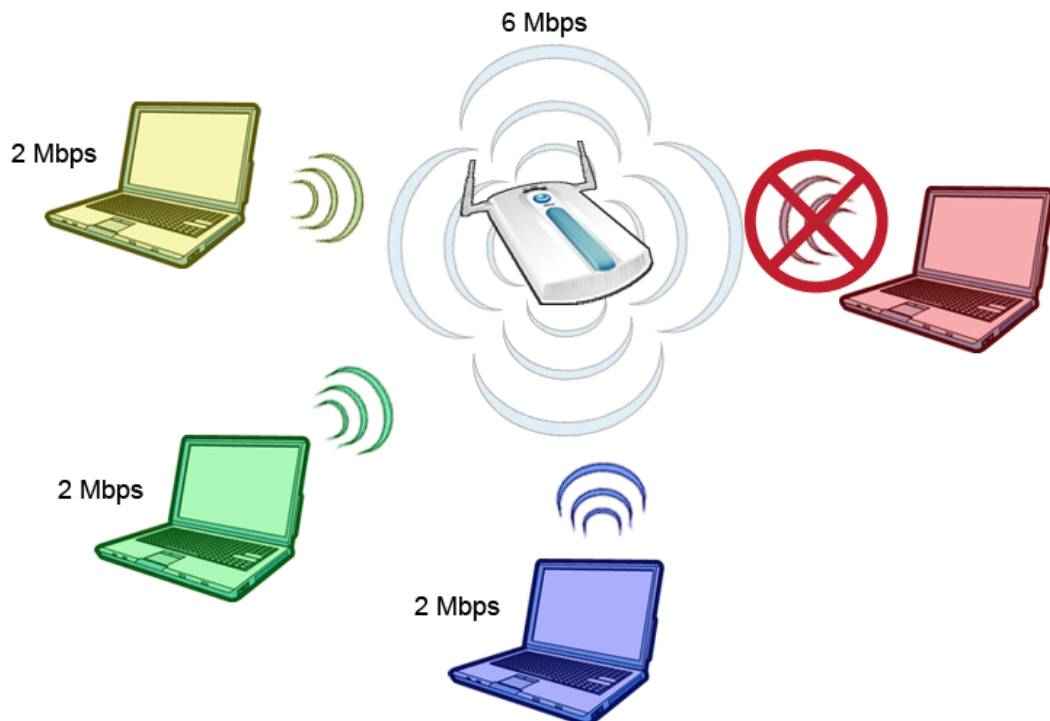
For example, if your company's graphic design team has their own NWA and they have 10 computers, you can load balance for 10. Later, if someone from the sales department visits the graphic design team's offices for a meeting and he tries to access the network, he won't be able to because his laptop is device number 11, which is one more than 10 and thus exceeds the load balance. If one of the graphic design team's computers disconnects from the network, then the sales computer can join.

**Load balancing by traffic level** limits the number of connections to the NWA based on maximum bandwidth available. If you are uncertain as to the exact number of wireless connections you will have then choose this option. By setting a maximum bandwidth cap, you allow any number of devices to connect as long as their total bandwidth usage does not exceed the bandwidth cap associated with this setting. Once the cap is hit, any new connections are rejected or delayed provided that there are other APs in range that have the same settings as the NWA (such as SSID, security mode, radio mode, and so on).

Imagine a coffee shop in a crowded business district that offers free wireless connectivity to its customers. The coffee shop owner can't possibly know how many connections his NWA will have at any given moment. As such, he decides to put a limit the bandwidth that is available to his customers but not on the actual number of connections he allows. This means anyone can connect to his wireless network as long as the NWA has the bandwidth to spare. If too many people connect and the NWA hits its bandwidth cap then all new connections must basically wait for their turn or get shunted to the nearest identical AP.

The following figure depicts an NWA with a hard bandwidth limit of 6 Megabits per second (Mbps). Bandwidth up to 6 Mbps is considered "balanced". More than that and it becomes "overloaded"; the AP must then work harder to serve each client.

**Figure 166** Load Balancing by Traffic Level Example



The yellow [Y], green [G] and blue [B] laptops are each using approximately 2 Mbps. Altogether, they consume the AP's entire "balanced" bandwidth allotment. When the red [R] laptop tries to make a connection, the AP (which does not want to overload itself) denies it if an identical AP is in range that can take on the burden of the new connection.

Note: If no other APs with matching settings are in range of the NWA, then it will still accept the connection despite becoming overloaded.



**The requirements for load balancing** are fairly straight forward and should be met in order for a group of similar NWAs to take advantage of the feature:

- They should all be within the same subnet.
- They should all have the same SSID, radio mode, and security mode.
- There should be a minimum of 2 NWAs within the same broadcast radius, or at the very least within an overlapping broadcast radius.

## 21.2 The Load Balancing Screen

Use this screen to configure the load balancing feature on the NWA. Click **Load Balancing** in the navigation menu. The following screen appears.

**Figure 167** Load Balancing

The following table describes the labels in this screen

**Table 82** Load Balancing

FIELD	DESCRIPTION
Enable Load Balancing	Select this option to turn on wireless load balancing.
Mode	Use the option to choose the specific method by which you want to enable load balancing on your NWA.
By station number	Enter the maximum number of stations the AP allows to connect to it. You can enter a value from 1-127.
By traffic level	Choose a load balancing traffic level. The traffic level you select here determines how much bandwidth the AP allows to pass through it before it becomes overloaded and starts delaying or rejecting connections. <ul style="list-style-type: none"> <li>• <b>Low</b> - Up to 6 Mbps before it becomes overloaded.</li> <li>• <b>Medium</b> - Up to 13 Mbps before it becomes overloaded.</li> <li>• <b>High</b> - Up to 20 Mbps before it becomes overloaded.</li> </ul>

**Table 82** Load Balancing

FIELD	DESCRIPTION
Dissociate station when overloaded	<p>Select this to “kick” connections to the AP when it becomes overloaded. If you leave this unchecked, then the AP simply delays the connection until it can afford the bandwidth it requires, or it shunts the connection to another AP within its broadcast radius.</p> <p>The kick priority is as follows:</p> <ul style="list-style-type: none"> <li>• <b>Idle Timeout</b> - Devices that have been idle the longest will be kicked first. If none of the connected devices are idle, then the priority shifts to <b>signal strength</b>.</li> <li>• <b>Signal Strength</b> - Devices with the weakest signal strength will be kicked first.</li> </ul> <p>Note: If you enable this function, you should ensure that there are multiple APs within the broadcast radius that can accept any rejected or kicked wireless clients; otherwise, a wireless client attempting to connect to an overloaded NWA will be kicked continuously and never be allowed to connect.</p>
Apply	Click this to save your changes to the NWA.
Reset	Click this to return this screen to its last-saved settings.

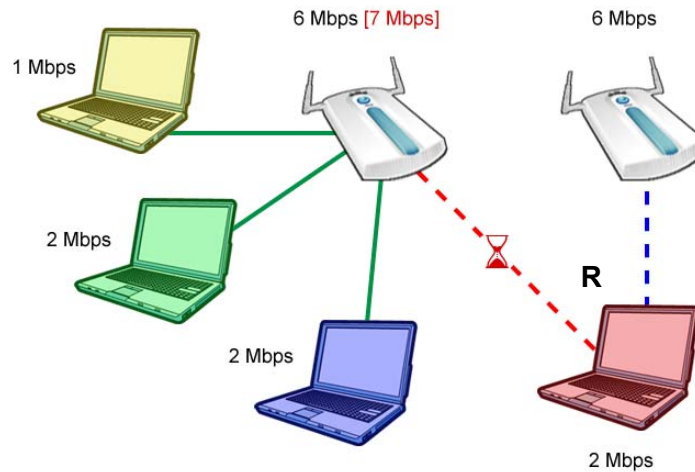
### 21.2.1 Disassociating and Delaying Connections

When your AP becomes overloaded, there are two basic responses it can take. The first one is to “delay” a client connection. This means that the AP withholds the connection until the data transfer throughput either is lowered or the client connection is picked up by another AP.

For example, here the AP has a balanced bandwidth allotment of 6 Mbps. If the red laptop [R] attempts to connect and it could potentially push the AP over its allotment, say to 7 Mbps, then the AP delays the red laptop’s connection until it

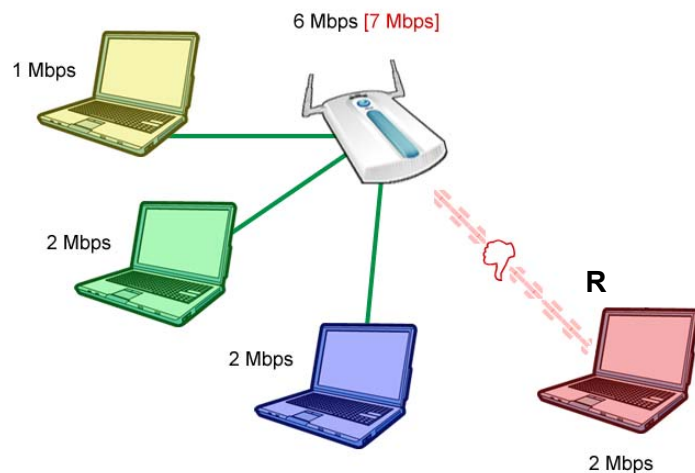
can afford the bandwidth for it or the red laptop is picked up by a different AP that has bandwidth to spare.

**Figure 168** Delaying a Connection



The second response your AP can take is to kick the connections that are pushing it over its balanced bandwidth allotment.

**Figure 169** Kicking a Connection



Connections are kicked based in either **idle timeout** or **signal strength**. The NWA first looks to see which devices have been idle the longest, then starts kicking them in order of highest idle time. If no connections are idle, the next criteria the NWA analyzes is signal strength. Devices with the weakest signal strength are kicked first.



# Dynamic Channel Selection

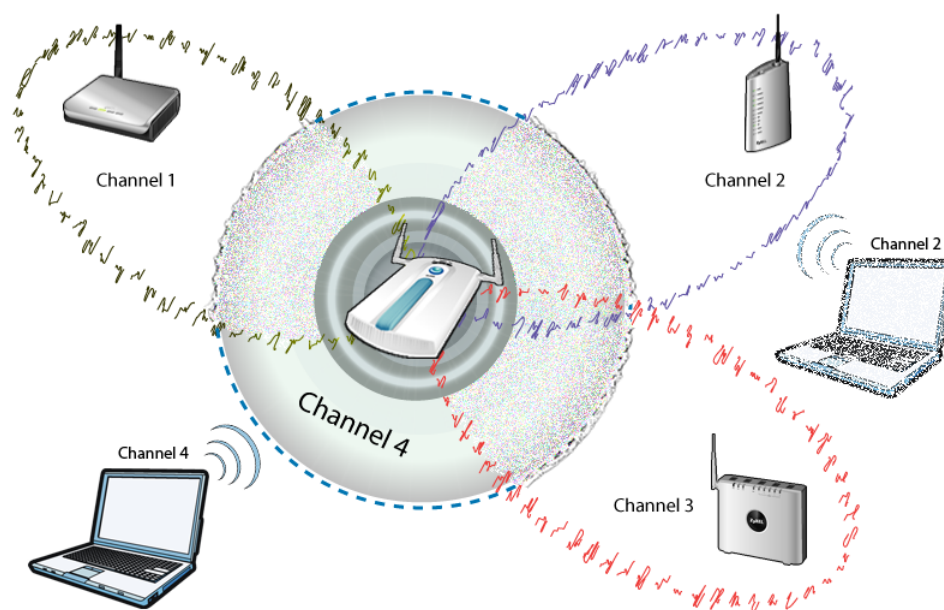
## 22.1 Overview

This chapter discusses how to configure dynamic channel selection on the NWA.

Dynamic channel selection is a feature that allows your NWA to automatically select the radio channel upon which it broadcasts by scanning the area around and determining what channels are currently being used by other devices.

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. This can make accessing the network potentially rather difficult for the stations connected to them. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using in order to give the connected stations a minimum degree of cross-channel interference.

**Figure 170** An example of cross-channel interference



In this example, if the NWA attempts to broadcast on **channels 1, 2, or 3** it is met with cross-channel interference from the other AP that shares the channel. This can result in noticeably slower data transfer rates, the dropping of the connection altogether, or even lost data packets.

However, if the NWA broadcasts on the otherwise empty **channel 4** then there will be minimal interference and a clearer connection to the network.

To alleviate this problem of having to manually change channels every time interference crops up, you would normally need to scan the area quite often to see which channels are currently unused then set your device to use one of them. But with **Dynamic Channel Selection**, the NWA does this automatically.

## 22.2 The DCS Screen

Use this screen to configure your Dynamic Channel Selection options. Click **DCS** in the navigation menu. The following screen appears.

**Figure 171** Load Balancing

The screenshot shows the 'DCS' configuration screen. At the top, there is a 'DCS' tab. Below it, the title 'Dynamic Channel Selection (DCS)' is displayed. The settings are as follows:

- Dynamic Channel Selection:** Enable (dropdown menu)
- DCS Time Interval:** 10 (input field) Minutes (label)
- DCS Sensitivity Level:** High (dropdown menu)
- DCS Client Aware:** Disable (dropdown menu) (If Enable, AP will not change channel when active client traffic on AP)
- DCS Allow Channel List (2.4G only):** 1.6, 11 (dropdown menu)
- DCS DFS Channel Aware (5G only):** Disable (dropdown menu) (If Enable, DCS will not select DFS channel for recommend channel)

At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen

**Table 83** Load Balancing

FIELD	DESCRIPTION
Dynamic Channel Selection	Select this to either <b>Enable</b> or <b>Disable</b> dynamic channel selection.
DCS Time Interval	Enter a number of minutes. This regulates how often the NWA surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the NWA will then dynamically select the next available empty channel.
DCS Sensitivity Level	Select the NWA's sensitivity level toward other channels. Options are <b>High</b> , <b>Medium</b> , and <b>Low</b> .

**Table 83** Load Balancing

FIELD	DESCRIPTION
DCS Client Aware	Select <b>Enable</b> to have the NWA wait until all connected clients have disconnected before switching channels.  If you select <b>Disable</b> then the NWA switches channels immediately regardless of any client connections. In this instance, clients that are connected to the AP when it switches channels are dropped.
DCS Allow Channel List (2.4G only)	Select the range of non-overlapping channel numbers for which you want the NWA to scan and subsequently use if available.
DCS DFS Channel Aware (5G only)	Select <b>Enable</b> to allow the NWA to broadcast on unused radar channels. If you select <b>Disable</b> to turn the feature off. See <a href="#">Section 8.4 on page 123</a> for more information on dynamic frequency.
Apply	Click this to save your changes to the NWA.
Reset	Click this to return this screen to its last-saved settings.





# Maintenance

## 23.1 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.

## 23.2 What You Can Do in the Maintenance Screens

The following is a list of the maintenance screens you can configure on the NWA.

- Use the **Status** screen ([Section 23.4 on page 266](#)) to monitor your NWA. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.
- Use the **Show Statistics** screen ([Section 23.4.1 on page 266](#)) to access read-only information such as port status, packet specific statistics and bridge link status. Also provided are "system up time" and "poll interval(s)".
- Use the **Association List** screen ([Section 23.5 on page 268](#)) to view the wireless stations that are currently associated with the NWA.
- Use the **Channel Usage** screen ([Section 23.6 on page 269](#)) 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.
- Use the **F/W Upload** screen ([Section 23.7 on page 270](#)) to upload the latest firmware for your NWA.
- Use the **Configuration** screen ([Section 23.8 on page 272](#)) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use **Restart** screen ([Section 23.9 on page 274](#)) to reboot the NWA without turning the power off.

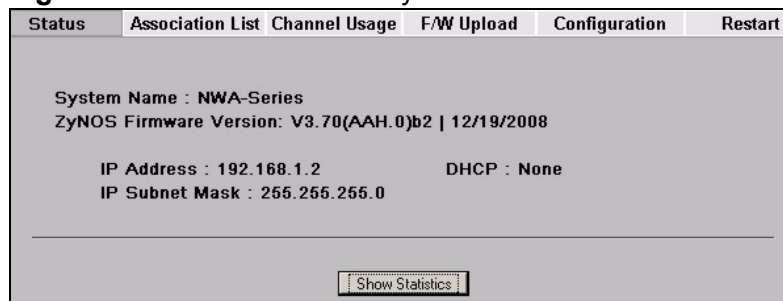
## 23.3 What You Need To Know About the Maintenance Screens

Find firmware at [www.zyxel.com](http://www.zyxel.com) in 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. See the Firmware and Configuration File Maintenance chapter for upgrading firmware using FTP/TFTP commands.

## 23.4 System Status Screen

Use this screen to get a quick summary of the status of your NWA. Click **Maintenance > System Status**. The following screen displays.

**Figure 172** Maintenance > System Status



The following table describes the labels in this screen.

**Table 84** Maintenance > System Status

LABEL	DESCRIPTION
System Name	This is the <b>System Name</b> you can configure in the <b>SYSTEM &gt; General</b> screen. It is for identification purposes
ZyNOS Firmware Version	This is the ZyNOS Firmware version and date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
IP Address	This is the Ethernet port IP address.
IP Subnet Mask	This is the Ethernet port subnet mask.
DHCP	This is the Ethernet port DHCP role - <b>Client</b> or <b>None</b> .
Show Statistics	Click <b>Show Statistics</b> to see the NWA performance statistics such as number of packets sent and number of packets received for each port.

### 23.4.1 System Statistics Screen

Use this screen to view diagnostic information about the NWA. Click **Maintenance > Show Statistics**. The following screen pops up.

Note: The Poll Interval field is configurable. The fields in this screen vary according to the current wireless mode of each WLAN adaptor.

**Figure 173** Maintenance > System Status: Show Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	12379	158304	0	64	0	0:24:47
WLAN1	54M	164442	7	0	64	0	0:00:37
WLAN2	Down	164334	0	0	0	0	00:00:00

WLAN1:						
#	Active	Remote Bridge MAC	Status	TxPkts	RxPkts	
1	No	00:00:00:00:00:00	Down	0	0	
2	No	00:00:00:00:00:00	Down	0	0	
3	No	00:00:00:00:00:00	Down	0	0	
4	No	00:00:00:00:00:00	Down	0	0	
5	No	00:00:00:00:00:00	Down	0	0	

WLAN2:						
#	Active	Remote Bridge MAC	Status	TxPkts	RxPkts	
1	No	00:00:00:00:00:00	Down	0	0	
2	No	00:00:00:00:00:00	Down	0	0	
3	No	00:00:00:00:00:00	Down	0	0	
4	No	00:00:00:00:00:00	Down	0	0	
5	No	00:00:00:00:00:00	Down	0	0	

Poll Interval(s) :  sec

The following table describes the labels in this screen.

**Table 85** Maintenance > System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet port ( <b>LAN</b> ) or wireless LAN adaptor ( <b>WLAN1</b> or <b>WLAN2</b> ).
Status	This shows the port speed and duplex setting if you are using Ethernet encapsulation for the Ethernet port. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.  This shows the transmission speed only for the wireless adaptors.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This shows the transmission speed in bytes per second on this port.
Rx B/s	This shows the reception speed in bytes per second on this port.
Up Time	This is total amount of time the line has been up.

**Table 85** Maintenance > System Status: Show Statistics

LABEL	DESCRIPTION
WLAN1	This section displays only when wireless LAN adaptor WLAN1 is in AP+Bridge or Bridge/Repeater mode.
WLAN2	This section displays only when wireless LAN adaptor WLAN2 is in AP+Bridge or Bridge/Repeater mode.
Bridge Link #	This is the index number of the bridge connection.
Active	This shows whether the bridge connection is activated or not.
Remote Bridge MAC	This is the MAC address of the peer device in bridge mode.
Status	This shows the current status of the bridge connection, which can be <b>Up</b> or <b>Down</b> .
TxPkts	This is the number of transmitted packets on the wireless bridge.
RxPkts	This is the number of received packets on the wireless bridge.
Poll Interval(s)	Enter the time interval for refreshing statistics.
Set Interval	Click this button to apply the new poll interval you entered above.
Stop	Click this button to stop refreshing statistics.

## 23.5 Association List Screen

Use this screen to know which wireless clients are associated with the NWA. Click **Maintenance > Association List**. The following screen displays.

**Figure 174** Maintenance > Association List

Status	Association List	Channel Usage	F/W Upload	Configuration	Restart
<b>WLAN1</b>					
<b>Stations</b>					
#	MAC Address	Association Time	SSID	Signal	
<b>WDS Link</b>					
#	Remote Bridge MAC	Link Time	Security	Signal	
<b>WLAN2</b>					
<b>WDS Link</b>					
#	Remote Bridge MAC	Link Time	Security	Signal	
Refresh					

The following table describes the labels in this screen.

**Table 86** Maintenance > Association List

LABEL	DESCRIPTION
Stations	
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.

**Table 86** Maintenance > Association List

LABEL	DESCRIPTION
Association Time	This field displays the time a wireless station first associated with the NWA.
SSID	This field displays the SSID to which the wireless station is associated.
Signal	This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection.
WDS Link	This section displays only when bridge mode is activated on one of the NWA's WLAN adaptors.
#	This field displays the index number of a bridge connection on the WDS.
Remote Bridge MAC	This field displays a remote bridge MAC address.
Link Time	This field displays the WDS link up-time.
Security	This field displays whether traffic on the WDS is encrypted ( <b>TKIP</b> or <b>AES</b> ) or not ( <b>None</b> ).
Signal	This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection.
Refresh	Click <b>Refresh</b> to reload the screen.

## 23.6 Channel Usage Screen

Use this screen to see what channel the wireless clients are using to associate with the NWA, as well as the signal strength and network mode. Click **Maintenance > Channel Usage**. The following figure displays.

Wait a moment while the NWA compiles the information.

**Figure 175** Maintenance > Channel Usage

Status	Association List	Channel Usage	F/W Upload	Configuration	Restart																																																												
		<table border="1"> <thead> <tr> <th>SSID</th> <th>MAC Address</th> <th>Channel</th> <th>Signal</th> <th>Network Mode</th> </tr> </thead> <tbody> <tr> <td>WLAN-7496fqz</td> <td>00:02:CF:DD:B7:8C</td> <td>1</td> <td>100 %</td> <td>Infra, WPA2-PSK-MIX</td> </tr> <tr> <td>WLAN-9471myf</td> <td>00:02:CF:DD:B7:AC</td> <td>1</td> <td>100 %</td> <td>Infra, WPA2-PSK-MIX</td> </tr> <tr> <td>6812-wifi</td> <td>00:19:CB:30:22:10</td> <td>3</td> <td>22 %</td> <td>Infra, WPA-PSK</td> </tr> <tr> <td>11795-Glenn</td> <td>00:13:49:00:00:05</td> <td>6</td> <td>82 %</td> <td>Infra, WEP</td> </tr> <tr> <td>ZyXEL_MIS</td> <td>00:19:CB:4A:85:41</td> <td>6</td> <td>46 %</td> <td>Infra, WEP</td> </tr> <tr> <td>11841</td> <td>00:00:AA:78:01:63</td> <td>7</td> <td>86 %</td> <td>Infra</td> </tr> <tr> <td>ZLD_STH</td> <td>00:17:42:08:69:25</td> <td>7</td> <td>28 %</td> <td>Infra, WPA-PSK</td> </tr> <tr> <td></td> <td>00:13:49:13:13:66</td> <td>9</td> <td>22 %</td> <td>Infra, WPA-PSK</td> </tr> <tr> <td>USG200_FieldTrial_01</td> <td>00:13:49:AF:A9:0F</td> <td>11</td> <td>62 %</td> <td>Infra</td> </tr> <tr> <td>USG200_FieldTrial_02</td> <td>06:13:49:AF:A9:0F</td> <td>11</td> <td>68 %</td> <td>Infra, WPA-PSK</td> </tr> <tr> <td>COE_6510_01</td> <td>00:11:50:20:98:DA</td> <td>11</td> <td>36 %</td> <td>Infra, WPA-PSK</td> </tr> </tbody> </table>	SSID	MAC Address	Channel	Signal	Network Mode	WLAN-7496fqz	00:02:CF:DD:B7:8C	1	100 %	Infra, WPA2-PSK-MIX	WLAN-9471myf	00:02:CF:DD:B7:AC	1	100 %	Infra, WPA2-PSK-MIX	6812-wifi	00:19:CB:30:22:10	3	22 %	Infra, WPA-PSK	11795-Glenn	00:13:49:00:00:05	6	82 %	Infra, WEP	ZyXEL_MIS	00:19:CB:4A:85:41	6	46 %	Infra, WEP	11841	00:00:AA:78:01:63	7	86 %	Infra	ZLD_STH	00:17:42:08:69:25	7	28 %	Infra, WPA-PSK		00:13:49:13:13:66	9	22 %	Infra, WPA-PSK	USG200_FieldTrial_01	00:13:49:AF:A9:0F	11	62 %	Infra	USG200_FieldTrial_02	06:13:49:AF:A9:0F	11	68 %	Infra, WPA-PSK	COE_6510_01	00:11:50:20:98:DA	11	36 %	Infra, WPA-PSK			
SSID	MAC Address	Channel	Signal	Network Mode																																																													
WLAN-7496fqz	00:02:CF:DD:B7:8C	1	100 %	Infra, WPA2-PSK-MIX																																																													
WLAN-9471myf	00:02:CF:DD:B7:AC	1	100 %	Infra, WPA2-PSK-MIX																																																													
6812-wifi	00:19:CB:30:22:10	3	22 %	Infra, WPA-PSK																																																													
11795-Glenn	00:13:49:00:00:05	6	82 %	Infra, WEP																																																													
ZyXEL_MIS	00:19:CB:4A:85:41	6	46 %	Infra, WEP																																																													
11841	00:00:AA:78:01:63	7	86 %	Infra																																																													
ZLD_STH	00:17:42:08:69:25	7	28 %	Infra, WPA-PSK																																																													
	00:13:49:13:13:66	9	22 %	Infra, WPA-PSK																																																													
USG200_FieldTrial_01	00:13:49:AF:A9:0F	11	62 %	Infra																																																													
USG200_FieldTrial_02	06:13:49:AF:A9:0F	11	68 %	Infra, WPA-PSK																																																													
COE_6510_01	00:11:50:20:98:DA	11	36 %	Infra, WPA-PSK																																																													
Refresh																																																																	

The following table describes the labels in this screen.

**Table 87** Maintenance > 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.
Signal	This field displays the strength of the AP's signal. If you must choose a channel that's currently in use, choose one with low signal strength for minimum interference.
Network Mode	"Network mode" in this screen refers to your wireless LAN infrastructure (refer to the Wireless LAN chapter) and security setup.
Refresh	Click <b>Refresh</b> to reload the screen.

## 23.7 F/W Upload Screen

Use this screen to upload firmware to your NWA.

Click **MAINTENANCE > F/W Upload**. The following screen displays. .

**Figure 176** Maintenance > F/W Upload

The screenshot shows the 'F/W Upload' screen. At the top, there is a navigation bar with tabs: Status, Association List, Channel Usage, F/W Upload (highlighted), Configuration, and Restart. Below the navigation bar, the main content area is titled 'Firmware Upload'. It contains the following text: 'To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure'. Below this text, there is a 'File Path:' label followed by a text input field and a 'Browse...' button. At the bottom right of the screen, there is an 'Upload' button.

The following table describes the labels in this screen.

**Table 88** Maintenance > F/W Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> 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 177** Firmware Upload In Process



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.

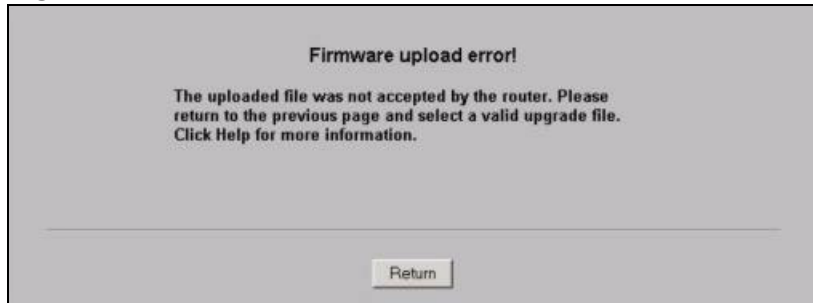
**Figure 178** Network Temporarily Disconnected



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.

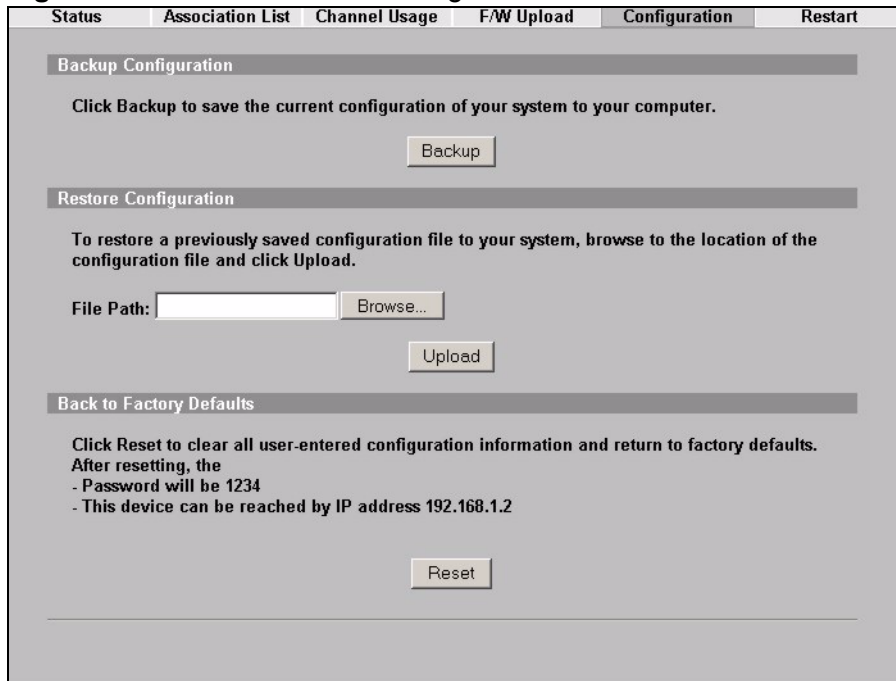
**Figure 179** Firmware Upload Error



## 23.8 Configuration Screen

Use this screen backup or upload your NWA's configuration file. You can also reset the configuration of your device in this screen. Click **Maintenance > Configuration**. The following figure displays.

**Figure 180** Maintenance > Configuration



### 23.8.1 Backup Configuration

Backup configuration allows you to back up (save) the NWA's current configuration to a file on your computer. Once your NWA is configured and functioning properly,



it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the NWA's current configuration to your computer.

## 23.8.2 Restore Configuration

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

**Table 89** Restore Configuration

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

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

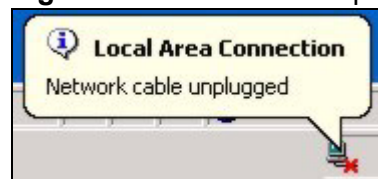
After you see a "restore configuration successful" screen, you must then wait one minute before logging into the NWA again.

**Figure 181** Configuration Upload Successful



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.

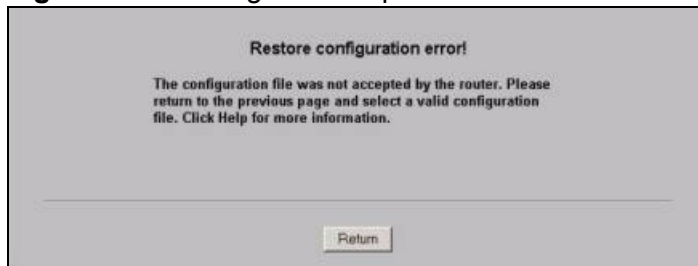
**Figure 182** Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default 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.

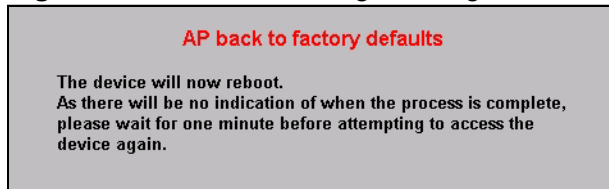
**Figure 183** Configuration Upload Error



### 23.8.3 Back to Factory Defaults

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

**Figure 184** Reset Warning Message



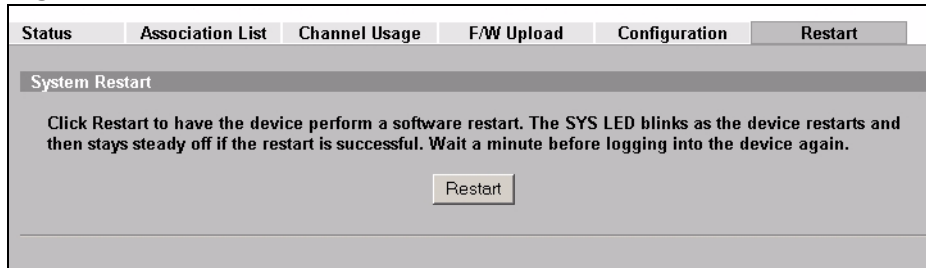
You can also press the **RESET** button to reset your NWA to its factory default settings. Refer to [Section 2.2 on page 37](#) for more information.

## 23.9 Restart Screen

Use this screen to restart the NWA without turning it off and on.

Click **Maintenance > Restart**. The following screen displays. Click **Restart** to have the NWA reboot. This does not affect the NWA's configuration.

**Figure 185** Restart Screen





---

# **PART III**

# **Troubleshooting and Specifications**

---

Troubleshooting (279)

Product Specifications (285)



# Troubleshooting

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

- [Power and Hardware Connections](#)
- [NWA Access and Login](#)
- [Internet Access](#)
- [Wireless Router/AP Troubleshooting](#)

## 24.1 Power and Hardware Connections

---

The NWA does not turn on.

---

- 1 Make sure you are using the PoE power injector included with the NWA.
- 2 Make sure the PoE power injector 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 PoE power injector to the NWA.
- 4 If the problem continues, contact the vendor.

## 24.2 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 static IP address and have forgotten it, you have to reset the device to its factory defaults. Contact your vendor.

If you set the NWA to get a dynamically assigned IP address from a DHCP server, check your DHCP server for the IP address assigned to the ZyXEL Device.

---

### 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. Contact your vendor.

---

### 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 14.4 on page 176](#)), 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. See the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Section 24.1 on page 279](#).
- 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. Contact your vendor.
- 6 If the problem continues, contact the network administrator or vendor, or try 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.

---

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 SMT or 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. Contact your vendor.

---

I cannot access the SMT.

---

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

---

I cannot use FTP to upload / download the configuration file. / 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.

## 24.3 Internet Access

---

I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the NWA is connected to a broadband modem or router that provides Internet access. See the Quick Start Guide.
- 2 Make sure your Internet account is activated and you entered your ISP account information correctly in the broadband modem or router to which the NWA is connected. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 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. See the Quick Start Guide.
- 2 Reboot the NWA.
- 3 If the problem continues, contact your ISP.

---

The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. 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 Make sure the NWA is installed in a position free of obstructions.
- 3 Check the signal strength. If the signal is weak, try moving your computer closer to the NWA (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).
- 4 Reboot the NWA.
- 5 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions.

**Advanced Suggestions**

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

## 24.4 Wireless Router/AP Troubleshooting

---

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

---

- 1 Make sure the wireless LAN is enabled on the NWA
- 2 Make sure the wireless adapter on the wireless client is working properly.
- 3 Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the NWA.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NWA.
- 5 Check that both the NWA and your wireless client are using the same wireless and wireless security settings.
- 6 Make sure you allow the NWA to be remotely accessed through the WLAN interface. Check your remote management settings.



## Product Specifications

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

**Table 90** NWA-3550 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	256 (W) x 246 (D) x 82 (H) mm
Weight	2000 g
Power	PoE draw: 48V 20W at least
Ethernet Port	Auto-negotiating: 10 Mbps or 100 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 Specifications	Two external antenna connectors (N-Type).
Output Power	IEEE 802.11b/g: 17 dBm IEEE 802.11a: 14 dBm
Operating Environment	Temperature: -30° C ~ 55° C Humidity: 20% ~ 95% RH
Storage Environment	Temperature: -40° C ~ 60° C Humidity: 5% ~ 95% RH

**Table 91** NWA-3500 Hardware Specifications

Dimensions	212.5 (W) x 138.5 (D) x 52mm (H) mm
Power Specification	12 V DC, 1 A
Reset button	Returns all settings to their factory defaults.
Ethernet Port	Auto-negotiating: 10 Mbps or 100 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.
Console Port	One MIL-C-5015 style RS-232 console port

Antenna Specifications	SMA antenna connectors, equipped by default with 2dBi omni antenna, 60°  When facing the front of the NWA, the antenna on the right is used by wireless LAN adaptor WLAN1, and the antenna on the left is used by wireless LAN adaptor WLAN2.
Output Power	IEEE 802.11b/g: 17 dBm  IEEE 802.11a: 14 dBm
Operating Environment	Temperature: 0° C ~ 5° C  Humidity: 20% ~ 95% RH
Storage Environment	Temperature: -40° C ~ 60° C  Humidity: 5% ~ 95% RH
Distance between the centers of wall-mounting holes on the device's back.	80 mm
Screw size for wall-mounting	6mm ~ 8mm (0.24" ~ 0.31") head width.

**Table 92** 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 802.11a, IEEE 802.11b, IEEE 802.11g
Wireless security	WEP, WPA(2), WPA(2)-PSK, IEEE 802.1x
Layer 2 isolation	Prevents wireless clients associated with your NWA from communicating with other wireless clients, APs, computers or routers in a network.
Multiple BSSID (MBSSID)	MBSSID mode allows the NWA to operate up to 8 different wireless networks (BSSs) simultaneously, each with independently-configurable wireless and security settings.
Rogue AP detection	Rogue AP detection detects and logs unknown access points (APs) operating in the area.
Internal RADIUS server	PEAP, 32-entry Trusted AP list, 128-entry Trusted Users list.
VLAN	802.1Q VLAN tagging.
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	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) 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.

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 manager station to manage and monitor the NWA through the network. The NWA supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The NWA-3165 also supports version 3 (SNMPv3).
DFS	DFS (Dynamic Frequency Selection) allows a wider choice of 802.11a wireless channels.
CAPWAP (Control and Provisioning of Wireless Access Points)	The NWA can be managed via CAPWAP, which allows multiple APs to be configured and managed by a single AP controller.

**Table 93** Other Specifications

Approvals	<p>Radio</p> <ul style="list-style-type: none"> <li>• USA: FCC Part 15C 15.247 FCC Part 15E 15.407 FCC OET65</li> <li>• EU: ETSI EN 300 328 V1.7.1 ETSI EN 301 893 V1.2.3</li> <li>• Taiwan: DGT LP0002</li> <li>• Canada: Industry Canada RSS-210</li> <li>• Australia: AS/NZS 4268</li> </ul> <p>EMC/ EMI</p> <ul style="list-style-type: none"> <li>• USA: FCC Part 15 Subpart B</li> <li>• EU: EN 301 489-17 V1.2.1: 08-2002 EN 55022:2006</li> <li>• Canada: ICES-003</li> <li>• Australia: AS/NZS CISPR22</li> </ul> <p>EMC/ EMS</p> <ul style="list-style-type: none"> <li>• EU: EN 301 489-1 V1.5.1: 11-2004</li> </ul> <p>Environmental</p> <ul style="list-style-type: none"> <li>• 2002/95/EC (RoHS) Restriction of Hazardous Substances Directive</li> <li>• 2002/96/EC (WEEE) Waste Electrical and Electronic Equipment Directive</li> <li>• European Parliament and Council Directive 94/62/EC of 20 December 1994 on packaging and packaging waste</li> </ul>
-----------	--



## Compatible ZyXEL Antennas

At the time of writing, you can use the following antennas in your NWA.

**Table 94** NWA Compatible Antennas

MODEL	EXT-108	EXR-109	EXT-114	EXT-118	ANT2206		ANT3108	ANT3218
FEATURES								
Frequency Band (MHz)	2400 ~ 2500	2400 ~ 2500	2400 ~ 2500	2400 ~ 2500	2400 ~ 2500	4900 ~ 5875	5150 ~ 5875	4900 ~ 5875
Gain (dBi)	8	9	14	18	6	8	8	18
Max. VSWR	2.0:1	1.5:1	1.5:1	1.5:1	2.0:1	2.0:1	2.0:1	2.0:1
HPBW/Horizontal	360°	65°	30°	15°	65°	50°	360°	18°
HPBW/Vertical	15°	60°	30°	5°	75°	50°	20°	18°
Impedance (Ohm)	50	50	50	50	50	50	50	50
Connector	N type female	N type female	N type female	N type female	RP SMA plug		N type female	N type female
Survival Wind Speed (km/hr)	216	216	216	180			216	216
Temperature	-40°C ~ 80°C	-40°C ~ 80°C	-40°C ~ 80°C	-40°C ~ 80°C	-10°C ~ 55°C		-40°C ~ 80°C	-40°C ~ 80°C
Humidity	95% at 25°C	95% at 55°C	95% at 55°C	95% at 55°C	95% at 55°C		95% at 55°C	95% at 55°C
Weight	337 gw	107 gw	407 g	1.6 kg	110 g		206 g	640 gw

## Compatible ZyXEL Antenna Cables

The following table shows you the cables you can use in the NWA to extend your connection to antennas at the time of writing.

**Table 95** NWA Compatible Antenna Cables

MODEL NAME	PART NUMBER (P/N)	LENGTH
LMR-400	91-005-075001G	N-PLUG to N-PLUG, for 6M
	91-005-075002G	N-PLUG to N-PLUG, for 9M
	91-005-075003G	N-PLUG to N-PLUG, for 12M
	91-005-075004G	N-PLUG to N-PLUG, for 1M
LMR-200	91-005-074001G	N-PLUG to RP-SMA PLUG, for 3M
	91-005-074002G	N-PLUG to RP-SMA PLUG, for 6M
	91-005-074003G	N-PLUG to RP-SMA PLUG, for 9M
EXT-300	91-005-082001B	Jumper Cable, Surge Arrstor

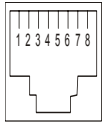
## Power over Ethernet (PoE) Specifications

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

**Table 96** Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

**Table 97** 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 -

---

# PART IV

# Appendices and Index

---

Setting Up Your Computer's IP Address  
(293)

Wireless LANs (319)

Pop-up Windows, JavaScripts and Java  
Permissions (335)

Importing Certificates (343)

IP Addresses and Subnetting (369)

Text File Based Auto Configuration (379)

Legal Information (387)

Index (391)



# Setting Up Your Computer's IP Address

Note: Your specific ZyXEL device 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:

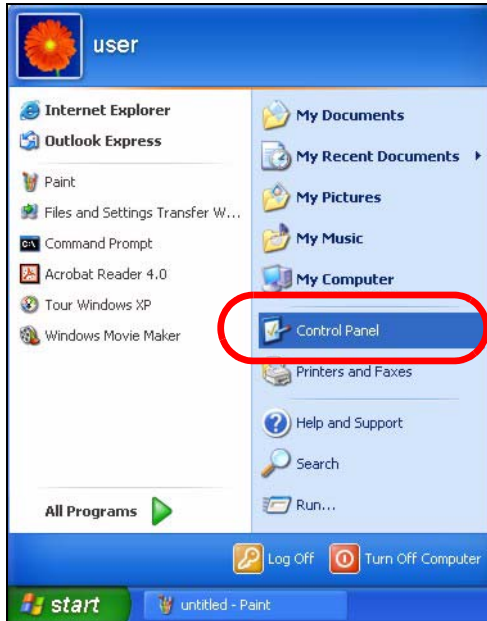
- [Windows XP/NT/2000](#) on [page 293](#)
- [Windows Vista](#) on [page 297](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 301](#)
- [Mac OS X: 10.5](#) on [page 304](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 308](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 313](#)

## Windows XP/NT/2000

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

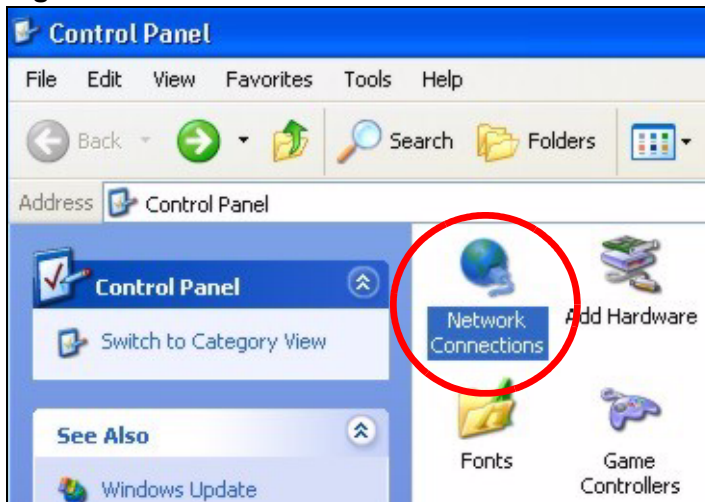
- 1 Click **Start > Control Panel**.

**Figure 186** Windows XP: Start Menu



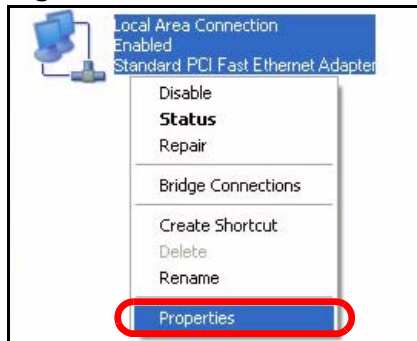
- 2 In the **Control Panel**, click the **Network Connections** icon.

**Figure 187** Windows XP: Control Panel



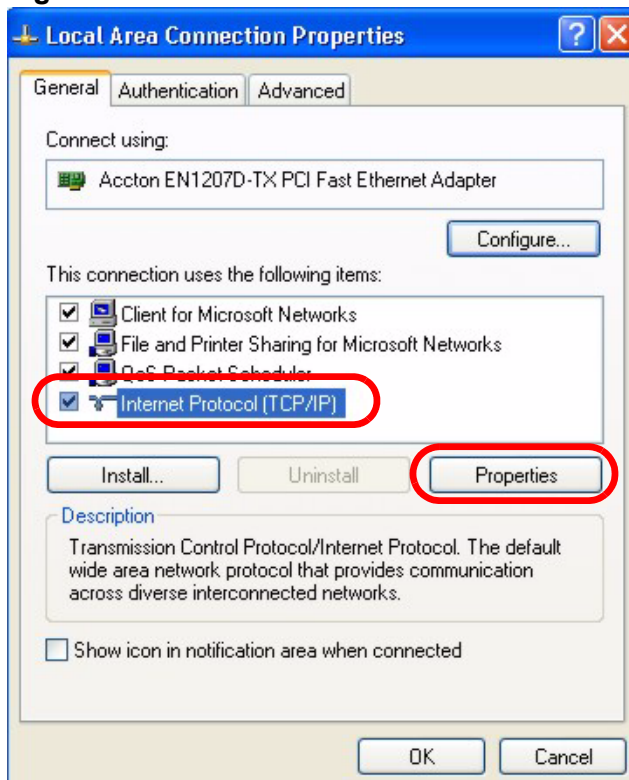
- 3 Right-click **Local Area Connection** and then select **Properties**.

**Figure 188** Windows XP: Control Panel > Network Connections > Properties



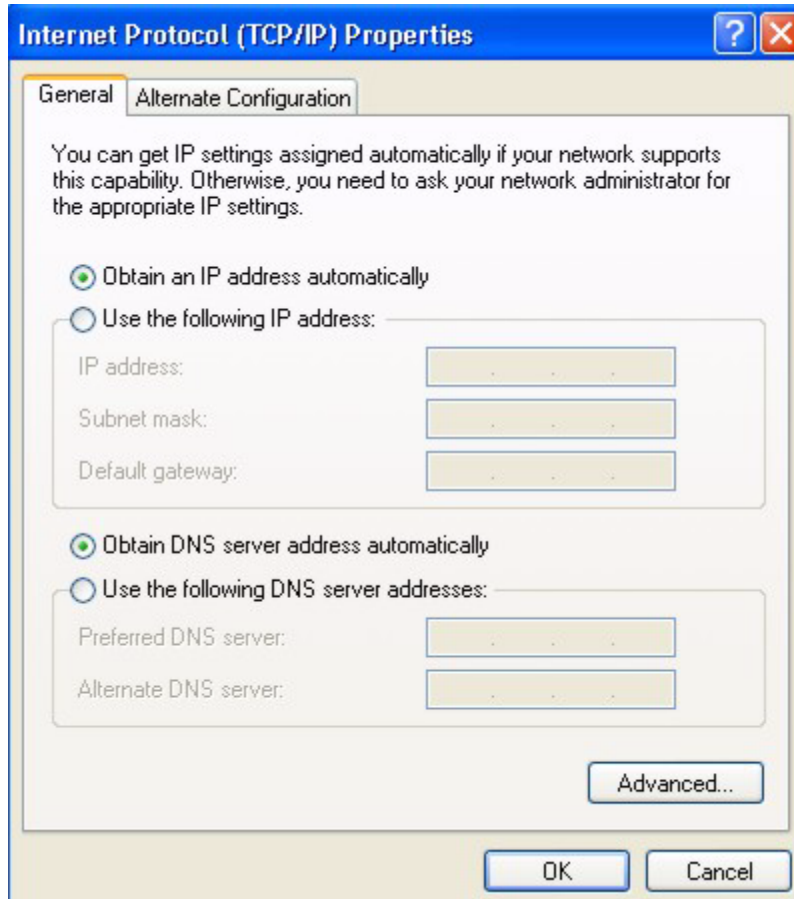
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

**Figure 189** Windows XP: Local Area Connection Properties



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

**Figure 190** Windows XP: Internet Protocol (TCP/IP) Properties



- 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.

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.

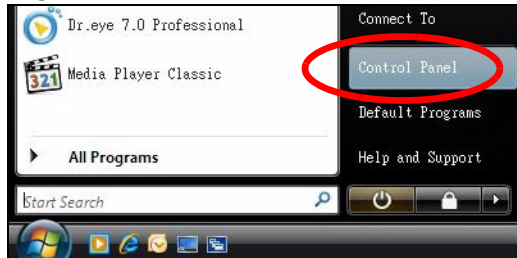


## Windows Vista

This section shows screens from Windows Vista Professional.

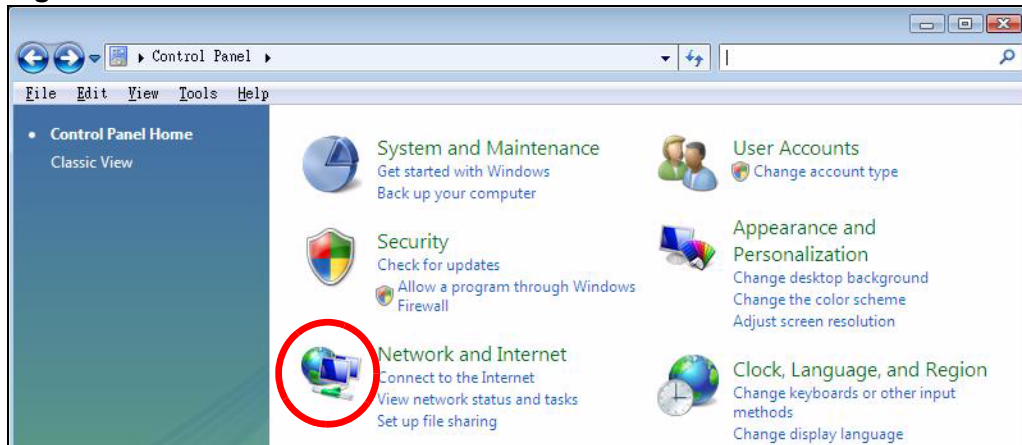
- 1 Click **Start > Control Panel**.

**Figure 191** Windows Vista: Start Menu



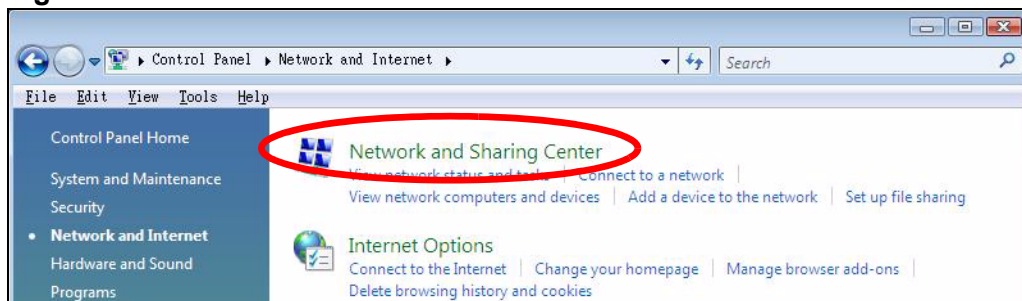
- 2 In the **Control Panel**, click the **Network and Internet** icon.

**Figure 192** Windows Vista: Control Panel



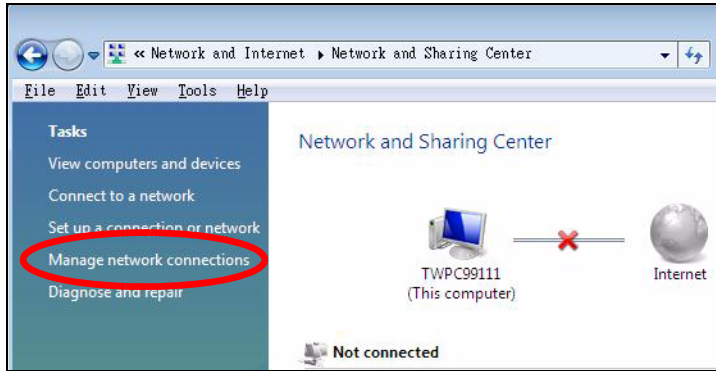
- 3 Click the **Network and Sharing Center** icon.

**Figure 193** Windows Vista: Network And Internet



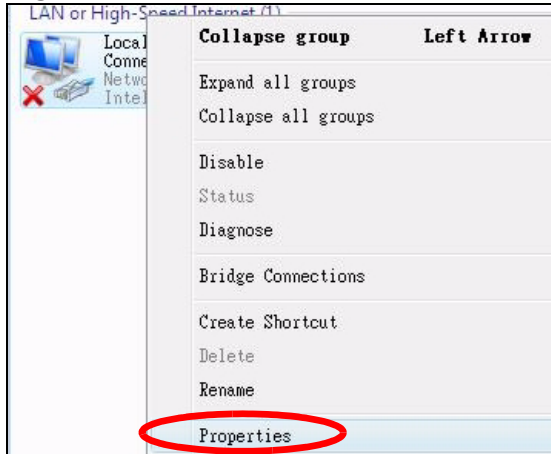
- 4 Click **Manage network connections**.

**Figure 194** Windows Vista: Network and Sharing Center



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

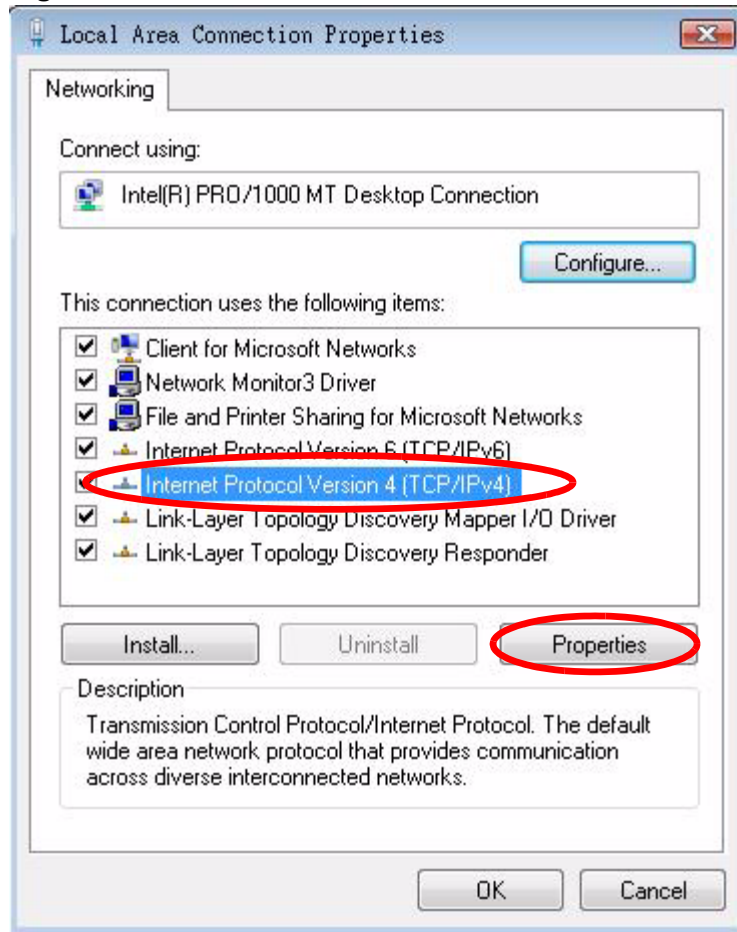
**Figure 195** Windows Vista: Network and Sharing Center



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

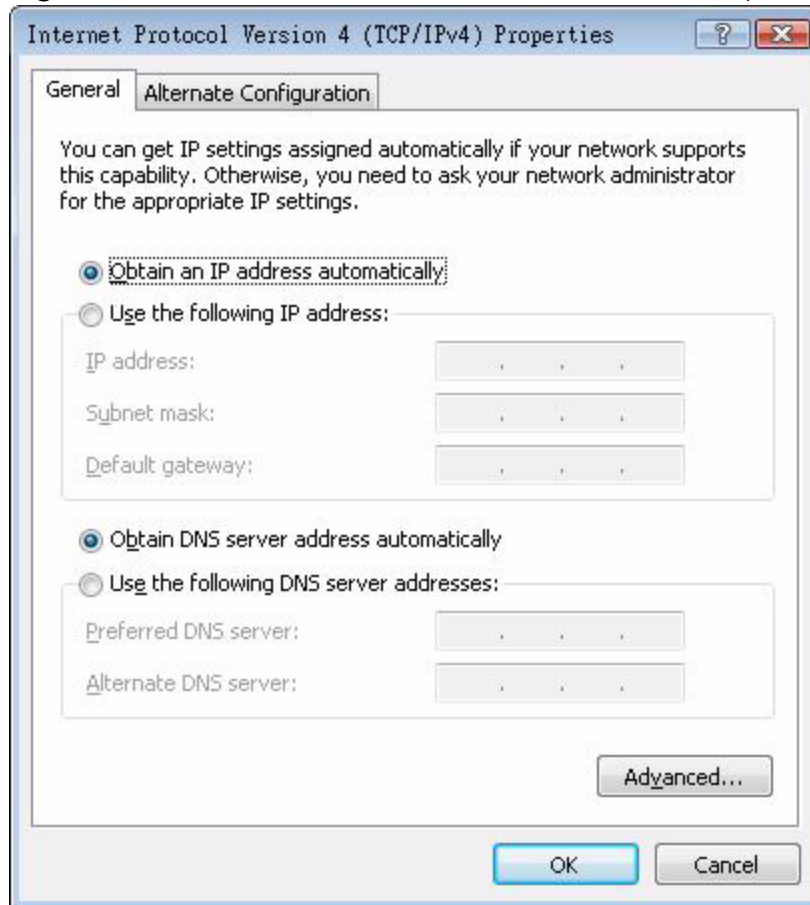
- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

**Figure 196** Windows Vista: Local Area Connection Properties



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

**Figure 197** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



- 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.

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].

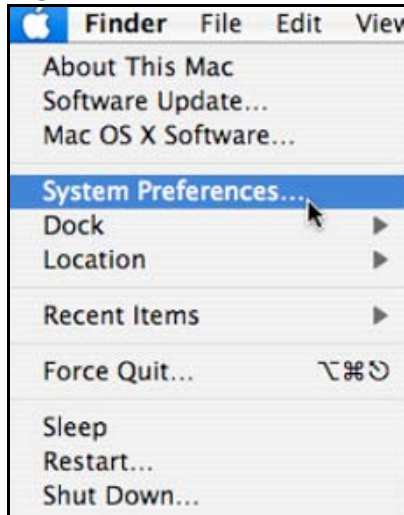
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

## 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**.

**Figure 198** Mac OS X 10.4: Apple Menu



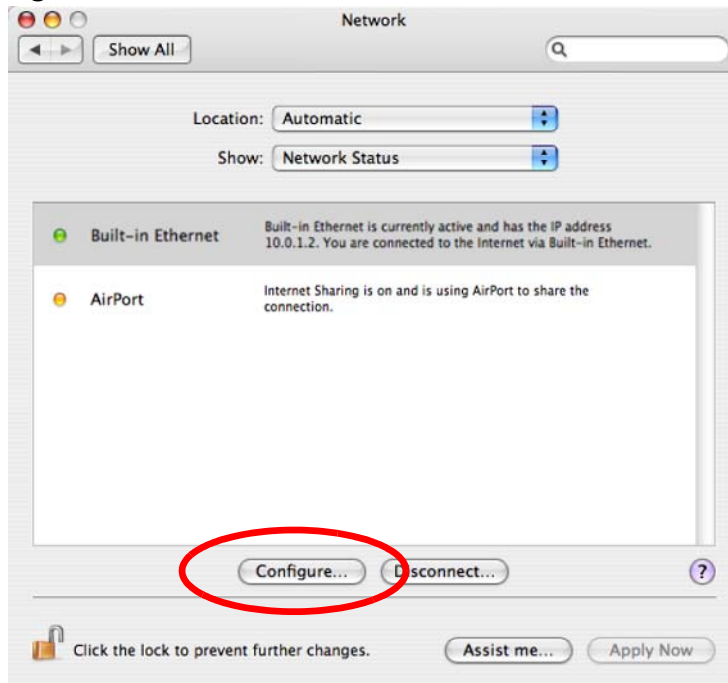
- 2 In the **System Preferences** window, click the **Network** icon.

**Figure 199** Mac OS X 10.4: System Preferences



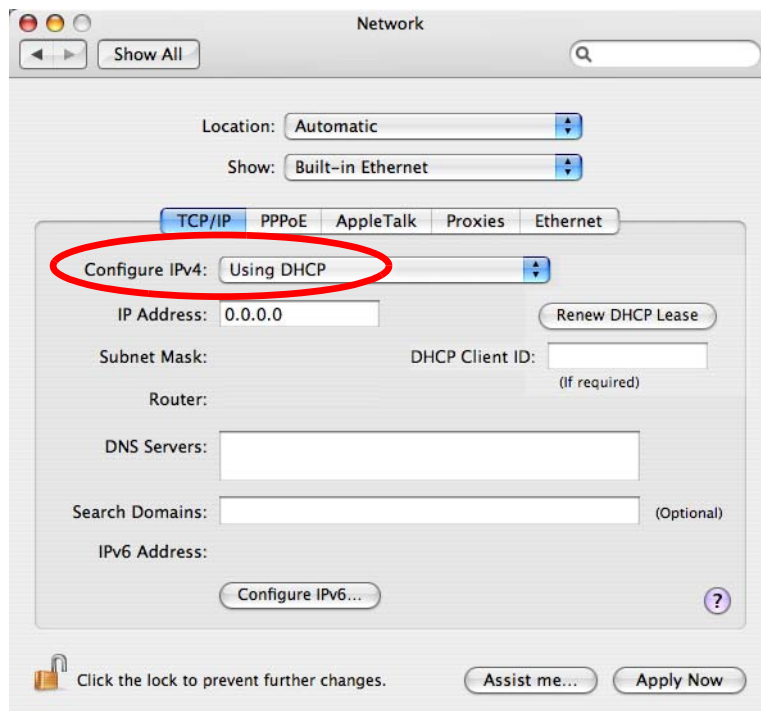
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

**Figure 200** Mac OS X 10.4: Network Preferences



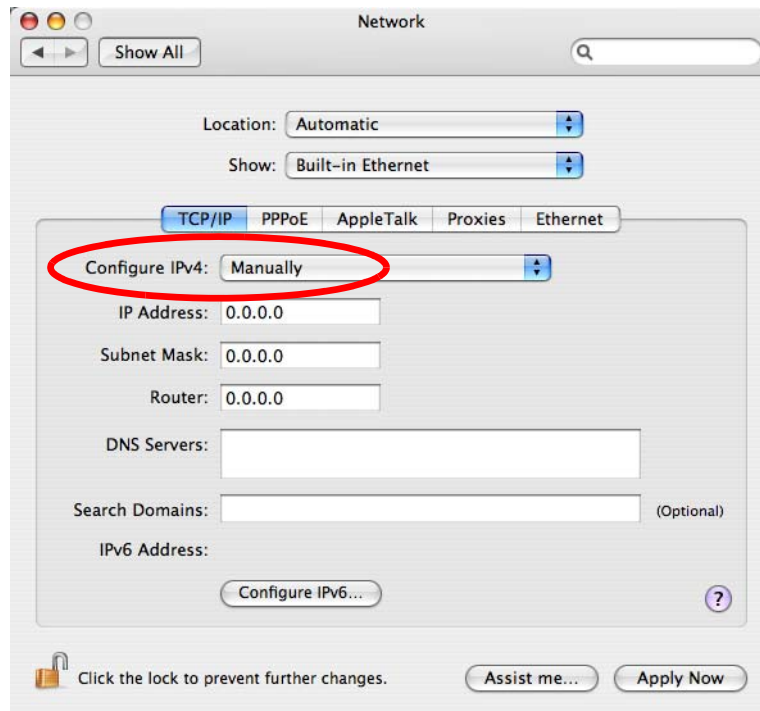
- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

**Figure 201** Mac OS X 10.4: Network Preferences > TCP/IP Tab.



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

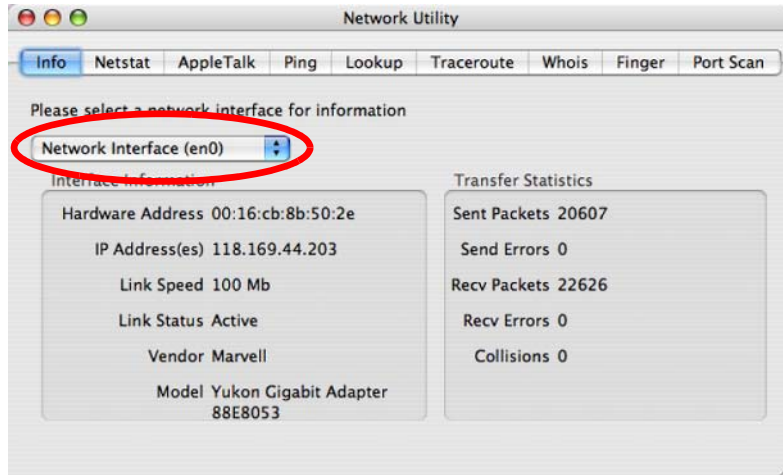
**Figure 202** Mac OS X 10.4: Network Preferences > Ethernet



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 203** Mac OS X 10.4: Network Utility

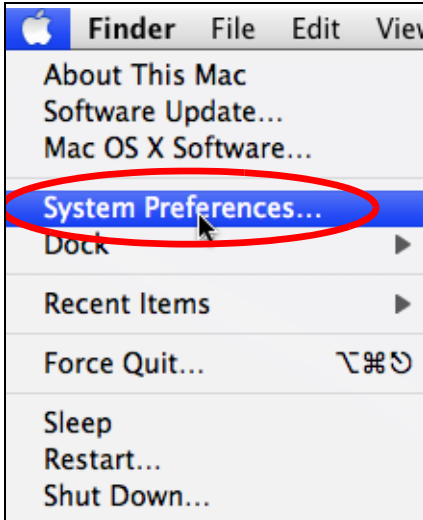


## Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

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

**Figure 204** Mac OS X 10.5: Apple Menu





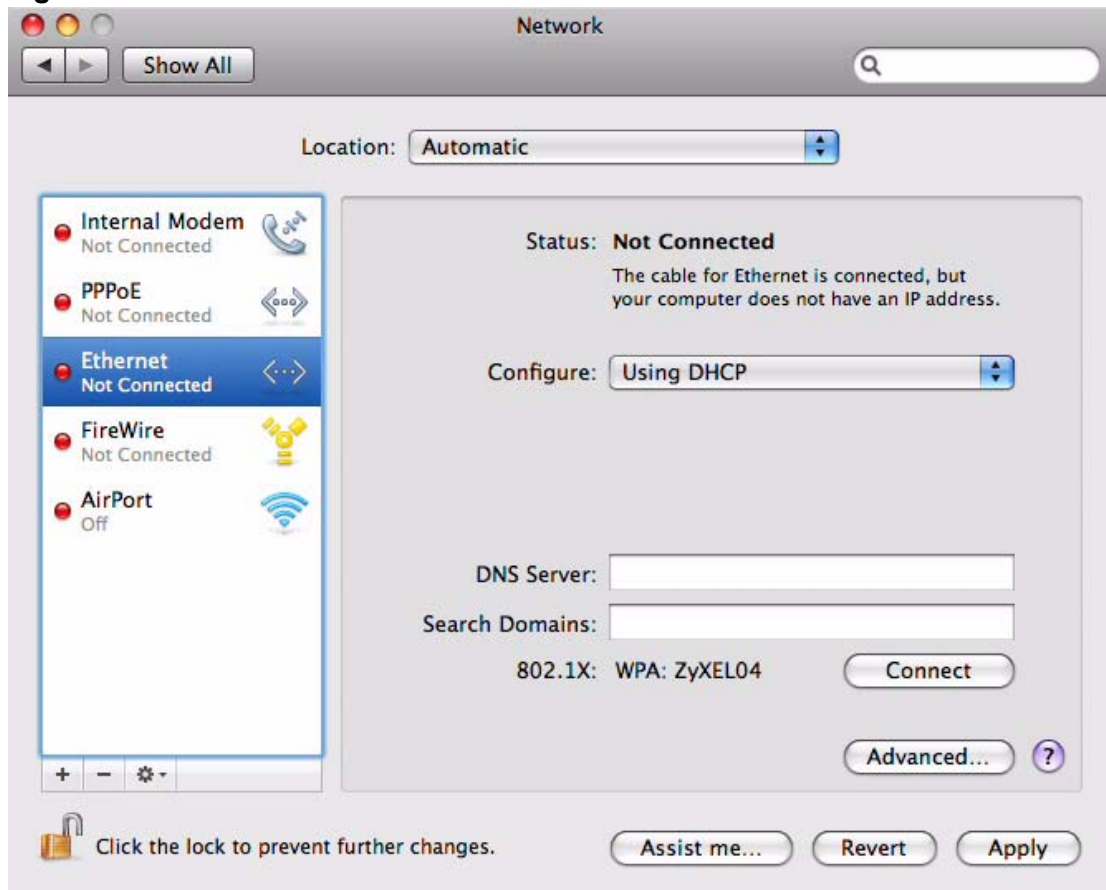
- 2 In **System Preferences**, click the **Network** icon.

**Figure 205** Mac OS X 10.5: Systems Preferences



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

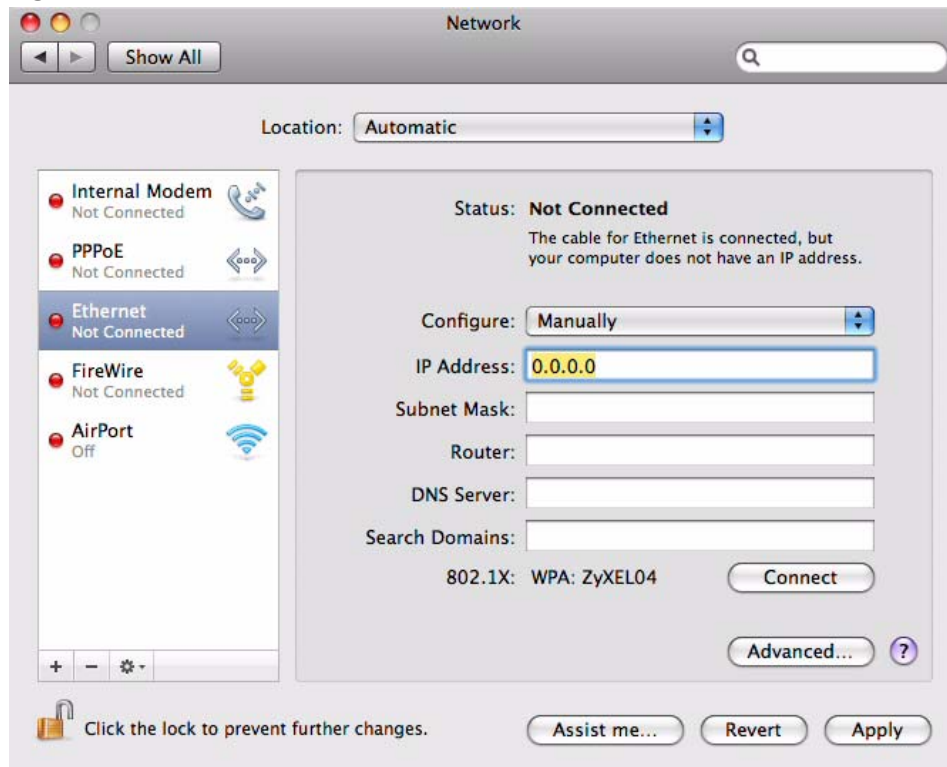
**Figure 206** Mac OS X 10.5: Network Preferences > Ethernet



- 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.

**Figure 207** Mac OS X 10.5: Network Preferences > Ethernet

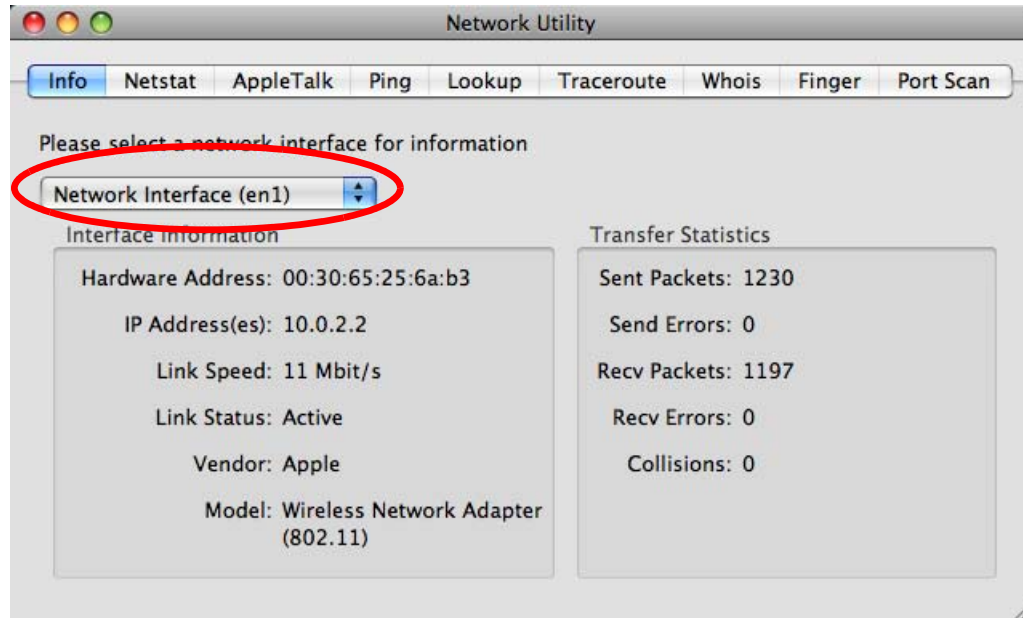


- 6 Click **Apply** and close the window.

## 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 208** Mac OS X 10.5: Network Utility



## Linux: Ubuntu 8 (GNOME)

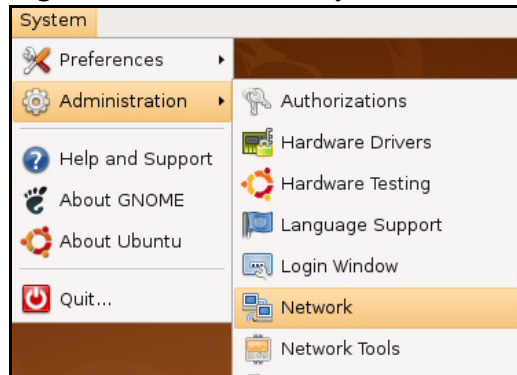
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

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

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

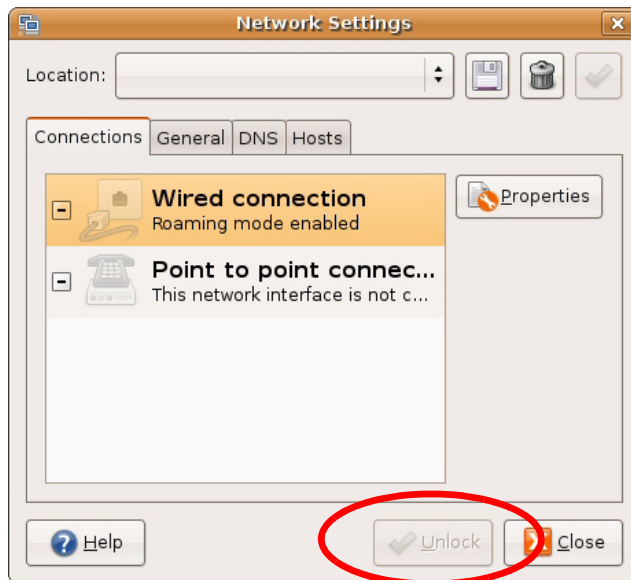
- 1 Click **System > Administration > Network**.

**Figure 209** Ubuntu 8: System > Administration Menu



- 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.

**Figure 210** Ubuntu 8: Network Settings > Connections



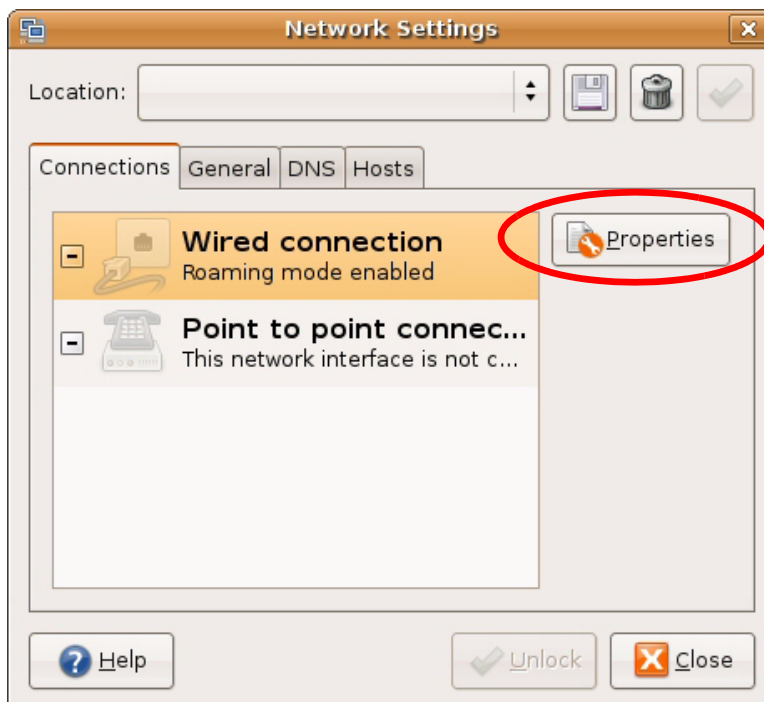
- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

**Figure 211** Ubuntu 8: Administrator Account Authentication



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

**Figure 212** Ubuntu 8: Network Settings > Connections



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

**Figure 213** Ubuntu 8: Network Settings > Properties



- 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.

**Figure 214** Ubuntu 8: Network Settings > DNS



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

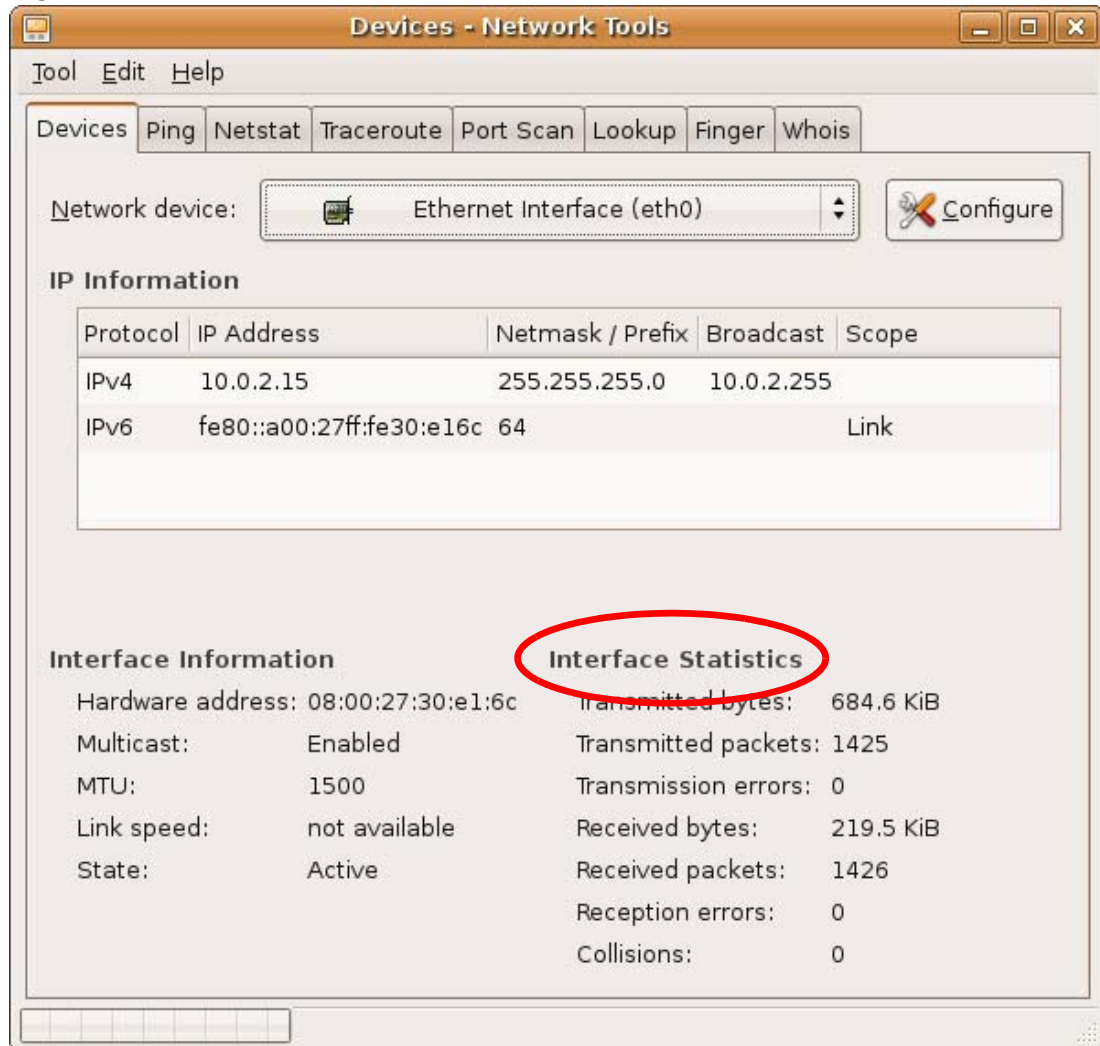
## Verifying Settings

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 215** Ubuntu 8: Network Tools



## Linux: openSUSE 10.3 (KDE)

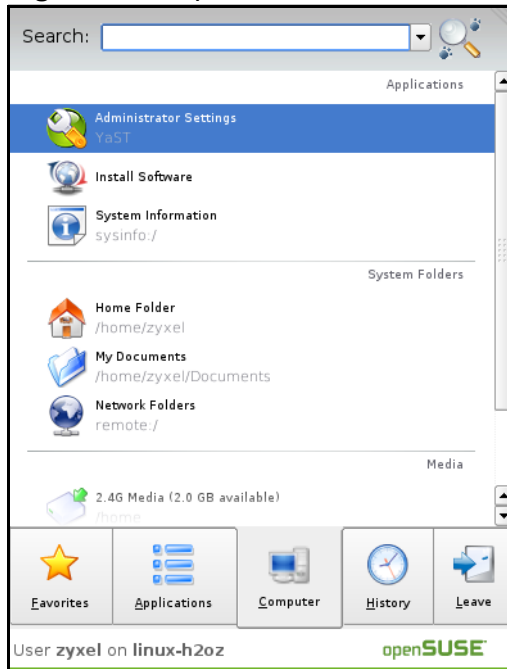
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

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

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

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

**Figure 216** openSUSE 10.3: K Menu > Computer Menu



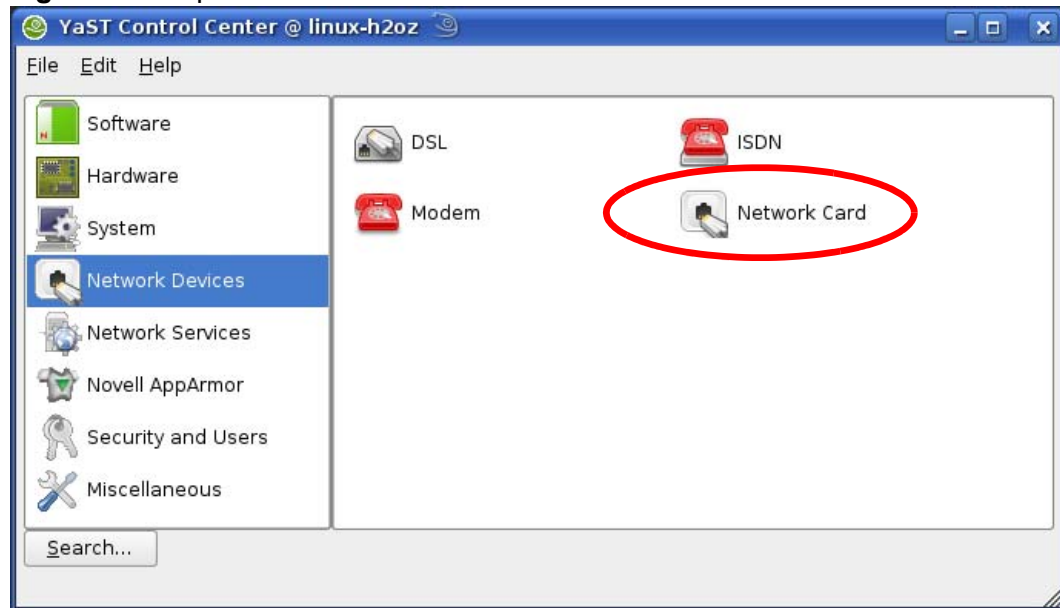
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

**Figure 217** openSUSE 10.3: K Menu > Computer Menu



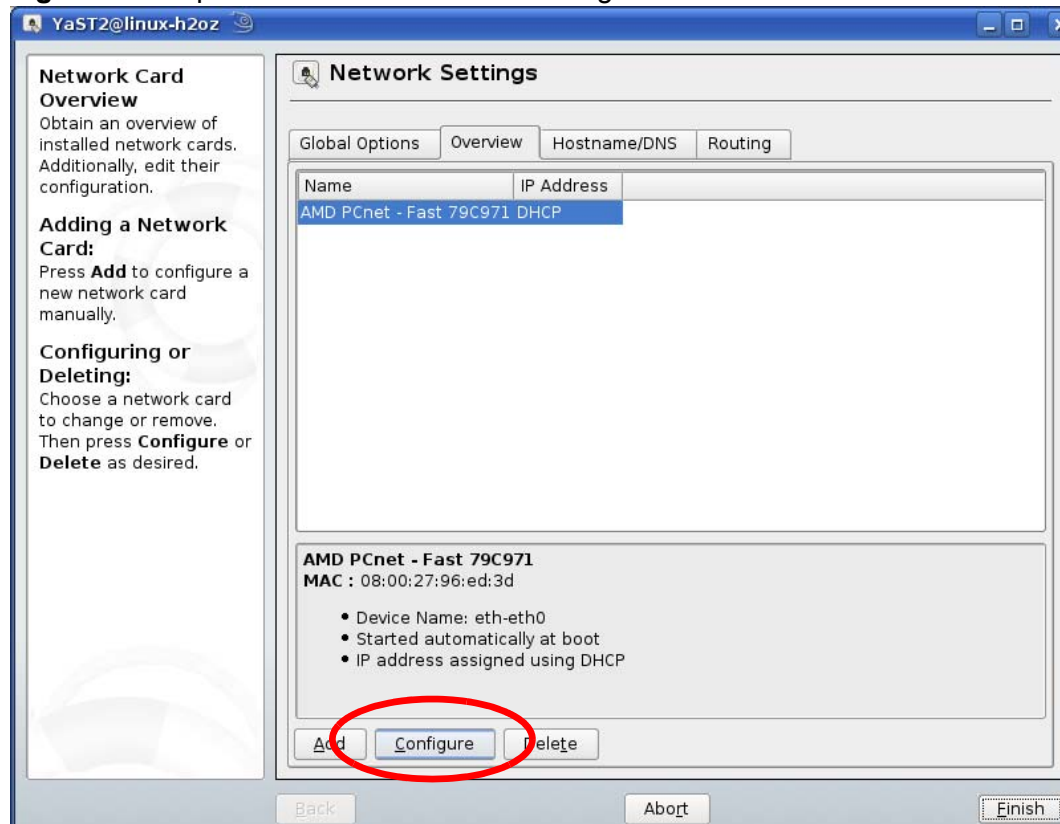
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

**Figure 218** openSUSE 10.3: YaST Control Center



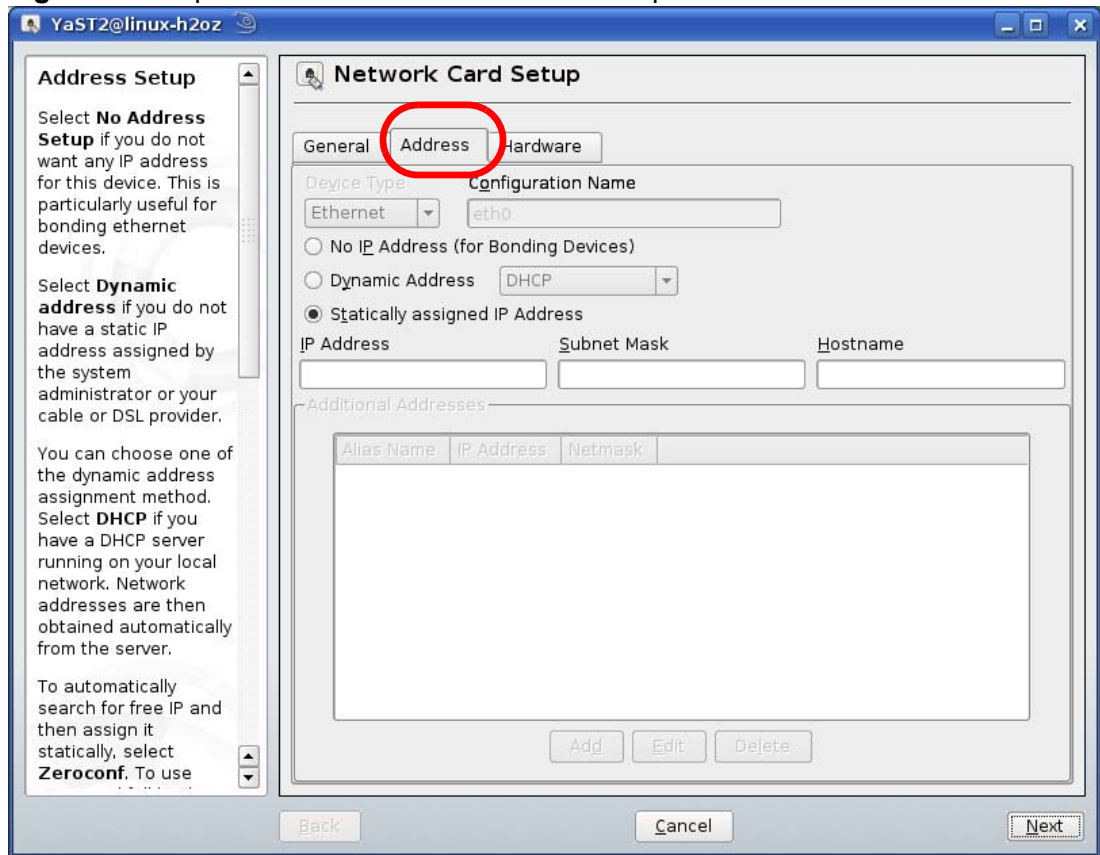
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

**Figure 219** openSUSE 10.3: Network Settings



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

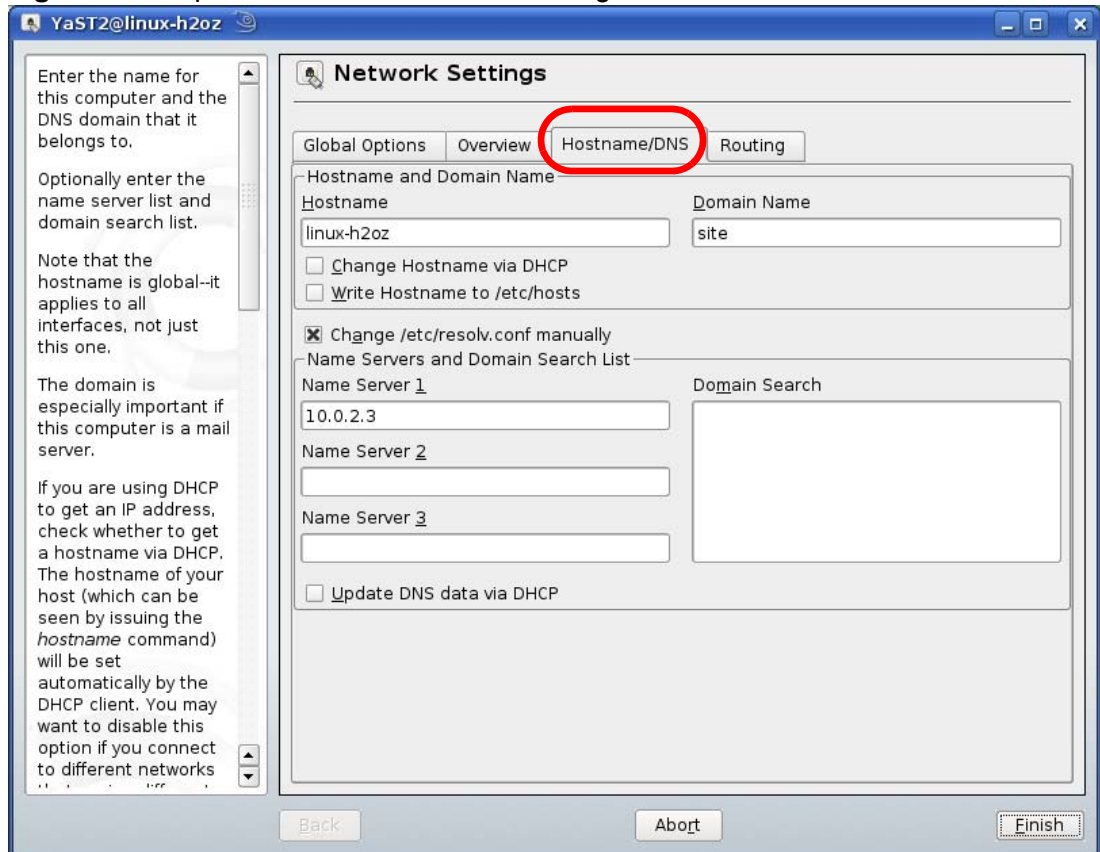
**Figure 220** openSUSE 10.3: Network Card Setup



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

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

**Figure 221** openSUSE 10.3: Network Settings

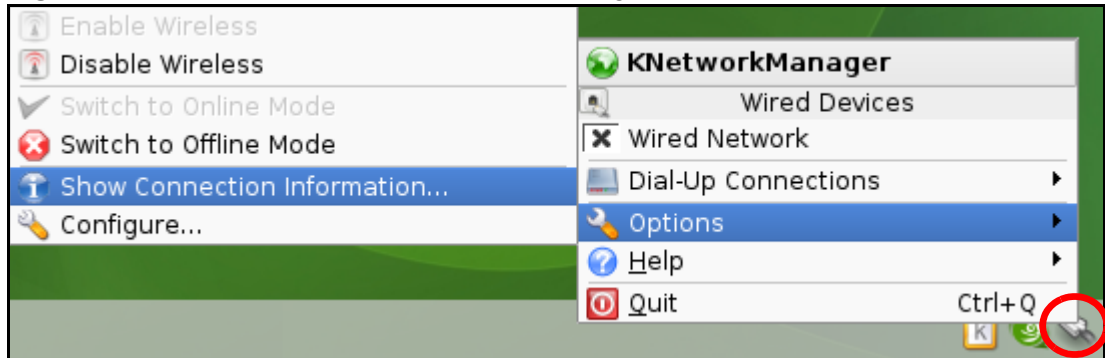


- 9 Click **Finish** to save your settings and close the window.

## Verifying Settings

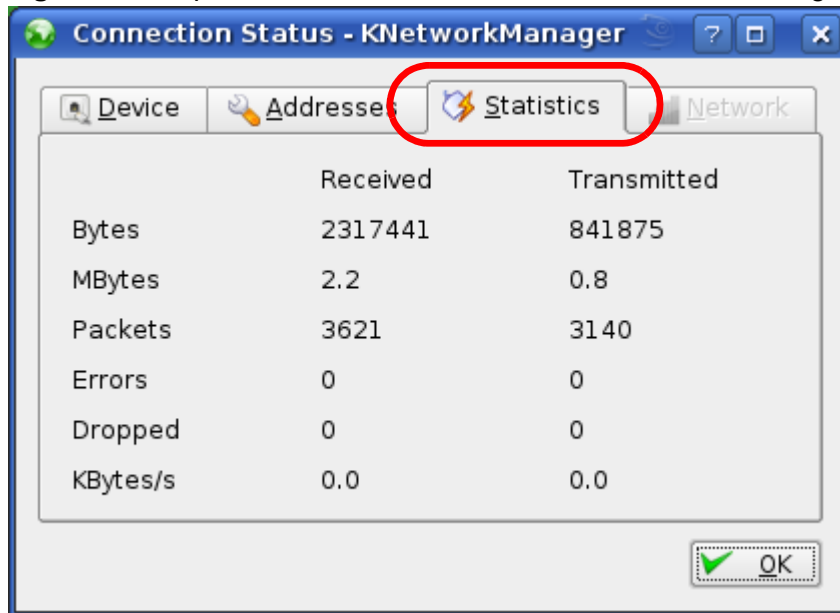
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

**Figure 222** 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 223** openSUSE: Connection Status - KNetwork Manager



# Wireless LANs

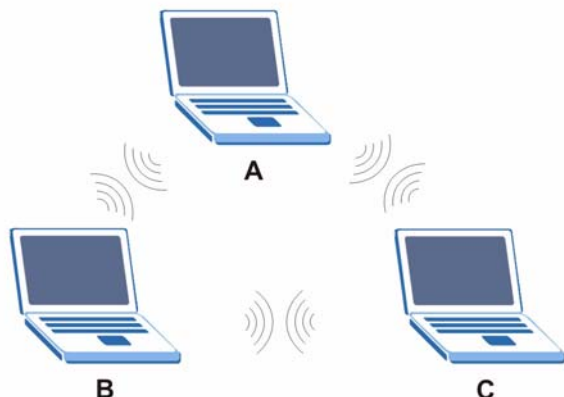
## Wireless LAN Topologies

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 224** Peer-to-Peer Communication in an Ad-hoc Network



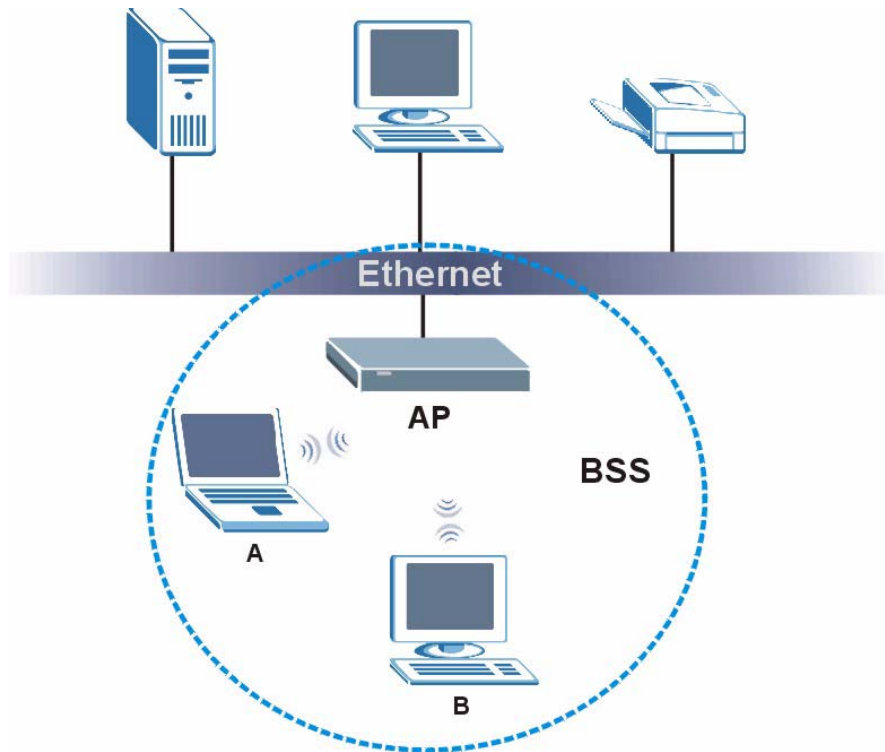
### BSS

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 225** Basic Service Set



## ESS

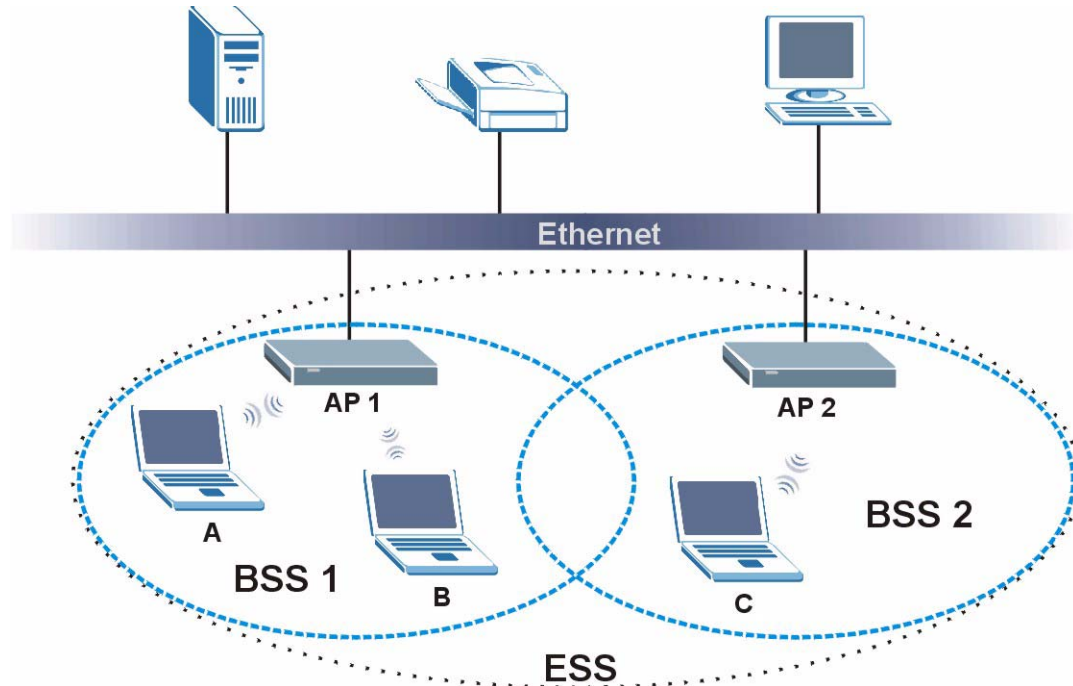
An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

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 226** Infrastructure WLAN



## 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. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

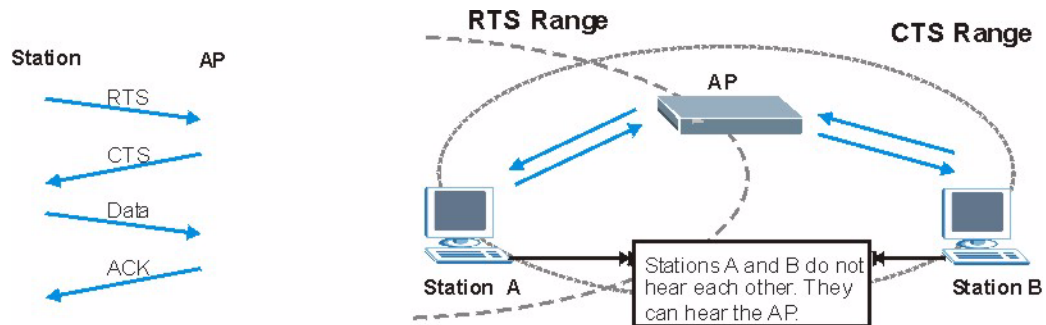
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel 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 227** 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 802.11b/g compliant wireless adapters support long preamble, but not all support short preamble.

Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.

Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.

Select **Dynamic** to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.

Note: The AP and the wireless adapters **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 98** 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 99** 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)
	WPA2
Most Secure	

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 screen. You may still configure and store keys here, 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 100** 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

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

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.

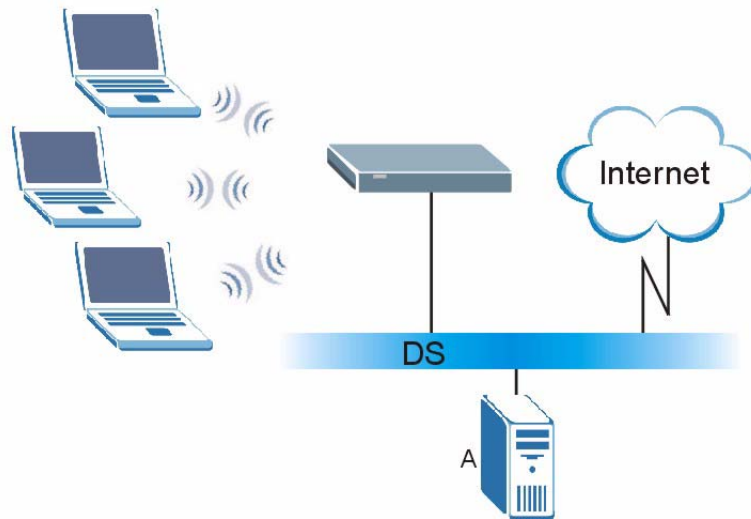
## WPA(2) with RADIUS Application Example

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

**Figure 228** WPA(2) with RADIUS Application Example



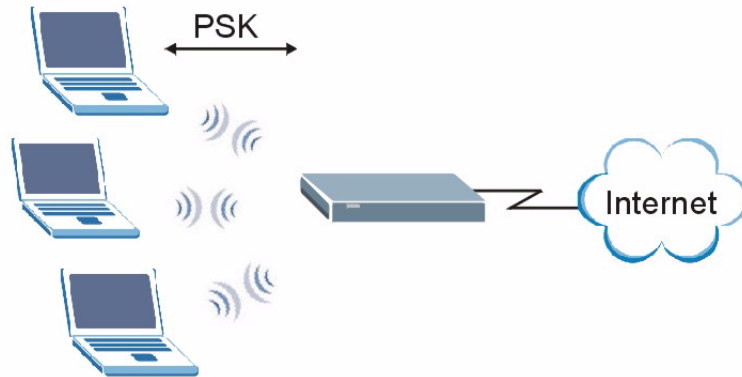
### WPA(2)-PSK Application Example

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 (only) allows it to join the network if the password matches.
- 3 The AP and wireless clients use the pre-shared key to generate a common PMK (Pairwise Master Key).

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

**Figure 229** WPA(2)-PSK Authentication



## Security Parameters Summary

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

**Table 101** Wireless Security Relational Matrix

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

## Antenna Overview

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

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

## Antenna Characteristics

### Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) 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.

# Pop-up Windows, JavaScripts and Java Permissions

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

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

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

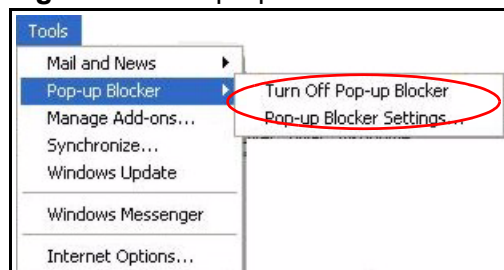
You may have to disable pop-up blocking to log into your device.

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**.

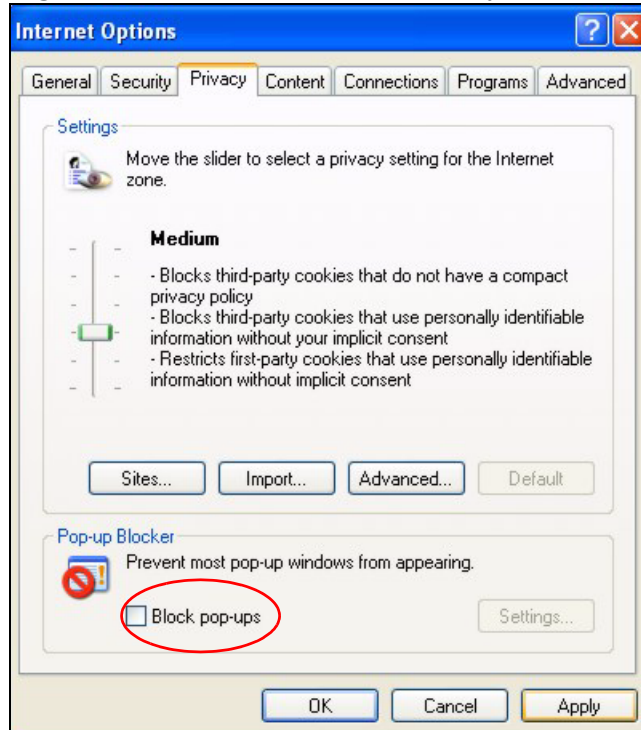
**Figure 230** Pop-up Blocker



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 231** Internet Options: Privacy



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

### Enable pop-up Blockers with Exceptions

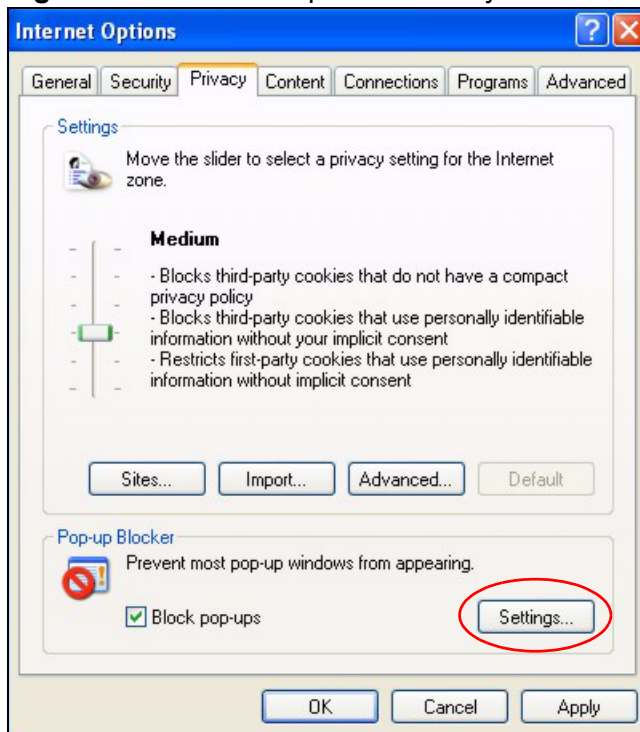
Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

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



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

**Figure 232** Internet Options: Privacy



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

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

**Figure 233** Pop-up Blocker Settings



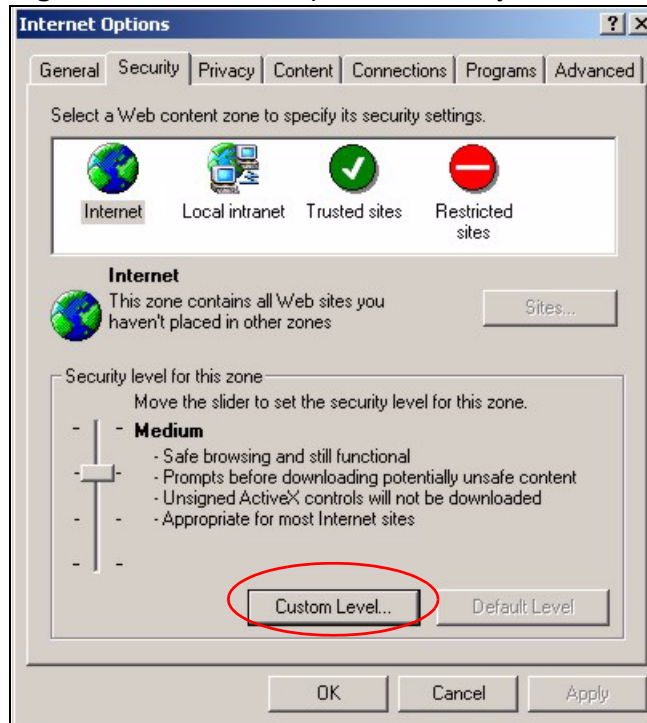
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScripts

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

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

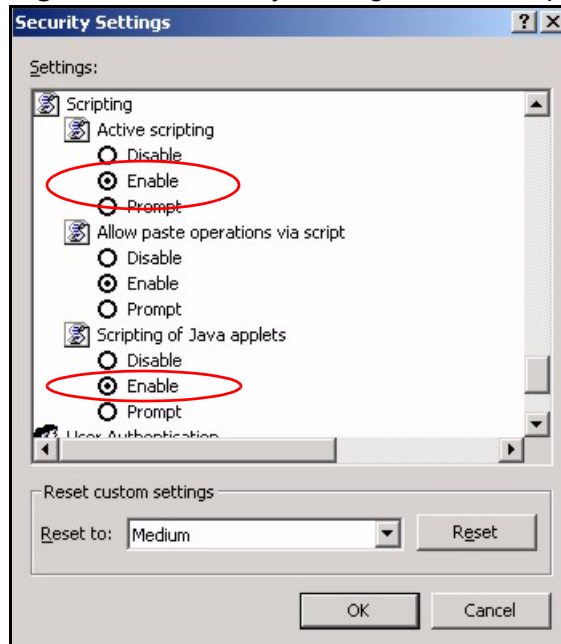
**Figure 234** Internet Options: Security



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

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

**Figure 235** Security Settings - Java Scripting

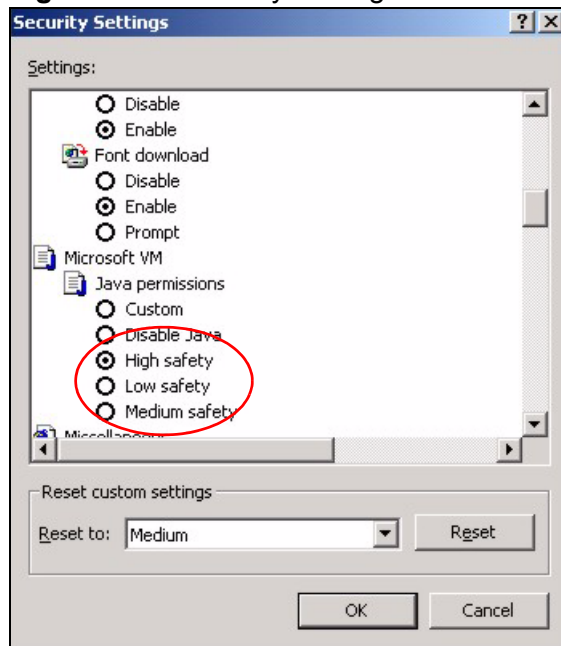


## Java Permissions

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

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

**Figure 236** Security Settings - Java

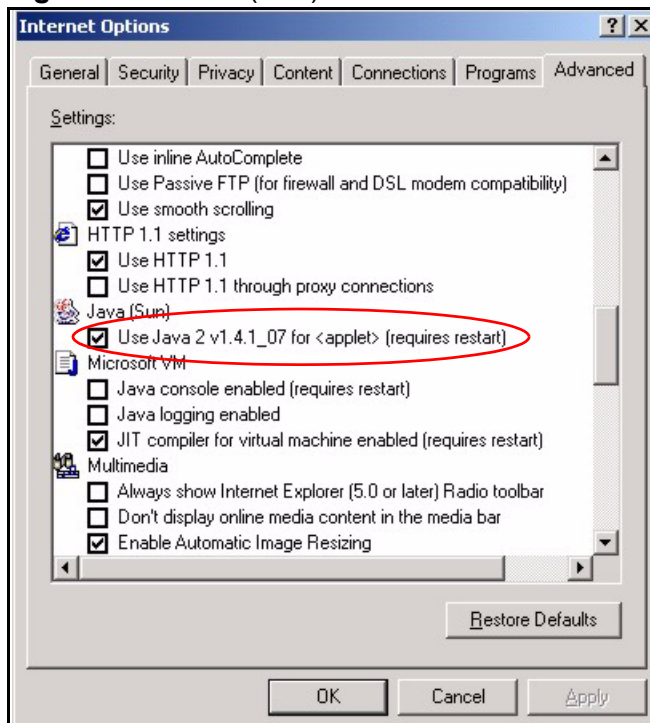


## JAVA (Sun)

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

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

**Figure 237** Java (Sun)




# Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon (  ) somewhere in the main browser window (not all browsers show the padlock in the same location.)

In this appendix, you can import a public key certificate for:

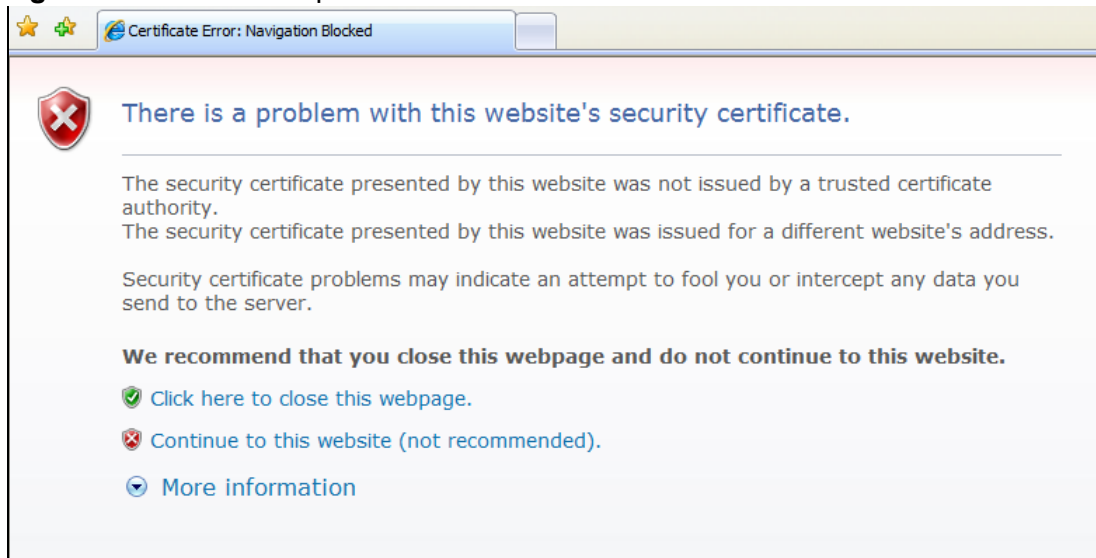
- Internet Explorer on [page 343](#)
- Firefox on [page 352](#)
- Opera on [page 357](#)
- Konqueror on [page 364](#)

## Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

**Figure 238** Internet Explorer 7: Certification Error



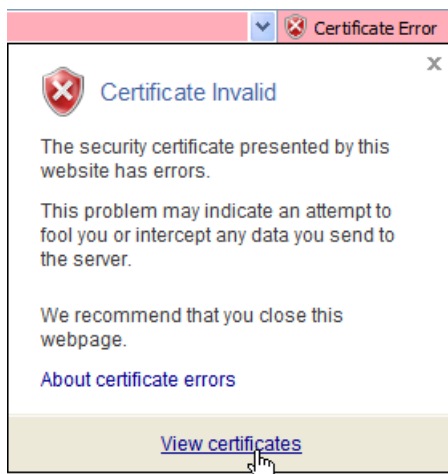
- 2 Click **Continue to this website (not recommended)**.

**Figure 239** Internet Explorer 7: Certification Error



- 3 In the **Address Bar**, click **Certificate Error > View certificates**.

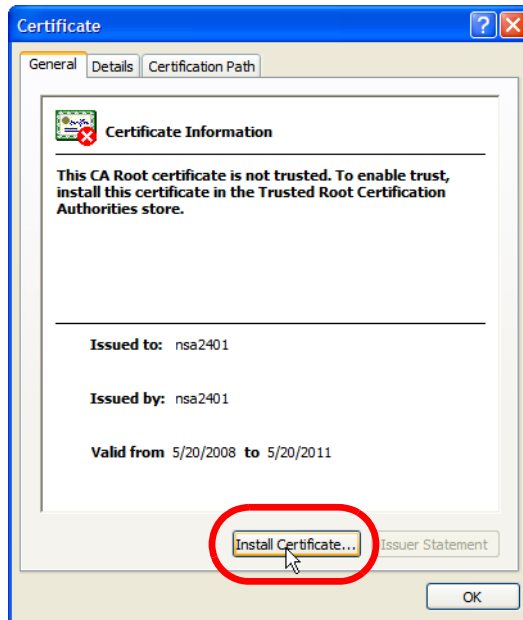
**Figure 240** Internet Explorer 7: Certificate Error





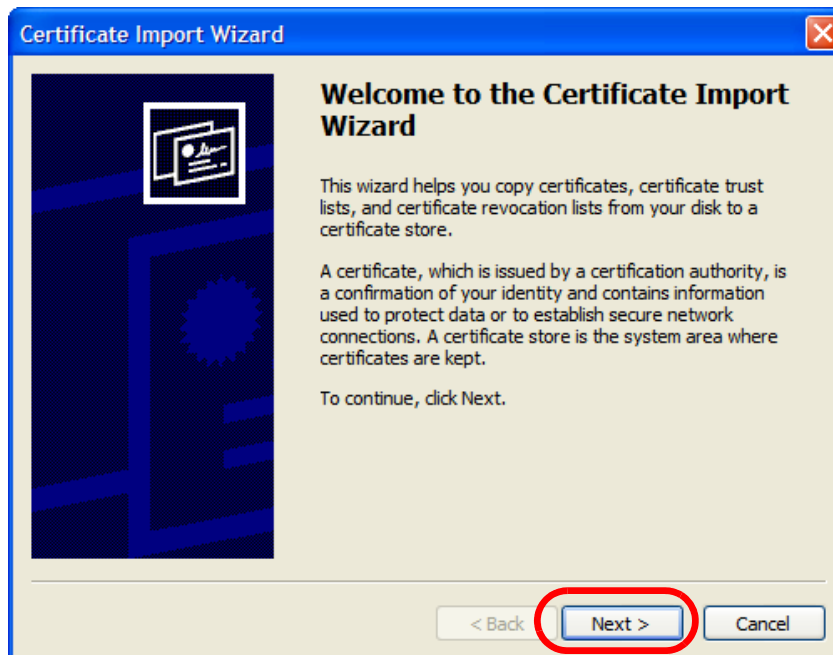
- 4 In the **Certificate** dialog box, click **Install Certificate**.

**Figure 241** Internet Explorer 7: Certificate



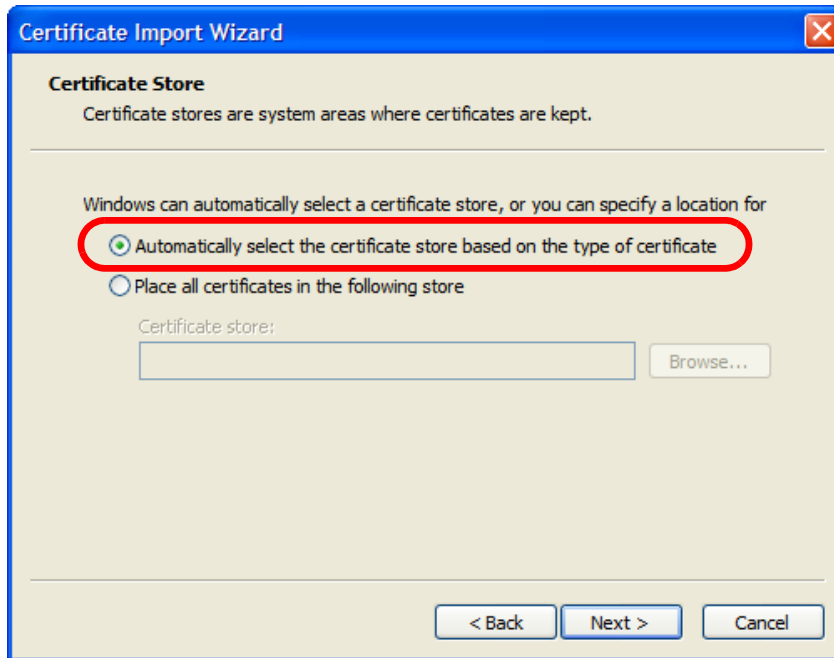
- 5 In the **Certificate Import Wizard**, click **Next**.

**Figure 242** Internet Explorer 7: Certificate Import Wizard



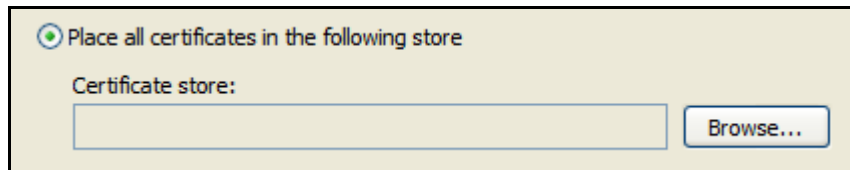
- 6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

**Figure 243** Internet Explorer 7: Certificate Import Wizard



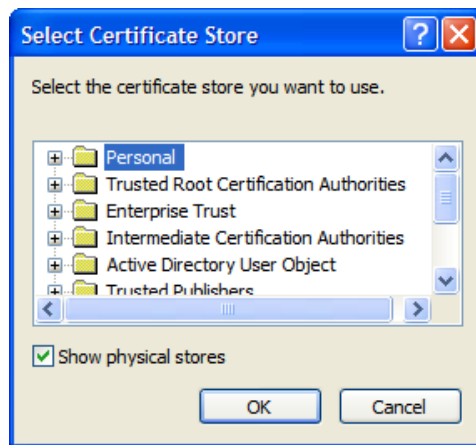
- 7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

**Figure 244** Internet Explorer 7: Certificate Import Wizard



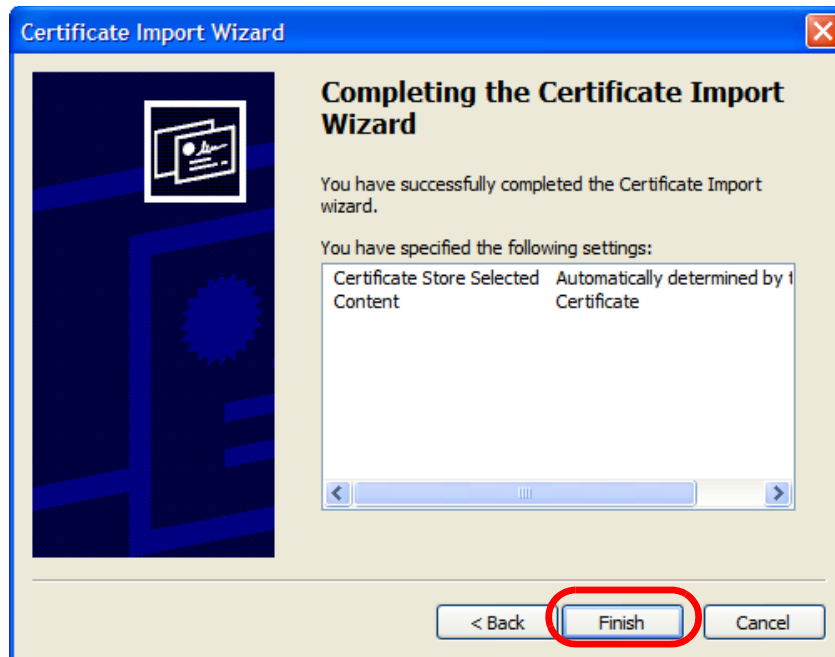
- 8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

**Figure 245** Internet Explorer 7: Select Certificate Store



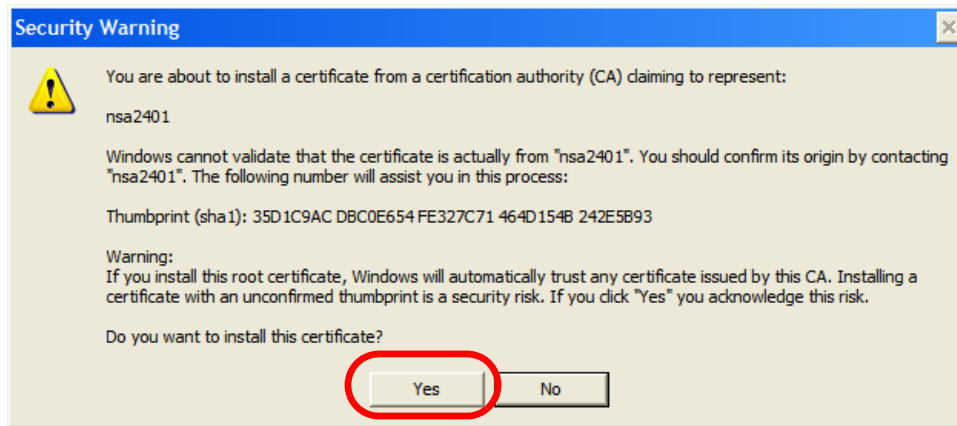
- 9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

**Figure 246** Internet Explorer 7: Certificate Import Wizard



- 10 If you are presented with another **Security Warning**, click **Yes**.

**Figure 247** Internet Explorer 7: Security Warning



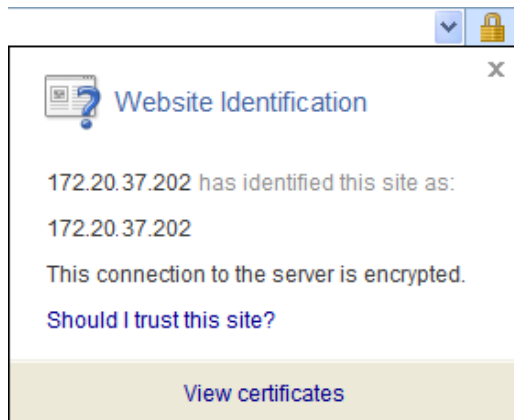
- 11 Finally, click **OK** when presented with the successful certificate installation message.

**Figure 248** Internet Explorer 7: Certificate Import Wizard



- 12 The next time you start Internet Explorer and go to a ZyXEL web configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

**Figure 249** Internet Explorer 7: Website Identification



## Installing a Stand-Alone Certificate File in Internet Explorer

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

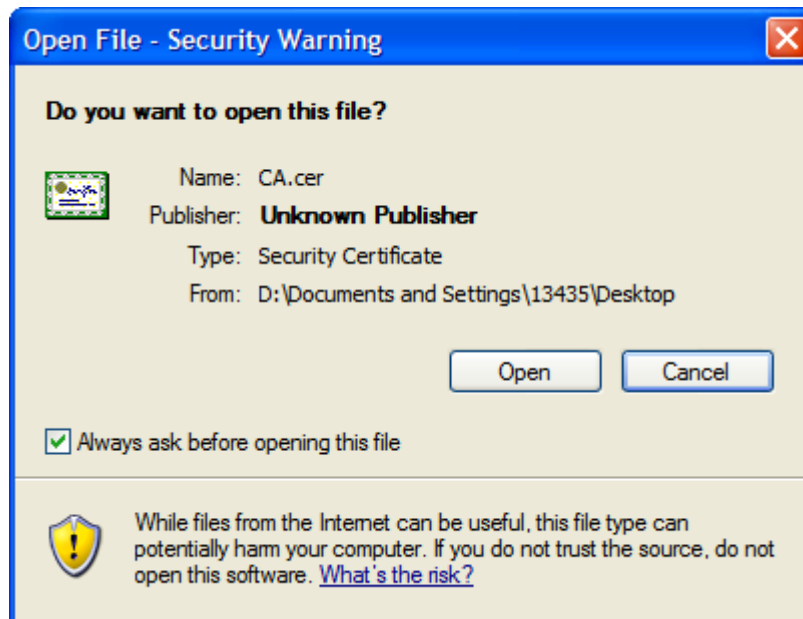
- 1 Double-click the public key certificate file.

**Figure 250** Internet Explorer 7: Public Key Certificate File



- 2 In the security warning dialog box, click **Open**.

**Figure 251** Internet Explorer 7: Open File - Security Warning



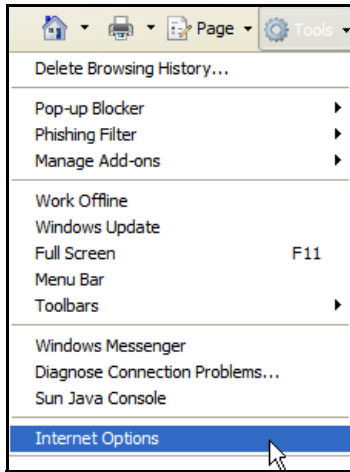
- 3 Refer to steps 4-12 in the Internet Explorer procedure beginning on [page 343](#) to complete the installation process.

## Removing a Certificate in Internet Explorer

This section shows you how to remove a public key certificate in Internet Explorer 7.

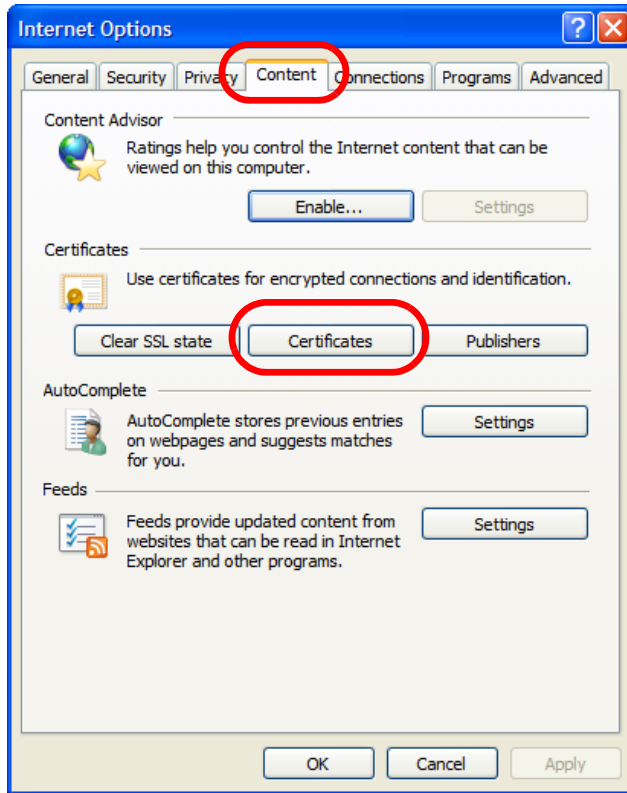
- 1 Open **Internet Explorer** and click **Tools > Internet Options**.

**Figure 252** Internet Explorer 7: Tools Menu



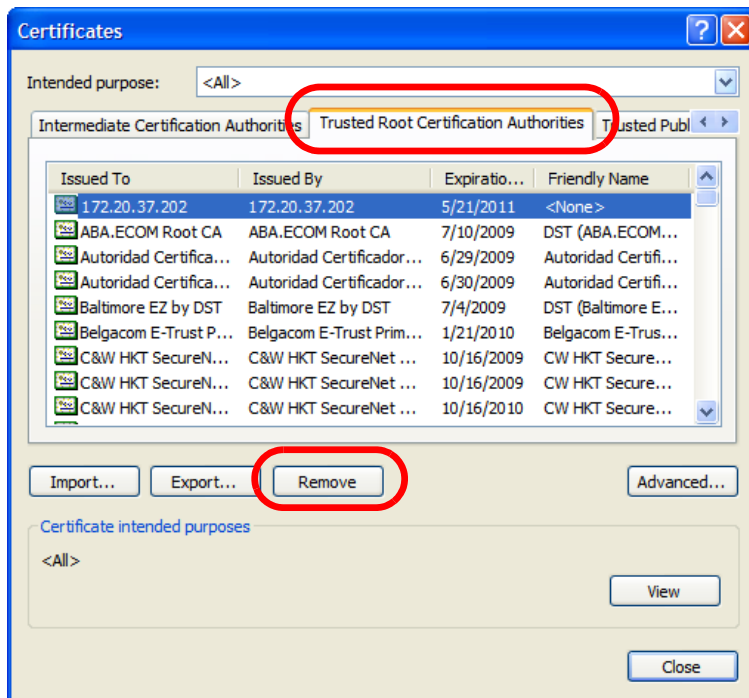
- 2 In the **Internet Options** dialog box, click **Content > Certificates**.

**Figure 253** Internet Explorer 7: Internet Options



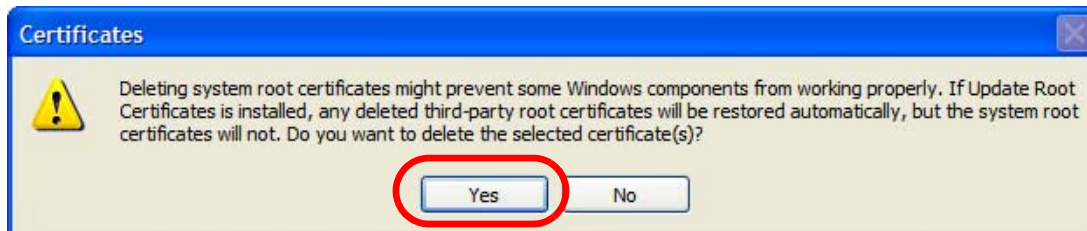
- 3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

**Figure 254** Internet Explorer 7: Certificates



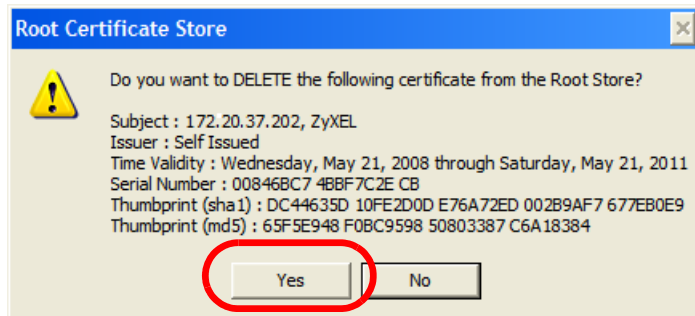
- 4 In the **Certificates** confirmation, click **Yes**.

**Figure 255** Internet Explorer 7: Certificates



- 5 In the **Root Certificate Store** dialog box, click **Yes**.

**Figure 256** Internet Explorer 7: Root Certificate Store



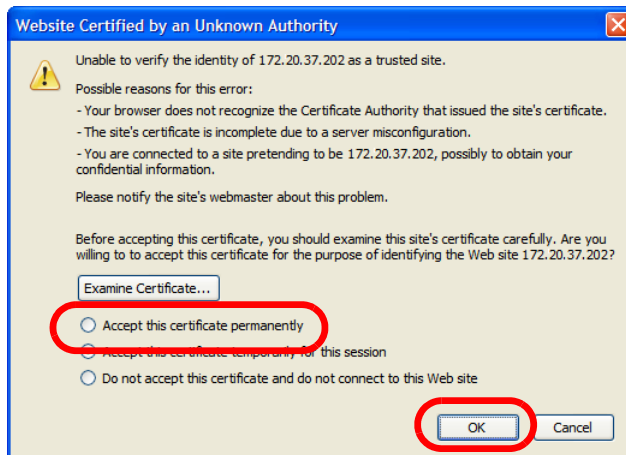
- 6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

## Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Select **Accept this certificate permanently** and click **OK**.

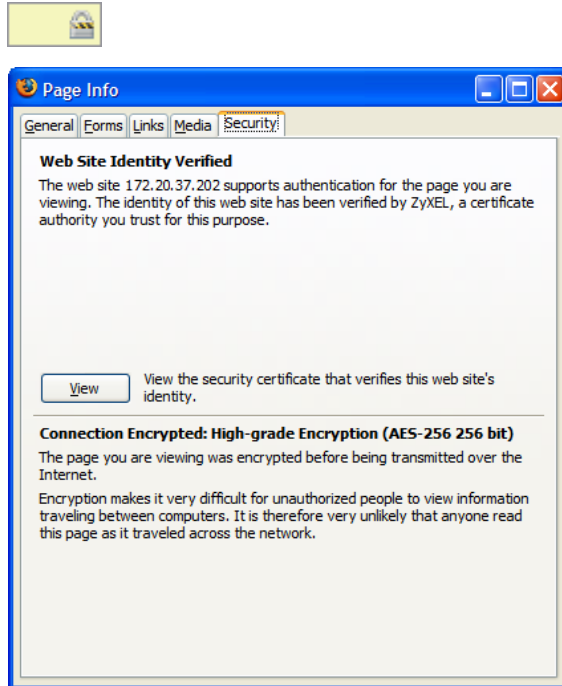
**Figure 257** Firefox 2: Website Certified by an Unknown Authority





- The certificate is stored and you can now connect securely to the web configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info > Security** window to view the web page's security information.

**Figure 258** Firefox 2: Page Info

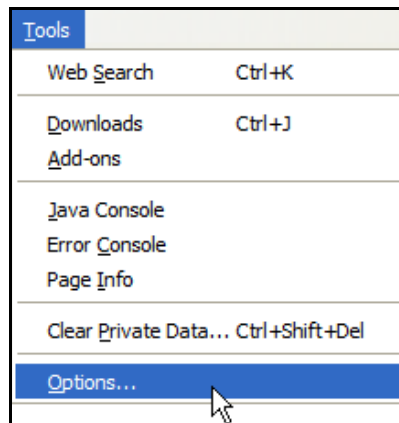


## Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

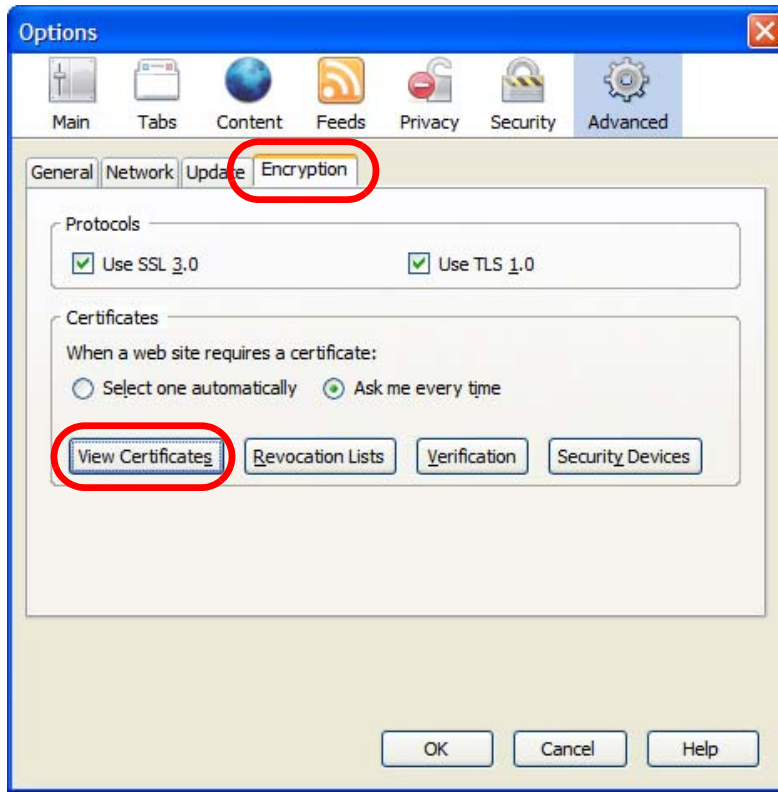
- Open **Firefox** and click **Tools > Options**.

**Figure 259** Firefox 2: Tools Menu



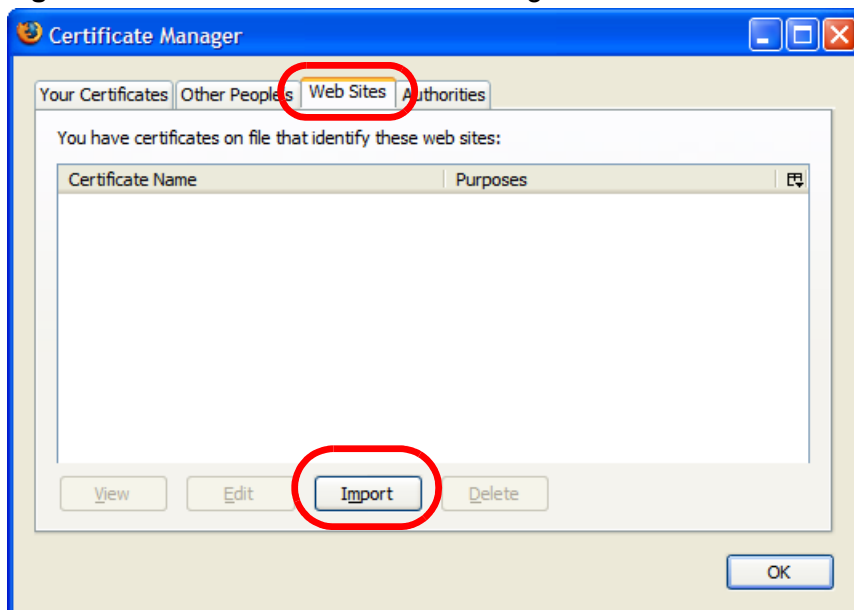
- 2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

**Figure 260** Firefox 2: Options



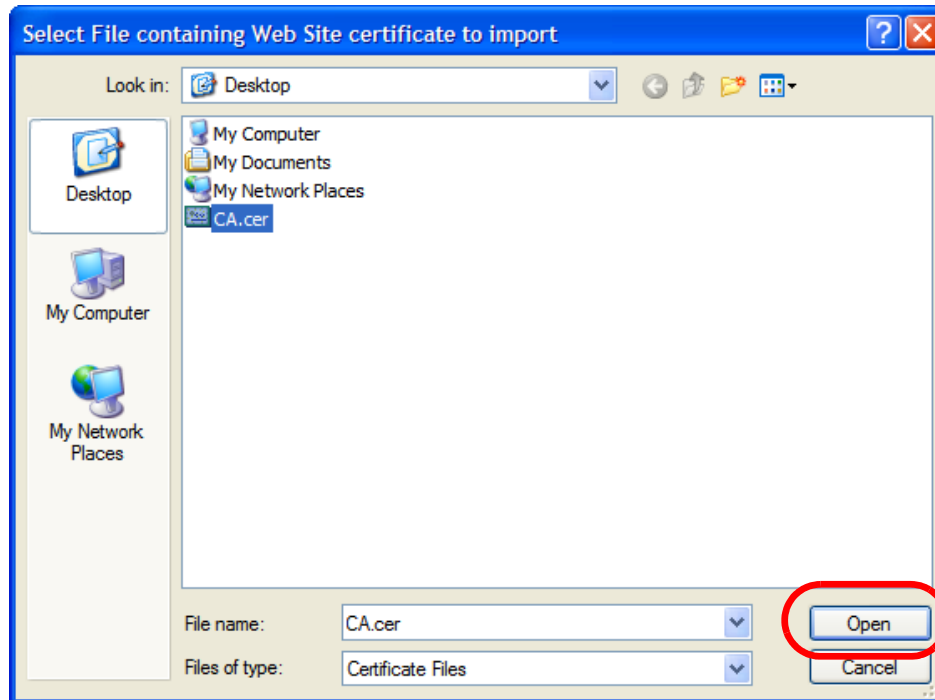
- 3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

**Figure 261** Firefox 2: Certificate Manager



- 4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

**Figure 262** Firefox 2: Select File



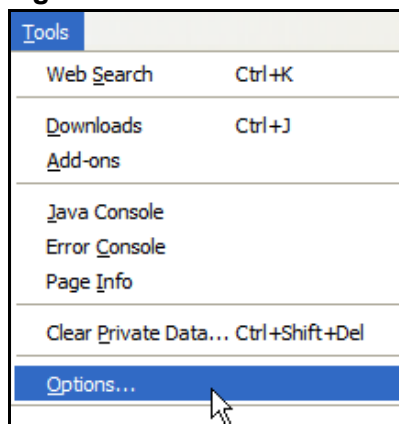
- 5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

## Removing a Certificate in Firefox

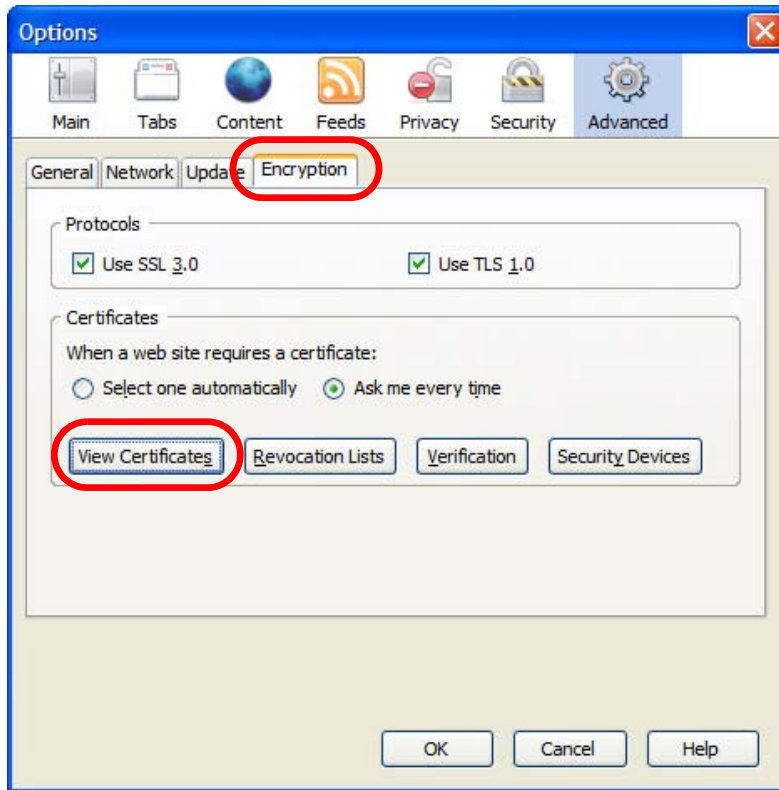
This section shows you how to remove a public key certificate in Firefox 2.

- 1 Open **Firefox** and click **Tools > Options**.

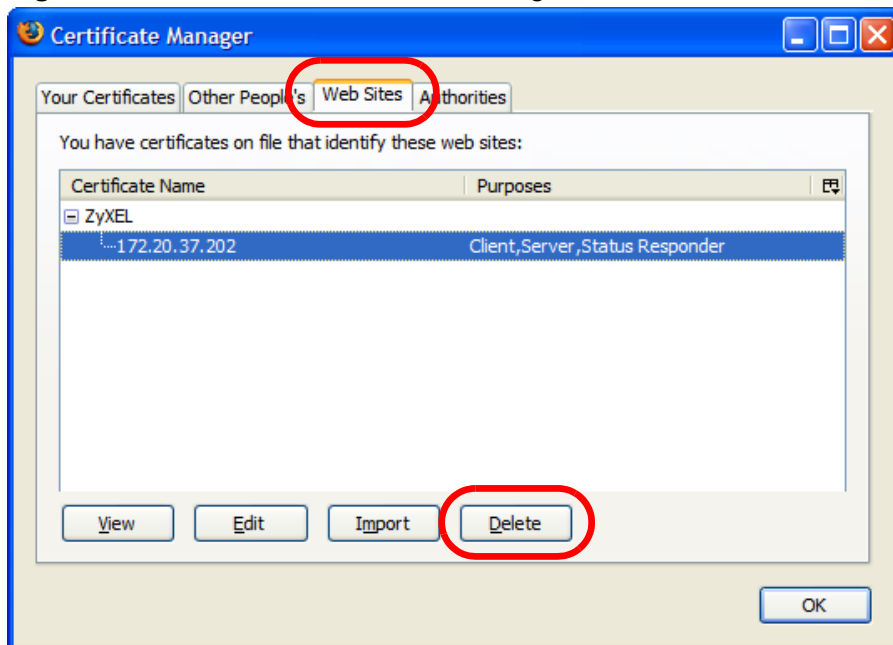
**Figure 263** Firefox 2: Tools Menu



- 2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

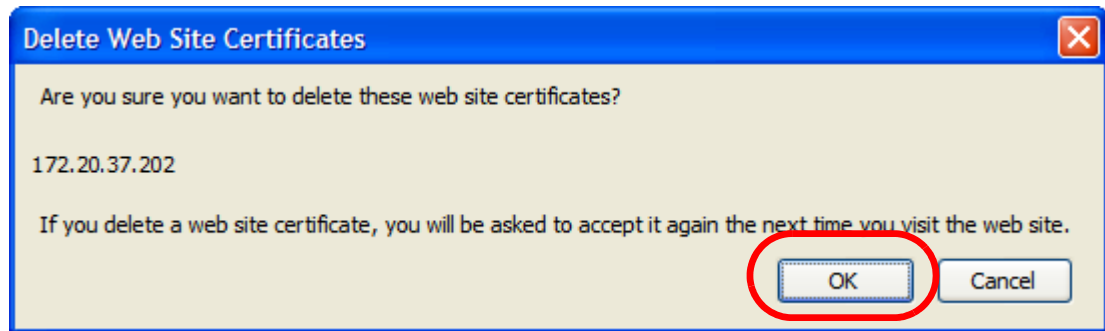
**Figure 264** Firefox 2: Options

- 3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

**Figure 265** Firefox 2: Certificate Manager

- 4 In the **Delete Web Site Certificates** dialog box, click **OK**.

**Figure 266** Firefox 2: Delete Web Site Certificates



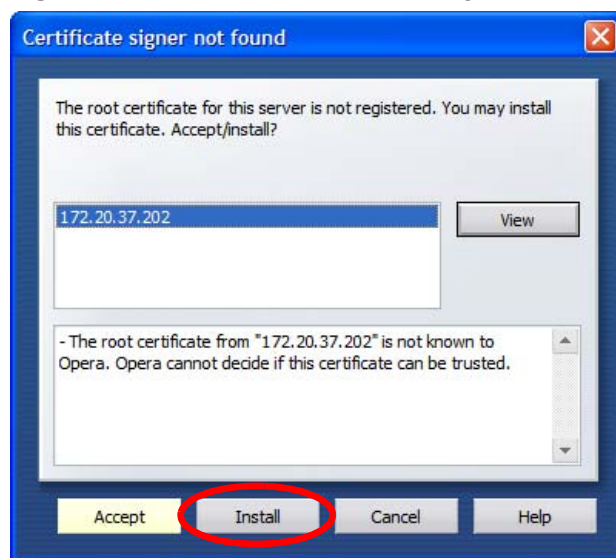
- 5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

## Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

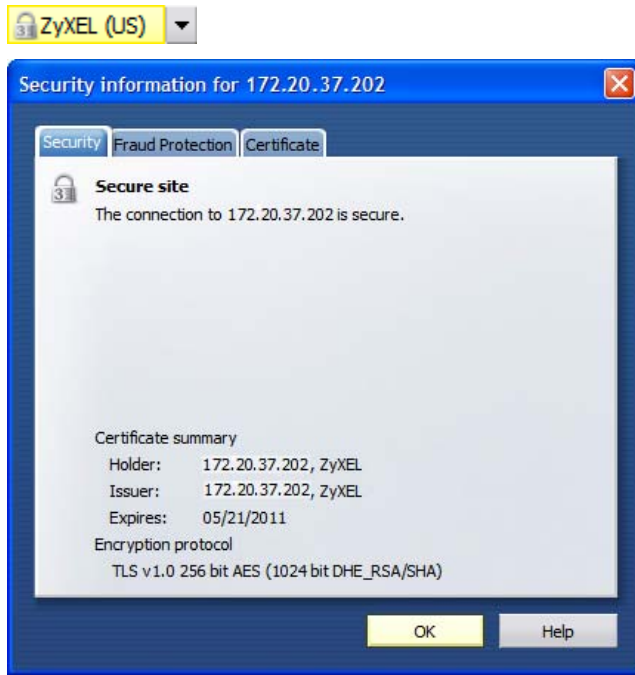
- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Click **Install** to accept the certificate.

**Figure 267** Opera 9: Certificate signer not found



- 3 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page’s security details.

**Figure 268** Opera 9: Security information

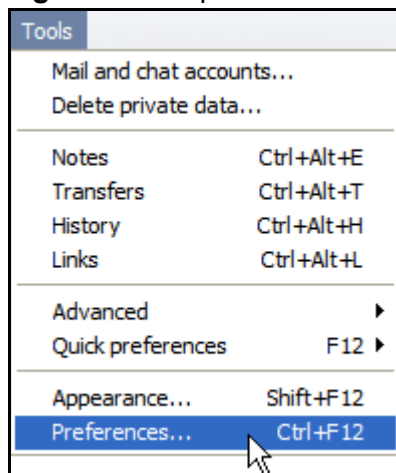


### Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

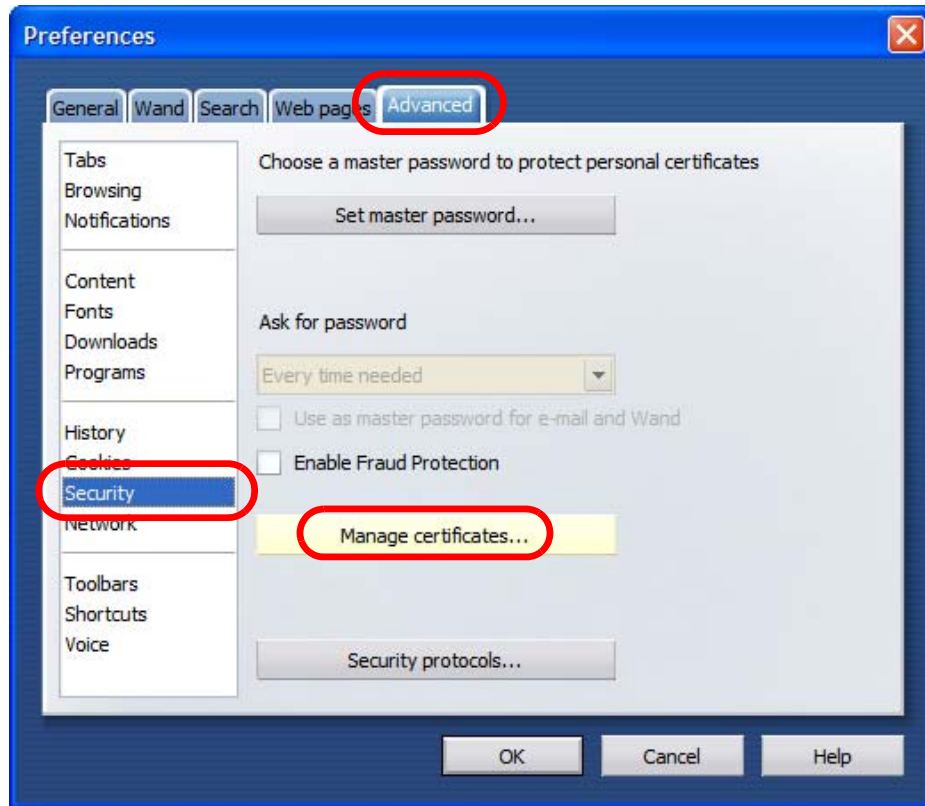
- 1 Open **Opera** and click **Tools > Preferences**.

**Figure 269** Opera 9: Tools Menu



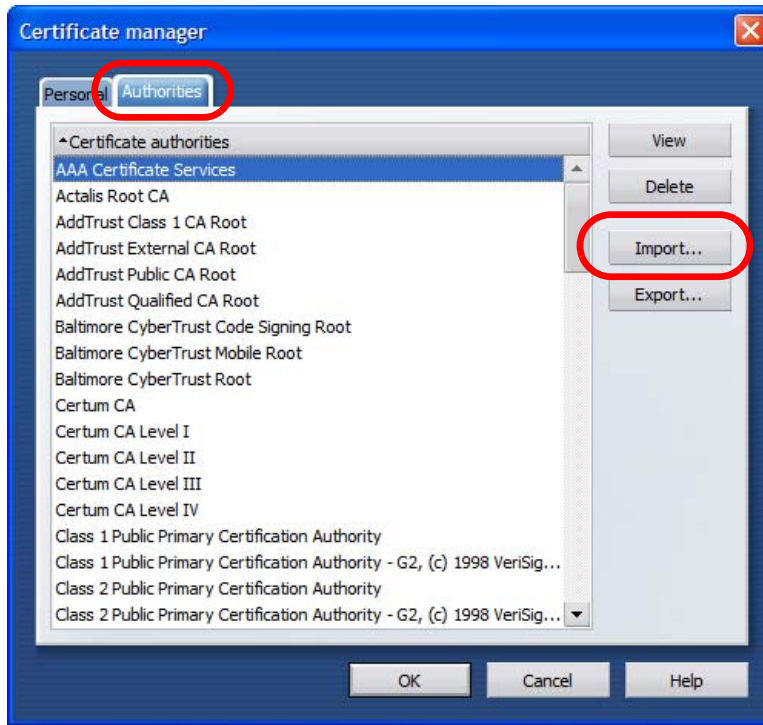
- 2 In **Preferences**, click **Advanced** > **Security** > **Manage certificates**.

**Figure 270** Opera 9: Preferences



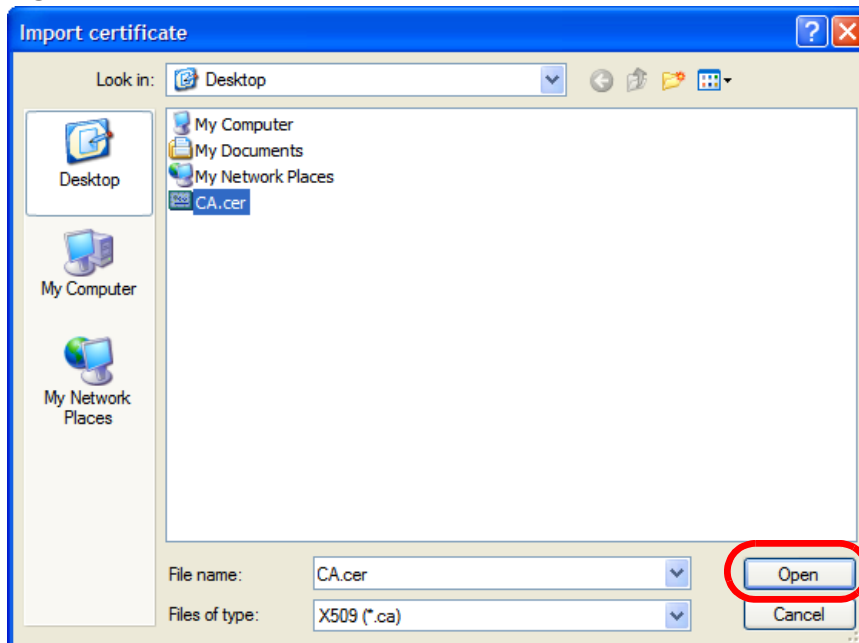
- 3 In the **Certificates Manager**, click **Authorities > Import**.

**Figure 271** Opera 9: Certificate manager



- 4 Use the **Import certificate** dialog box to locate the certificate and then click **Open**.

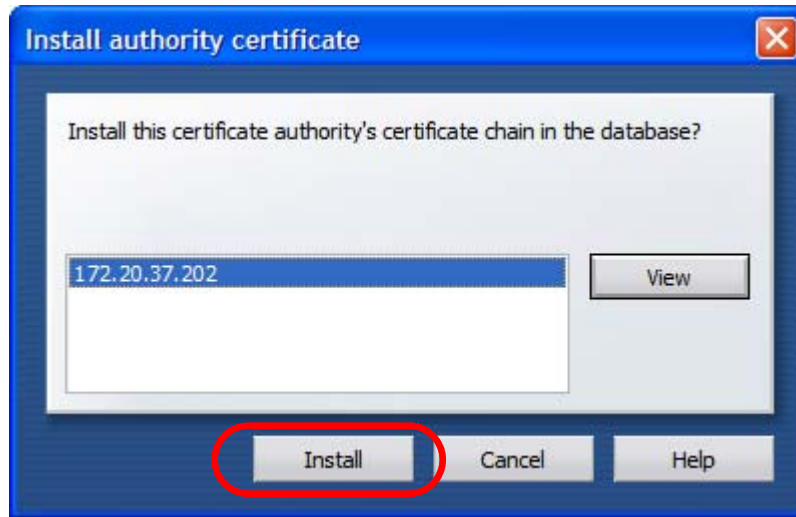
**Figure 272** Opera 9: Import certificate





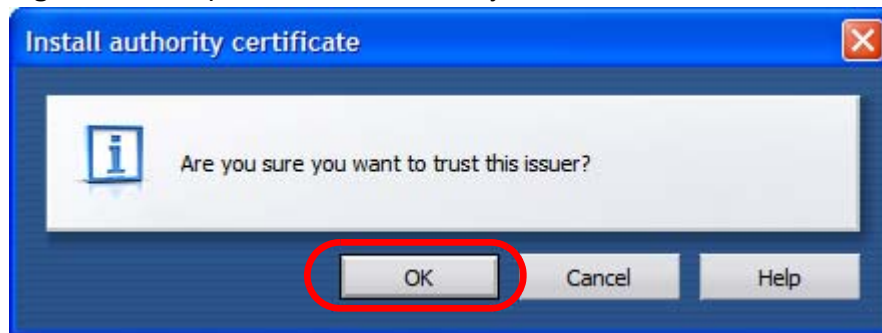
- 5 In the **Install authority certificate** dialog box, click **Install**.

**Figure 273** Opera 9: Install authority certificate



- 6 Next, click **OK**.

**Figure 274** Opera 9: Install authority certificate



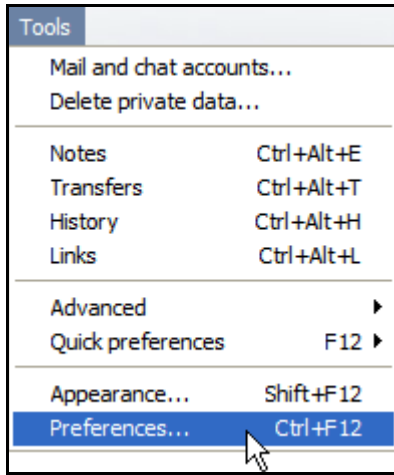
- 7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

## Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

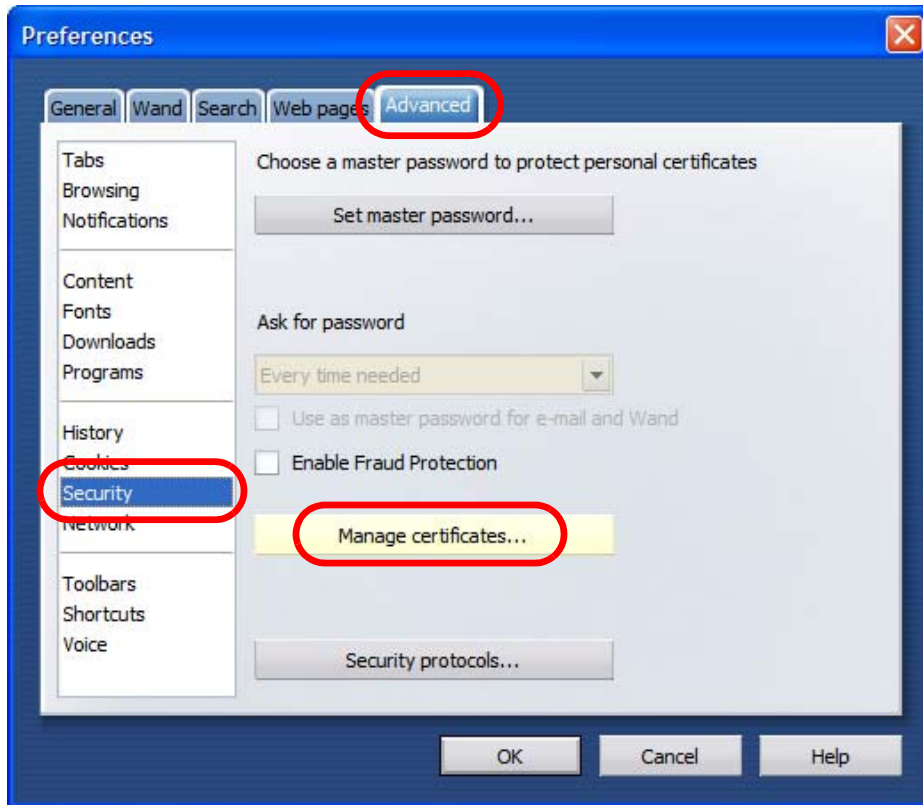
- 1 Open **Opera** and click **Tools > Preferences**.

**Figure 275** Opera 9: Tools Menu



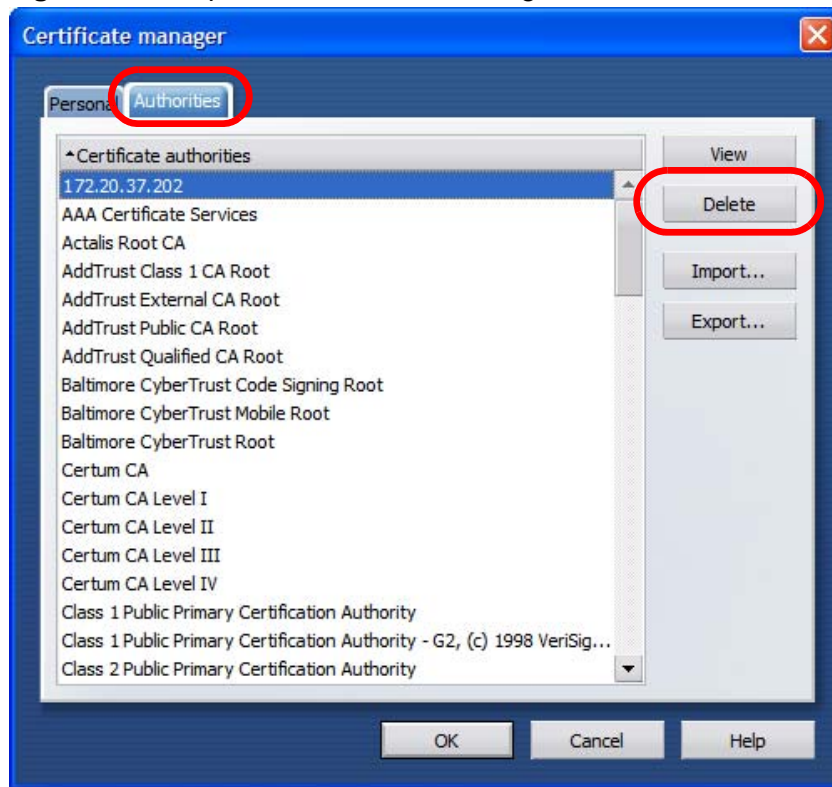
- 2 In **Preferences, Advanced > Security > Manage certificates**.

**Figure 276** Opera 9: Preferences



- 3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

**Figure 277** Opera 9: Certificate manager



- 4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Note: There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

## Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

- 2 Click **Continue**.

**Figure 278** Konqueror 3.5: Server Authentication



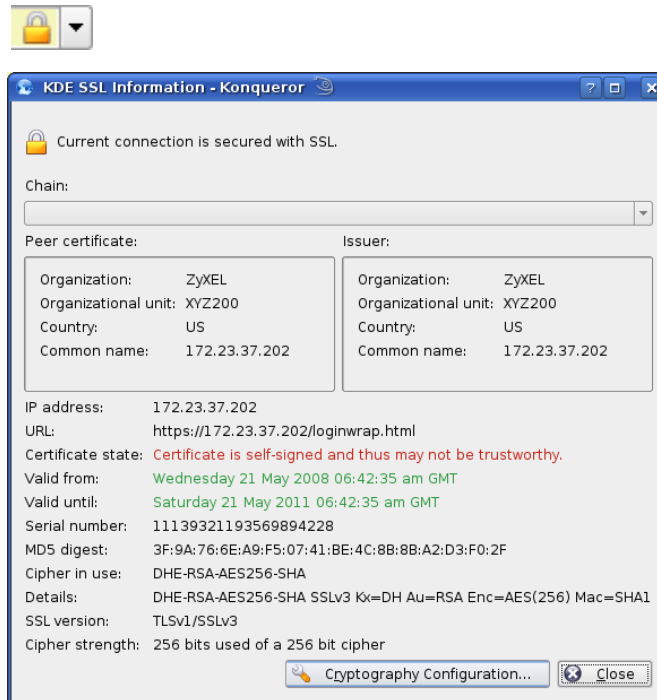
- 3 Click **Forever** when prompted to accept the certificate.

**Figure 279** Konqueror 3.5: Server Authentication



- 4 Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

**Figure 280** Konqueror 3.5: KDE SSL Information



## Installing a Stand-Alone Certificate File in Konqueror

Rather than browsing to a ZyXEL web configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

- 1 Double-click the public key certificate file.

**Figure 281** Konqueror 3.5: Public Key Certificate File



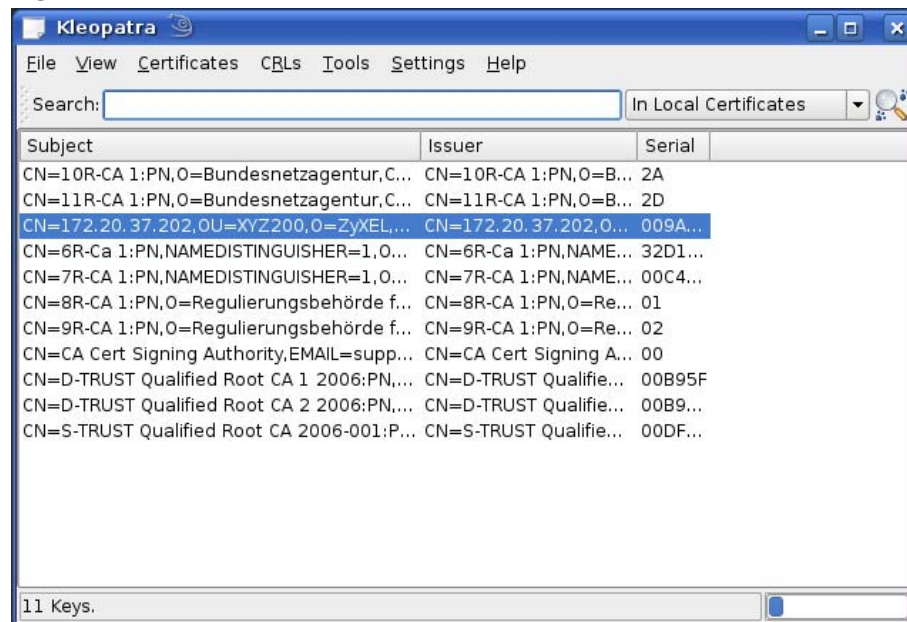
- 2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

**Figure 282** Konqueror 3.5: Certificate Import Result



The public key certificate appears in the KDE certificate manager, **Kleopatra**.

**Figure 283** Konqueror 3.5: Kleopatra



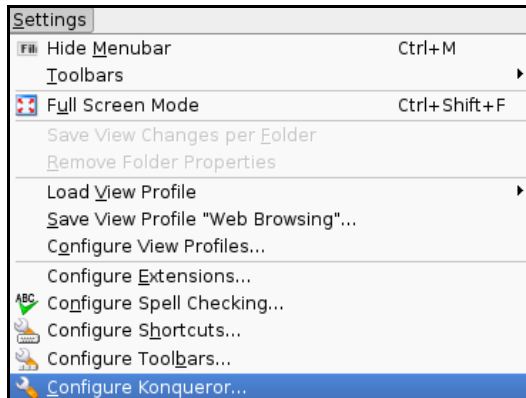
- 3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

## Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

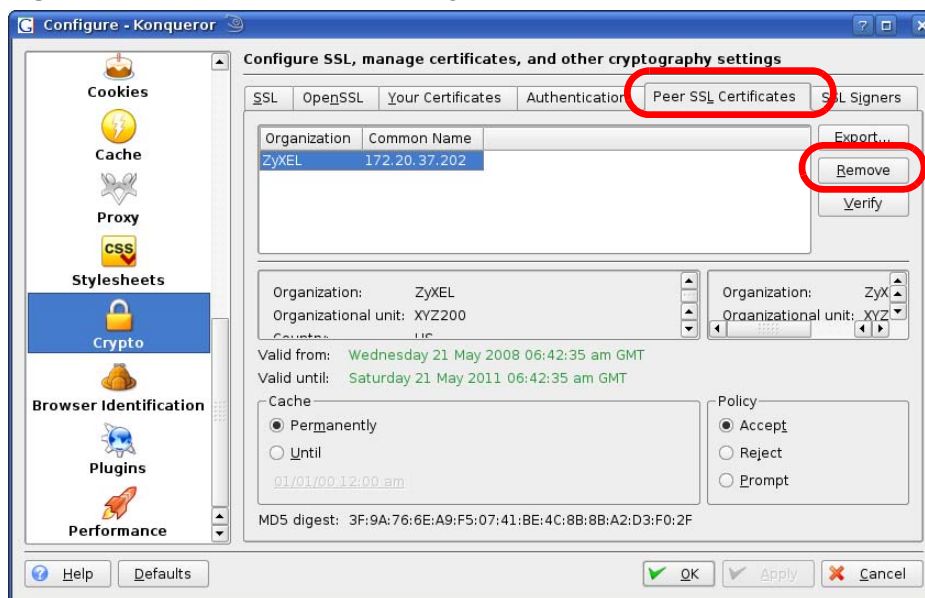
- 1 Open **Konqueror** and click **Settings > Configure Konqueror**.

**Figure 284** Konqueror 3.5: Settings Menu



- 2 In the **Configure** dialog box, select **Crypto**.
- 3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

**Figure 285** Konqueror 3.5: Configure



- 4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Note: There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.





# 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.

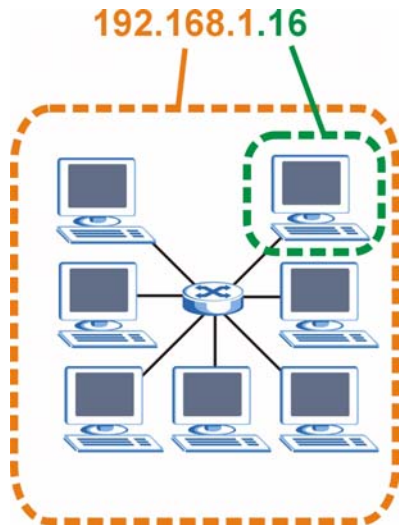
## Structure

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 286** 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 102** Subnet Masks

	<b>1ST OCTET:</b> (192)	<b>2ND OCTET:</b> (168)	<b>3RD OCTET:</b> (1)	<b>4TH OCTET:</b> (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	<b>11111111</b>	<b>11111111</b>	<b>11111111</b>	00000000

**Table 102** Subnet Masks

	<b>1ST OCTET: (192)</b>	<b>2ND OCTET: (168)</b>	<b>3RD OCTET: (1)</b>	<b>4TH OCTET (2)</b>
Network Number	<b>11000000</b>	<b>10101000</b>	<b>00000001</b>	
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 103** Subnet Masks

	<b>BINARY</b>				<b>DECIMAL</b>
	<b>1ST OCTET</b>	<b>2ND OCTET</b>	<b>3RD OCTET</b>	<b>4TH OCTET</b>	
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 104** 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 105** 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

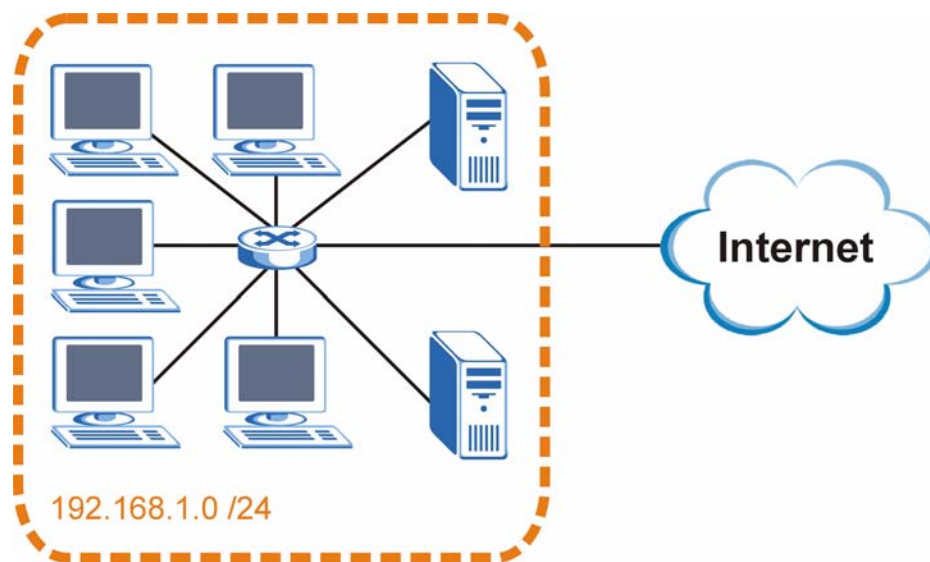
## Subnetting

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 287** Subnetting Example: Before Subnetting

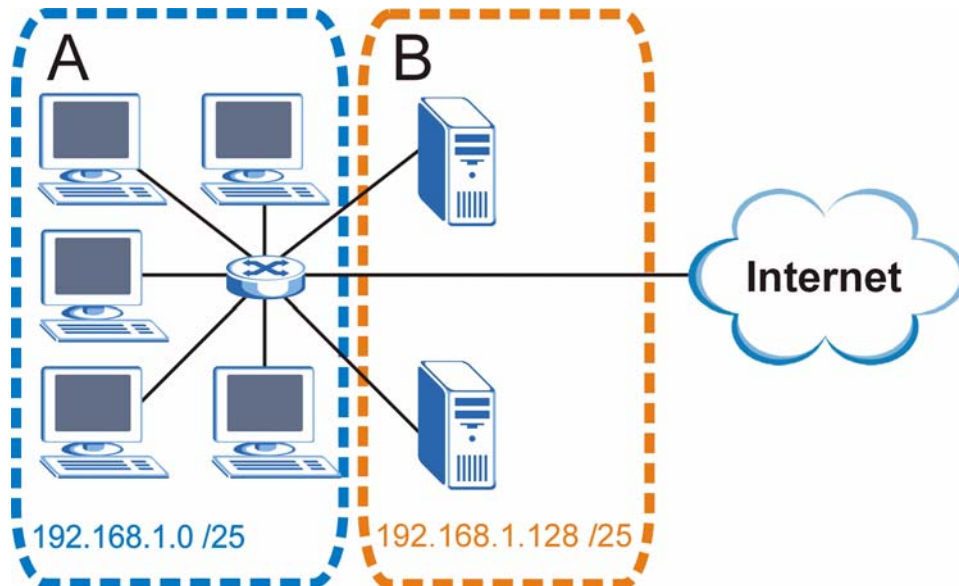


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 288** Subnetting Example: After Subnetting



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

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

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

## Example: Four Subnets

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

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

**Table 106** Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 107** Subnet 2

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

**Table 108** Subnet 3

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

**Table 109** Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001. .	11000000
Subnet Mask (Binary)	11111111.11111111.11111111. .	11000000

**Table 109** Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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 110** 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 111** 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 112** 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
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*.

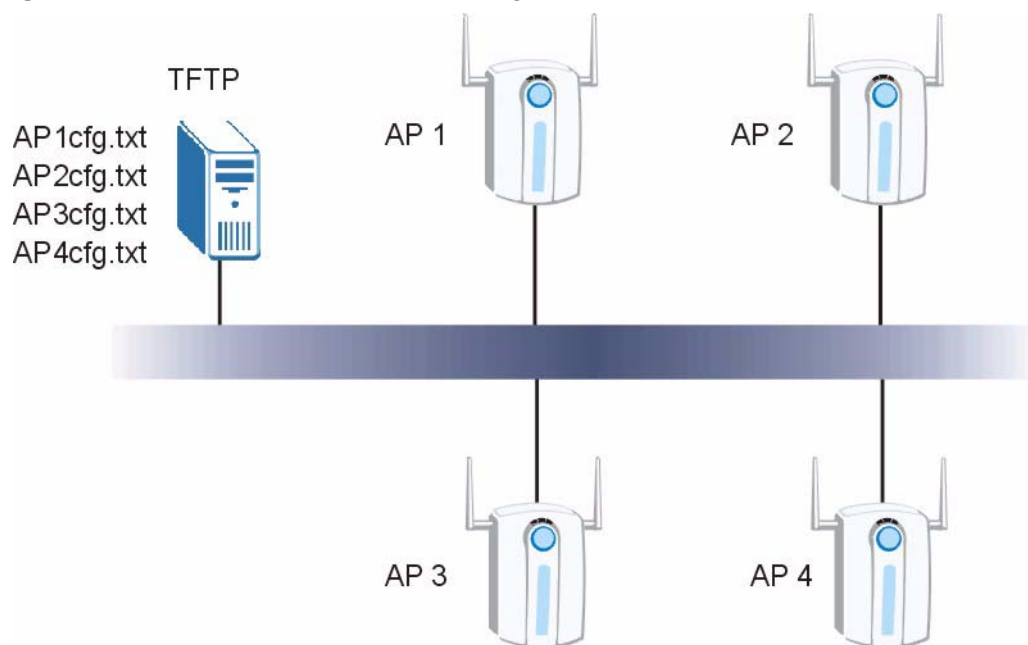
# Text File Based Auto Configuration

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 289** 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.

## Auto Configuration by DHCP

A DHCP response can use options 66 and 67 to assign a TFTP server IP address and a filename. If the AP is configured as a DHCP client, these settings can be used to perform auto configuration.

**Table 113** Auto Configuration by DHCP

COMMAND	DESCRIPTION
wcfg autocfg dhcp [enable   disable]	Turn configuration of TFTP server IP address and filename through DHCP on or off.

If this feature is enabled and the DHCP response provides a TFTP server IP address and a filename, the AP will try to download the file from the specified TFTP server. The AP then uses the file to configure wireless LAN settings.

Note: Not all DHCP servers allow you to specify options 66 and 67.

## Manual Configuration

Use the following command to manually configure a TFTP server IP address and a file name for the AP to use for auto provisioning whenever the AP starts up. See [Section 25.1 on page 257](#) for how to access the Command Interpreter (CI).

**Table 114** Manual Configuration

COMMAND	DESCRIPTION
wcfg autocfg server [IP] [filename]	Specify the TFTP server IP address and file name from which the AP is to download a configuration file whenever the AP starts up.

## 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 115** 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 116** 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 117** 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.

## Configuration File Format

The text based configuration file must use the following format.

**Figure 290** Configuration File Format

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 1 xxx
wcfg security save
wcfg ssid 1 xxx
wcfg ssid save
```

The first line must be !#ZYXEL PROWLAN.

The second line must specify the file version. The AP compares the file version with the version of the last configuration file that it downloaded. If the version of the downloaded file is the same or smaller (older), the AP ignores the file. If the version of the downloaded file is larger (newer), the AP uses the file.

## Configuration File Rules

You can only use the `wlan` and `wcfg` commands in the configuration file. The AP ignores other ZyNOS commands but continues to check the next command.

The AP ignores any improperly formatted commands and continues to check the next line.

If there are any errors while processing the configuration file, the AP generates a message with the line number and reason for the first error (subsequent errors during the processing of an individual configuration file are not recorded). You can use SNMP management software to display the message by using the following MIB.

**Table 118** Displaying the Auto Configuration Status

ITEM	OBJECT ID	DESCRIPTION
pwAutoCfgMessage	1.3.6.1.4.1.890.1.9.1.9	Auto configuration status message string

The commands will be executed line by line just like if you entered them in a console or Telnet CI session. Be careful to ensure the integrity of the whole AP configuration. If there are existing settings in the AP, the newly loaded configuration file will either coexist with the previous settings or replace them.

You can zip each configuration file. You must use the store compression method and a .zip file extension. When zipping a configuration file, you can also add password protection using the same password that you use to log into the AP.

## Wcfg Command Configuration File Examples

These example configuration files use the `wcfg` command to configure security and SSID profiles.

**Figure 291** WEP Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 11
wcfg security 1 name Test-wep
wcfg security 1 security wep
wcfg security 1 wep keysize 64 ascii
wcfg security 1 wep key1 abcde
wcfg security 1 wep key2 bcdef
wcfg security 1 wep key3 cdefg
wcfg security 1 wep key4 defgh
wcfg security 1 wep keyindex 1
wcfg security save
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 1 l2isolation disable
wcfg ssid 1 macfilter disable
wcfg ssid save
```

**Figure 292** 802.1X Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 2 name Test-8021x
wcfg security 2 mode 8021x-static128
wcfg security 2 wep key1 abcdefghijklm
wcfg security 2 wep key2 bcdefghijklmn
wcfg security 2 wep keyindex 1
wcfg security 2 reauthtime 1800
wcfg security 2 idletime 3600
wcfg security save
wcfg radius 2 name radius-rd
wcfg radius 2 primary 172.23.3.4 1812 1234 enable
wcfg radius 2 backup 172.23.3.5 1812 1234 enable
wcfg radius save
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 2 qos 4
wcfg ssid 2 l2isolation disable
wcfg ssid 2 macfilter disable
wcfg ssid save
```

**Figure 293** WPA-PSK Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 13
wcfg security 3 name Test-wpapsk
wcfg security 3 mode wpapsk
wcfg security 3 passphrase qwertyuiop
wcfg security 3 reauthtime 1800
wcfg security 3 idletime 3600
wcfg security 3 groupkeytime 1800
wcfg security save
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 3 qos 4
wcfg ssid 3 l2isolation disable
wcfg ssid 3 macfilter disable
wcfg ssid save
```

**Figure 294** WPA Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 14
wcfg security 4 name Test-wpa
wcfg security 4 mode wpa
wcfg security 4 reauthtime 1800
wcfg security 4 idletime 3600
wcfg security 4 groupkeytime 1800
wcfg security save
wcfg radius 4 name radius-rd1
wcfg radius 4 primary 172.0.20.38 1812 20 enable
wcfg radius 4 backup 172.0.20.39 1812 20 enable
wcfg radius save
wcfg ssid 4 name ssid-wpa
wcfg ssid 4 security Test-wpa
wcfg ssid 4 qos 4
wcfg ssid 4 l2isolation disable
wcfg ssid 4 macfilter disable
wcfg ssid save
```

### Wlan Command Configuration File Example

This example configuration file uses the `wlan` command to configure the AP to use the security and SSID profiles from the `wcfg` command configuration file examples and general wireless settings. You could actually combine all of this chapter's example configuration files into a single configuration file. Remember that the commands are applied in order. So for example, you would place the



commands that create security and SSID profiles before the commands that tell the AP to use those profiles.

**Figure 295** Wlan Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 15
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 4 name ssid-wpa2psk
wcfg ssid 4 security Test-wpa2psk
wcfg ssid save
!line starting with '!' is comment
!change to channel 8
wlan chid 8
!change operating mode -> AP mode,
!then select ssid-wep as running WLAN profile
wlan opmode 0
wlan ssidprofile ssid-wep
!change operating mode -> MBSSID mode,
!then select ssid-wpapsk, ssid-wpa2psk as running WLAN profiles
wlan opmode 3
wlan ssidprofile ssid-wpapsk ssid-wpa2psk
! set output power level to 50%
wlan output power 2
```



# Legal Information

## Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimer

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.

## Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

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

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

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

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

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



### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- 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.

## 注意！

依據 低功率電波輻射性電機管理辦法

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

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

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

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

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。

## 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 has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

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.

## 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 materials or workmanship for a period of up to two years from the date of purchase. 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](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](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

# Index

## A

access [24](#)  
access point [24](#)  
access privileges [26](#)  
address [110](#)  
address assignment [110](#), [177](#)  
address filtering [23](#)  
administrator authentication on RADIUS [111](#)  
Advanced Encryption Standard  
  See AES.  
AES [329](#)  
alternative subnet mask notation [372](#)  
antenna [285](#), [286](#)  
  directional [334](#)  
  gain [333](#)  
  omni-directional [334](#)  
AP [23](#), [24](#), [25](#), [179](#), [321](#)  
AP (access point) [122](#)  
AP+Bridge [23](#), [25](#)  
applications [23](#)  
  Access Point [24](#)  
  AP/Bridge [26](#)  
  Bridge/Repeater [24](#)  
  MBSSID [26](#)  
ATC [138](#), [145](#)  
ATC+WMM [145](#)  
ATM [138](#)  
authentication server [23](#)  
auto configuration [379](#)  
auto configuration status [382](#)

## B

backup [272](#)  
Basic Service Set [120](#)  
  see BSS  
bridge [24](#), [25](#)

Bridge Protocol Data Units (BPDUs) [132](#)  
Bridge/Repeater [23](#), [24](#)  
BSS [26](#), [319](#)  
BSSID [23](#)

## C

CA [224](#), [327](#)  
CAPWAP [47](#), [53](#)  
Certificate Authority  
  See CA.  
certificates [201](#)  
  CA [224](#)  
  thumbprint algorithms [225](#)  
  thumbprints [225](#)  
  verifying fingerprints [225](#)  
Certification Authority. See CA.  
certifications [387](#)  
  notices [389](#)  
  viewing [389](#)  
channel [24](#), [122](#), [321](#)  
  interference [321](#)  
command interface [29](#)  
configuration [23](#)  
configuration file  
  examples [383](#)  
  format [381](#)  
configuration file rules [382](#)  
Control and Provisioning of Wireless Access  
  Points  
  See CAPWAP  
copyright [387](#)  
CTS (Clear to Send) [322](#)

## D

default [274](#)  
DFS [133](#)

dimensions [285](#)  
disclaimer [387](#)  
Distribution System [120](#)  
Dynamic Frequency Selection [133](#)  
dynamic WEP key exchange [328](#)

## E

EAP authentication [326](#)  
encryption [26](#), [329](#)  
ESS [120](#), [320](#)  
ESS IDentification [120](#)  
ESSID [283](#)  
Extended Service Set [120](#)  
    see ESS  
Extended Service Set IDentification [122](#), [125](#),  
    [131](#)

## F

FCC interference statement [387](#)  
file version [381](#)  
filtering [23](#)  
firmware file  
    maintenance [266](#)  
fragmentation threshold [323](#)  
friendly AP list [180](#), [183](#)  
FTP [30](#), [189](#)  
    restrictions [189](#)

## G

general setup [112](#)  
guest SSID [27](#)

## H

hidden node [321](#)  
honeypot attack [181](#)  
host [114](#)

host ID [110](#)  
humidity [285](#), [286](#)

## I

IANA [110](#), [378](#)  
IBSS [319](#)  
IEEE 802.11g [323](#)  
IEEE 802.1x [23](#)  
in-band management [240](#)  
Independent Basic Service Set [270](#)  
    see IBSS  
initialization vector (IV) [329](#)  
installation [23](#)  
interference [24](#)  
internal authentication server [23](#)  
Internal RADIUS Server Setting Screen [200](#)  
Internet Assigned Numbers Authority  
    See IANA  
Internet security gateway [23](#)  
Internet telephony [27](#)  
IP address [110](#), [177](#), [286](#)  
IPSec VPN capability [286](#)  
isolation [23](#)

## L

LAN [268](#)  
layer-2 isolation [23](#), [27](#)  
LEDs [32](#)  
log descriptions [232](#)  
logs [227](#)

## M

MAC address [23](#), [166](#), [172](#)  
MAC address filter action [173](#)  
MAC filter [27](#)  
MAC filtering [287](#)  
MAC service data unit [65](#), [125](#)



maintenance [23](#)  
management [23](#)  
Management Information Base (MIB) [196](#)  
management VLAN [240](#)  
managing the device  
  good habits [31](#)  
  using FTP. See FTP.  
  using Telnet. See command interface.  
  using the command interface. See command interface.  
mask [110](#)  
max age [132](#)  
MBSSID [23](#), [26](#)  
Message Integrity Check (MIC) [329](#)  
mobile access [23](#)  
mode [23](#)  
MSDU [65](#), [125](#)

## N

NAT [377](#)  
network [23](#)  
network access [23](#)  
network bridge [24](#)  
network number [110](#)  
network traffic [23](#)

## O

operating mode [23](#)  
out-of-band management [240](#)

## P

Pairwise Master Key (PMK) [329](#), [331](#)  
password [113](#), [286](#)  
path cost [132](#)  
PoE [290](#)  
power specification [285](#)  
power specifications [285](#), [290](#)  
preamble mode [323](#)

pre-configured profiles [27](#)  
priorities [138](#)  
prioritization [23](#)  
private IP address [110](#), [177](#)  
private networks [110](#)  
product registration [390](#)  
PSK [329](#)

## Q

QoS [23](#), [137](#), [145](#)  
QoS priorities [138](#)  
Quick Start Guide [35](#)

## R

radio [24](#)  
RADIUS [325](#)  
  message types [325](#)  
  messages [325](#)  
  shared secret key [326](#)  
rapid STP [131](#)  
reauthentication time [153](#), [155](#), [156](#), [157](#), [158](#)  
registration  
  product [390](#)  
related documentation [3](#)  
remote management limitations [188](#)  
repeater [24](#)  
reset button [285](#)  
restore [273](#)  
RF interference [24](#)  
roaming [133](#)  
  requirements [135](#)  
rogue AP [23](#), [179](#), [180](#), [181](#), [182](#), [183](#)  
root bridge [132](#)  
RTS (Request To Send) [322](#)  
  threshold [321](#), [322](#)  
RTS/CTS handshake [65](#), [125](#)

**S**

- safety warnings [7](#)
- security [24](#)
- security profiles [23](#)
- server [23](#)
- Service Set [122](#), [125](#), [131](#)
- Service Set Identifier
  - see SSID
- SNMP [287](#)
  - MIBs [196](#)
  - traps [196](#)
- specifications [290](#)
- SSID [26](#)
- SSID profile [142](#)
  - pre-configured [27](#)
- SSID profiles [26](#), [27](#)
- STP [131](#)
- STP - how it works [132](#)
- STP (Spanning Tree Protocol) [286](#)
- STP path costs [132](#)
- STP port states [133](#)
- STP terminology [132](#)
- subnet [369](#)
- subnet mask [110](#), [286](#), [370](#)
- subnetting [373](#)
- syntax conventions [5](#)
- system name [112](#)
- system timeout [190](#)

**T**

- tagged VLAN example [240](#)
- telnet [190](#)
- temperature [285](#), [286](#)
- Temporal Key Integrity Protocol (TKIP) [329](#)
- text file based auto configuration [287](#), [379](#)
- TFTP restrictions [189](#)
- time setting [116](#)
- time-sensitive [23](#)
- trademarks [387](#)
- traffic security [23](#)

**U**

- use [23](#)

**V**

- Virtual Local Area Network [235](#)
- VLAN [235](#), [255](#), [261](#)
- VoIP [23](#), [27](#), [145](#)
- VoIP SSID [27](#)

**W**

- warranty [389](#)
  - note [390](#)
- wcfc command [383](#)
- WDS [24](#), [26](#), [136](#)
- web configurator [23](#), [35](#), [37](#)
- WEP [23](#)
- WEP encryption [152](#)
- Wi-Fi Multimedia QoS [137](#)
- Wi-Fi Protected Access [23](#), [328](#)
- wired network [23](#), [24](#)
- wireless channel [283](#)
- wireless client WPA supplicants [330](#)
- Wireless Distribution System (WDS) [26](#)
- wireless Internet connection [24](#)
- wireless LAN [283](#)
- wireless security [27](#), [147](#), [283](#), [324](#)
- WLAN
  - interference [321](#)
  - security parameters [332](#)
- WLAN interface [24](#)
- WMM [137](#), [145](#)
- WMM priorities [138](#)
- WPA [23](#), [328](#)
  - key caching [330](#)
  - pre-authentication [330](#)
  - user authentication [330](#)
  - vs WPA-PSK [329](#)
  - wireless client supplicant [330](#)
  - with RADIUS application example [330](#)

- WPA2 [23](#), [328](#)
  - user authentication [330](#)
  - vs WPA2-PSK [329](#)
  - wireless client supplicant [330](#)
  - with RADIUS application example [330](#)
- WPA2-Pre-Shared Key [328](#)
- WPA2-PSK [328](#), [329](#)
  - application example [331](#)
- WPA-PSK [329](#)
  - application example [331](#)

