

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 2, 8/2009

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 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

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 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 expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on top of 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. (Note: The NWA is an indoor device.)
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- 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

Introduction	21
Introducing the NWA	23
The Web Configurator	37
Tutorial	41
The Web Configurator	81
Status Screens	83
Management Mode	87
AP Controller Mode	93
System Screens	109
Wireless Configuration	119
SSID Screen	145
Wireless Security Screen	155
RADIUS Screen	169
Layer-2 Isolation Screen	173
MAC Filter Screen	179
IP Screen	183
Rogue AP Detection	187
Remote Management Screens	195
Internal RADIUS Server	209
Certificates	217
Log Screens	235
VLAN	245
Load Balancing	265
Dynamic Channel Selection	271
Maintenance	275
Troubleshooting and Specifications	287
Troubleshooting	289
Product Specifications	297
Appendices and Index	303

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Safety Warnings.....	7
Contents Overview	9
Table of Contents.....	11
Part I: Introduction.....	21
Chapter 1	
Introducing the NWA	23
1.1 Overview	23
1.2 Applications for the NWA	24
1.2.1 Access Point	24
1.2.2 Bridge / Repeater	25
1.2.2.1 Bridge / Repeater Mode Example	26
1.2.3 AP + Bridge	28
1.2.4 MBSSID	28
1.2.5 Pre-Configured SSID Profiles	30
1.2.6 Configuring Dual WLAN Adaptors	30
1.3 CAPWAP	31
1.4 Ways to Manage the NWA	32
1.5 Good Habits for Managing the NWA	32
1.6 Configuring Your NWA's Security Features	32
1.6.1 Control Access to Your Device	33
1.6.2 Wireless Security	33
1.7 Hardware Connections	34
1.7.1 Antennas	34
1.8 LEDs	34
Chapter 2	
The Web Configurator	37
2.1 Overview	37
2.2 Accessing the Web Configurator	37
2.3 Resetting the NWA	38

2.3.1 Methods of Restoring Factory-Defaults	38
2.4 Navigating the Web Configurator	39
Chapter 3	
Tutorial.....	41
3.1 Overview	41
3.2 How to Configure the Wireless LAN	41
3.2.1 Choosing the Wireless Mode	41
3.2.2 Wireless LAN Configuration Overview	42
3.2.3 Further Reading	43
3.3 How to Configure Multiple Wireless Networks	43
3.3.1 Change the Operating Mode	45
3.3.1.1 Access Point	45
3.3.1.2 MBSSID	46
3.3.2 Configure the VoIP Network	47
3.3.2.1 Set Up Security for the VoIP Profile	48
3.3.2.2 Activate the VoIP Profile	50
3.3.3 Configure the Guest Network	50
3.3.3.1 Set Up Security for the Guest Profile	52
3.3.3.2 Set up Layer 2 Isolation	53
3.3.3.3 Activate the Guest Profile	54
3.3.4 Testing the Wireless Networks	54
3.4 How to Set Up and Use Rogue AP Detection	55
3.4.1 Set Up and Save a Friendly AP list	57
3.4.2 Activate Periodic Rogue AP Detection	60
3.4.3 Set Up E-mail Logs	61
3.4.4 Configure Your Other Access Points	62
3.4.5 Test the Setup	63
3.5 Using MAC Filters and L-2 Isolation Profiles	63
3.5.1 Scenario	63
3.5.2 Your Requirements	64
3.5.3 Setup	64
3.5.4 Configure the SERVER_1 Network	65
3.5.5 Configure the SERVER_2 Network	68
3.5.6 Checking your Settings and Testing the Configuration	69
3.5.6.1 Checking Settings	69
3.5.6.2 Testing the Configuration	70
3.6 How to Configure Management Modes	71
3.6.1 Scenario	71
3.6.2 Your Requirements	72
3.6.3 Setup	72
3.6.4 Configure Your NWA in Controller AP Mode	73
3.6.4.1 Secondary AP Controller	74

3.6.4.2 Primary AP Controller	75
3.6.5 Setting Your NWA in Managed AP Mode	75
3.6.6 Configuring the Managed Access Points List	76
3.6.7 Checking your Settings and Testing the Configuration	79
Part II: The Web Configurator	81
Chapter 4	
Status Screens	83
4.1 Overview	83
4.2 The Status Screen	83
4.2.1 System Statistics Screen	86
Chapter 5	
Management Mode.....	87
5.1 Overview	87
5.2 About CAPWAP	87
5.2.1 CAPWAP Discovery and Management	88
5.2.2 CAPWAP and DHCP	88
5.2.3 CAPWAP and IP Subnets	88
5.2.4 Notes on CAPWAP	89
5.3 The Management Mode Screen	90
Chapter 6	
AP Controller Mode	93
6.1 Overview	93
6.1.1 What You Can Do in AP Controller Mode	93
6.1.2 What You Need to Know	93
6.1.3 Before You Begin	94
6.2 Controller AP Navigation Menu	94
6.3 Controller AP Status Screen	95
6.4 AP Lists Screen	97
6.4.1 The AP Lists Edit Screen	100
6.5 Configuration Screen	101
6.6 Redundancy Screen	102
6.7 The Profile Edit Screens	102
6.7.1 The Radio Profile Screen	103
6.7.2 The Radio Profile Edit Screen	104
Chapter 7	
System Screens	109

7.1 Overview	109
7.1.1 What You Can Do in the System Screens	109
7.1.2 What You Need To Know About the System Screens	110
7.2 General Screen	111
7.3 Password Screen	113
7.4 Time Setting Screen	115
7.5 Technical Reference	117
7.5.1 Administrator Authentication on RADIUS	117
7.5.2 Pre-defined NTP Time Servers List	117
Chapter 8	
Wireless Configuration.....	119
8.1 Overview	119
8.2 What You Can Do in the Wireless Screen	119
8.2.1 What You Need To Know About the Wireless Screen	120
8.3 The Wireless Screen	123
8.3.1 Access Point Mode	123
8.3.2 Bridge / Repeater Mode	126
8.3.3 AP + Bridge Mode	131
8.3.4 MBSSID Mode	136
8.4 Technical Reference	139
8.4.1 Spanning Tree Protocol (STP)	139
8.4.1.1 Rapid STP	139
8.4.1.2 STP Terminology	140
8.4.1.3 How STP Works	140
8.4.1.4 STP Port States	141
8.4.2 DFS	141
8.4.3 Roaming	141
8.4.3.1 Requirements for Roaming	143
Chapter 9	
SSID Screen.....	145
9.1 Overview	145
9.1.1 What You Can Do in the SSID Screen	145
9.1.2 What You Need To Know About SSID	146
9.2 The SSID Screen	147
9.2.1 Configuring SSID	148
9.3 Technical Reference	149
9.3.1 WMM QoS	149
9.3.1.1 WMM QoS Priorities	150
9.3.2 ATC	150
9.3.3 ATC+WMM	151
9.3.3.1 ATC+WMM from LAN to WLAN	152

9.3.3.2 ATC+WMM from WLAN to LAN	152
9.3.4 Type Of Service (ToS)	152
9.3.4.1 DiffServ	152
9.3.4.2 DSCP and Per-Hop Behavior	153
9.3.4.3 ToS (Type of Service) and WMM QoS	153
Chapter 10	
Wireless Security Screen	155
10.1 Overview	155
10.1.1 What You Can Do in the Wireless Security Screen	155
10.1.2 What You Need To Know About Wireless Security	156
10.2 The Security Screen	157
10.2.1 Security: WEP	159
10.2.2 Security: 802.1x Only	161
10.2.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit	162
10.2.4 Security: WPA	163
10.2.5 Security: WPA2 or WPA2-MIX	164
10.2.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX	166
10.3 Technical Reference	167
Chapter 11	
RADIUS Screen	169
11.1 Overview	169
11.1.1 What You Can Do in the RADIUS Screen	170
11.1.2 What You Need To Know About RADIUS	170
11.2 The RADIUS Screen	171
Chapter 12	
Layer-2 Isolation Screen	173
12.1 Overview	173
12.1.1 What You Can Do in the Layer-2 Isolation Screen	174
12.1.2 What You Need To Know About Layer-2 Isolation	174
12.2 The Layer-2 Isolation Screen	175
12.2.1 Configuring Layer-2 Isolation	176
12.3 Technical Reference	177
Chapter 13	
MAC Filter Screen	179
13.1 Overview	179
13.1.1 What You Can Do in the MAC Filter Screen	179
13.1.2 What You Should Know About MAC Filter	179
13.2 The MAC Filter Screen	180
13.2.1 Configuring the MAC Filter	180

Chapter 14	
IP Screen.....	183
14.1 Overview	183
14.1.1 What You Can Do in the IP Screen	183
14.1.2 What You Need To Know About IP	183
14.2 The IP Screen	184
14.3 Technical Reference	185
14.3.1 WAN IP Address Assignment	185
Chapter 15	
Rogue AP Detection	187
15.1 Overview	187
15.1.1 What You Can Do in the Rogue AP Screen	188
15.1.2 What You Need To Know About Rogue AP	188
15.2 Configuration Screen	190
15.2.1 Friendly AP Screen	191
15.2.2 Rogue AP Screen	192
Chapter 16	
Remote Management Screens.....	195
16.1 Overview	195
16.1.1 What You Can Do in the Remote Management Screens	196
16.1.2 What You Need To Know About Remote Management	196
16.2 The Telnet Screen	198
16.3 The FTP Screen	199
16.4 The WWW Screen	200
16.5 The SNMP Screen	203
16.5.1 SNMPv3 User Profile	205
16.6 Technical Reference	206
16.6.1 MIB	206
16.6.2 Supported MIBs	207
16.6.3 SNMP Traps	207
Chapter 17	
Internal RADIUS Server	209
17.1 Overview	209
17.1.1 What You Can Do in this Chapter	210
17.1.2 What You Need To Know	210
17.2 Internal RADIUS Server Setting Screen	210
17.3 The Trusted AP Screen	212
17.4 The Trusted Users Screen	213
17.5 Technical Reference	214

Chapter 18	
Certificates	217
18.1 Overview	217
18.1.1 What You Can Do in the Certificates Screen	217
18.1.2 What You Need To Know About Certificates	218
18.2 My Certificates Screen	218
18.2.1 My Certificates Import Screen	220
18.2.2 My Certificates Create Screen	222
18.2.3 My Certificates Details Screen	225
18.3 Trusted CAs Screen	228
18.3.1 Trusted CAs Import Screen	229
18.3.2 Trusted CAs Details Screen	230
18.4 Technical Reference	233
18.4.1 Private-Public Certificates	233
18.4.2 Certification Authorities	233
18.4.3 Checking the Fingerprint of a Certificate	234
Chapter 19	
Log Screens	235
19.1 Overview	235
19.1.1 What You Can Do in the Log Screens	235
19.1.2 What You Need To Know About Logs	236
19.2 The View Log Screen	236
19.3 The Log Settings Screen	238
19.4 Technical Reference	240
19.4.1 Example Log Messages	240
19.4.2 Log Commands	242
19.4.3 Configuring What You Want the NWA to Log	242
19.4.4 Displaying Logs	242
19.4.5 Log Command Example	243
Chapter 20	
VLAN	245
20.1 Overview	245
20.1.1 What You Can Do in the VLAN Screen	245
20.1.2 What You Need To Know About VLAN	246
20.2 Wireless VLAN Screen	247
20.2.1 RADIUS VLAN Screen	248
20.3 Technical Reference	250
20.3.1 VLAN Tagging	250
20.3.2 Configuring Management VLAN Example	250
20.3.3 Configuring Microsoft's IAS Server Example	253
20.3.3.1 Configuring VLAN Groups	254

20.3.3.2 Configuring Remote Access Policies	255
20.3.4 Second Rx VLAN ID Example	263
20.3.4.1 Second Rx VLAN Setup Example	263
Chapter 21	
Load Balancing	265
21.1 Overview	265
21.1.1 What You Need to Know About Load Balancing	265
21.2 The Load Balancing Screen	267
21.2.1 Disassociating and Delaying Connections	268
Chapter 22	
Dynamic Channel Selection.....	271
22.1 Overview	271
22.2 The DCS Screen	272
Chapter 23	
Maintenance	275
23.1 Overview	275
23.2 What You Can Do in the Maintenance Screens	275
23.3 What You Need To Know	275
23.4 System Status Screen	276
23.4.1 Show Statistics Screen	276
23.5 Association List Screen	278
23.6 Channel Usage Screen	279
23.7 F/W Upload Screen	280
23.8 Configuration Screen	282
23.8.1 Backup Configuration	282
23.8.2 Restore Configuration	283
23.8.3 Back to Factory Defaults	284
23.9 Restart Screen	284
Part III: Troubleshooting and Specifications.....	287
Chapter 24	
Troubleshooting.....	289
24.1 Overview	289
24.2 Power, Hardware Connections, and LEDs	289
24.3 NWA Access and Login	290
24.4 AP Management Modes	292
24.5 Internet Access	294

24.6 Wireless Router/AP Troubleshooting	295
Chapter 25	
Product Specifications	297
Part IV: Appendices and Index	303
Appendix A Setting Up Your Computer's IP Address.....	305
Appendix B Wireless LANs	331
Appendix C Pop-up Windows, JavaScripts and Java Permissions.....	347
Appendix D Importing Certificates.....	355
Appendix E IP Addresses and Subnetting	381
Appendix F Text File Based Auto Configuration	391
Appendix G Legal Information.....	399
Index.....	403

PART I

Introduction

Introducing the NWA (23)

The Web Configurator (37)

Status Screens (83)

Management Mode (87)

Tutorial (41)

Introducing the NWA

Note: This User's Guide includes the NWA-3500 and the NWA-3550. Illustrations used throughout this book are based on the NWA-3500 (unless otherwise stated). The Web Configuration screens are based on the NWA-3500 (unless otherwise stated).

1.1 Overview

This chapter introduces the main applications and features of the NWA. It also introduces the ways you can manage 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, featuring dual wireless modules and supporting up to eight Basic Service Set Identifiers (BSSID) 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.

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

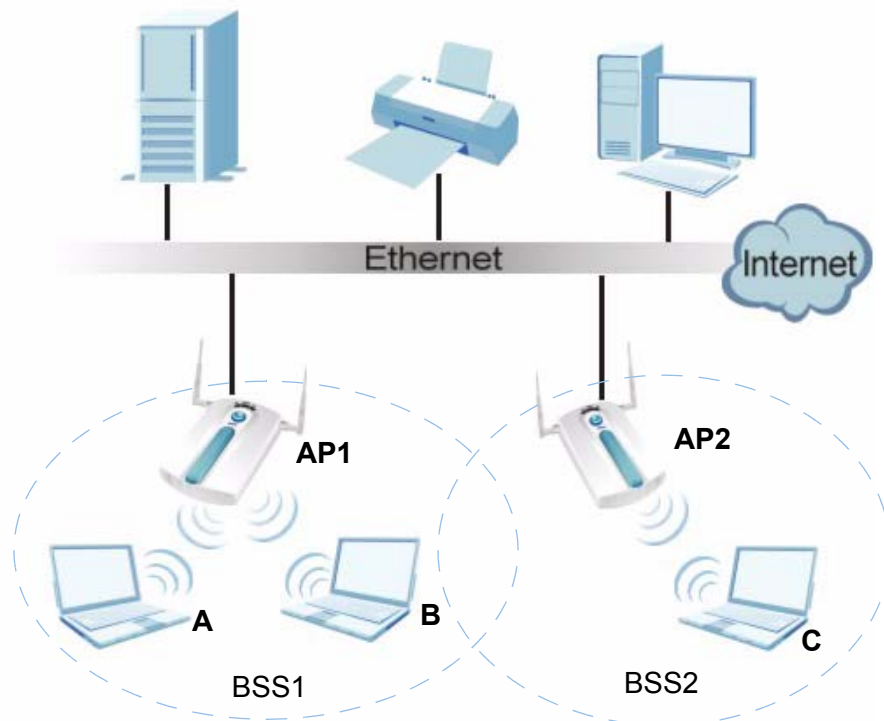
Applications for each operating mode are shown below.

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** in Figure 3) has no Ethernet connection. When the NWA is in bridge mode, you should enable Spanning Tree Protocol (STP) to prevent bridge loops.

When the NWA is in Bridge / Repeater mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See [Section 8.2.2 on page 127](#) 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

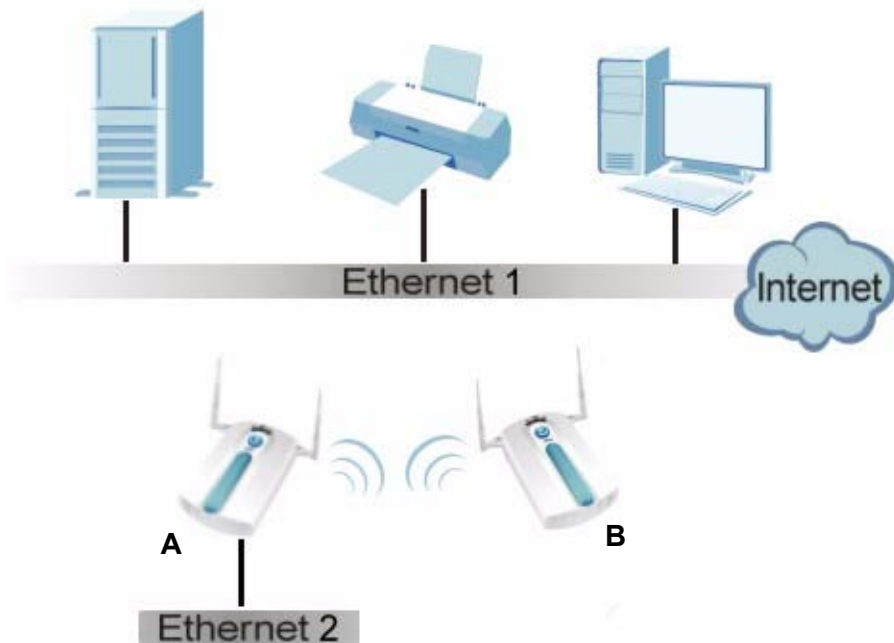
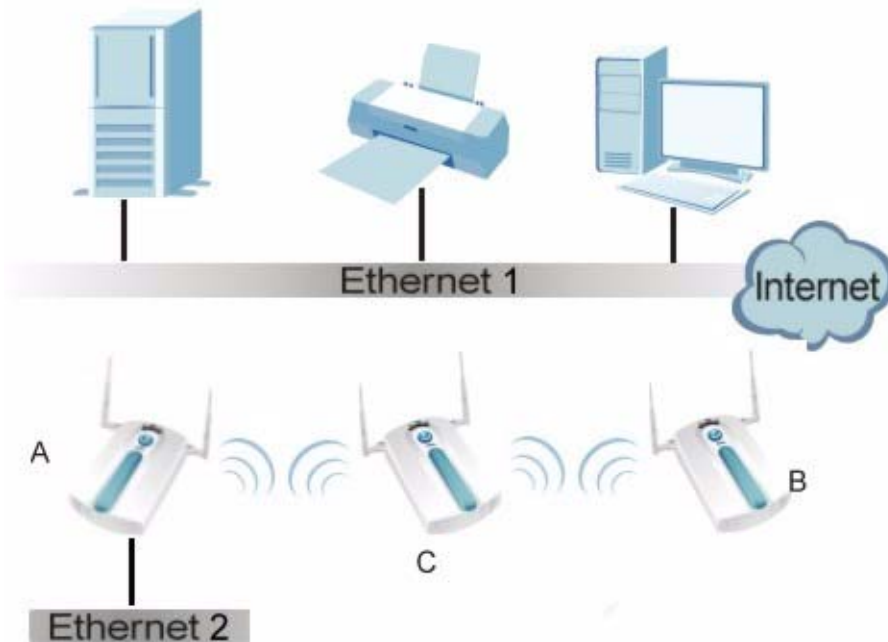
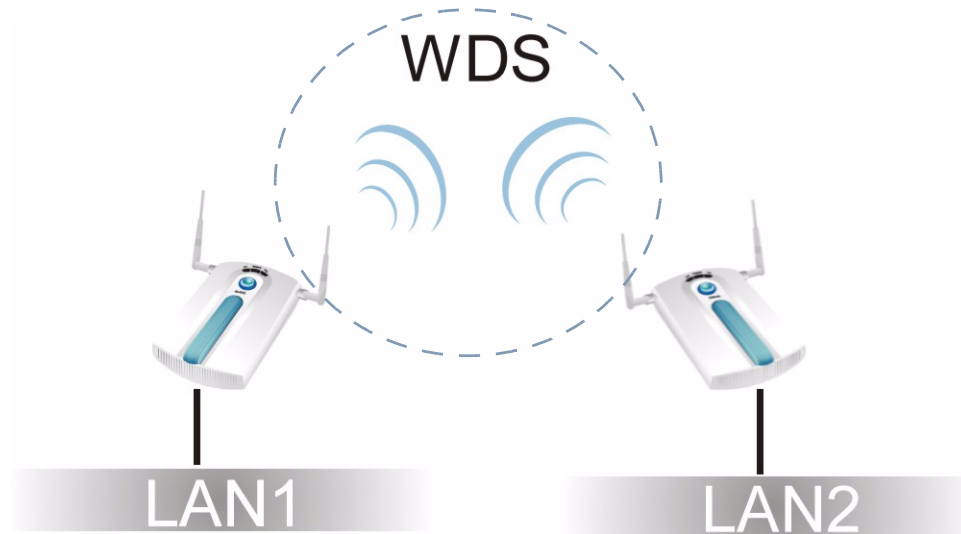


Figure 3 Repeater Application

1.2.2.1 Bridge / Repeater Mode Example

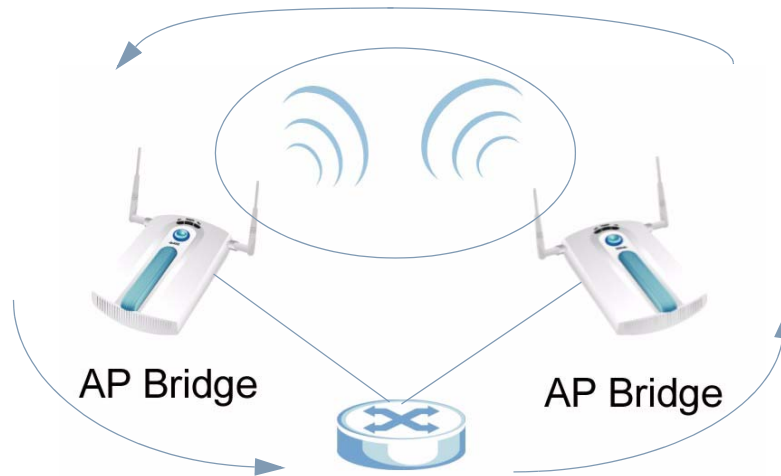
In the example below, when both NWAs are in Bridge / Repeater mode, they form a WDS (Wireless Distribution System) allowing the computers in **LAN 1** to connect to the computers in **LAN 2**.

Figure 4 Bridging Example

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

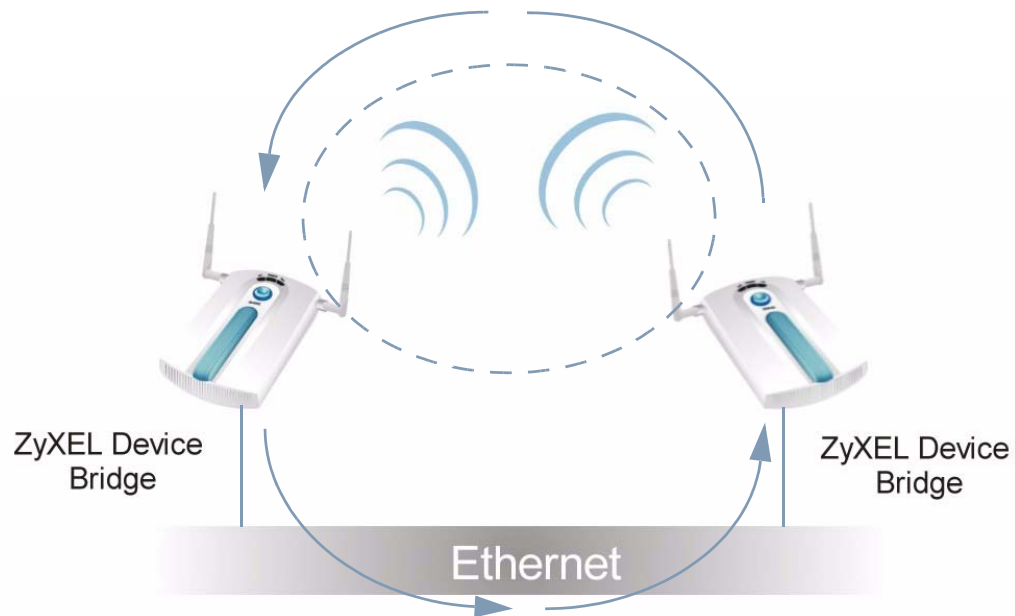
- If two or more NWAs (in bridge mode) are connected to the same hub.

Figure 5 Bridge Loop: Two Bridges Connected to Hub



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

Figure 6 Bridge Loop: Bridge Connected to Wired LAN



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

1.2.3 AP + Bridge

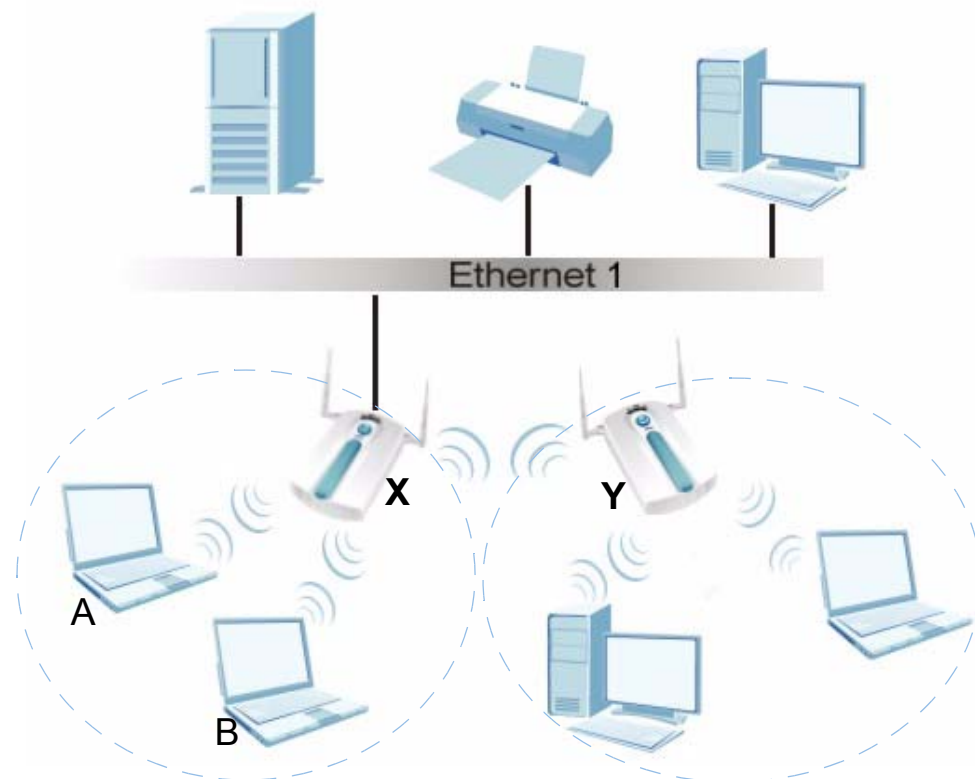
In AP + Bridge mode, the NWA supports both AP and bridge connection at the same time.

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

When the NWA is in AP + Bridge mode, security between APs (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.

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

Figure 7 AP + Bridge Application



1.2.4 MBSSID

A Basic Service Set (BSS) is the set of devices forming a single wireless network (usually an access point and one or more wireless clients). The Service Set Identifier (SSID) is the name of a BSS. In Multiple BSS (MBSSID) mode, the NWA

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

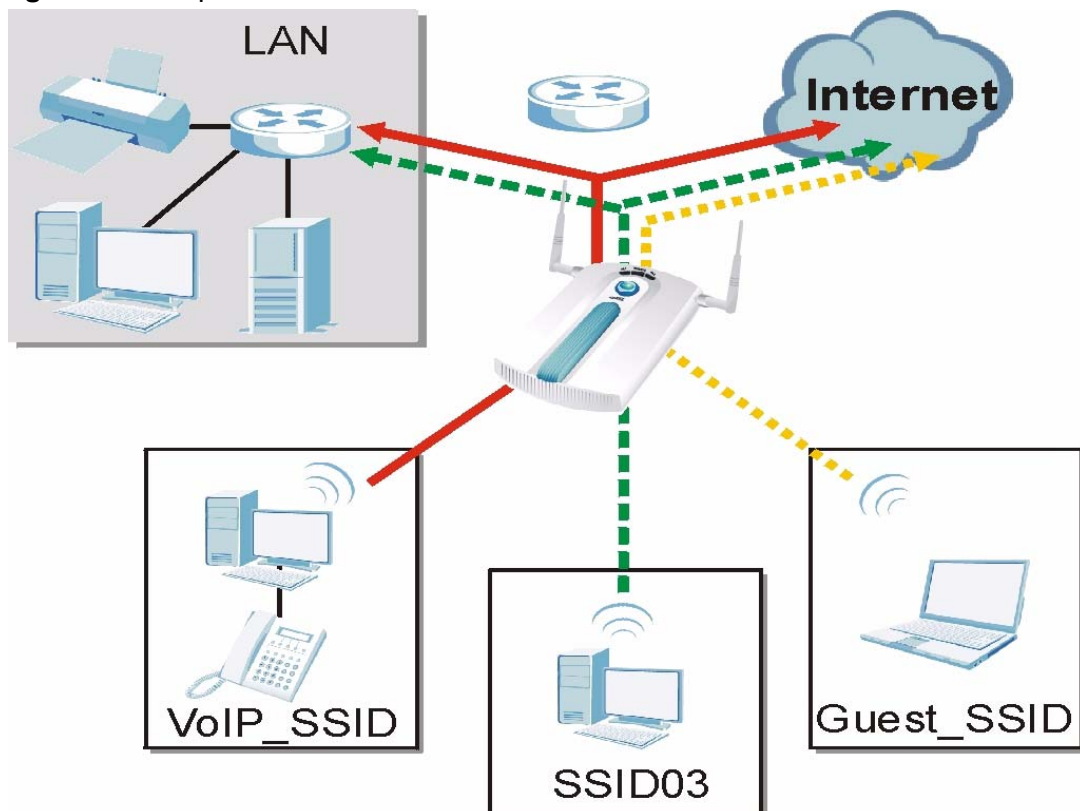
You can configure up to sixteen SSID profiles, and have up to eight active at any one time.

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 (VoIP) users have priority. You also want a regular wireless network for standard users, as well as a 'guest' wireless network for visitors. In the following figure, **VoIP_SSID** users have QoS priority, **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 Land Area Network (LAN) behind the AP and can access only the Internet.

Figure 8 Multiple BSSs



1.2.5 Pre-Configured SSID Profiles

The NWA has two pre-configured SSID profiles.

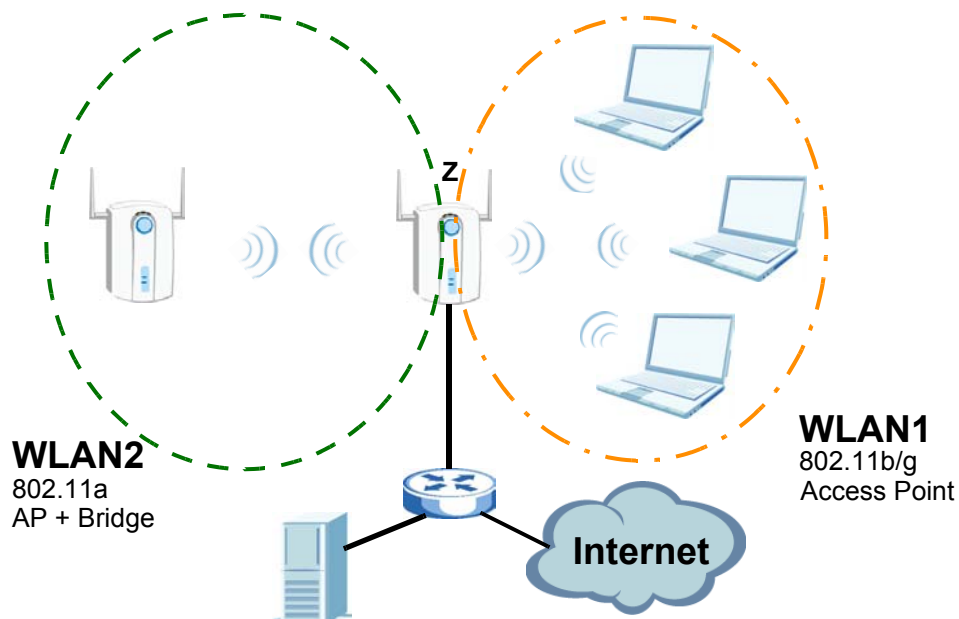
- **VoIP_SSID.** This profile is intended for use by wireless clients requiring the highest QoS level for VoIP telephony and other applications requiring low latency. The QoS level of this profile is not user-configurable.
- **Guest_SSID.** This profile is intended for use by visitors and others who 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 178](#)), and QoS is set to **NONE**. Intra-BSS traffic blocking is also enabled (see [Section 8.1.2 on page 120](#)). 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 9 Dual WLAN Adaptors Example



1.3 CAPWAP

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

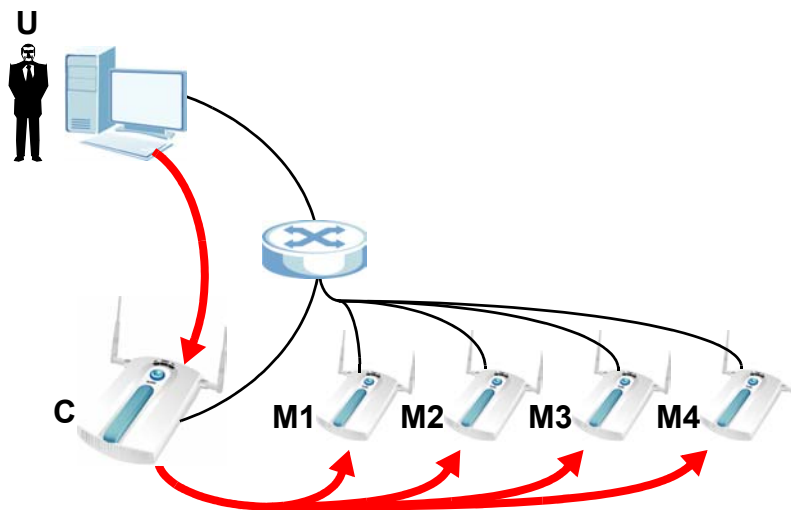
ZyXEL's CAPWAP allows a single access point to manage up to eight other access points. The managed APs receive all their configuration information from the controller AP. The CAPWAP dataflow is protected by Datagram Transport Layer Security (DTLS).

The following ZyXEL AP models can be CAPWAP managed APs:

- NWA-3160
- NWA-3163
- NWA-3500
- NWA-3550
- NWA-3166

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 10 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 (CLI).** Line commands are mostly used for troubleshooting by service engineers.
- **File Transfer Protocol (FTP).** This protocol can be used for firmware upgrades and configuration backup and restore.
- **Simple Network Management Protocol (SNMP).** The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.5 Good Habits for Managing the NWA

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

- Change the password often. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NWA to its factory default settings. If you backed up an earlier configuration file, you won't have to totally re-configure the NWA; you can simply restore your last configuration.
- Check the ZyXEL website (www.zyxel.com.tw) regularly for new firmware for your NWA. Ensure you download the correct firmware for your model.

1.6 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.

1.6.1 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 195](#) 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.

1.6.2 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 10.2 on page 157](#) 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 8.2.1 on page 120](#) 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 13.2 on page 180](#) for directions on configuring the MAC filter.

1.7 Hardware Connections

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

1.7.1 Antennas

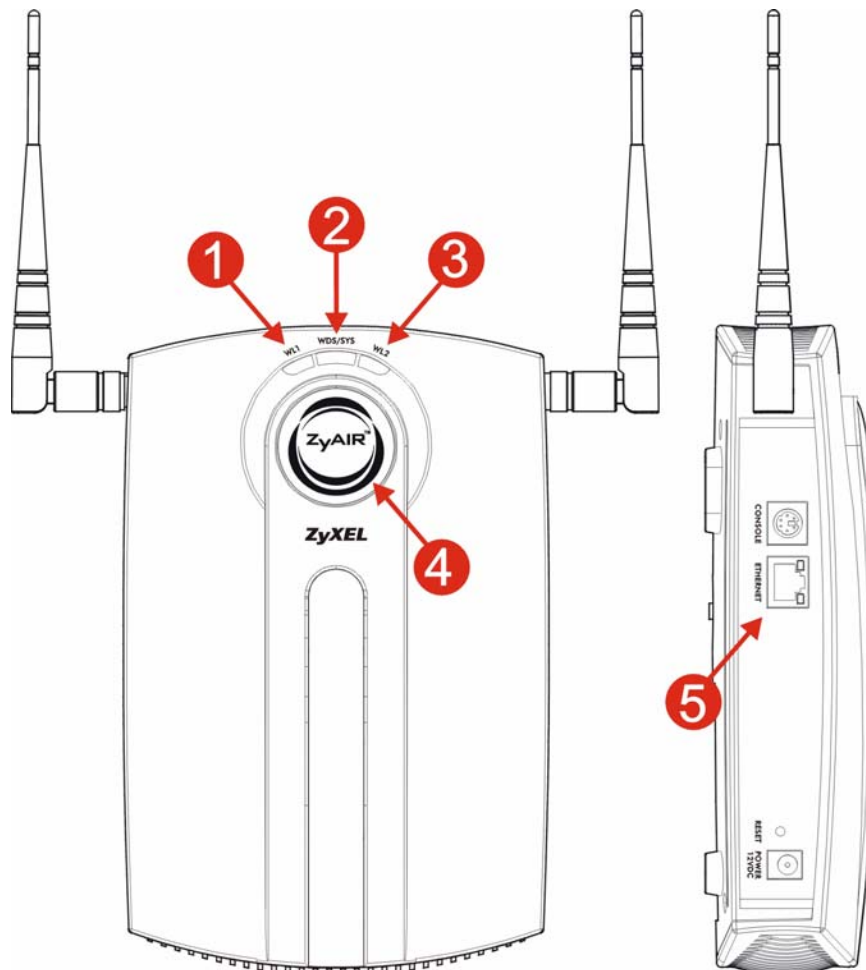
Your NWA has two wireless LAN adaptors, WLAN1 and WLAN2.

WLAN1 uses the **RF1** antenna or the antenna on the right (when facing the device). 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 11 LEDs



The following table describes the behavior of the device 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.
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 Enable Breathing LED in Section 8.3 on page 123 .
			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 Section 8.3 on page 123 for how to enable the ZyAIR LED.

LABEL	LED	COLOR	STATUS	DESCRIPTION
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.

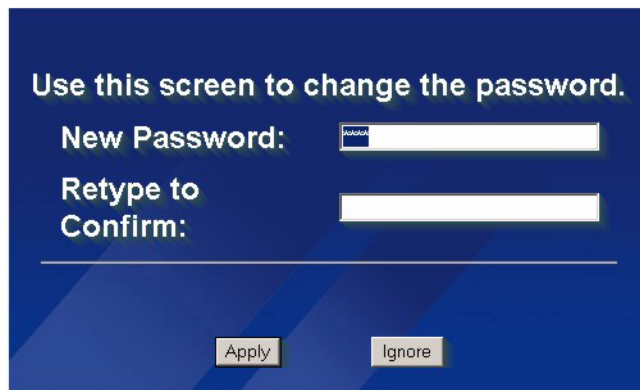
The Web Configurator

2.1 Overview

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

2.2 Accessing the Web Configurator

- 1 Make sure your hardware is properly connected and prepare your computer or computer network to connect to the NWA (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "http://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**.



Use this screen to change the password.

New Password:

Retype to Confirm:

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

- 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.



You should now see the **Status** screen. See [Chapter 2 on page 37](#) 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.

2.3 Resetting the NWA

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button. 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.

2.3.1 Methods of Restoring Factory-Defaults

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

- Use the **RESET** button to upload the default configuration file. Hold this button in for about 10 seconds (the lights will begin to blink). Use this method for cases when the password or IP address of the NWA is not known.
- Use the web configurator to restore defaults (refer to [Section 23.8 on page 282](#)).
- Transfer the configuration file to your NWA using File Transfer Protocol (FTP).

2.4 Navigating the Web Configurator

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

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 12 The Status Screen

ZyXEL

STATUS

Automatic Refresh Interval:

System Information		System Resources				
System Name	NWA-Series	Flash	2/4 MB			
Model	NWA-3500	Memory	17/32 MB			
Firmware Version	V3.70(AAH.1)B2 07/06/2009	CPU	0%			
System UP Time	00:54:23	WLAN1 Associations	0/128			
Current Date Time	00:54:20 2000/01/01	WLAN2 Associations	0/128			
WLAN1 Operating Mode	AP	Interface Status				
WLAN2 Operating Mode	AP	Interface	Status	Rate		
Management VLAN	Disable	LAN	Up	100M/Full		
IP	172.23.31.203	WLAN1	Up(Ch165)	54M		
LAN MAC	00:19:cb:88:81:0c	WLAN2	Up(Ch48)	54M		
WLAN1 MAC	00:19:cb:88:81:0c	SSID Status				
WLAN2 MAC	00:19:cb:88:81:0d	Interface	SSID	BSSID	Security	VLAN
		WLAN1	NWA	00:19:cb:88:81:0c	WPA-PSK	Disabled
		WLAN2	ZyXEL04	00:19:cb:88:81:0d	WPA-PSK	Disabled

System Status

Status: **Ready**

- Click the links on the left of the screen to configure advanced features such as **MGNT MODE** (Controller AP, 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 **Association List**, **Channel Usage**, **F/W (Firmware) Upload**, **Configuration** (Backup, Restore and Default) and **Restart**.

3.1 Overview

This chapter first provides a basic 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.

3.2 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 3.2.3 on page 43](#) for links to more information on each step.

3.2.1 Choosing the Wireless Mode

- Use **Access Point (AP)** 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 25](#) for details.

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

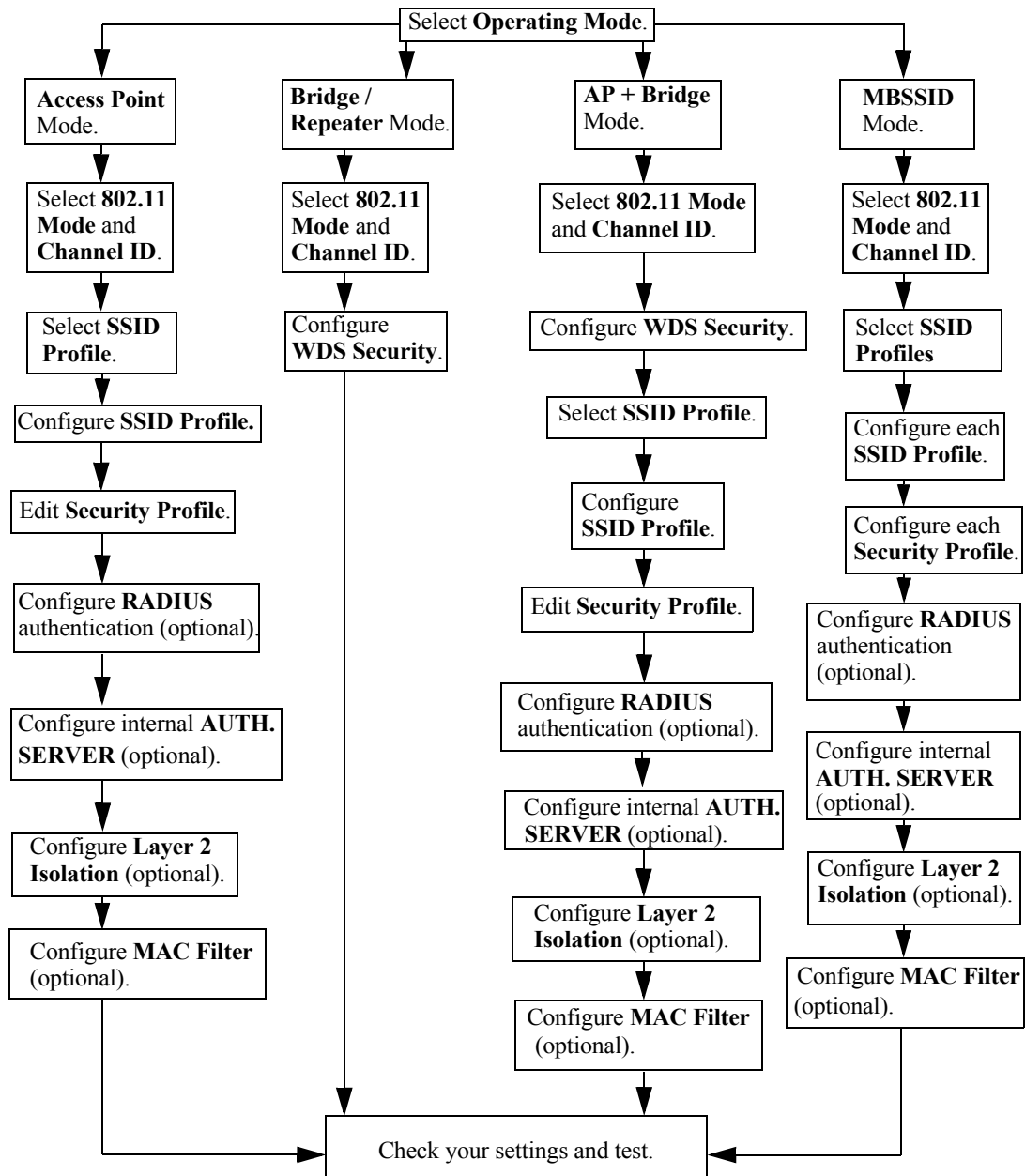
The NWA is a repeater when it has no Ethernet connection and allows other APs to communicate with one another through the NWA.

- 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 1.2.2.1 on page 26](#) for details.
- Use **MBSSID** (Multiple Basic Service Set Identifier) operating mode if you want to use the NWA as an access point with some groups of users having different security or QoS settings from other groups of users. See [Section 1.2.4 on page 28](#) for details.

3.2.2 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 13 Configuring Wireless LAN



3.2.3 Further Reading

Use these links to find more information on the steps:

- Choosing **802.11 Mode**: see [Section 8.2.1 on page 120](#).
- Choosing a wireless **Channel ID**: see [Section 8.2.1 on page 120](#).
- Selecting and configuring **SSID profile(s)**: see [Section 8.2.1 on page 120](#) and [Section 9.2 on page 151](#).
- Configuring and activating **WDS Security**: see [Section 8.2.2 on page 127](#).
- Editing **Security Profile(s)**: see [Section 10.2 on page 161](#).
- Configuring an external **RADIUS** server: see [Section 11.2 on page 175](#).
- Configuring and activating the internal **AUTH. SERVER**: see [Chapter 17 on page 209](#).
- Configuring **Layer 2 Isolation**: see [Section 12.2.1 on page 176](#).
- Configuring **MAC Filtering**: see [Section 13.2 on page 180](#).

3.3 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 8.3.4 on page 136](#)) to provide multiple wireless networks. Each wireless network will cater for a different type of user.

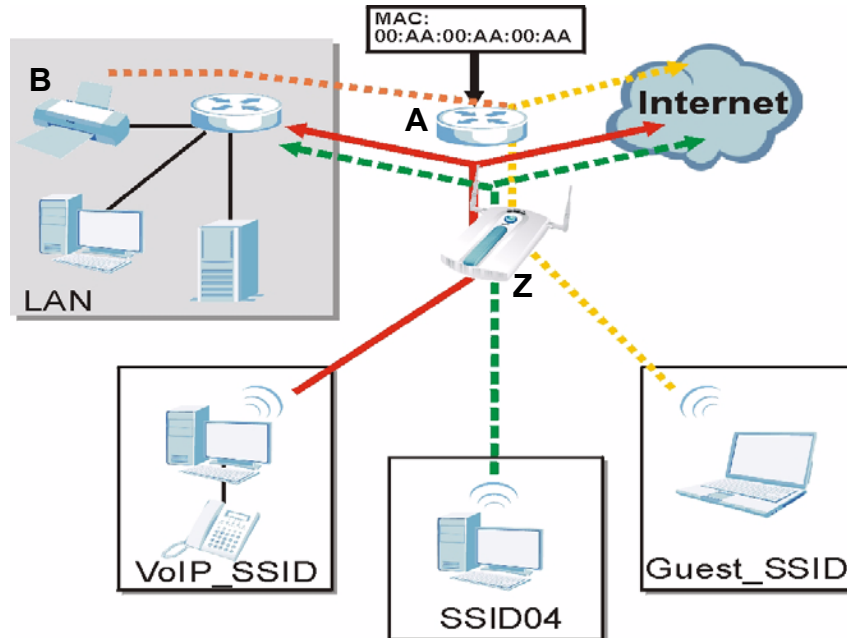
You want to make three wireless networks: one standard office wireless network with all the same settings you already have, another wireless network with high QoS settings for Voice over IP (VoIP) users, and a guest network that allows visitors to your office to access only the Internet and the network 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 VoIP 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 14 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 QoS setting. 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 Media Access Control (MAC) addresses of the devices you want to allow users of the guest network to access. The following table shows the addresses used in this example.

Table 2 Tutorial: Example Information

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

3.3.1 Change the Operating Mode

Log in to the NWA (see [Section 2.2 on page 37](#)). Click **Wireless** > **Wireless**. The **Wireless** screen appears.

3.3.1.1 Access Point

Set the NWA's WLAN Interface **WLAN1** is set to **Access Point** operating mode, and is currently using the **SSID03** profile.

Figure 15 Tutorial: Wireless LAN: Before

The screenshot shows the configuration page for a Wireless LAN interface. The 'Wireless' tab is selected. The 'WLAN Interface' is set to 'WLAN1' and the 'Operating Mode' is set to 'Access Point'. The 'SSID Profile' is set to 'SSID03'. The '802.11 Mode' is set to '802.11b+g'. The 'Super Mode' checkbox is checked. The 'Choose Channel ID' is set to 'Channel-06 2437MHz'. The 'RTS/CTS Threshold' is set to '2346'. The 'Fragmentation Threshold' is set to '2346'. The 'Beacon Interval' is set to '100'. The 'DTIM' is set to '1'. The 'Output Power' is set to '100%'. The 'Rates Configuration' table is shown below, with columns for Rate and Configuration. The 'Enable Antenna Diversity', 'Enable Breathing LED', 'Enable Spanning Tree Protocol (STP)', and 'Enable Roaming' checkboxes are all checked. The 'Apply' and 'Reset' buttons are at the bottom.

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

3.3.1.2 MBSSID

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

Figure 16 Tutorial: Wireless LAN: Change Mode

The screenshot shows the configuration page for a Wireless LAN interface. The **Operating Mode** is set to **MBSSID**. Below this, there are various configuration options for 802.11 Mode, Super Mode, Channel ID, and thresholds. The **Rates Configuration** table shows various rates and their configurations. The **Select SSID Profile** table is highlighted, showing a table with columns for Index, Active, and Profile. The entry for Index 3 is selected, with the Profile set to SSID04. Below the table, there are checkboxes for **Enable Antenna Diversity**, **Enable Breathing LED**, **Enable Spanning Tree Protocol (STP)**, and **Enable Roaming**. The **Apply** and **Reset** buttons are at the bottom.

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

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 **SSID03** profile, so select **SSID04** in one of the **Profile** list boxes (number **3** in this example).

Select the **Index** box for the entry and click **Apply** to activate the profile. Your standard wireless network (**SSID03**) is now accessible to your wireless clients as before. You do not need to configure anything else for your standard network.

3.3.2 Configure the VoIP Network

Next, click **Wireless** > **SSID**. The following screen displays. Note that the **SSID03** 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 17 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 18 Tutorial: VoIP SSID Profile Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name		VoIP_SSID			
SSID		VOIP_SSID_Example			
Hide Name(SSID)		Enable			
Security		security02			
RADIUS		radius01			
QoS		VoIP			
Layer-2 Isolation		Disable			
Intra-BSS Traffic blocking		Disable			
MAC Filtering		Disable			

- 1 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.
- 2 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.
- 3 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.
- 4 Leave all the other fields at their defaults and click **Apply**.

3.3.2.1 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 19 Tutorial: VoIP Security

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																																																			
		<table border="1"> <thead> <tr> <th>Index</th> <th>Profile Name</th> <th>Security Mode</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>security01</td> <td>WPA2-PSK</td> </tr> <tr style="border: 2px solid red;"> <td>2</td> <td>security02</td> <td>None</td> </tr> <tr> <td>3</td> <td>security03</td> <td>None</td> </tr> <tr> <td>4</td> <td>security04</td> <td>None</td> </tr> <tr> <td>5</td> <td>security05</td> <td>None</td> </tr> <tr> <td>6</td> <td>security06</td> <td>None</td> </tr> <tr> <td>7</td> <td>security07</td> <td>None</td> </tr> <tr> <td>8</td> <td>security08</td> <td>None</td> </tr> <tr> <td>9</td> <td>security09</td> <td>None</td> </tr> <tr> <td>10</td> <td>security10</td> <td>None</td> </tr> <tr> <td>11</td> <td>security11</td> <td>None</td> </tr> <tr> <td>12</td> <td>security12</td> <td>None</td> </tr> <tr> <td>13</td> <td>security13</td> <td>None</td> </tr> <tr> <td>14</td> <td>security14</td> <td>None</td> </tr> <tr> <td>15</td> <td>security15</td> <td>None</td> </tr> <tr> <td>16</td> <td>security16</td> <td>None</td> </tr> </tbody> </table>	Index	Profile Name	Security Mode	1	security01	WPA2-PSK	2	security02	None	3	security03	None	4	security04	None	5	security05	None	6	security06	None	7	security07	None	8	security08	None	9	security09	None	10	security10	None	11	security11	None	12	security12	None	13	security13	None	14	security14	None	15	security15	None	16	security16	None			
Index	Profile Name	Security Mode																																																						
1	security01	WPA2-PSK																																																						
2	security02	None																																																						
3	security03	None																																																						
4	security04	None																																																						
5	security05	None																																																						
6	security06	None																																																						
7	security07	None																																																						
8	security08	None																																																						
9	security09	None																																																						
10	security10	None																																																						
11	security11	None																																																						
12	security12	None																																																						
13	security13	None																																																						
14	security14	None																																																						
15	security15	None																																																						
16	security16	None																																																						
<input type="button" value="Edit"/>																																																								

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 20 Tutorial: VoIP Security Profile Edit

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
<p>Profile Name: VoIP_Security</p> <p>Security Mode: WPA2-PSK</p> <p>Pre-Shared Key: ThisismyWPA2-PSKpre-sharedkey</p> <p>ReAuthentication Timer: 1000 (seconds, 0 means no ReAuthentication)</p> <p>Idle Timeout: 3600 (seconds)</p> <p>Group Key Update Timer: 1800 (seconds)</p> <p>Apply Reset</p>					

- 1 Change the **Name** field to "VoIP_Security" to make it easier to remember and identify.
- 2 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".
- 3 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**.

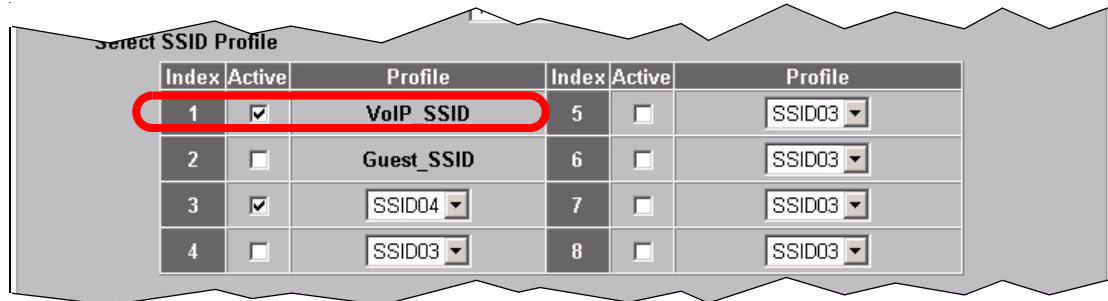
Figure 21 Tutorial: VoIP Security: Updated

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																								

3.3.2.2 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 22 Tutorial: Activate VoIP 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

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.

3.3.3 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 174](#)), and "intra-BSS traffic blocking" means that the client cannot access other clients on the same wireless network (see [Section 8.3 on page 123](#)).

Click **Wireless** > **SSID**. Select **Guest_SSID**'s entry in the list and click **Edit**. The following screen appears.

Figure 23 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	

- 1 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.
- 2 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.
- 3 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.
- 4 Leave all the other fields at their defaults and click **Apply**.

3.3.3.1 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 24 Tutorial: Guest Security Profile Edit

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

- 1 Change the **Name** field to "Guest_Security" to make it easier to remember and identify.
- 2 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.
- 3 Enter the PSK you want to use in your network in the **Pre-Shared Key** field. In this example, the PSK is "ThisismyGuestWPApre-sharedkey".
- 4 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**.

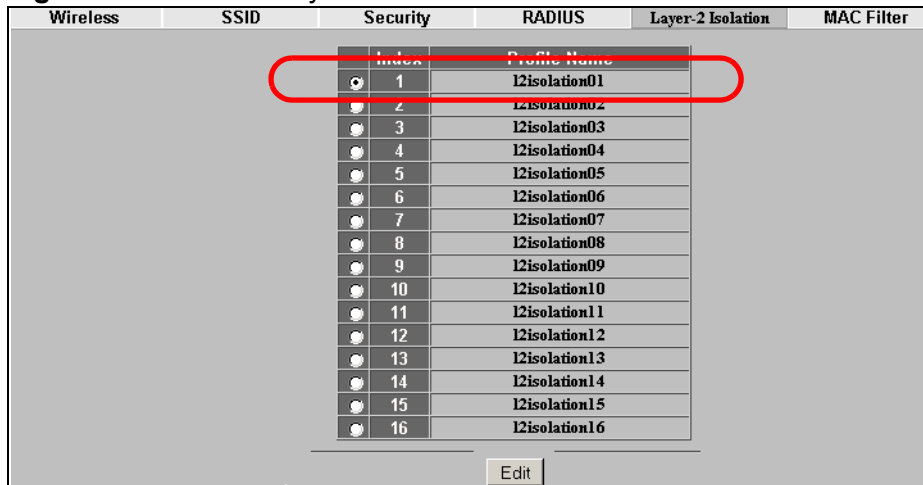
Figure 25 Tutorial: Guest Security: Updated

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																						

3.3.3.2 Set up Layer 2 Isolation

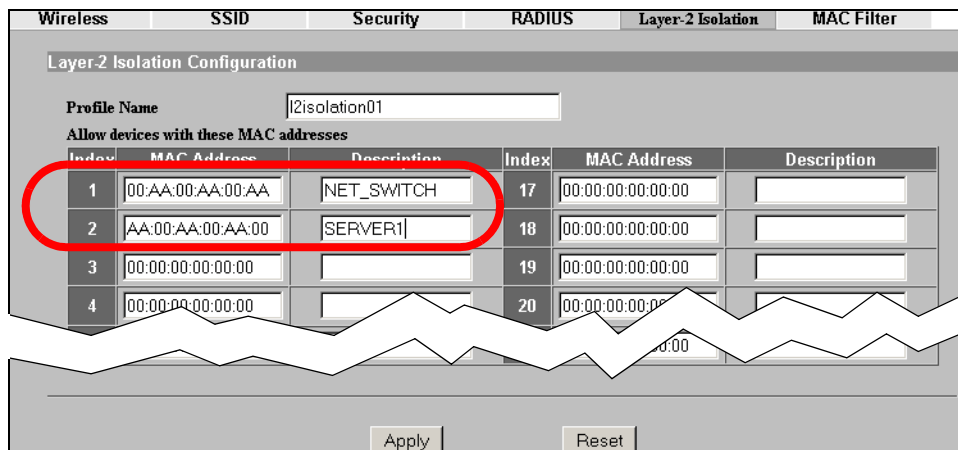
Configure layer 2 isolation to control the specific devices you want the users on your guest network to access. Click **WIRELESS** > **Layer-2 Isolation**. The following screen appears.

Figure 26 Tutorial: Layer 2 Isolation



The **Guest_SSID** network uses the **I2isolation01** profile by default, so select its entry and click **Edit**. The following screen displays.

Figure 27 Tutorial: Layer 2 Isolation Profile

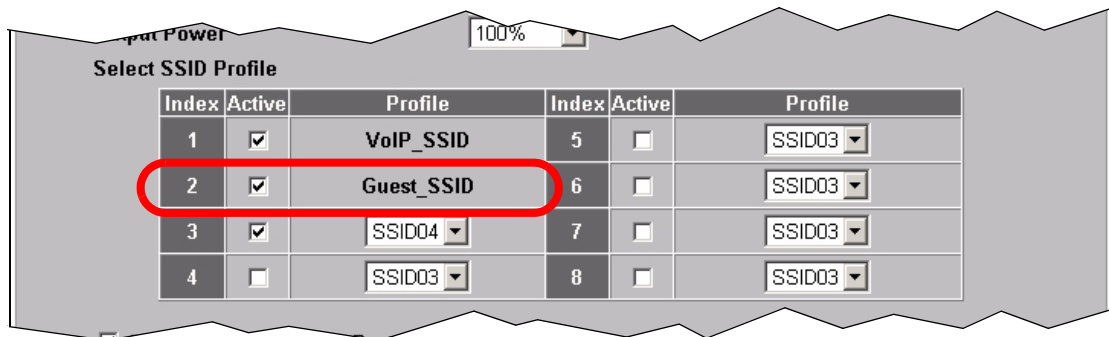


Enter the MAC addresses and descriptions of the two network devices you want users on the guest network to be able to access: the main network router (00:AA:00:AA:00:AA) and the network printer (AA:00:AA:00:AA:00). Click **Apply**.

3.3.3.3 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 28 Tutorial: Activate Guest Profile



Your guest wireless network is now ready to use.

3.3.4 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.

3.4 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 187](#) for background information on the rogue AP function and security considerations.

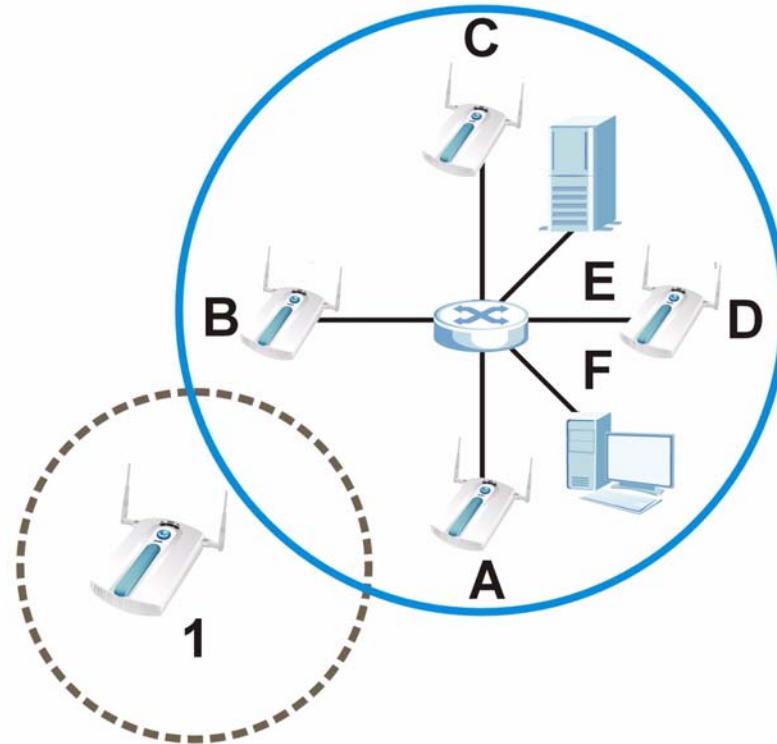
In this example, you want to ensure that your company's data is not accessible to an attacker gaining entry to your wireless network through a rogue AP.

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 29 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 3 Tutorial: Rogue AP Example Information

DEVICE	IP ADDRESS	MAC ADDRESS
Access Point A	192.168.1.1	00:AA:00:AA:00:AA
Access Point B	192.168.1.2	AA:00:AA:00:AA:00
Access Point C	192.168.1.3	A0:0A:A0:0A:A0:0A
Access Point D	192.168.1.4	0A:A0:0A:A0:0A:A0
File / Mail Server E	192.168.1.25	N/A
Access Point 1	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.

3.4.1 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 30 Tutorial: Friendly AP (Before Data Entry)

- 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.

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_

MAC ADDRESS	DESCRIPTION
0A:A0:0A:A0:0A:A0	My Access Point _D_
AF:AF:AF:FA:FA:FA	Coffee Shop Access Point _1_

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.

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

Figure 31 Tutorial: Friendly AP (After Data Entry)

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

Index	MAC Address	SSID	Channel	Radio Mode	Security	Last Seen	Description	
1	00:aa:00:aa:00:aa	N/A	N/A	N/A	N/A	N/A	My Access Point _A_	
2	aa:00:aa:00:aa:00	N/A	N/A	N/A	N/A	N/A	My Access Point _B_	
3	a0:0a:a0:0a:a0:0a	N/A	N/A	N/A	N/A	N/A	My Access Point _C_	
4	0a:a0:0a:a0:0a:a0	N/A	N/A	N/A	N/A	N/A	My Access Point _D_	
5	af:af:af:fa:fa:fa	N/A	N/A	N/A	N/A	N/A	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.

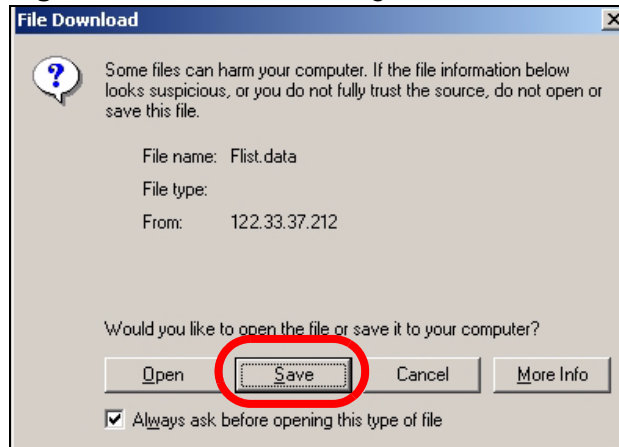
Click the **Configuration** tab. The following screen appears.

Figure 32 Tutorial: Configuration

The screenshot shows the 'Configuration' screen. At the top, there are tabs for 'Configuration', 'Friendly AP', and 'Rogue AP'. The 'Configuration' tab is active. Below the tabs, there are settings for 'Rogue AP Period Detection' (set to 'Disable'), 'Period' (set to '10 (minutes)'), and 'Expiration Time' (set to '30 (minutes)'). Below these settings is a section titled 'Friendly AP List' with an 'Export' button circled in red. Below the 'Export' button is a 'File Path' input field with 'Browse...' and 'Import' buttons. At the bottom of the screen are 'Apply' and 'Reset' buttons.

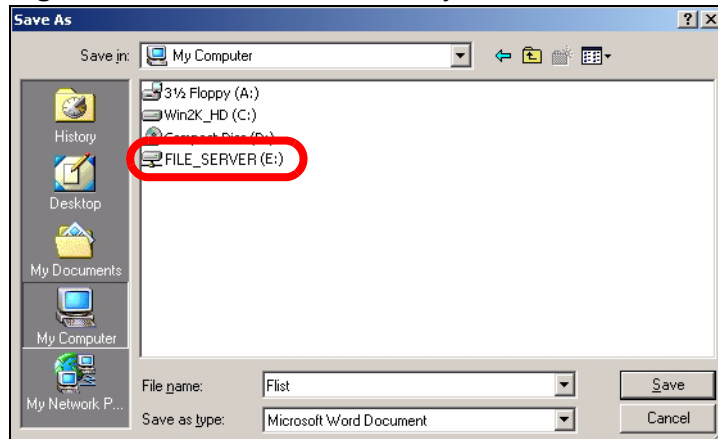
- 4 Click **Export**. If a window similar to the following appears, click **Save**.

Figure 33 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 29 on page 56](#)). The default filename is "Flist".

Figure 34 Tutorial: Save Friendly AP list

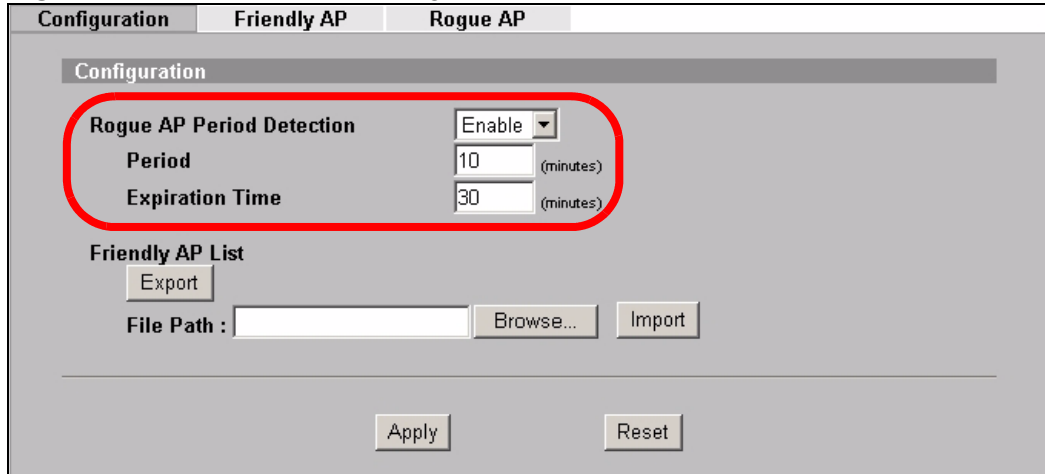


3.4.2 Activate Periodic Rogue AP Detection

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 35 Tutorial: Periodic Rogue AP Detection



The screenshot shows the 'Rogue AP' configuration screen with three tabs: 'Configuration', 'Friendly AP', and 'Rogue AP'. The 'Configuration' tab is active. Under the 'Configuration' header, the 'Rogue AP Period Detection' section is highlighted with a red circle. It contains a dropdown menu set to 'Enable', a 'Period' field with the value '10' (minutes), and an 'Expiration Time' field with the value '30' (minutes). Below this is the 'Friendly AP List' section with an 'Export' button, a 'File Path' input field, a 'Browse...' button, and an 'Import' button. At the bottom of the screen are 'Apply' and 'Reset' buttons.

- 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**.

3.4.3 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 36 Tutorial: Log Settings

The screenshot shows the 'Log Settings' configuration page. It is divided into three main sections: 'Address Info', 'Syslog Logging', and 'Send Log'.
 - **Address Info:** Contains fields for 'Mail Server' (192.168.1.25), 'Mail Subject' (ALERT_Access_Point_A), 'Send log to', and 'Send alerts to' (myname@myfirm.com).
 - **Syslog Logging:** Includes a checkbox for 'Active', 'Syslog IP Address' (0.0.0.0), and 'Log Facility' (Local 1).
 - **Send Log:** Features 'Log Schedule' (None), 'Day for Sending Log' (Sunday), 'Time for Sending Log' (0 hours, 0 minutes), and a checkbox for 'Clear log after sending mail'.
 - **Log Categories:** Two columns of checkboxes. The left column lists 'Log' categories: System Maintenance, System Errors, PKI, SSL/TLS, 802.1x, Wireless, Internal RADIUS Server, Rogue AP Detection, Radar Event, and Load Balancing. The right column, titled 'Send immediate alert', includes System Errors, PKI, Rogue AP Detection, Radar Event, and Load Balancing.
 - **Buttons:** 'Apply' and 'Reset' buttons are located at the bottom.

- 2 In this example, your mail server's IP address is **192.168.1.25**. Enter this IP address in the **Mail Server** field.
- 3 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**".
- 4 Enter the email address to which you want alerts to be sent (**myname@myfirm.com**, in this example).

- 5 In the **Send Immediate Alert** section, select the events you want to trigger immediate e-mails. Ensure that **Rogue AP Detection** is selected.
- 6 Click **Apply**.

3.4.4 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 3 on page 56](#) 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 3.4.2 on page 60](#).
- 5 Set up e-mail logs as in [Section 3.4.3 on page 61](#), but change the **Mail Subject** field so you can tell which AP the alerts come from ("ALERT_Access_Point_B", etc.)

3.4.5 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 [Section 3.4.1 on page 57](#) 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 [Section 3.4.1 on page 57](#), 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).

3.5 Using 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.

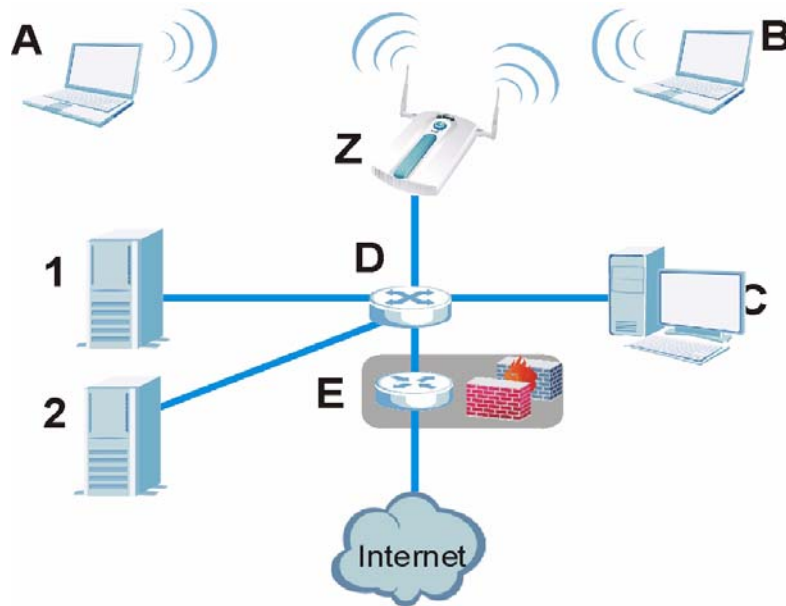
3.5.1 Scenario

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 37 Tutorial: Example Network



3.5.2 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.

3.5.3 Setup

In this example, you have already set up the NWA in MBSSID mode (see [Chapter 12 on page 173](#)). It uses two SSID profiles simultaneously. You have configured each SSID profile as shown in the following table.

Table 4 Tutorial: SSID Profile Security Settings

SSID Profile Name	SERVER_1	SERVER_2
SSID	SSID_S1	SSID_S2
Security	Security Profile security03 : WPA2-PSK Hide SSID	Security Profile security04 : 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 5 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 6 Tutorial: Example User MAC Addresses

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

3.5.4 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 38 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	
<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 checked="" type="radio"/>	3	SERVER_1	SSID03	security03	radius01	NONE	Disable	Disable
<input type="radio"/>	4	SERVER_2	SSID04	security04	radius01	NONE	Disable	Disable
<input type="radio"/>	5	SSID05	ZyXEL05	security03	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

- 2 Select **SERVER_1**'s entry and click **Edit**. The following screen displays.

Figure 39 Tutorial: SSID Edit

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

- 3 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 40 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	

- 4 Enter the network switch's **MAC Address** and add a **Description** ("NET_SWITCH" in this case) in **Index 1**'s entry.
- 5 Enter server 1's **MAC Address** and add a **Description** ("SERVER_1" in this case) in **Index 2**'s entry.
- 6 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.
- 7 Click the **MAC Filter** tab. When the **MAC Filter** screen appears, select **macfilter03**'s entry and click **Edit**.

- 8 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 41 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					

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.

3.5.5 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 3.5.4 on page 65](#), substituting the following information.

Table 7 Tutorial: SERVER_2 Network Information

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

Table 7 Tutorial: SERVER_2 Network Information

MAC Filter (macfilter04) Edit Screen	
Profile Name	MacFilter_SERVER_2
Set 1	MAC Address: 22:33:44:55:66:77
	Description: Bob

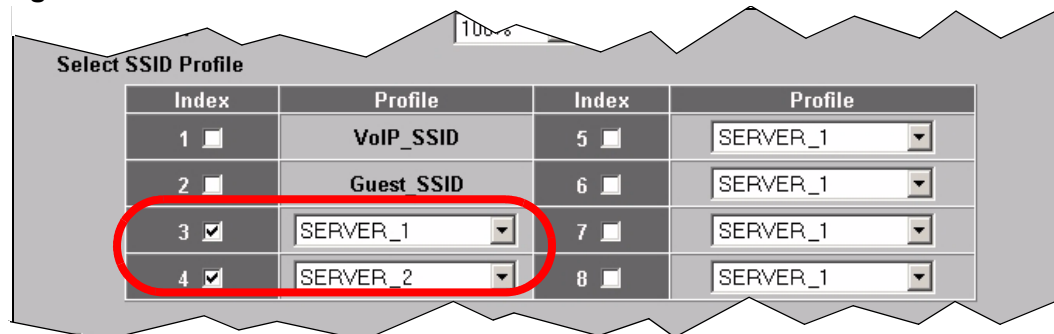
3.5.6 Checking your Settings and Testing the Configuration

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

3.5.6.1 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 42 Tutorial: SSID Profiles Activated

- 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 43 Tutorial: SSID Tab Correct Settings

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter			
	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	SSID_S1	security03	radius01	NONE	L-2-ISO_SERVER_1	MacFilter_SERVER_1
	4	SERVER_2	SSID_S2	security04	radius01	NONE	L-2-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.

3.5.6.2 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.

- 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.
- 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 3.5.6.1 on page 69](#), 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.

3.6 How to Configure Management Modes

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

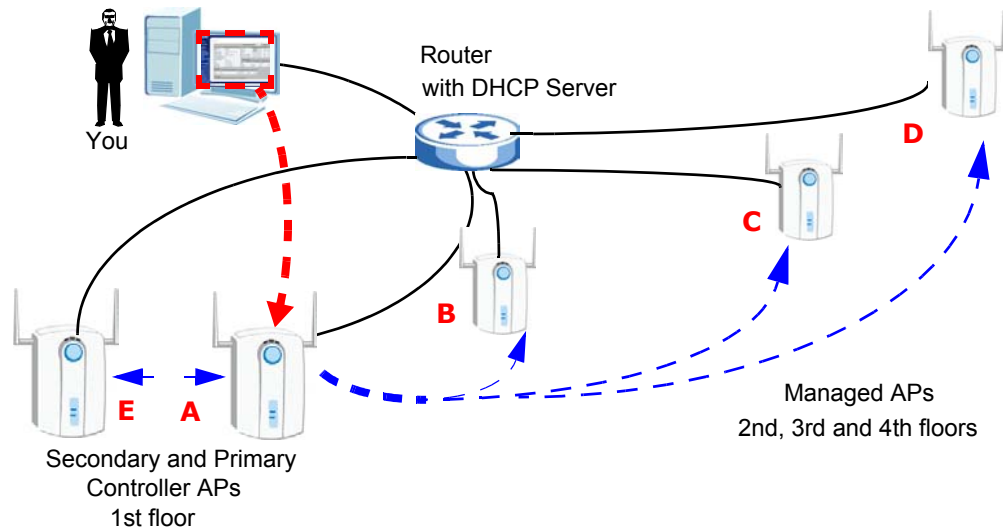
3.6.1 Scenario

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 44 Tutorial: Controller AP with Backup and Managed APs Example



3.6.2 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.

3.6.3 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 282](#) 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 14.2 on page 184](#)).

- 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.

3.6.4 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 282](#)) 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 45 Tutorial: MGNT Mode (AP Controller)

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

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

3.6.4.1 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 46 Tutorial: Secondary Controller AP

The screenshot shows the 'Redundancy' web configurator screen. At the top, there are tabs for 'AP Lists', 'Configuration', and 'Redundancy'. The 'Redundancy' section is active. A dropdown menu labeled 'Redundancy' is set to 'Enable' and is circled in red. Below it are two radio button options: 'Primary AP Controller' and 'Secondary AP Controller' (selected and circled in red). There is an input field for 'Secondary IP'. At the bottom are 'Apply' and 'Reset' buttons.

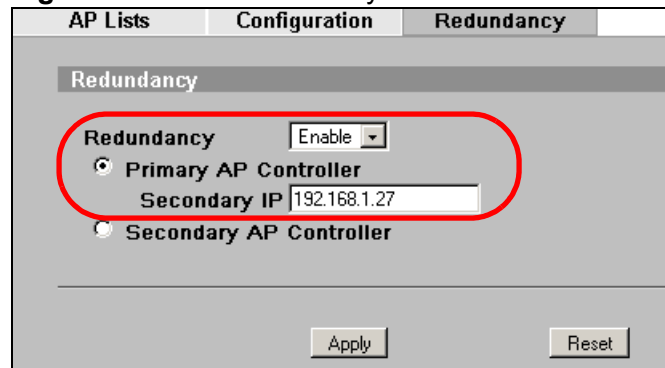
- 2 Enable **Redundancy**. Then select **Secondary AP Controller** and click **Apply**.

3.6.4.2 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 47 Tutorial: Primary Controller AP



- 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.

3.6.5 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 SMNP 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 48 Tutorial: Managed AP

The screenshot shows the 'MGNT Mode' configuration page. Under the 'Management Mode' section, three radio buttons are visible: '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 text 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 form 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.

3.6.6 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 49 Tutorial: Registration Type

The screenshot shows the 'Controller Setting' configuration page. It has three tabs: 'AP Lists', 'Configuration', and 'Redundancy'. The 'Configuration' tab is active. Under the 'Registration Type' section, there are two radio buttons: 'Manual' and 'Always Accept'. The 'Manual' option is selected and highlighted with a red rounded rectangle. Above this section is a 'Pre-Shared Key' field with the value '12345678' and a note '(8-32 characters)'. At the bottom of the form are 'Apply' and 'Reset' buttons.

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 50 Tutorial: AP List (Un-Managed)

AP Lists						
Configuration						
Redundancy						
Managed Access Points List						
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-3500 802.11a/g	NWA-Primary Controller	Edit
Delete						
Un-Managed Access Points List						
Index	<input type="checkbox"/>	IP	MAC Address	Model	Description	
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	
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	
Add						
Automatic Refresh Interval <input type="text" value="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 **Managed 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 51 Tutorial:AP List (Managed)

AP Lists							
Configuration		Redundancy					
Managed Access Points List							
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 type="checkbox"/>	192.168.1.35	00:19:27:DF:42:16	NWA-3500 802.11a/g	NWA-Managed AP-2nd floor		Edit
Delete							
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 52 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
<input checked="" type="checkbox"/>	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 8.3 on page 123](#) for instructions on how to set up WLAN radio profiles in the NWA controller APs.

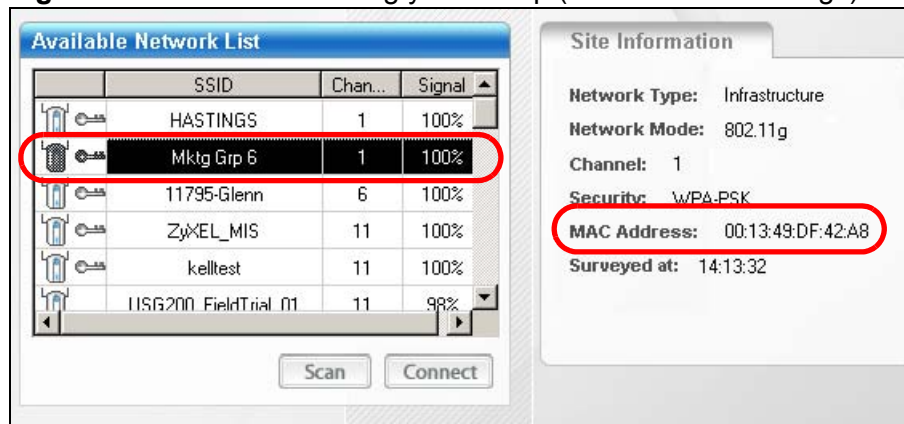
3.6.7 Checking your Settings and Testing the Configuration

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 53 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 (145)

Wireless Security Screen (155)

RADIUS Screen (169)

Layer-2 Isolation Screen (173)

MAC Filter Screen (179)

IP Screen (183)

Rogue AP Detection (187)

Remote Management Screens (195)

Internal RADIUS Server (209)

Certificates (217)

Log Screens (235)

VLAN (245)

Maintenance (275)

Status Screens

4.1 Overview

The **Status** screen displays when you log into the NWA or click **Status** in the navigation menu. Use this screen to look at the current status of the device, system resources, and interfaces. The **Status** screen also provides detailed information about system statistics, associated wireless clients, and logs.

4.2 The Status Screen

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

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

Figure 54 The Status Screen

The screenshot shows the 'STATUS' screen with the following sections:

System Information

System Name	NWA-Series
Model	NWA-3500
Firmware Version	V3.70(AAH.1)b2 07/06/2009
System UP Time	00:54:23
Current Date Time	00:54:20 2000/01/01
WLAN1 Operating Mode	AP
WLAN2 Operating Mode	AP
Management VLAN	Disable
IP	172.23.31.203
LAN MAC	00:19:cb:88:81:0c
WLAN1 MAC	00:19:cb:88:81:0c
WLAN2 MAC	00:19:cb:88:81:0d

System Resources

Flash	<div style="width: 25%;"></div>	2/4 MB
Memory	<div style="width: 40%;"></div>	17/32 MB
CPU	<div style="width: 0%;"></div>	0%
WLAN1 Associations	<div style="width: 0%;"></div>	0/128
WLAN2 Associations	<div style="width: 0%;"></div>	0/128

Interface Status

Interface	Status	Rate
LAN	Up	100M/Full
WLAN1	Up(Ch165)	54M
WLAN2	Up(Ch48)	54M

SSID Status

Interface	SSID	BSSID	Security	VLAN
WLAN1	NWA	00:19:cb:88:81:0c	WPA-PSK	Disabled
WLAN2	ZyXEL04	00:19:cb:88:81:0d	WPA-PSK	Disabled

System Status

Show Statistics | Association List | Channel Usage | LOGS | Rogue AP List

The following table describes the labels in this screen.

Table 8 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.
System Information	
System Name	This field displays the NWA system name. It is used for identification. You can change this in the System > General screen's System Name 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 Maintenance > F/W Upload .
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 System > Time Setting screen.
WLAN1 Operating Mode	This field displays the current operating mode of the first wireless module (AP, Bridge / Repeater, AP + Bridge or MBSSID). You can change the operating mode in the Wireless > Wireless screen.
WLAN2 Operating Mode	This field displays the current operating mode of the second wireless module (AP, Bridge / Repeater, AP + Bridge or MBSSID). You can change the operating mode in the Wireless > Wireless screen.
Management VLAN	This field displays the management VLAN ID if VLAN is active, or Disabled if it is not active. You can enable or disable VLAN, or change the management VLAN ID, in the VLAN > Wireless VLAN screen.
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.
WLAN1 MAC	This displays the MAC address of the first wireless module.
WLAN2 MAC	This displays the MAC address of the second wireless module.
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.

Table 8 The Status Screen

LABEL	DESCRIPTION
WLAN1 Associations	This field displays the number of wireless clients currently associated with the first wireless module. It supports up to 128 concurrent associations.
WLAN2 Associations	This field displays the number of wireless clients currently associated with the second wireless module. It supports up to 128 concurrent associations.
Interface Status	
Interface	This column displays each interface of the NWA.
Status	This field indicates whether or not the NWA is using the interface. For each interface, this field displays Up when the NWA is using the interface and Down when the NWA is not using the interface.
Rate	For the LAN port this displays the port speed and duplex setting. For the WLAN interface, it displays the downstream and upstream transmission rate or N/A if the interface is not in use.
SSID Status	
Interface	This column displays each of the NWA's wireless interfaces.
SSID	This field displays each of the SSIDs currently in use.
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 Disabled if the SSID does not use VLAN.
System Status	
Show Statistics	Click this link to view port status and packet specific statistics. See Section 4.2.1 on page 86 .
Association List	Click this to see a list of wireless clients currently associated to each of the NWA's wireless modules. See Section 23.2 on page 280 .
Channel Usage	Click this to see which wireless channels are currently in use in the local area. See Section 23.3 on page 281 .
Logs	Click this to see a list of logs produced by the NWA. See Chapter 19 on page 239 .
Rogue AP List	Click this to see a list of unauthorized access points in the local area. See Section 15.2.2 on page 196 .

4.2.1 System Statistics Screen

Use this screen to view diagnostic information about the NWA. Click **Show Statistics** in the **Status** screen. 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 55 System Status: Show Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
LAN	100M/Full	431	1321	0	203	441	0:05:38
WLAN1	54M	1010	0	0	258	0	0:05:39
WLAN2	54M	1010	0	0	258	0	0:05:39

Poll Interval(s) : <input type="text" value="5"/> sec <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>

The following table describes the labels in this screen.

Table 9 System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet port (LAN) or wireless LAN adaptor (WLAN).
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.
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.

Management Mode

5.1 Overview

This chapter discusses using the NWA in management mode. This screen determines whether the NWA is used in its default standalone mode, or as part of a Control And Provisioning of Wireless Access Points (CAPWAP) network.

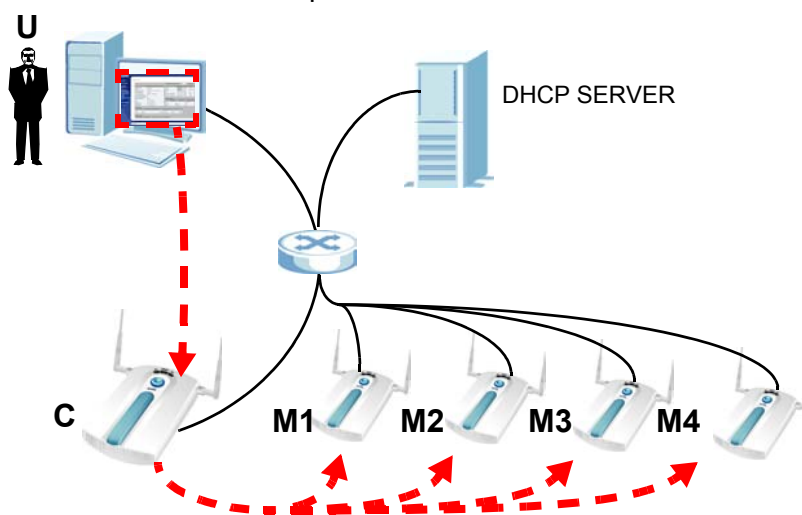
5.2 About CAPWAP

The NWA supports CAPWAP. This is ZyXEL's implementation of the IETF's CAPWAP protocol (RFC 4118).

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

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

Figure 56 CAPWAP Network Example



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

5.2.1 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. If the AP controller is in **Manual** mode it adds the details of the AP to its **Unmanaged Access Points** list, and you decide which available APs to manage. If the AP is in **Always Accept** mode, it automatically adds the AP to its **Managed Access Points** list and provides the managed AP with default configuration information, as well as securely transmitting the DTLS pre-shared key. The managed AP is ready for association with wireless clients.

5.2.2 CAPWAP and DHCP

CAPWAP managed APs must be Dynamic Host Configuration Protocol (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.

5.2.3 CAPWAP and IP Subnets

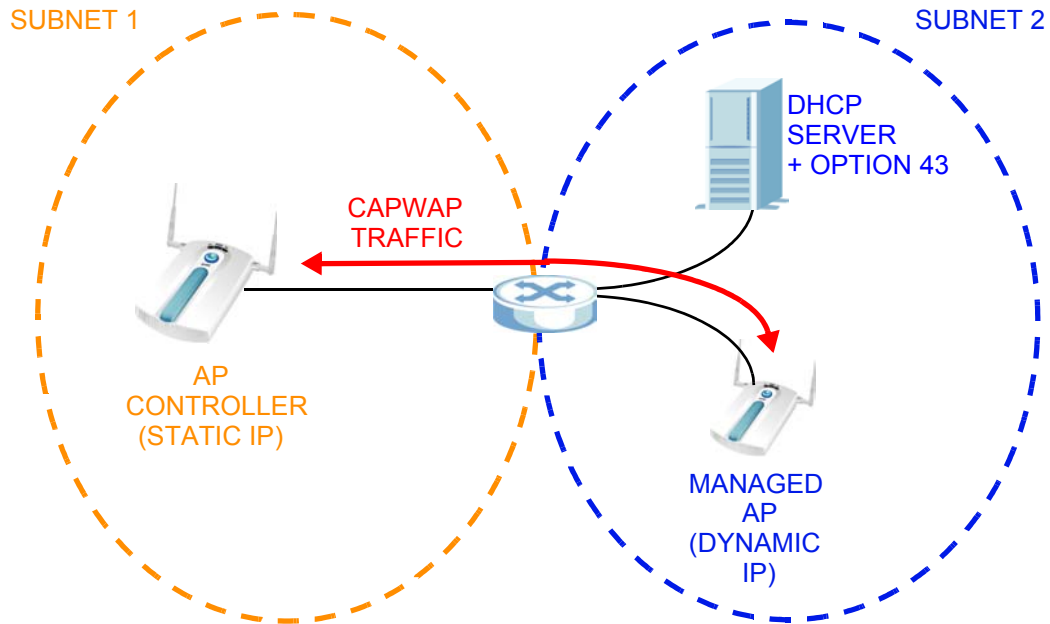
By default, CAPWAP works only between devices with IP addresses in the same subnet (see the appendices for information on IP addresses and subnetting).

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 57 CAPWAP and DHCP Option 43



5.2.4 Notes on CAPWAP

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

- When the AP controller uses its internal Remote Authentication Dial In User Service (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.

5.3 The Management Mode Screen

Use this screen to configure the NWA as a CAPWAP controller AP, a 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 58 Management Mode

The following table describes the labels in this screen.

Table 10 Management Mode

LABEL	DESCRIPTION
AP Controller	Select this option to have the NWA act as a managing device for other NWAs on your network.
Standalone AP	Select this to manage the NWA using its own web configurator, neither managing nor managed by other devices.
Managed AP	<p>Select this to have the NWA managed by another NWA on your network.</p> <p>When you do this, the NWA can be configured ONLY 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 RESET button. All settings are returned to their default values.</p> <p>Options are:</p> <ul style="list-style-type: none"> • Auto AP Controller IP - Select this option to have the NWA issue a request to be managed by any available NWA-based AP controller within its broadcast radius. • Manual AP Controller IP - Select this option if you know the IP address of the AP controller that you want to manage your NWA. You can assign a primary and secondary controller IP. At the very least, you need a primary IP. <p>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 Controller > AP Lists screen of the AP controller on your network.</p>

Table 10 Management Mode

LABEL	DESCRIPTION
Apply	Click this to save your changes. 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 Managed AP , you cannot log in as the web configurator is disabled; you must manage the NWA through the management AP on your network.
Reset	Click this to return this screen to its previously-saved settings.

AP Controller Mode

6.1 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 5.2 on page 87](#) for more information on CAPWAP.

6.1.1 What You Can Do in AP Controller Mode

- Use the **Navigation Menu** ([Section 6.2 on page 94](#)) to manage settings across all connected APs.
- Use the **Status** screen ([Section 6.3 on page 95](#)) to view information about your managed wireless network.
- Use the **AP Lists** screen ([Section 6.4 on page 97](#)) to manage connected APs.
- Use the **Configuration** screen ([Section 6.5 on page 101](#)) to control the way in which the NWA accepts new APs to manage.
- Use the **Redundancy** screen ([Section 6.6 on page 102](#)) to set the controller AP as a primary or secondary controller.
- Use the **Profile Edit** screens ([Section 6.7 on page 102](#)) to edit an individual AP's Radio, SSID, Security, RADIUS, Layer-2 Isolation, and MAC Address settings.

6.1.2 What You Need to Know

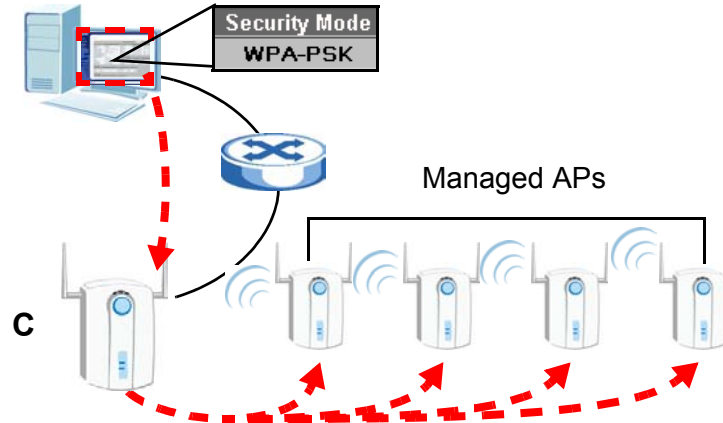
The following terms and concepts may help as you read through this chapter.

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 59 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.

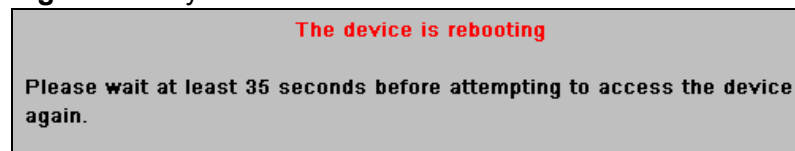
6.1.3 Before You Begin

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 5.3 on page 90](#) before continuing.

6.2 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.

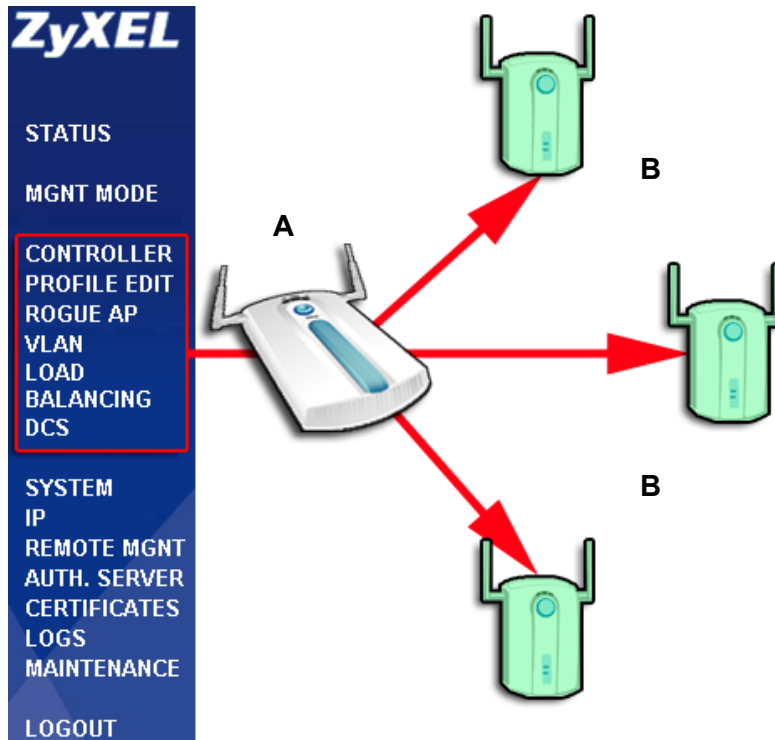
Figure 60 System Restart



Note: The NWA reboots every time you change mode in the **MGMT 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 61 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.

6.3 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 62 Status Screen

The following table describes the new labels in this screen.

Table 11 Status Screen

LABEL	DESCRIPTION
System Information	
Registration Type	This field displays how the managed APs are registered with the NWA. Manual displays if you add unmanaged APs to the NWA's list of managed APs manually. Always Accept displays if the NWA automatically manages any CAPWAP-enabled AP that transmits a management request over the network.
Management Mode	When the NWA is in AP controller mode, this displays Controller .
AP Status	
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.
WLAN Association	
802.11a	This field displays the number of wireless clients associated with APs managed by the NWA (including the NWA itself) using 802.11a radio mode.

Table 11 Status Screen

LABEL	DESCRIPTION
802.11b/g	This field displays the number of wireless clients associated with APs managed by the NWA (including the NWA itself) using 802.11b/g radio mode.
Redundancy	The table below shows when redundancy is enabled (see Section 6.6 on page 102) and the NWA acts as the primary AP controller.
Redundancy Device	This field displays the IP address of the secondary AP controller.
Last Synchronization Result	This field displays whether the last synchronization with the secondary AP controller succeeded (SUCCESS) or failed (DISABLED).
Last Synchronization Time	This field displays the last date and time when the NWA synchronized settings with the secondary AP controller.
Alive Status	This field displays either NO RESPONSE (the secondary AP controller is down) or ALIVE (the secondary AP controller is active).
System Status	
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. This does not include the NWA itself.
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.

6.4 AP Lists Screen

Use this screen to view and add managed APs. By default, the controller 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 63 AP Lists Screen

The screenshot shows the 'AP Lists' configuration page 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'.

Managed Access Points List

Index	<input type="checkbox"/>	IP	MAC Address	Model	Description	Status	Edit
1	<input checked="" type="checkbox"/>	127.0.0.1	00:19:CB:88:81:0C	NWA-3500 802.11a/g	AP-PRIMARY-CONTROLLER		Edit
2	<input type="checkbox"/>	0.0.0.0	00:19:CB:88:82:0A	NWA-3500 802.11a/g	AP-Managed		Edit
3	<input type="checkbox"/>	0.0.0.0	00:19:CB:88:82:0C	NWA-3500 802.11a/g	AP-Secondary AP		Edit

Delete

Un-Managed Access Points List

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

Automatic Refresh Interval: Refresh

The following table describes the labels in this screen.

Table 12 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	<p>Click the topmost box either to select or deselect all NWAs in the list.</p> <p>Click an NWA's checkbox to select it and apply a corresponding action. You can also click several items at the same time and do the following:</p> <ul style="list-style-type: none"> Click Edit to configure the managed AP's settings. Click Delete 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. You can assign this in Section 6.4.1 on page 100 .

Table 12 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"> • Red: the AP is not active. • Green: the AP is active. • Yellow: the AP is upgrading its firmware. <p>Note: 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	<p>Click the topmost box either to select or deselect all NWAs in the list.</p> <p>Click an NWA's checkbox to select it and apply a corresponding action. You can also click several items at the same time and do the following:</p> <p>Click Add to include the unmanaged AP in the NWA's managed AP list.</p>
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.

6.4.1 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 64 AP Configuration Screen

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

- Model:** NWA-3500
- MAC Address:** 00:19:CB:88:81:0C
- Description:** AP-PRIMARY-CONTROLLER
- Enable Breathing LED:** A checked checkbox.
- WLAN1 Radio Profile:** A dropdown menu showing 'radio01'.
- WLAN2 Radio Profile:** A dropdown menu showing 'radio01'.

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

The following table describes the labels in this screen.

Table 13 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	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 Edit > Radio screen. Select Disable if you do not want to use a radio profile. The AP's radio is not active when you select Disable .
WLAN2 Radio Profile	Your AP has dual radios. Select the second radio profile you want to use for this AP. Configure radio profiles in the Profile Edit > Radio screen. Select Disable if you do not want to use a second radio profile. The AP's radio is not active when you select Disable .
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.

6.5 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 used 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 65 Configuration Screen

The screenshot shows a web interface with three tabs: 'AP Lists', 'Configuration', and 'Redundancy'. The 'Configuration' tab is active. Below the tabs is a section titled 'Controller Setting'. It contains a text input field for 'Pre-Shared Key' with the value '12345678' and a character count '(8-32 characters)'. Below this is a 'Registration Type' section with two radio buttons: 'Manual' (which is selected) and 'Always Accept'. At the bottom of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 14 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 you to select which APs to manage. <ul style="list-style-type: none"> Select Manual to choose which APs to manage (select the APs you want to manage in the Controller > AP Lists screen). Select Always Accept to have the NWA manage any AP on your network that transmits a CAPWAP request for management.
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.

6.6 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 66 Redundancy Screen

The following table describes the labels in this screen.

Table 15 Redundancy Screen

LABEL	DESCRIPTION
Redundancy	Select Enable to set the NWA either as a Primary AP Controller or as a Secondary Controller AP . Select Disable 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.

6.7 The Profile Edit Screens

This section describes the **Profile Edit** screens, which are available only in AP controller mode.

The following **Profile Edit** screens are identical to those in standalone mode:

Table 16 Radio Screen

LABEL	DESCRIPTION
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 Edit to go to the radio profile configuration screen.

6.7.2 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 68 Radio Edit Screen

Radio	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name <input type="text" value="radio01"/>					
802.11 Mode <input type="text" value="802.11a"/>					
<input checked="" type="checkbox"/> Super Mode					
<input checked="" type="checkbox"/> Disable channel switching for DFS					
Choose Channel ID <input type="text" value="Channel-036 5180MHz"/> Disable DCS to unlock.					
RTS/CTS Threshold <input type="text" value="2346"/> (256 - 2346)					
Fragmentation Threshold <input type="text" value="2346"/> (256 - 2346) (Fragmentation threshold shall be an even number)					
Beacon Interval <input type="text" value="100"/> (30ms - 1000ms)					
DTIM <input type="text" value="1"/> (1 - 100)					
Output Power <input type="text" value="100%"/>					
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"/>		
Select SSID Profile					
Index	Active	Profile	Index	Active	Profile
1	<input checked="" type="checkbox"/>	<input type="text" value="NWA"/>	5	<input type="checkbox"/>	<input type="text" value="NWA"/>
2	<input type="checkbox"/>	<input type="text" value="NWA"/>	6	<input type="checkbox"/>	<input type="text" value="NWA"/>
3	<input type="checkbox"/>	<input type="text" value="NWA"/>	7	<input type="checkbox"/>	<input type="text" value="NWA"/>
4	<input type="checkbox"/>	<input type="text" value="NWA"/>	8	<input type="checkbox"/>	<input type="text" value="NWA"/>
<input checked="" type="checkbox"/> Enable Antenna Diversity					
<input type="button" value="Apply"/>			<input type="button" value="Reset"/>		

The following table describes the labels in this screen.

Table 17 Radio Edit Screen

LABEL	DESCRIPTION
Profile Name	Enter a name identifying this profile.
802.11 Mode	<p>This makes sure that only compliant WLAN devices can associate with the NWA.</p> <p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced.</p> <p>Select 802.11a 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.
Disable channel switching for DFS	<p>This field displays only when you select 802.11a in the 802.11 Radio Mode field. Select this if you do not want to use DFS (Dynamic Frequency Selection).</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>
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. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.</p> <p>To have the NWA automatically select a channel, click Auto Selection instead.</p>
Disable DCS to unlock	<p>This appears if the DCS feature is enabled.</p> <p>Click this to disable DCS and select a channel ID manually.</p> <p>DCS is Disabled by default</p> <p>If the NWA is configured in Controller AP mode, it is recommended that you enable Dynamic Channel Selection (DCS). This allows the NWA to select channels with less interference for Managed APs.</p>

Table 17 Radio Edit Screen

LABEL	DESCRIPTION
RTS/CTS Threshold	<p>Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).</p> <p>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.</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 256 and 2346.</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 30ms 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>
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 100%(Full Power), 50%, 25%, 12.5% or Minimum. See the product specifications for more information on your NWA's output power.</p> <p>Note: Reducing the output power also reduces the NWA's effective broadcast radius.</p>
Rates Configuration	<p>This section controls the data rates permitted for clients.</p> <p>For each Rate, select an option from the Configuration list. The options are:</p> <ul style="list-style-type: none"> • Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. • Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. • Disabled: Clients cannot connect to the access point at this speed.
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 Profile Edit > SSID screens.</p>
Enable Antenna Diversity	<p>Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.</p>

Table 17 Radio Edit Screen

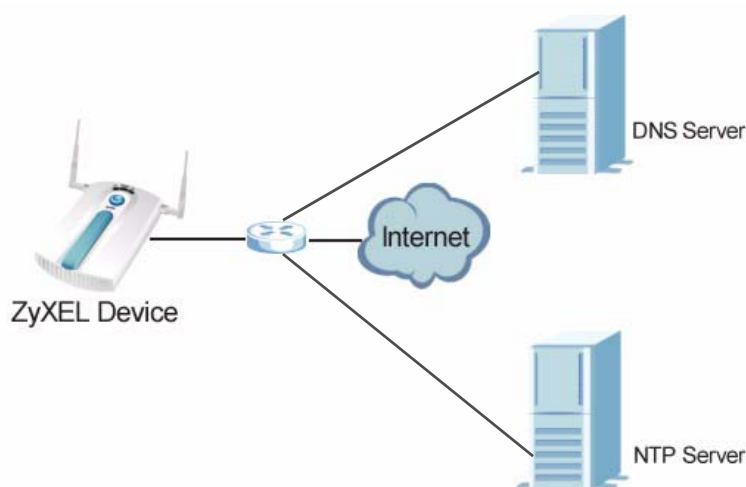
LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

System Screens

7.1 Overview

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

Figure 69 NWA Setup



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

7.1.1 What You Can Do in the System Screens

- Use the **General** screen (see [Section 7.2 on page 111](#)) 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 **System > Password** screen (see [Section 7.3 on page 113](#)) to manage the password for your NWA and have a RADIUS server authenticate management logins to the NWA.
- Use the **Time Setting** screen (see [Section 7.4 on page 115](#)) to change your NWA's time and date. This screen allows you to configure the NWA's time based on your local time zone.

7.1.2 What You Need To Know About the System Screens

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

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 18 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.

7.2 General Screen

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

Figure 70 System > General

The following table describes the labels in this screen.

Table 19 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. If you want to log into the NWA using the System Name , enter a name not longer than 15 alphanumeric characters.
Domain Name	This is not a required field. Leave this field blank or enter the domain name here if you know it.

Table 19 System > General

LABEL	DESCRIPTION
Administrator Inactivity Timer	<p>Type how many minutes a management session can be left idle before the session times out.</p> <p>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.</p> <p>A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).</p>
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	<p>Select From DHCP 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.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p> <p>The default setting is None.</p>
Apply	Click Apply to save your changes.
Reset	Click Reset to reload the previous configuration for this screen.

7.3 Password Screen

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

Figure 71 System > Password.

Note: Even if you uncheck **Enable Admin at Local**, you still use the password set here to log in via the console port (not available on all models).

The following table describes the labels in this screen.

Table 20 System > Password

LABEL	DESCRIPTIONS
Enable Admin at Local	Select this check box to have the device authenticate local 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.

Table 20 System > Password

LABEL	DESCRIPTIONS
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.
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 in your RADIUS server, 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"> • The user name and password must already be configured in the RADIUS server. • You must already have a RADIUS profile configured for the RADIUS server (see Section 11.2 on page 171). • The server must be set to Active in the profile.
Apply	Click Apply to save your changes.
Reset	Click Reset to reload the previous configuration for this screen.

7.4 Time Setting Screen

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

Figure 72 System > Time Setting

The following table describes the labels in this screen.

Table 21 System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NWA. Each time you reload this page, the NWA synchronizes the time with the time server (if configured).
Current Date	This field displays the last updated date from the time server.
Time and Date Setup	
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 Time and Date Setup to Manual , enter the new time in this field and then click Apply .

Table 21 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 Time and Date Setup to Manual , enter the new date in this field and then click Apply .
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 and Date Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Time Zone Setup	
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	Configure the day and time when Daylight Saving Time starts if you selected Enable Daylight Saving . The at field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00 . 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 Last, Sunday, March . The time you type in the at field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 21 System > Time Setting

LABEL	DESCRIPTION
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected Enable Daylight Saving. The o'clock 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 First, Sunday, November and 2:00.</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 Last, Sunday, October. The time you type in the at field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click Apply to save your changes.
Reset	Click Reset to reload the previous configuration for this screen.

7.5 Technical Reference

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

7.5.1 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.

7.5.2 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 22 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 73 Wireless Mode



In the figure above, the NWA (**ZyXEL Device**) 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 8.3 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.

8.2.1 What You Need To Know About the Wireless Screen

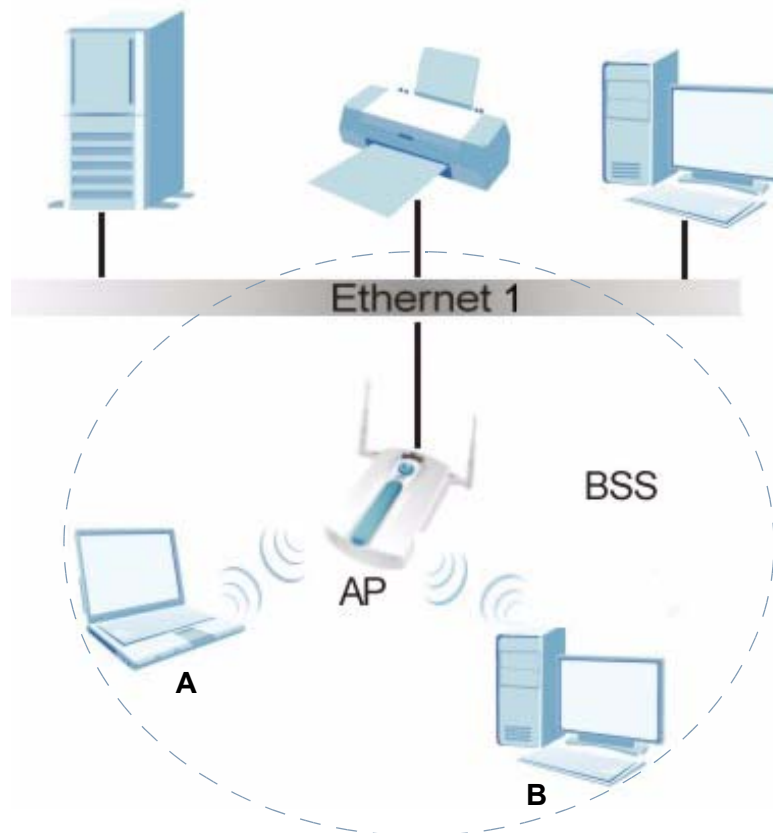
The following terms and concepts may help as you read through this chapter.

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

Figure 74 Basic Service set

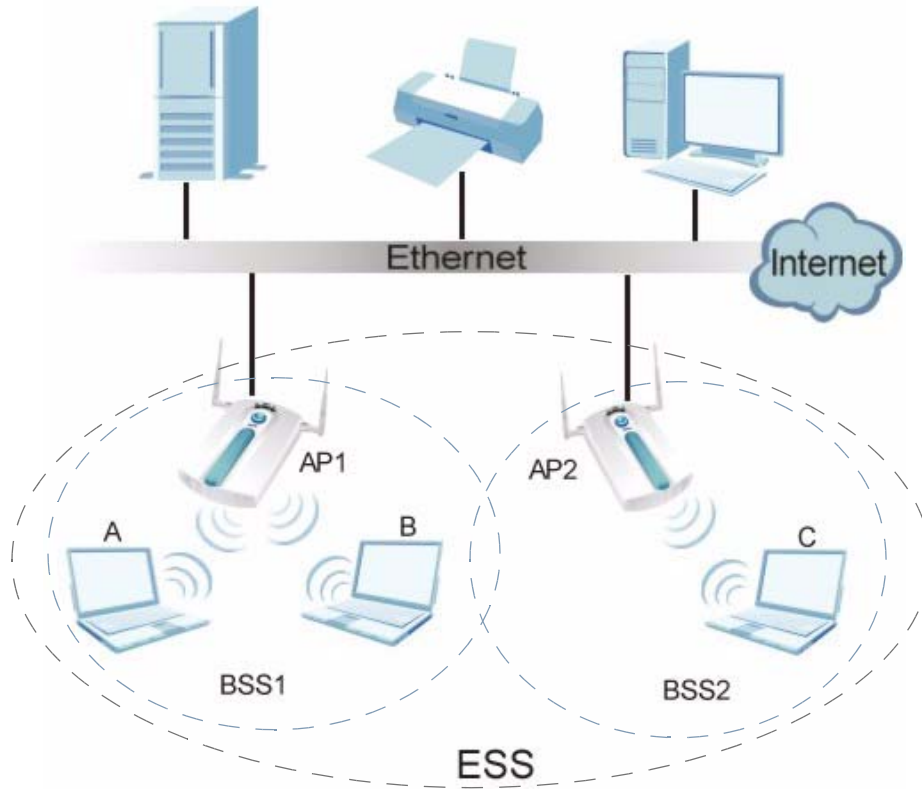


ESS

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 75 Extended Service Set



Operating Mode

The NWA can run in four operating modes as follows:

- **AP (Access Point).** The NWA is a 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 [Section 1.2 on page 24](#) for illustrations of these wireless applications.

SSID

The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID.

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

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

Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g/n 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. Wireless Mode supports **802.11b Only**, **802.11g Only**, **802.11b/g**, and **802.11a**.

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.

8.3 The Wireless Screen

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

Note: Some fields in this screen may not apply to your NWA model.

8.3.1 Access Point Mode

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

Figure 76 Wireless: Access Point

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																				
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>WLAN Interface: WLAN1</p> <p>Operating Mode: Access Point</p> <p>802.11 Mode: 802.11a</p> <p><input checked="" type="checkbox"/> Super Mode</p> <p><input checked="" type="checkbox"/> Disable channel switching for DFS</p> <p>Choose Channel ID: Channel-036 5180MHz Disable DCS to unlock.</p> <p>Operating Channel: Channel-044</p> <p>RTS/CTS Threshold: 2346 (256 - 2346)</p> <p>Fragmentation Threshold: 2307 (256 - 2346) (Fragmentation threshold shall be an even number)</p> <p>Beacon Interval: 100 (30ms - 1000ms)</p> <p>DTIM: 1 (1 - 100)</p> <p>Output Power: 100%</p> <p>SSID Profile: NWA</p> </div> <div style="width: 50%;"> <p>Rates Configuration</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> <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> </div> </div>						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																						
<div style="display: flex; justify-content: center; gap: 20px;"> Apply Reset </div>																									

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

Table 23 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> <p>In addition, it is recommended that you set the WLAN interfaces into different 802.11 modes. For example, set WLAN1 to 802.11b/g (2.4 GHz) and set WLAN2 to 802.11a (5 GHz).</p>
Operating Mode	<p>Select Access Point from the drop-down list.</p>
802.11 Mode	<p>This makes sure that only compliant WLAN devices can associate with the NWA.</p> <p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced.</p> <p>Select 802.11a to allow only IEEE 802.11a compliant WLAN devices to associate with the NWA.</p> <p>If you are configuring both WLAN interfaces, it is recommended that you set the WLAN interfaces into different 802.11 modes. For example, set WLAN1 to 802.11b/g (2.4 GHz) and set WLAN2 to 802.11a (5 GHz).</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 802.11a in the 802.11 Radio Mode field. Select this if you do not want to use DFS (Dynamic Frequency Selection).</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>
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. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.</p> <p>To have the NWA automatically select a channel, click Auto Selection instead.</p>

Table 23 Wireless: Access Point

LABEL	DESCRIPTION
Disable DCS to unlock	<p>This appears if the DCS feature is enabled.</p> <p>Click this to disable DCS and select a channel ID manually.</p> <p>Note: DCS is Disabled by default</p>
Operating Channel	<p>This field displays only when you select 802.11a in the 802.11 Radio Mode field.</p> <p>This is the channel currently being used by your AP.</p>
RTS/CTS Threshold	<p>Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).</p> <p>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.</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 256 and 2346.</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 30ms 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>
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 100%(Full Power), 50%, 25%, 12.5% or Minimum. See the product specifications for more information on your NWA's output power.</p> <p>Note: Reducing the output power also reduces the NWA's effective broadcast radius.</p>

Table 23 Wireless: Access Point

LABEL	DESCRIPTION
SSID Profile	<p>The SSID (Service Set Identifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Select an SSID Profile from the drop-down list box.</p> <p>Configure SSID profiles in the SSID screen (see Section 9.2 on page 147 for information on configuring SSID).</p> <p>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>
Rates Configuration	<p>This section controls the data rates permitted for clients.</p> <p>For each Rate, select an option from the Configuration list. The options are:</p> <ul style="list-style-type: none"> • Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. • Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. • Disabled: Clients cannot connect to the access point at this speed.
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Breathing LED	Select this box to disable the WLAN LED (light). Clear this box to enable the WLAN LED.
Enable Spanning Tree Control (STP)	(R)STP (Section 8.4.1 on page 139) detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the NWA.
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 checkbox 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 Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

8.3.2 Bridge / Repeater Mode

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

Note: You can view an example of this setup in [Section 8.4.3 on page 141](#).

Figure 77 Wireless: Bridge / Repeater

Wireless

WLAN Interface:

Operating Mode:

802.11 Mode:

Disable channel switching for DFS

Choose Channel ID: [Disable DCS to unlock.](#)

Operating Channel: **Channel-044**

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 (ZyAIR PRO Series Compatible)

TKIP

AES

Index	Active	Remote Bridge MAC	PSK
1	<input type="checkbox"/>	<input type="text" value="00:00:00:05:00:00"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text" value="00:00:00:05:00:00"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text" value="00:00:00:05:00:00"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text" value="00:00:00:05:00:00"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text" value="00:00:00:05:00:00"/>	<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 24 Wireless: Bridge / Repeater

LABEL	DESCRIPTIONS
WLAN Interface	Select which WLAN adapter you want to configure. It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.
Operating Mode	Select Bridge / Repeater in this field.

Table 24 Wireless: Bridge / Repeater

LABEL	DESCRIPTIONS
802.11 mode	<p>This makes sure that only compliant WLAN devices can associate with the NWA.</p> <p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced.</p> <p>Select 802.11a to allow only IEEE 802.11a compliant WLAN devices to associate with the NWA.</p>
Disable channel switching for DFS	<p>This field displays only when you select 802.11a in the 802.11 Radio Mode field. Select this if you do not want to use DFS (Dynamic Frequency Selection).</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>
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. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.</p> <p>To have the NWA automatically select a channel, click Scan instead.</p>
Disable DCS to unlock	<p>This appears if the DCS feature is enabled.</p> <p>Click this to disable DCS and select a channel ID manually.</p> <p>Note: DCS is Disabled by default</p>
Operating Channel	<p>This field displays only when you select 802.11a in the 802.11 Radio Mode field.</p> <p>This is the channel currently being used by your AP.</p>
RTS/CTS Threshold	<p>Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).</p> <p>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.</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 256 and 2346.</p>

Table 24 Wireless: Bridge / Repeater

LABEL	DESCRIPTIONS
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 from 100% (Full Power), 50%, 25%, 12.5% and Minimum. See the product specifications for more information on your NWA's output power.</p> <p>Note: Reducing the output power also reduces the NWA's effective broadcast radius.</p>
Rates Configuration	<p>This section controls the data rates permitted for clients.</p> <p>For each Rate, select an option from the Configuration list. The options are:</p> <ul style="list-style-type: none"> • Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. • Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. • Disabled: Clients cannot connect to the access point at this speed.
Enable WDS Security (ZyAIR PRO Series Compatible)	<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>Note: 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"> • Select the type of security you want to use (TKIP or AES) to secure traffic on your WDS. • Enter a pre-shared key in the PSK field for each access point in your WDS. Each access point can use a different pre-shared key. • Configure WDS security and the relevant PSK in each of your other access point(s). <p>Note: Other APs must use the same encryption method to enable WDS security.</p>
TKIP	<p>Select this to enable Temporal Key Integrity Protocol (TKIP) security on your WDS. This option is compatible with other ZyXEL access points 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>Note: Check your other AP's documentation to make sure it supports WDS security.</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>
Index	<p>This is the index number of the bridge connection.</p>
Active	<p>Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.</p>

Table 24 Wireless: Bridge / Repeater

LABEL	DESCRIPTIONS
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.
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Breathing LED	Select this box to disable the WLAN LED (light). Clear this box to enable the WLAN LED.
Enable Spanning Tree Control (STP)	(R)STP (Section 8.4.1 on page 139) detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the NWA.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

8.3.3 AP + Bridge Mode

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

Figure 78 AP + Bridge

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
WLAN Interface		WLAN1			
Operating Mode		AP+Bridge			
802.11 Mode		802.11a			
<input checked="" type="checkbox"/> Super Mode					
<input checked="" type="checkbox"/> Disable channel switching for DFS					
Choose Channel ID		Channel-036 5180MHz Disable DCS to unlock.			
Operating Channel		Channel-044			
RTS/CTS Threshold		2346 (256 ~ 2346)			
Fragmentation Threshold		2307 (256 ~ 2346)(Fragmentation threshold shall be an even number)			
Beacon Interval		100 (30ms ~ 1000ms)			
DTIM		1 (1 ~ 100)			
Output Power		100%			
SSID Profile		NWA			
Rates Configuration					
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"/> Enable WDS Security (ZyAIR PRO Series Compatible)					
<input type="radio"/> TKIP					
<input type="radio"/> AES					
Index	Active	Remote Bridge MAC	PSK		
1	<input type="checkbox"/>	00:00:00:05:00:00			
2	<input type="checkbox"/>	00:00:00:05:00:00			
3	<input type="checkbox"/>	00:00:00:05:00:00			
4	<input type="checkbox"/>	00:00:00:05:00:00			
5	<input type="checkbox"/>	00:00:00:05:00:00			
<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 bridge labels in this screen.

Table 25 Wireless: AP + Bridge

LABEL	DESCRIPTIONS
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 AP + Repeater in this field.</p>
802.11 mode	<p>This makes sure that only compliant WLAN devices can associate with the NWA.</p> <p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced.</p> <p>Select 802.11a 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 802.11a in the 802.11 Radio Mode field. Select this if you do not want to use DFS (Dynamic Frequency Selection).</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>
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. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.</p> <p>To have the NWA automatically select a channel, click Scan instead.</p>
Disable DCS to unlock	<p>This appears if the DCS feature is enabled.</p> <p>Click this to disable DCS and select a channel ID manually.</p> <p>Note: DCS is Disabled by default</p>
Operating Channel	<p>This field displays only when you select 802.11a in the 802.11 Radio Mode field.</p> <p>This is the channel currently being used by your AP.</p>

Table 25 Wireless: AP + Bridge

LABEL	DESCRIPTIONS
RTS/CTS Threshold	<p>Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).</p> <p>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.</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 256 and 2346.</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 30ms 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>
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 from 100% (Full Power), 50%, 25%, 12.5% and Minimum. See the product specifications for more information on your NWA's output power.</p> <p>Note: Reducing the output power also reduces the NWA's effective broadcast radius.</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 SSID Profile from the drop-down list box.</p> <p>Configure SSID profiles in the SSID screen (see Section 9.2 on page 147 for information on configuring SSID).</p> <p>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>

Table 25 Wireless: AP + Bridge

LABEL	DESCRIPTIONS
Rates Configuration	<p>This section controls the data rates permitted for clients.</p> <p>For each Rate, select an option from the Configuration list. The options are:</p> <ul style="list-style-type: none"> • Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. • Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. • Disabled: Clients cannot connect to the access point at this speed.
Enable WDS Security (ZyAIR PRO Series Compatible)	<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>Note: 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"> • Select the type of security you want to use (TKIP or AES) to secure traffic on your WDS. • Enter a pre-shared key in the PSK field for each access point in your WDS. Each access point can use a different pre-shared key. • Configure WDS security and the relevant PSK in each of your other access point(s). <p>Note: Other APs must use the same encryption method to enable WDS security.</p>
TKIP	<p>Select this to enable Temporal Key Integrity Protocol (TKIP) security on your WDS. This option is compatible with other ZyXEL access points 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>Note: Check your other AP's documentation to make sure it supports WDS security.</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>
Index	<p>This is the index number of the bridge connection.</p>
Active	<p>Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.</p>
Remote Bridge MAC	<p>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.</p>
PSK	<p>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.</p>

Table 25 Wireless: AP + Bridge

LABEL	DESCRIPTIONS
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Breathing LED	Select this box to disable the WLAN LED (light). Clear this box to enable the WLAN LED.
Enable Spanning Tree Control (STP)	(R)STP (Section 8.4.1 on page 139) detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the NWA.
Enable Roaming	Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this checkbox to enable roaming on the NWA if you have two or more NWAs on the same subnet. Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

8.3.4 MBSSID Mode

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

Figure 79 Wireless: MBSSID

Wireless SSID Security RADIUS Layer-2 Isolation MAC Filter

WLAN Interface: WLAN1

Operating Mode: MBSSID

802.11 Mode: 802.11a

Super Mode

Disable channel switching for DFS

Choose Channel ID: Channel-036 5180MHz [Disable DCS to unlock.](#)

Operating Channel: Channel-044

RTS/CTS Threshold: 2346 (256 ~ 2346)

Fragmentation Threshold: 2307 (256 ~ 2346)(Fragmentation threshold shall be an even number)

Beacon Interval: 100 (30ms ~ 1000ms)

DTIM: 1 (1 ~ 100)

Output Power: 100%

Rates Configuration

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

Select SSID Profile

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

Enable Antenna Diversity

Enable Breathing LED

Enable Spanning Tree Protocol (STP)

Enable Roaming

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

Apply Reset

The following table describes the labels in this screen.

Table 26 Wireless: MBSSID

LABEL	DESCRIPTION
WLAN Interface	Select which WLAN adapter you want to configure. It is recommended that you configure the first WLAN adapter for AP functions and use the second WLAN adapter for bridge functions.
Operating Mode	Select MBSSID in this field to display the screen as shown

Table 26 Wireless: MBSSID

LABEL	DESCRIPTION
802.11 Mode	<p>This makes sure that only compliant WLAN devices can associate with the NWA.</p> <p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the NWA.</p> <p>Select 802.11b/g to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NWA. The transmission rate of your NWA might be reduced.</p> <p>Select 802.11a 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 802.11a in the 802.11 Radio Mode field. Select this if you do not want to use DFS (Dynamic Frequency Selection).</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>
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. Click MAINTENANCE and then the Channel Usage tab to open the Channel Usage screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network.</p> <p>To have the NWA automatically select a channel, click Scan instead.</p>
Disable DCS to unlock	<p>This appears if the DCS feature is enabled.</p> <p>Click this to disable DCS and select a channel ID manually.</p> <p>Note: DCS is Disabled by default</p>
Operating Channel	<p>This field displays only when you select 802.11a in the 802.11 Radio Mode field.</p> <p>This is the channel currently being used by your AP.</p>
RTS/CTS Threshold	<p>Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).</p> <p>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.</p>

Table 26 Wireless: MBSSID

LABEL	DESCRIPTION
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 256 and 2346 .
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 to reduce interference with other APs. Select one of the following 100%(Full Power) , 50% , 25% , 12.5% or Minimum . See the product specifications for more information on your NWA's output power. Note: Reducing the output power also reduces the NWA's effective broadcast radius.
Rates Configuration	This section controls the data rates permitted for clients. For each Rate , select an option from the Configuration list. The options are: <ul style="list-style-type: none"> • Basic (1~11 Mbps only): Clients can always connect to the access point at this speed. • Optional: Clients can connect to the access point at this speed, when permitted to do so by the AP. • Disabled: Clients cannot connect to the access point at this speed.
Select SSID Profile	An SSID profile is the set of parameters relating to one of the NWA's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating with the access point (AP) must have the same SSID. 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.
Index	Select the check box to activate an SSID profile.
Active	Select the check box to enable the bridge connection. Otherwise, clear the check box to disable it.

Table 26 Wireless: MBSSID

LABEL	DESCRIPTION
Profile	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. Configure SSID profiles in the SSID screen.
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Breathing LED	Select this box to disable the WLAN LED (light). Clear this box to enable the WLAN LED.
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 the check box to activate STP on the NWA.
Enable Roaming	Roaming allows wireless stations to switch from one access point to another as they move from one coverage area to another. Select this checkbox to enable roaming on the NWA if you have two or more NWAs on the same subnet. Note: All APs on the same subnet and the wireless stations must have the same SSID to allow roaming.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

8.4 Technical Reference

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

8.4.1 Spanning Tree Protocol (STP)

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

8.4.1.1 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.

8.4.1.2 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 27 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.

8.4.1.3 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.

8.4.1.4 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 28 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.

8.4.2 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.

8.4.3 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.

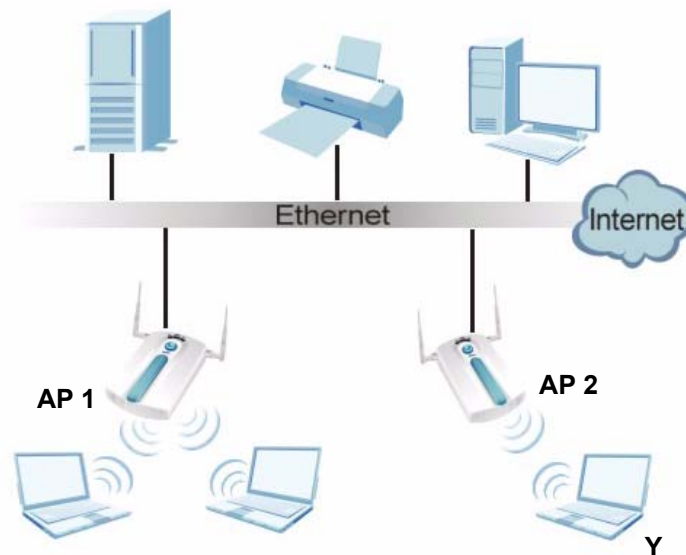
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is known as roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access 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 80 on page 142](#).

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 80 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**.

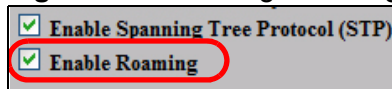
8.4.3.1 Requirements for Roaming

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 81 Enabling Roaming



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

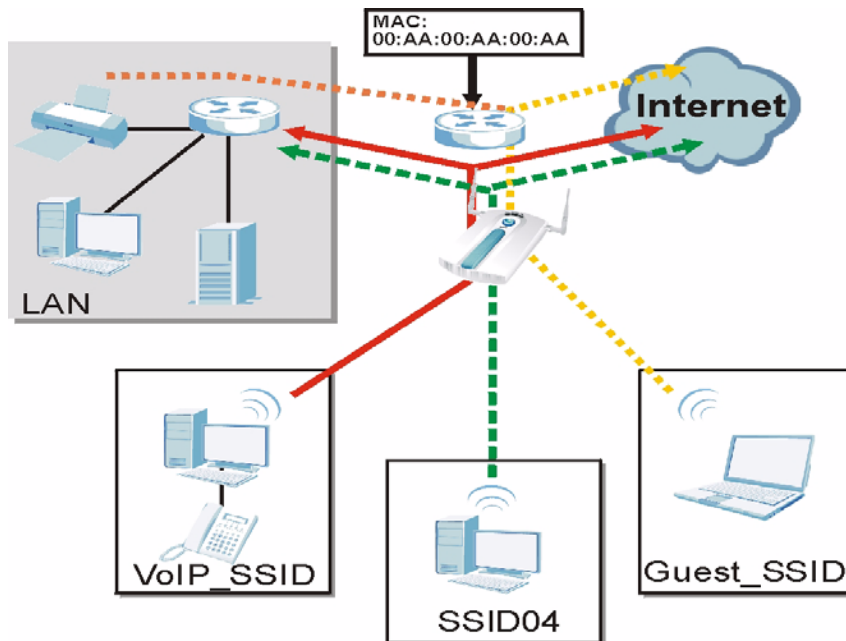
Note: Roaming cannot be enabled in Bridge / Repeater mode.

SSID Screen

9.1 Overview

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

Figure 82 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**).

9.1.1 What You Can Do in the SSID Screen

Use the **Wireless > SSID** screen (see [Section 9.2 on page 147](#)) to configure up to 16 SSID profiles for your NWA.

9.1.2 What You Need To Know About SSID

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

When the NWA is set to Access Point, AP + Bridge or MBSSID mode, you need to choose the SSID profile(s) you want to use in your wireless network (see [Section 8.3 on page 123](#) 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.

9.2 The SSID Screen

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

Figure 83 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 29 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 Section 10.2 on page 157 for more information.
RADIUS	This field displays which RADIUS profile is currently associated with each SSID profile, if you have a RADIUS server configured.
QoS	This field displays the Quality of Service setting for this profile or NONE if QoS is not configured on a profile.

Table 29 SSID

LABEL	DESCRIPTION
Layer-2 Isolation	This field displays which layer 2 isolation profile is currently associated with each SSID profile, or Disable 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 Disable if MAC filtering is not configured on an SSID profile.
Edit	Click the radio button next to the profile you want to configure and click Edit to go to the SSID configuration screen.

9.2.1 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 84 Configuring SSID

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name	VoIP_SSID				
SSID	ZyXEL01				
Hide Name(SSID)	Disable				
Security	security01				
RADIUS	radius01				
QoS	VoIP				
Layer-2 Isolation	Disable				
Intra-BSS Traffic blocking	Disable				
MAC Filtering	Disable				
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

The following table describes the labels in this screen.

Table 30 Configuring SSID

LABEL	DESCRIPTION
Profile Name	Displays the 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 Disable if you want the NWA to broadcast this SSID (a wireless client scanning for an AP will find this SSID). Alternatively, select Enable 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 Section 10.2 on page 157 for more information.
RADIUS	Select a RADIUS profile from the drop-down list box, if you have a RADIUS server configured. If you do not need to use RADIUS authentication, ignore this field. See Section 11.2 on page 171 for more information.

Table 30 Configuring SSID

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

9.3 Technical Reference

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

9.3.1 WMM QoS

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

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

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

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

9.3.1.1 WMM QoS Priorities

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

Table 31 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.

9.3.2 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 32 Typical Packet Sizes

APPLICATION	TIME SENSITIVITY	TYPICAL PACKET SIZE (BYTES)
Voice over IP (SIP)	High	< 250
Online Gaming	High	60 ~ 90
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 33 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.

9.3.3 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 9.2.1 on page 148](#) 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 9.3.3.1 on page 152](#)).
- automatically prioritize all packets going from your wireless network to the wired network (see [Section 9.3.3.2 on page 152](#)).

9.3.3.1 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 34 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

9.3.3.2 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 35 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

9.3.4 Type Of Service (ToS)

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

9.3.4.1 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route

based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

9.3.4.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

Figure 85 DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)
-----------------	-------------------

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

9.3.4.3 ToS (Type of Service) and WMM QoS

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

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

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

Table 36 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping

DSCP VALUE	WMM QOS PRIORITY LEVEL
224, 192	voice
160, 128	video
96, 0 ^A	besteffort
64, 32	background

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

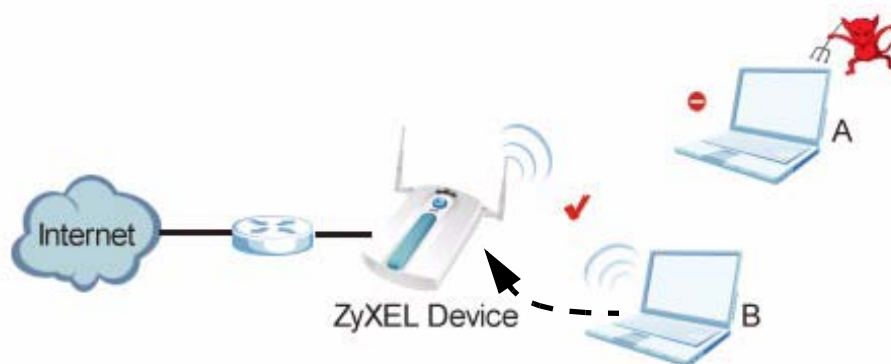
Wireless Security Screen

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 86 Securing the Wireless Network



In the figure above, the NWA (**ZyXEL Device**) checks the identity of devices (**A** and **B**) before giving them access to the network. In this scenario, **A** is denied access to the network, while **B** is granted connectivity.

The NWA secures communications via data encryption, wireless client authentication and MAC address filtering. It can also hide its identity in the network.

10.1.1 What You Can Do in the Wireless Security Screen

Use the **Wireless > Security** screen (see [Section 10.2 on page 157](#)) to choose the security mode for your NWA.

10.1.2 What You Need To Know About Wireless Security

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

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 37 Wireless Security Levels

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

The available security modes in your NWA are as follows:

- **None.** No data encryption.
- **WEP.** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.
- **802.1x-Only.** This is a standard that extends the features of IEEE 802.11 to support extended authentication. It provides additional accounting and control features. This option does not support data encryption.

- **802.1x-Static64.** This provides 802.1x-Only authentication with a static 64bit WEP key and an authentication server.
- **802.1x-Static128.** This provides 802.1x-Only authentication with a static 128bit WEP key and an authentication server.
- **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.

10.2 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 87 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 38 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 Security configuration screen.
Security Mode	This field displays the security mode this security profile uses.
Edit	Select an entry from the list and click Edit 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 88 Security Profile

The screenshot shows a configuration window with tabs for Wireless, SSID, Security, RADIUS, Layer-2 Isolation, and MAC Filter. The Security tab is active. It contains two input fields: 'Profile Name' with the text 'security01' and 'Security Mode' with a dropdown menu showing 'None'. At the bottom, there are 'Apply' and 'Reset' buttons.

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

10.2.1 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 89 Security: WEP

The screenshot shows the Security: WEP configuration screen. It includes fields for 'Profile Name' (security03), 'Security Mode' (WEP), 'WEP Encryption' (64-bit WEP), and 'Authentication Method' (Auto). Below these are instructions for 64-bit and 128-bit WEP, radio buttons for 'ASCII' and 'Hex', and four radio buttons for 'Key 1' through 'Key 4', each with an input field. 'Apply' and 'Reset' buttons are at the bottom.

The following table describes the labels in this screen.

Table 39 Security: WEP

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose WEP in this field.
WEP Encryption	Select Disable to allow wireless stations to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to enable data encryption.

Table 39 Security: WEP

LABEL	DESCRIPTION
Authentication Method	<p>There are two types of WEP authentication namely, Open System and Shared Key.</p> <p>Open system is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.</p> <p>Shared key mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.</p> <ul style="list-style-type: none"> • Select Shared Key to have the NWA authenticate only those wireless clients that use Shared Key mode and have the correct WEP key. • Select Auto to have the NWA allow association with wireless clients that use Open System mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. The NWA authenticates wireless clients using Shared Key mode that have the correct WEP key.
ASCII	Select this option to enter ASCII characters as the WEP keys.
Hex	<p>Select this option to enter hexadecimal characters as the WEP keys.</p> <p>The preceding "0x" is entered automatically.</p>
Key 1 to Key 4	<p>The WEP keys are used to encrypt data. Both the NWA and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.</p>
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

10.2.2 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 90 Security: 802.1x Only

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

The following table describes the labels in this screen.

Table 40 Security: 802.1x Only

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose 802.1x Only in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. The default value is 0 , which means the 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 3600 seconds (or 1 hour).
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

10.2.3 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 91 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

Radio	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name		security03			
Security Mode		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		0 (seconds, 0 means no ReAuthentication)			
Idle Timeout		3600 (seconds)			
		<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

The following table describes the labels in this screen.

Table 41 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 802.1x Static 64 or 802.1x Static 128 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 802.1x Static 64, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</p> <p>If you chose 802.1x Static 128-bit, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.</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 41 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. The default value is 0 , which means the 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 3600 seconds (or 1 hour).
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

10.2.4 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 92 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 42 Security: WPA

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

Table 42 Security: WPA

LABEL	DESCRIPTION
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. The default value is 0 , which means the 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 3600 seconds (or 1 hour).
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK mode. The NWA default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

10.2.5 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 93 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 43 Security: WPA2 or WPA2-MIX

LABEL	DESCRIPTIONS
Profile Name	Type a name to identify this security profile.
Security Mode	Choose WPA2 or WPA2-MIX in this field.
ReAuthentication Timer	<p>Specify how often wireless stations have to resend usernames and passwords in order to stay connected.</p> <p>The default value is 0, which means the 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 3600 seconds (or 1 hour).</p>
Group Key Update Timer	<p>The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK mode. 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 Enable to allow PMK caching, or Disable 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 Enable to allow pre-authentication, or Disable to switch it off.</p>
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

10.2.6 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 94 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Profile Name		security01			
Security Mode		WPA2-PSK-MIX			
Pre-Shared Key					
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 not previously discussed

Table 44 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Profile Name	Type a name to identify this security profile.
Security Mode	Choose WPA-PSK , WPA2-PSK or WPA2-PSK-MIX in this field.
Pre-Shared Key	<p>The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials.</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>The default value is 0, which means the 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 3600 seconds (or 1 hour).</p>

Table 44 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK mode. The NWA's default is 1800 seconds (30 minutes).
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

10.3 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 or WPA2 security if you have WPA/WPA2-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK or WPA2-PSK if you have WPA/WPA2-aware wireless clients but no RADIUS server.
- If you don't have WPA/WPA2-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 A on page 303](#).

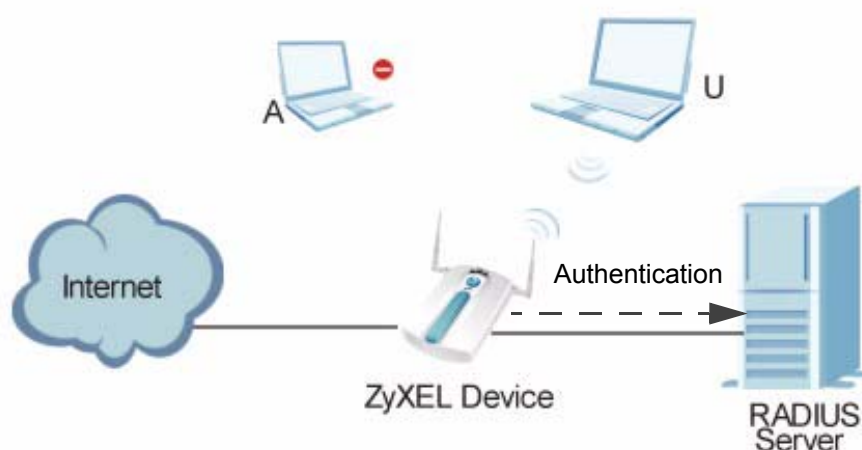
RADIUS Screen

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 95 RADIUS Server Setup



In the figure above, wireless clients **A** and **U** are trying to access the Internet using the NWA (**ZyXEL Device**). 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.

11.1.1 What You Can Do in the RADIUS Screen

Use the **Security > RADIUS** screen (see [Section 11.2 on page 171](#)) if you want to authenticate wireless users using a RADIUS Server and/or Accounting Server.

11.1.2 What You Need To Know About RADIUS

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.

11.2 The RADIUS Screen

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

Figure 96 RADIUS

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Index : <input type="text" value="1"/>					
Profile Name : <input type="text" value="radius01"/>					
		Primary <input type="radio"/> Internal <input checked="" type="radio"/> External <input type="checkbox"/> Active		Backup <input type="radio"/> Internal <input checked="" type="radio"/> External <input type="checkbox"/> Active	
RADIUS Option					
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 45 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 Index number above.
Primary	Configure the fields below to set up user authentication and accounting.
Backup	<p>If the NWA cannot communicate with the Primary accounting server, you can have the NWA use a Backup RADIUS server. Make sure the Active check boxes are selected if you want to use backup servers.</p> <p>The NWA will attempt to communicate three times before using the Backup servers. Requests can be issued from the client interface to use the backup server. The length of time for each authentication is decided by the wireless client or based on the configuration of the ReAuthentication Timer field in the Security screen.</p>
RADIUS Option	

Table 45 RADIUS

LABEL	DESCRIPTION
Internal	Select this check box to use the NWA's internal authentication server. The Active , RADIUS Server IP Address , RADIUS Server Port and Share Secret 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 Internal .
RADIUS Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation. This field is not available when you select Internal .
RADIUS Server Port	Enter the port number of the external authentication server. 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 Internal .
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the NWA. The key must be the same on the external authentication server and your NWA. The key is not sent over the network. This field is not available when you select Internal .
Active	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. 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 Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

Layer-2 Isolation Screen

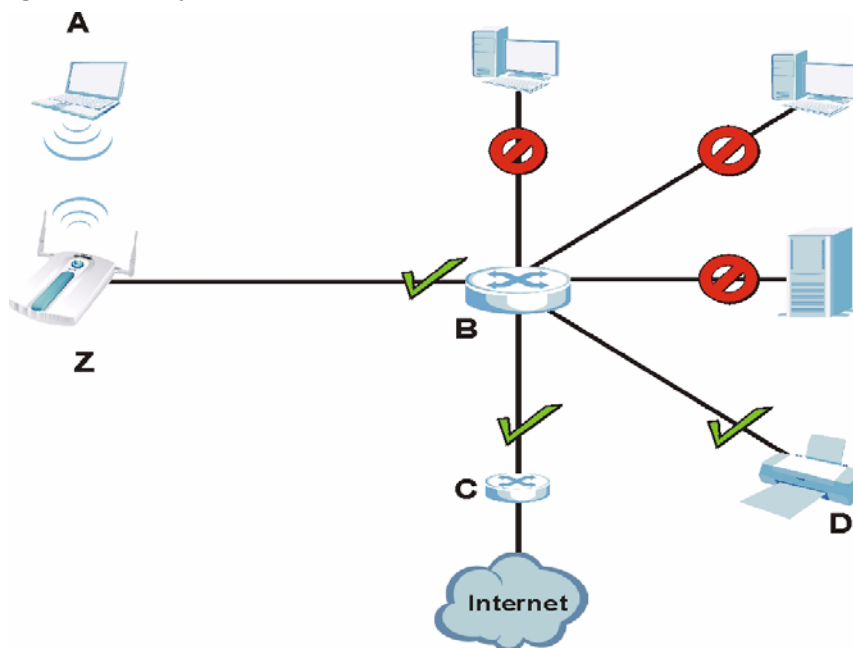
12.1 Overview

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 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 97 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.

12.1.1 What You Can Do in the Layer-2 Isolation Screen

Use the **Wireless > Layer-2 Isolation** screen (see [Section 12.2 on page 175](#)) to configure the MAC addresses of the wireless client, AP, computer or router to which you want to allow the associated wireless clients to have access.

12.1.2 What You Need To Know About Layer-2 Isolation

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 NWA's wireless clients.

12.2 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 98 Layer 2 Isolation

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter																																																			
<table border="1"> <thead> <tr> <th></th> <th>Index</th> <th>Profile Name</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/></td> <td>1</td> <td>I2isolation01</td> </tr> <tr> <td><input type="radio"/></td> <td>2</td> <td>I2isolation02</td> </tr> <tr> <td><input type="radio"/></td> <td>3</td> <td>I2isolation03</td> </tr> <tr> <td><input type="radio"/></td> <td>4</td> <td>I2isolation04</td> </tr> <tr> <td><input type="radio"/></td> <td>5</td> <td>I2isolation05</td> </tr> <tr> <td><input type="radio"/></td> <td>6</td> <td>I2isolation06</td> </tr> <tr> <td><input type="radio"/></td> <td>7</td> <td>I2isolation07</td> </tr> <tr> <td><input type="radio"/></td> <td>8</td> <td>I2isolation08</td> </tr> <tr> <td><input type="radio"/></td> <td>9</td> <td>I2isolation09</td> </tr> <tr> <td><input type="radio"/></td> <td>10</td> <td>I2isolation10</td> </tr> <tr> <td><input type="radio"/></td> <td>11</td> <td>I2isolation11</td> </tr> <tr> <td><input type="radio"/></td> <td>12</td> <td>I2isolation12</td> </tr> <tr> <td><input type="radio"/></td> <td>13</td> <td>I2isolation13</td> </tr> <tr> <td><input type="radio"/></td> <td>14</td> <td>I2isolation14</td> </tr> <tr> <td><input type="radio"/></td> <td>15</td> <td>I2isolation15</td> </tr> <tr> <td><input type="radio"/></td> <td>16</td> <td>I2isolation16</td> </tr> </tbody> </table>							Index	Profile Name	<input checked="" type="radio"/>	1	I2isolation01	<input type="radio"/>	2	I2isolation02	<input type="radio"/>	3	I2isolation03	<input type="radio"/>	4	I2isolation04	<input type="radio"/>	5	I2isolation05	<input type="radio"/>	6	I2isolation06	<input type="radio"/>	7	I2isolation07	<input type="radio"/>	8	I2isolation08	<input type="radio"/>	9	I2isolation09	<input type="radio"/>	10	I2isolation10	<input type="radio"/>	11	I2isolation11	<input type="radio"/>	12	I2isolation12	<input type="radio"/>	13	I2isolation13	<input type="radio"/>	14	I2isolation14	<input type="radio"/>	15	I2isolation15	<input type="radio"/>	16	I2isolation16
	Index	Profile Name																																																						
<input checked="" type="radio"/>	1	I2isolation01																																																						
<input type="radio"/>	2	I2isolation02																																																						
<input type="radio"/>	3	I2isolation03																																																						
<input type="radio"/>	4	I2isolation04																																																						
<input type="radio"/>	5	I2isolation05																																																						
<input type="radio"/>	6	I2isolation06																																																						
<input type="radio"/>	7	I2isolation07																																																						
<input type="radio"/>	8	I2isolation08																																																						
<input type="radio"/>	9	I2isolation09																																																						
<input type="radio"/>	10	I2isolation10																																																						
<input type="radio"/>	11	I2isolation11																																																						
<input type="radio"/>	12	I2isolation12																																																						
<input type="radio"/>	13	I2isolation13																																																						
<input type="radio"/>	14	I2isolation14																																																						
<input type="radio"/>	15	I2isolation15																																																						
<input type="radio"/>	16	I2isolation16																																																						
<input type="button" value="Edit"/>																																																								

The following table describes the labels in this screen.

Table 46 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 Layer-2 Isolation Configuration screen.
Edit	Select an entry from the list and click Edit to configure settings for that profile.

12.2.1 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 99 Layer-2 Isolation Configuration Screen

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

The following table describes the labels in this screen.

Table 47 Layer-2 Isolation Configuration

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.

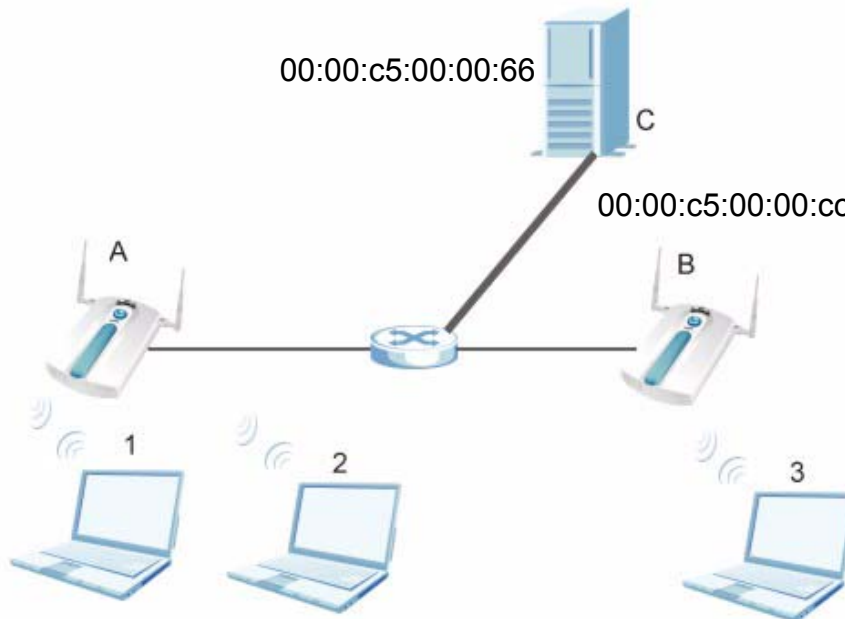
Table 47 Layer-2 Isolation Configuration

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

12.3 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 100 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 101 Layer-2 Isolation Example 1

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Layer-2 Isolation Configuration					
Profile Name		i2isolation01			
Allow devices with these MAC addresses					
Index	MAC Address	Description	Index	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.

Layer-2 Isolation Example 2

Wireless	SSID	Security	RADIUS	Layer-2 Isolation	MAC Filter
Layer-2 Isolation Configuration					
Profile Name		i2isolation01			
Allow devices with these MAC addresses					
Index	MAC Address	Description	Index	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	

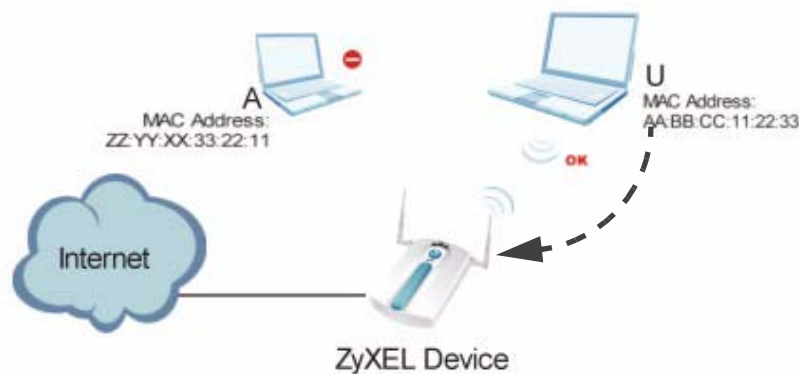
MAC Filter Screen

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 102 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 (**ZyXEL Device**). The MAC address of client **A** is either denied association or is not in the list of allowed wireless clients specified in the NWA.

13.1.1 What You Can Do in the MAC Filter Screen

Use the **Wireless > MAC Filter** screen (see [Section 13.2 on page 180](#)) to specify which wireless station is allowed or denied access to the NWA.

13.1.2 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.

13.2 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 128 MAC addresses.

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

13.2.1 Configuring the MAC Filter

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

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**.

Figure 103 Wireless > MAC Filter > Edit

Index	MAC Address	Description	Index	MAC Address	Description
1	00:00:00:00:00:00		65	00:00:00:00:00:00	
2	00:00:00:00:00:00		66	00:00:00:00:00:00	
3	00:00:00:00:00:00		67	00:00:00:00:00:00	
4	00:00:00:00:00:00		68	00:00:00:00:00:00	
5	00:00:00:00:00:00		69	00:00:00:00:00:00	
6	00:00:00:00:00:00		70	00:00:00:00:00:00	
7	00:00:00:00:00:00		71	00:00:00:00:00:00	
8	00:00:00:00:00:00		72	00:00:00:00:00:00	

The following table describes the labels in this screen.

Table 48 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 Deny Association to block access to the router. MAC addresses not listed will be allowed to access the router. Select Allow Association to permit access to the router. MAC addresses not listed will be denied access to the router.
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 Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

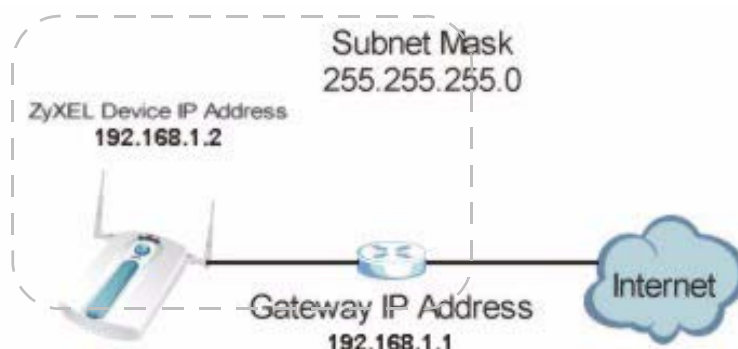
Note: If you configure both the **MAC Address Filter** table and **Group Settings** table and a client matches a MAC address specified in both tables, the settings in the **Group Settings** is applied by the NWA first.

IP Screen

14.1 Overview

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 104 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.

14.1.1 What You Can Do in the IP Screen

Use the **IP Screen** (see [Section 14.2 on page 184](#)) to configure the IP address of your NWA.

14.1.2 What You Need To Know About IP

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

- IP address of 192.168.1.2
- Subnet mask of 255.255.255.0 (24 bits)

These parameters should work for the majority of installations.

14.2 The IP Screen

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

Figure 105 IP Setup

The following table describes the labels in this screen.

Table 49 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.
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 Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

14.3 Technical Reference

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

14.3.1 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 50 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.

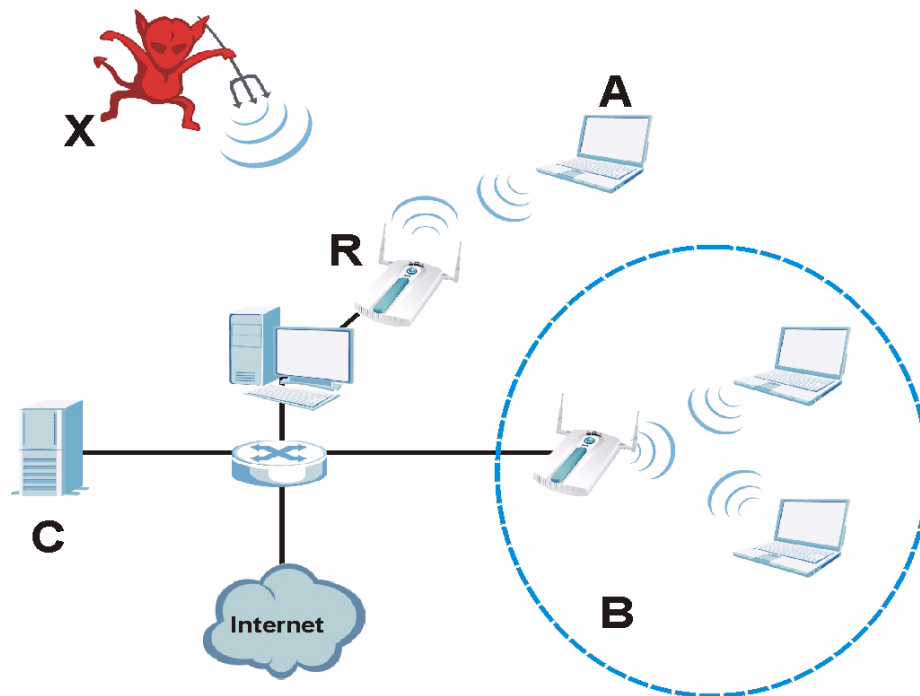
Rogue AP Detection

15.1 Overview

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 106 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**).

15.1.1 What You Can Do in the Rogue AP Screen

- Use the **Rogue AP > Configuration** screen (see [Section 15.2 on page 190](#)) 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 15.2.1 on page 191](#)) to specify APs as trusted.
- Use the **Rogue AP > Rogue AP** screen (see [Section 15.2.2 on page 192](#)) to display details of all IEEE 802.11a/b/g/n wireless access points within the NWA's coverage area, except for the NWA itself and the access points included in the friendly AP list.

15.1.2 What You Need To Know About Rogue AP

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

You can configure the NWA to detect rogue IEEE 802.11a/n (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 242](#) 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 15.2 on page 190](#)).

Friendly APs

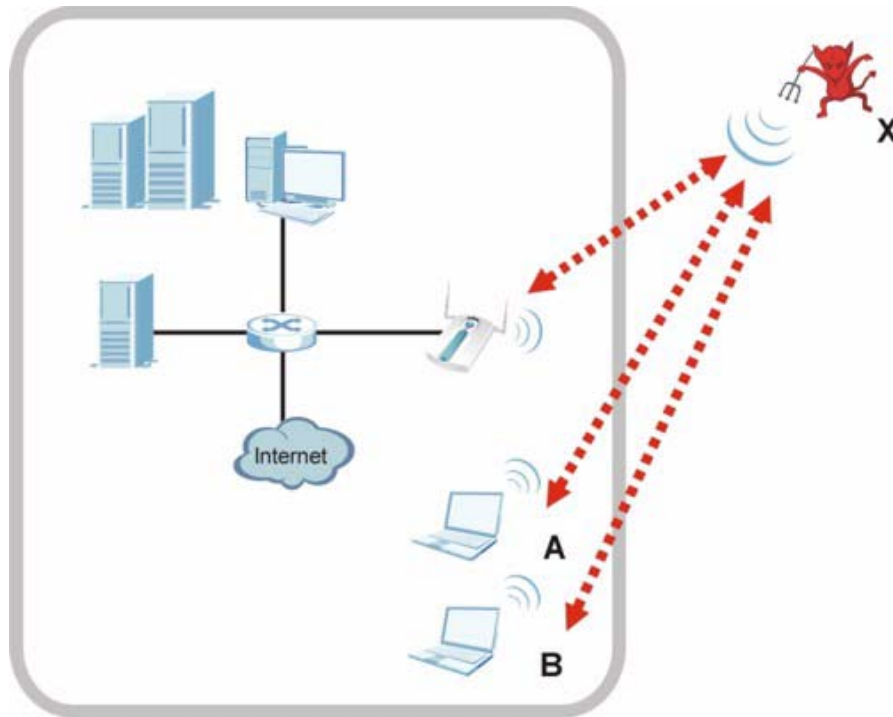
If you have more than one AP in your wireless network, you can configure a list of "friendly" APs. Friendly APs are other wireless access points, aside from the NWA, that are detected in your network, as well as any others that you know are not a threat (those from neighboring networks, for example). 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.

“Honeytrap” 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 107 “Honeytrap” 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.

15.2 Configuration Screen

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

Figure 108 Rogue AP Configuration

The following table describes the labels in this screen.

Table 51 Rogue AP Configuration

LABEL	DESCRIPTION
Rogue AP Period Detection	Select Enable to turn rogue AP detection on. You must also enter a time value in the Period field. Select No 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 Enable in the Active Rogue AP Period Detection field.
Expiration Time (minutes)	Specify how long (between 30 and 180 minutes) an AP's entry can remain in the Rogue AP List 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 ROGUE AP > Friendly AP screen) to your computer.
File Path	Enter the location of a previously-saved friendly AP list to upload to the NWA. Alternatively, click the Browse button to locate a list.
Browse	Click this button to locate a previously-saved list of friendly APs to upload to the NWA.

Table 51 Rogue AP Configuration

LABEL	DESCRIPTION
Import	Click this button to upload the previously-saved list of friendly APs displayed in the File Path field to the NWA.
Apply	Click Apply to save your settings.
Reset	Click Reset to return all fields in this screen to their previously-saved values.

15.2.1 Friendly AP Screen

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

Figure 109 Rogue AP Friendly AP

Index	MAC Address	SSID	Channel	Radio Mode	Security	Last Seen	Description
1	06:19:cb:51:ef:cf	ZyXEL04	6		WPA2-MIX	8:58:26	N/A

The following table describes the labels in this screen.

Table 52 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. This shows N/A if you do not enter anything.
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.

Table 52 Rogue AP Friendly AP

LABEL	DESCRIPTION
Radio Mode	The field displays the radio mode the AP is currently using.
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.

15.2.2 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 110 Rogue AP

The screenshot shows a web interface with three tabs: Configuration, Friendly AP, and Rogue AP. The Rogue AP tab is active. Below the tabs is a 'Rogue AP List' section with a 'Refresh' button. A table lists 10 detected access points with columns for Index, Select, MAC Address, SSID, Channel, Radio Mode, Security, Last Seen, and Description. At the bottom of the table are 'Add To Friendly AP List' and 'Reset' buttons.

Index	Select	MAC Address	SSID	Channel	Radio Mode	Security	Last Seen	Description
1	<input type="checkbox"/>	00:19:cb:4b:22:0f	ZyXEL_MIS	1	G	WEP	2:21:30	
2	<input type="checkbox"/>	06:19:cb:4b:22:0f	ZyXEL_MIS_WPA	1	G	WPA2-MIX	2:21:30	
3	<input type="checkbox"/>	0a:19:cb:4b:22:0f	ZyXEL_Guest	1	G	WPA2-MIX	2:21:30	
4	<input type="checkbox"/>	00:17:9a:50:24:9f	dlink	1	N	None	2:21:30	
5	<input type="checkbox"/>	00:13:49:aa:01:32	e2DSL	1	G	None	2:21:30	
6	<input type="checkbox"/>	00:19:cb:30:22:10	6812-wifi	3	G	WPA-PSK	2:21:22	
7	<input type="checkbox"/>	00:23:19:20:34:e1	ZyXEL	6	G	WPA-PSK	2:21:30	
8	<input type="checkbox"/>	00:19:cb:0a:e0:80	ZyXEL	6	G	None	2:21:30	
9	<input type="checkbox"/>	00:19:cb:0a:e0:87	ZyXEL	6	G	None	2:21:30	
10	<input type="checkbox"/>	00:19:cb:3c:21:22	ZyXEL	6	G	None	2:21:22	

The following table describes the labels in this screen.

Table 53 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 Section 15.2.1 on page 191)
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 Section 15.2.1 on page 191)

Table 53 Rogue AP

LABEL	DESCRIPTION
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	The field displays the radio mode the AP is currently using.
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	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 Add to Friendly AP List . 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 Active check box, enter a short description in the Description field and click this button to add the entry to the friendly AP list (see Section 15.2.1 on page 191). When the NWA next scans for rogue APs, the selected AP does not appear in the rogue AP list.
Reset	Click Reset to return all fields in this screen to their default values.

Remote Management Screens

16.1 Overview

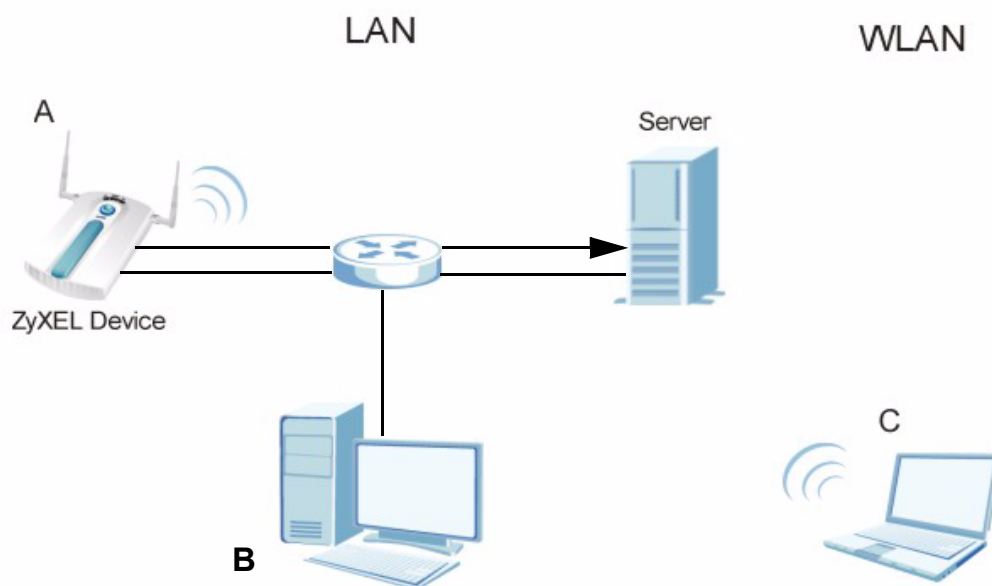
This chapter shows you how to enable remote management of your NWA. It provides information on determining which services or protocols can access which of the NWA's interfaces.

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)

In the figure below, 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).

Figure 111 Remote Management Example



16.1.1 What You Can Do in the Remote Management Screens

- Use the **Telnet** screen (see [Section 16.2 on page 198](#)) to configure through which interface(s) and from which IP address(es) you can use Telnet to manage the NWA. A Telnet connection is prioritized by the NWA over other remote management sessions.
- Use the **FTP** screen (see [Section 16.3 on page 199](#)) to configure through which interface(s) and from which IP address(es) you can use File Transfer Protocol (FTP) to manage the NWA. You can use FTP to upload the latest firmware for example.
- Use the **WWW** screen (see [Section 16.4 on page 200](#)) to configure through which interface(s) and from which IP address(es) you can use the Web Browser to manage the NWA.
- Use the **SNMP** screen (see [Section 16.5 on page 203](#)) to configure through which interface(s) and from which IP address(es) a network systems manager can access the NWA.

16.1.2 What You Need To Know About Remote Management

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

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).

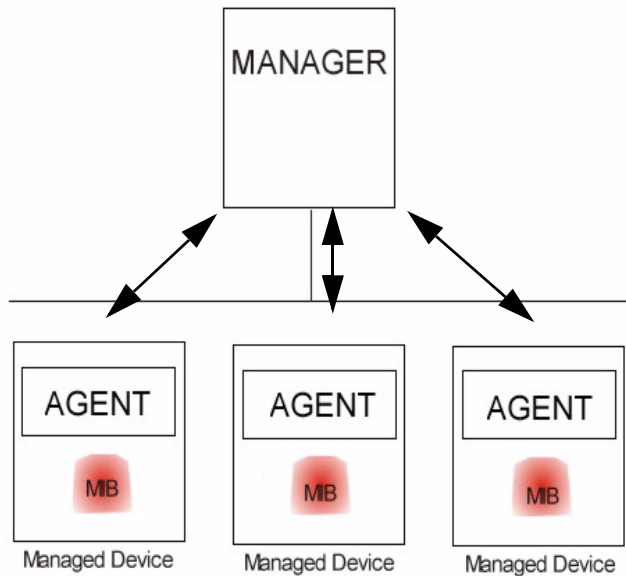
SNMP

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 112 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:
 - Telnet
 - 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.

16.2 The Telnet Screen

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

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

Figure 113 Remote Management: Telnet

The following table describes the labels in this screen.

Table 54 Remote Management: Telnet

LABEL	DESCRIPTION
TELNET	
Server Port	This is set to port 23 by default. 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 54 Remote Management: Telnet

LABEL	DESCRIPTION
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 All to allow any computer to access the NWA using this service.</p> <p>Choose Selected to just allow the computer with the IP address that you specify to access the NWA using this service.</p>
SSH	
Server Certificate	<p>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 Certificates > My Certificates screen.</p>
Server Port	<p>This is set to port 22 by default.</p> <p>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.</p>
Server Access	<p>Select the interface(s) through which a computer may access the NWA using SSH.</p>
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 All to allow any computer to access the NWA using this service.</p> <p>Choose Selected to just allow the computer with the IP address that you specify to access the NWA using this service.</p>
Apply	<p>Click Apply to save your customized settings and exit this screen.</p>
Reset	<p>Click Reset to begin configuring this screen afresh.</p>

16.3 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 114 Remote Management: FTP

The following table describes the labels in this screen.

Table 55 Remote Management: FTP

LABEL	DESCRIPTION
Server Port	This is set to port 21 by default. You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NWA using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NWA using this service. Select All to allow any computer to access the NWA using this service. Choose Selected to just allow the computer with the IP address that you specify to access the NWA using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

16.4 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 115 Remote Management: WWW

The following table describes the labels in this screen.

Table 56 Remote Management: WWW

LABEL	DESCRIPTION
WWW	
Server Port	This is set to port 80 by default. You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NWA using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NWA using this service. Select All to allow any computer to access the NWA using this service. Choose Selected to just allow the computer with the IP address that you specify to access the NWA using this service.
HTTPS	
Server Certificate	Select the Server Certificate 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 Authenticate Client Certificates (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).

Table 56 Remote Management: WWW

LABEL	DESCRIPTION
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: 8443 " as the URL.
Server Access	Select a NWA interface from Server Access on which incoming HTTPS access is allowed. You can allow only secure web configurator access by setting the HTTP Server Access field to Disable and setting the HTTPS Server Access 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 All to allow any computer to access the NWA using this service. Choose Selected to just allow the computer with the IP address that you specify to access the NWA using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

16.5 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 116 Remote Management: SNMP

The screenshot shows the 'SNMP Configuration' section with the following fields and values:

- Get Community: public
- Set Community: public
- Trap Destination: 0.0.0.0
- SNMP Version: SNMPv2
- Trap Community: public
- User Profile: SNMPv3Admin

The 'SNMP' section includes:

- Service Port: 161
- Service Access: WLAN & LAN
- Secured Client IP Address: All Selected, 0.0.0.0

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

The following table describes the labels in this screen.

Table 57 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , 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 which you want the NWA to send SNMP traps.

Table 57 Remote Management: SNMP

LABEL	DESCRIPTION
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 (SNMPv1), SNMP version 2 (SNMPv2) or SNMP version 3 (SNMPv3).
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 SNMPv1 or SNMPv2 is selected in the SNMP Version field.
User Profile	This field is available only when you select SNMPv3 in the SNMP Version field. 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. The NWA has two SNMP version 3 login accounts, User and Admin . Each account has different security settings. You can use either account's security settings for authenticating SNMP traps. Select User to have the NWA use the User account's security settings, or select Admin to have the NWA use the Admin account's security settings. Use the Configure SNMPv3 User Profile link to set up each account's security settings.
Configure SNMPv3 User Profile	Click this to go to the SNMPv3 User Profile screen, where you can configure administration and user login details. Refer to Section 16.5.1 on page 205 to see this screen.
SNMP	
Service Port	This is set to port 161 by default. 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	A secured client is a "trusted" computer that is allowed to communicate with the NWA using this service. Select All to allow any computer to access the NWA using this service. Choose Selected to just allow the computer with the IP address that you specify to access the NWA using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

16.5.1 SNMPv3 User Profile

Use this screen to configure the SNMPv3 profile. Click **Configure SNMPv3 User Profile** in the **REMOTE MGMT > SNMP** screen, the following screen displays.

Figure 117 Remote Management: SNMPv3 User Profile

The screenshot shows a web-based configuration interface for SNMPv3 user profiles. It is organized into two main sections: 'SNMPv3Admin' and 'SNMPv3User'. Each section contains a 'Enable' checkbox, followed by input fields for 'User Name', 'Password', and 'Confirm Password'. Below these are dropdown menus for 'Access Type' (with 'Set' selected), 'Authentication Protocol' (with 'MD5' selected), and 'Privacy Protocol' (with 'None' selected). At the bottom of the form are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 58 Remote Management: SNMPv3 User Profile

LABEL	DESCRIPTION
SNMPv3Admin	
Enable SNMPv3Admin	Click this to activate the security settings for this Admin account.
User Name	Enter the name you want to use for authentication with managers using SNMP v3.
Password	Enter the password for the user name.
Confirm Password	Retype the password for verification.
Access Type	The default value for this is Set . This allows the manager to set values for object variables within an agent.
Authentication Protocol	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.

Table 58 Remote Management: SNMPv3 User Profile

LABEL	DESCRIPTION
Privacy Protocol	Select the encryption method for SNMP communication from this user. You can choose one of the following: <ul style="list-style-type: none"> • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
SNMPv3User	
Enable SNMPv3User	Click this to activate the security settings for this User account.
User Name	Enter the name you want to use for authentication with managers using SNMP v3.
Password	Enter the password for the user name.
Confirm Password	Retype the password for verification.
Access Type	The default value for this is Get . This allows the manager to retrieve an object variable from the agent.
Authentication Protocol	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy Protocol	Select the encryption method for SNMP communication from this user. You can choose one of the following: <ul style="list-style-type: none"> • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

16.6 Technical Reference

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

16.6.1 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.

16.6.2 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.

16.6.3 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 59 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 59 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 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 60 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

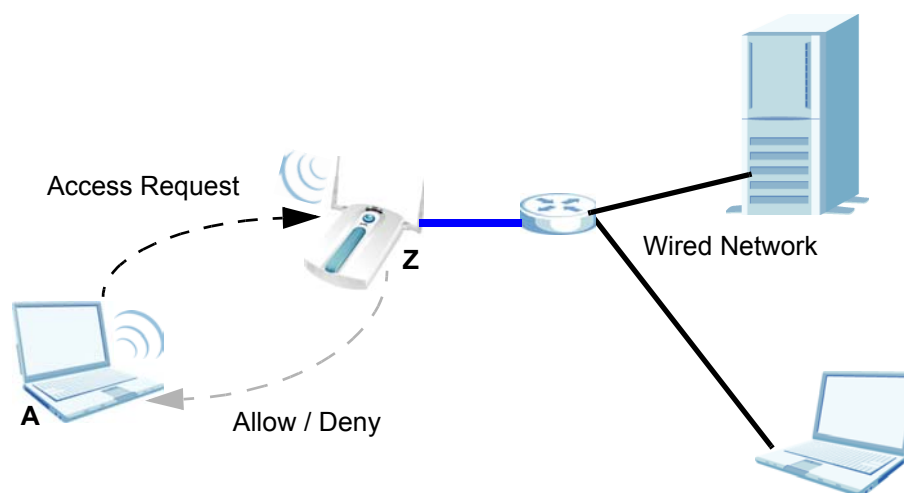
17.1 Overview

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 118 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 11.2](#) on page 175.

17.1.1 What You Can Do in this Chapter

- Use the **Setting** screen (see [Section 17.2 on page 210](#)) to turn the NWA's internal RADIUS server off or on and to view information about the NWA's certificates.
- Use the **Trusted AP** screen (see [Section 17.3 on page 212](#)) to specify APs as trusted. Trusted APs can use the NWA's internal RADIUS server to authenticate wireless clients.
- Use the **Trusted Users** screen (see [Section 17.4 on page 213](#)) to configure a list of wireless client user names and passwords.

17.1.2 What You Need To Know

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

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.

17.2 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 119 Internal RADIUS Server Setting

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

The following table describes the labels in this screen.

Table 61 Internal RADIUS Server Setting

LABEL	DESCRIPTION
Active	Select this to have the NWA use its internal RADIUS server to authenticate wireless clients or other APs.
#	<p>This field displays the certificate index number. The certificates are listed in alphabetical order. Use the CERTIFICATES screens to manage certificates. The internal RADIUS server uses one of the certificates listed in this screen for authentication with each wireless client. The exact certificate used depends on the certificate information configured on the wireless client.</p> <p>Select the certificate you want the NWA to use for authentication.</p>
Name	<p>This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.</p> <p>auto_generated_self_signed_cert is the factory default certificate common to all NWAs that use certificates.</p> <p>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 CERTIFICATES > My Certificates screen.</p>
Type	<p>This field displays what kind of certificate this is.</p> <p>REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request.</p> <p>SELF represents a self-signed certificate.</p> <p>*SELF represents the default self-signed certificate, which the NWA uses to sign imported trusted remote host certificates.</p> <p>CERT represents a certificate issued by a certification authority.</p>
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Apply	Click Apply to have the NWA use certificates to authenticate wireless clients.
Reset	Click Reset to start configuring this screen afresh.

17.3 The Trusted AP Screen

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

Figure 120 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	
6	<input type="checkbox"/>	0.0.0.0	
7	<input type="checkbox"/>	0.0.0.0	
8	<input type="checkbox"/>	0.0.0.0	
9	<input type="checkbox"/>	0.0.0.0	
10	<input type="checkbox"/>	0.0.0.0	
11	<input type="checkbox"/>	0.0.0.0	
12	<input type="checkbox"/>	0.0.0.0	
13	<input type="checkbox"/>	0.0.0.0	
14	<input type="checkbox"/>	0.0.0.0	
15	<input type="checkbox"/>	0.0.0.0	
16	<input type="checkbox"/>	0.0.0.0	
17	<input type="checkbox"/>	0.0.0.0	
18	<input type="checkbox"/>	0.0.0.0	
19	<input type="checkbox"/>	0.0.0.0	
20	<input type="checkbox"/>	0.0.0.0	

Apply Reset

The following table describes the labels in this screen.

Table 62 Trusted AP Screen

LABEL	DESCRIPTION
#	This field displays the trusted AP index number.
Active	Select this check box to have the NWA use the IP Address and Shared Secret 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>Note: The first trusted AP fields are for the NWA itself.</p>

Table 62 Trusted AP Screen

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

17.4 The Trusted Users Screen

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

Figure 121 Trusted Users

#	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"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		
11	<input type="checkbox"/>		
12	<input type="checkbox"/>		

Note: Password: Maximum 14 ASCII characters with PEAP

Apply Reset

The following table describes the labels in this screen.

Table 63 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.

Table 63 Trusted Users

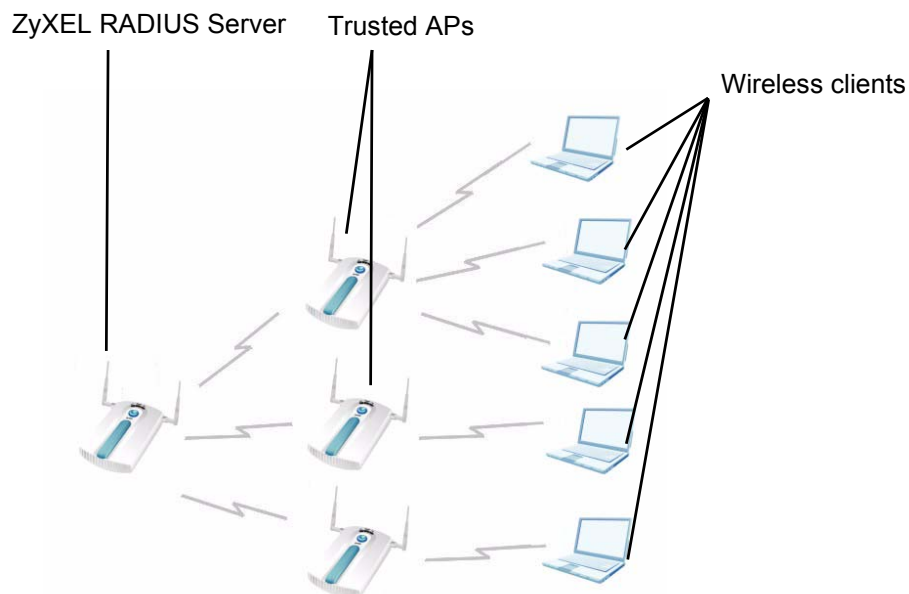
LABEL	DESCRIPTION
Password	Type a password (up to 31 ASCII characters) for this user profile. Note that as you type a password, the screen displays a (*) for each character you type. The password on the wireless client's utility must be the same as this password. Note: If you are using PEAP authentication, this password field is limited to 14 ASCII characters in length.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh.

17.5 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 122 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 A on page 303](#) 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.

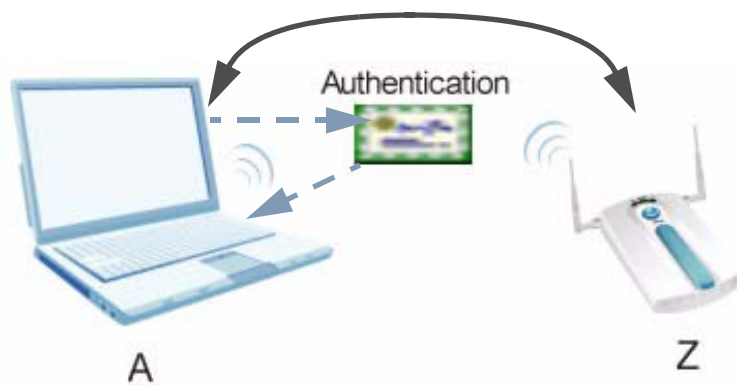
Certificates

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 123 Certificates Example



18.1.1 What You Can Do in the Certificates Screen

- Use the **My Certificate** screens (see [Chapter 18 on page 225](#)) to view details of certificates storage space and settings. This screen also allows you to import or create a new certificate.
- Use the **Trusted CAs** screens (see [Chapter 18 on page 229](#)) 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.

18.1.2 What You Need To Know About Certificates

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

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

18.2 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.

Figure 124 Certificates > My Certificates

My Certificates Trusted CAs

PKI Storage Space in Use

0% 1% 100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

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

Replace

My Certificates Setting

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

Details Create Import Delete Refresh

The following table describes the labels in this screen.

Table 64 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.
Replace	This button displays when the NWA has the factory default certificate. The factory default certificate is common to all NWAs that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your NWA's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	<p>This field displays what kind of certificate this is.</p> <p>REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request.</p> <p>SELF represents a self-signed certificate.</p> <p>*SELF represents the default self-signed certificate, which the NWA uses to sign imported trusted remote host certificates.</p> <p>CERT represents a certificate issued by a certification authority.</p>
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Details	Click Details to open a screen with an in-depth list of information about the certificate.
Create	Click Create to go to the screen where you can have the NWA generate a certificate or a certification request.
Import	Click Import to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the NWA.

Table 64 Certificates > My Certificates (continued)

LABEL	DESCRIPTION
Delete	<p>Click Delete to delete an existing certificate. A window display 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 *SELF in the Type field.</p> <ol style="list-style-type: none"> 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the *SELF certificate. 2. Click the details icon next to another self-signed certificate (see the description on the Create button if you need to create a self-signed certificate). 3. Select the Default self-signed certificate which signs the imported remote host certificates check box. 4. Click Apply to save the changes and return to the My Certificates screen. 5. The certificate that originally showed *SELF displays SELF and you can delete it now. <p>Note that subsequent certificates move up by one when you take this action.</p>
Refresh	Click Refresh to display the current validity status of the certificates.

18.2.1 My Certificates Import Screen

Use this screen to import a certificate from your local computer to the NWA.

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

Click **Certificates > My Certificates** and then **Import** to open the **My Certificate Import** screen.

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

Figure 125 Certificates > My Certificates Import

The following table describes the labels in this screen.

Table 65 Certificates > My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the NWA. Note: The certificate you import replaces the corresponding request in the My Certificates screen.
Cancel	Click Cancel to quit and return to the My Certificates screen.

18.2.2 My Certificates Create Screen

Use this screen 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 126 Certificates > My Certificate Create

The following table describes the labels in this screen.

Table 66 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 Common Name is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.

Table 66 Certificates > My Certificate Create (continued)

LABEL	DESCRIPTION
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.
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 Create a self-signed certificate 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 Create a certification request and save it locally for later manual enrollment to have the NWA generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority.</p> <p>Copy the certification request from the My Certificate Details screen (Section 18.2.3 on page 225) and then send it to the certification authority.</p>
Create a certification request and enroll for a certificate immediately online	<p>Select Create a certification request and enroll for a certificate immediately online 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 Trusted CAs 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 Reference Number and Key if the certification authority requires them.</p>

Table 66 Certificates > My Certificate Create (continued)

LABEL	DESCRIPTION
Enrollment Protocol	<p>Select the certification authority's enrollment protocol from the drop-down list box.</p> <p>Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.</p> <p>Certificate Management Protocol (CMP) is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.</p>
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	<p>Select the certification authority's certificate from the CA Certificate drop-down list box.</p> <p>You must have the certification authority's certificate already imported in the Trusted CAs screen. Click Trusted CAs to go to the Trusted CAs screen where you can view (and manage) the NWA's list of certificates of trusted certification authorities.</p>
Request Authentication	When you select Create a certification request and enroll for a certificate immediately online , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just fill in the Key field if your certification authority uses the SECP enrollment protocol.
Apply	Click Apply to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the 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.

18.2.3 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 124 on page 218). Click the details button to open the **My Certificate Details** screen.

Figure 127 Certificates > My Certificate Details

The screenshot displays the 'My Certificate Details' screen. At the top, the 'Name' field contains 'auto_generated_self_signed_cert'. Below it, the 'Property' section has a checked checkbox for 'Default self-signed certificate which signs the imported remote host certificates.' The 'Certificate Path' section shows a search box with 'Searching...' and a 'Refresh' button. The 'Certificate Information' section lists various details:

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946684801
Subject	CN=NWA-Series Factory Default Certificate
Issuer	CN=NWA-Series Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2000 Jan 1st, 00:00:00 GMT
Valid To	2030 Jan 1st, 00:00:00 GMT
Key Algorithm	rsaEncryption (512 bits)
Subject Alternative Name	EMAIL=factory@auto.gen.cert
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	3ce1.5c:28:c3:17:eb:76:3f:46:02:55:20:ff:0b:3e
SHA1 Fingerprint	9e:c1:94:f9:5a:a3:9c:bb:20:0e:c6:c8:41:ce:03:55:56:d9:4d:ac

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

```
-----BEGIN CERTIFICATE-----
MIIBOTCCAxugAwIBAgIEOG1DgTANBgkqhkiG9w0BAQUFADAxMS8wLQYDVQQDEyZn
Qk4tU2VyaWVzIEZhY3RvcnkgRGVmYXVsdCBDZXJ0aWZpY2FOZTAeFw0wMDAxMDEw
MDAwMDBaFw0zMDAxMDEwMDAwMDBaMDEwLzAtBgNVBAMTJk1CTi1TZk1pZk1pZk1pZk1p
dG9yeSBZ2ZhdWx0IENlcnRpZmljYXR1MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJB
AJx6vMSj4TRieQRG17jiyLnRH1wJEhh6IV/+tZ1YtGgHaavoUhsLLc0YoNEazp1U
KCNVMR2Sm5vZrvc+I1jdoP8CAwEAAN7MHkwdgYDVROPAQEABADAgKkMCAgA1Ud
EQQZMBEeBFwZh3Rvcn1AYXV0by5nZW4uY2Y2VydASBgNVHRMBAQECDAQAQH/AgEB
MDEGA1UdJQQqMCgGCCsGAQUFCAICBggrBgEFBQcDAQYIKwYBBQUHAWQGCCsGAQUF
BwMCAOGCSqGSIs3DQEBBQUAAOEAI1IHMemiGaB7DiHGwFSgYH90sLTi82i2AyS3
prKSb45+9OAErgrOzYFqw96eCUXfx1JkLEGSzB82a0x1FYEFpW==
```

At the bottom, there are 'Export', 'Apply', and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 67 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 Refresh 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 Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the 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 Subject Name 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 67 Certificates > My Certificate Details (continued)

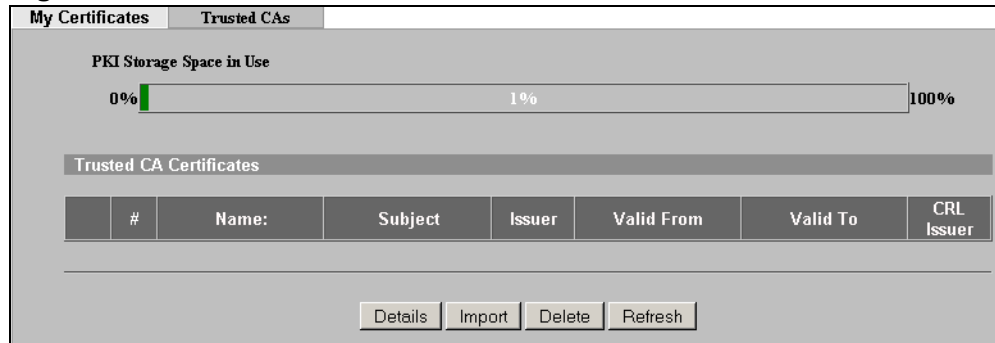
LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in 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 Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Apply	Click Apply to save your changes. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click Cancel to quit and return to the My Certificates screen.

18.3 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.

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

Figure 128 Certificates > Trusted CAs



The following table describes the labels in this screen.

Table 68 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.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

Table 68 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 Issues certificate revocation lists (CRL) 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 Details 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 Import 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 Delete 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.

18.3.1 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 129 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 69 Certificates > Trusted CA Import

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

18.3.2 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 130 Certificates > Trusted CAs Details

Name:

Property Check incoming certificates issued by this CA against a CRL

Certificate Path

Certificate Information

Type	Self-signed X.509 Certificate
Version	V3
Serial Number	946691189
Subject	CN= .203, OU=ZYXEL-TW, O=ZYXEL, C=TW
Issuer	CN= .203, OU=ZYXEL-TW, O=ZYXEL, C=TW
Signature Algorithm	rsa-pkcs1-sha1
Valid From	1999 Dec 31st, 01:46:29 GMT
Valid To	2002 Dec 31st, 01:46:29 GMT
Key Algorithm	rsaEncryption (1024 bits)
Subject Alternative Name	IP= .203
Key Usage	DigitalSignature, KeyEncipherment, KeyCertSign
Basic Constraint	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint	0d:d7:47:4a:d2:b6:27:13:f3:c9:ef:6d:77:b6:44:0b
SHA1 Fingerprint	fc:f2:0a:07:0c:3f:c2:9c:d7:ef:2f:6c:c1:49:b4:42:65:48:03:d6

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN CERTIFICATE-----
MIICczCCAdygAwIBAgIEOG1cdTANBgkqhkiG9w0BAQUFADBIMQswCOYDVQQGEwJU
VzEOMAwGA1UEChMFU1lYRUxwETAPBgNVBAsTCFp2WEVMLVRXMRyWFAyDVQQDEw0x
NzIuIuHjHuHzEuHjAzNB4XDTKSHTIzHTAxDYyOVoXDTAyHTIzHTAxDYyOVoSDEL
HAKGA1UEBhMCVFcxZjAMBQNVBAoTEVp2WEVMMREwDwYDVQLEwhaWVhFTCIUVzEM
MBQGA1UEAxMNMTcyLjIzLjMxLjIwMzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYKCo
gYEAwUpmSRx5E2nBeYhIpphNNIfcturnZb7diA13+FGNmq5yM2qBKZJV3Ky4agx91
mLE7/14kRKHASSWnSdIY96tCyHEWTJy+DEquhE3JbCbxCi2NW1FloSotWtOIZNE
qTMOt2Y3mdZ+gS7wZoas3o6joP5dcsoSD96MDJFJyhNLNVcCAwEAAsNgMGwDgYD
VROPAQEABAQDAGKkMA8GA1UdEQQIMAsHBKwXH8swEgYDVROTAQEABAgwBgEB/wIB
ATAxBgNVHSUEKjAoBggrBgEFBQcAgYIKYBBQUHAwEGCCsGAQUFBwMEBggrBgEF
```

The following table describes the labels in this screen.

Table 70 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).
Certificate Path	Click the Refresh button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The 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 Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use 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.

Table 70 Certificates > Trusted CAs Details (continued)

LABEL	DESCRIPTION
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).
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 Section 18.1.2 on page 218 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 Section 18.1.2 on page 218 for how to verify a remote host's certificate before you import it into the NWA.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Apply	Click Apply to save your changes. 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 Cancel to quit and return to the Trusted CAs screen.

18.4 Technical Reference

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

18.4.1 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.

18.4.2 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.

18.4.3 Checking the Fingerprint of a Certificate

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.

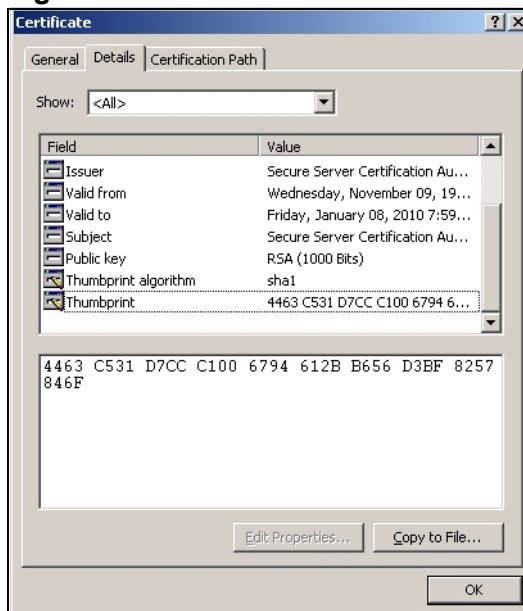
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 131 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 132 Certificate Details



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.

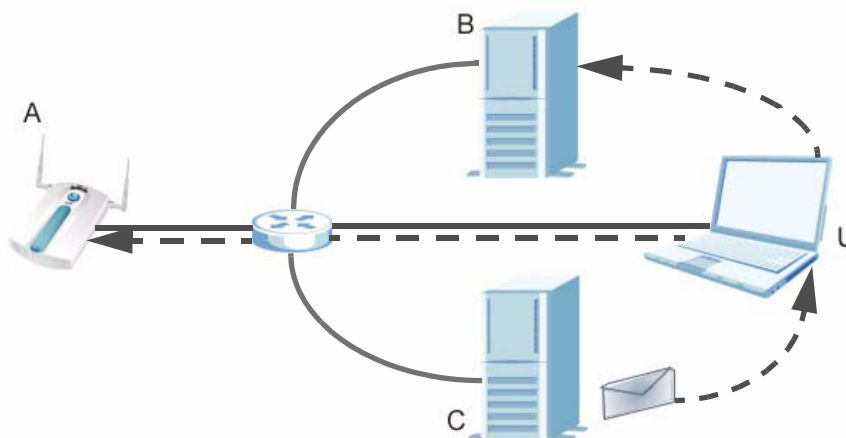
Log Screens

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, and so on. 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 133 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.

19.1.1 What You Can Do in the Log Screens

- Use the **View Log** screen ([Section 19.2 on page 236](#)) 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, old logs will be deleted.

- Use the **Log Settings** screen ([Section 19.3 on page 238](#)) to configure where and when the NWA will send the logs, and which logs and/or immediate alerts it will send.

19.1.2 What You Need To Know About Logs

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

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).

19.2 The View Log Screen

Use this screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Figure 135 on page 238](#)). 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 134 Logs > View Log

Index	Time	Message	Source	Destination	Notes
1	01/01/2000 01:00:10	WLAN STA Association			MACAddr:001302171185
2	01/01/2000 00:27:26	Successful HTTP login	172.23.37.27		User:admin

The following table describes the labels in this screen.

Table 71 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 All Logs . The number of categories shown in the drop down list box depends on the selection in the Log Settings page.
Index	This field displays the log entry index number.
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 Email Log Now to send the log screen to the e-mail address specified in the Log Settings page.
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to clear all the logs.

19.3 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 135 Logs > Log Settings

The screenshot shows the 'Log Settings' configuration page. At the top, there are two tabs: 'View Log' and 'Log Settings', with 'Log Settings' selected. The page is divided into three main sections: 'Address Info', 'Syslog Logging', and 'Send Log'.

Address Info: This section contains fields for 'Mail Server' (with a note '(Outgoing SMTP Server NAME or IP Address)'), 'Mail Subject', 'Send log to' (with a note '(E-Mail Address)'), and 'Send alerts to' (with a note '(E-Mail Address)'). Below these are checkboxes for 'SMTP Authentication', and fields for 'User Name' and 'Password'.

Syslog Logging: This section includes a checkbox for 'Active', a 'Syslog IP Address' field (with a note '(Server NAME or IP Address)') containing '0.0.0.0', and a 'Log Facility' dropdown menu set to 'Local 1'.

Send Log: This section features a 'Log Schedule' dropdown set to 'None', a 'Day for Sending Log' dropdown set to 'Sunday', and 'Time for Sending Log' fields for hours (0) and minutes (0). There is also a checkbox for 'Clear log after sending mail'.

At the bottom, there are two columns of checkboxes. The left column, titled 'Log', includes: System Maintenance, System Errors, PKI, SSL/TLS, 802.1x, Wireless, Internal RADIUS Server, Rogue AP Detection, Radar Event, and Load Balancing. The right column, titled 'Send immediate alert', includes: System Errors, PKI, Rogue AP Detection, Radar Event, and Load Balancing. All these checkboxes are checked.

At the very bottom of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

Table 72 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.
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 Active to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	<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"> • Daily • Weekly • Hourly • When Log is Full • None <p>If the Weekly or the Daily option is selected, specify a time of day when the E-mail should be sent. If the Weekly option is selected, then also specify which day of the week the E-mail should be sent. If the When Log is Full option is selected, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	<p>This field is only available when you select Weekly in the Log Schedule 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.

Table 72 Logs > Log Settings

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

19.4 Technical Reference

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

19.4.1 Example Log Messages

This section provides descriptions of some example log messages.

Table 73 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 74 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
	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 75 Sys log

LOG MESSAGE	DESCRIPTION
<pre>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>"</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.

19.4.2 Log Commands

Go to the command interpreter interface (refer to [Appendix E on page 357](#) for a discussion on how to access and use the commands).

19.4.3 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 76 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).

19.4.4 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.

19.4.5 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
```

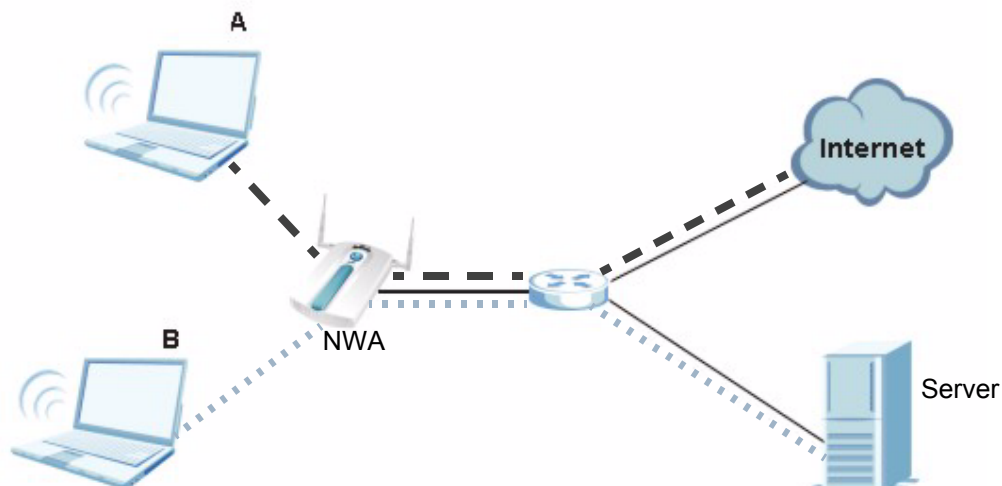
#.	time	source	destination	notes
0	11/11/2002 15:10:12	172.22.3.80:137	172.22.255.255:137	ACCESS BLOCK

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 136 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.

20.1.1 What You Can Do in the VLAN Screen

- Use the **Wireless VLAN** screen ([Section 20.2 on page 247](#)) 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 20.2.1 on page 248](#)) 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.

20.1.2 What You Need To Know About VLAN

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

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 20.3.3 on page 253](#) 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).

20.2 Wireless VLAN Screen

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

Figure 137 VLAN > Wireless VLAN

Wireless VLAN RADIUS VLAN

VIRTUAL LAN Setup

Enable VIRTUAL LAN

Wireless VIRTUAL LAN Setup

Management VLAN ID (1 - 4094) Native VLAN

VLAN Mapping Table

Index	Name	SSID	VLAN ID	Second Rx VLAN ID
1	VoIP_SSID	VOIP_SSID_Example	<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"/>

The following table describes the labels in this screen

Table 77 VLAN > Wireless VLAN

FIELD	DESCRIPTION
VIRTUAL LAN Setup	
Enable VIRTUAL LAN	Select this box to enable VLAN tagging.
Wireless VIRTUAL LAN Setup	
Management VLAN ID	Enter a number from 1 to 4094 to define this VLAN group. At least one device in your network must belong to this VLAN group in order to manage the NWA. Note: Mail and FTP servers must have the same management VLAN ID to communicate with the NWA. See Section 20.3.2 on page 250 for more information.

Table 77 VLAN > Wireless VLAN

FIELD	DESCRIPTION
Native VLAN	<p>Check this to assign the Management VLAN ID as a Native VLAN. Leave this blank if you do not know the native VLAN ID assigned by the network administrator.</p> <p>A native VLAN is the default VLAN where untagged traffic can pass through between two switches.</p> <p>Note: The Native VLAN assignment must be the same on two switches for it to work.</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 VLAN ID . Traffic received from the LAN that is tagged with this VLAN ID is sent to all SSIDs with this VLAN ID configured in the VLAN ID or Second Rx VLAN ID fields. See Section 20.3.4 on page 263 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.

20.2.1 RADIUS VLAN Screen

Use this screen 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.

Click **VLAN > RADIUS VLAN**. The following screen appears.

Figure 138 VLAN > RADIUS VLAN

Wireless VLAN RADIUS VLAN

RADIUS VIRTUAL LAN Setup

Block station if RADIUS server assigns VLAN name error.

VLAN Mapping Table

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

Apply Reset

The following table describes the labels in this screen.

Table 78 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 Name 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 Section 20.3.3 on page 253 for more information.
Index	This is the index number of the SSID profile.
Active	Select a check box to enable the SSID 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 78 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 Name fields are checked against these attributes. If a configured Name 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 Name field, a wireless station is assigned the wireless VLAN ID associated with its SSID (unless the Block station if RADIUS server assign VLAN error! check box is selected).
Apply	Click Apply to save your changes to the NWA.
Reset	Click Reset to begin configuring this screen afresh.

20.3 Technical Reference

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

20.3.1 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.

20.3.2 Configuring Management VLAN Example

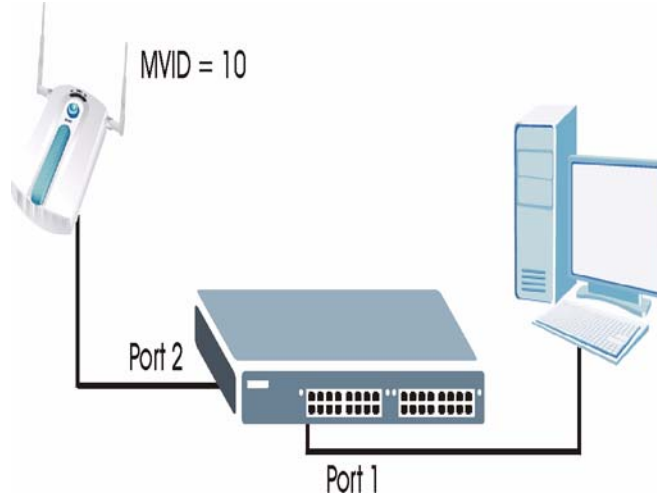
This section shows you how to create a VLAN on an Ethernet switch.

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 and your computer connected to port 1. The management VLAN ID is 10.

Figure 139 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 140 VLAN-Aware Switch - Static VLAN

Static VLAN		VLAN Status	
ACTIVE	<input checked="" type="checkbox"/>		
Name	MD1		
VLAN Group ID	10		
Port	Control		Tagging
1	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input type="checkbox"/> Tx Tagging
2	<input type="radio"/> Normal	<input checked="" type="radio"/> Fixed	<input checked="" type="checkbox"/> Tx Tagging

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

Figure 141 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 142 VLAN-Aware Switch - VLAN Status

VLAN Status		VLAN Port Setting																Static VLAN	
The Number Of VLAN = 5																			
Index	VID	Port Number																Elapsed Time	Status
		2	4	6	8	10	12	14	16	18	20	22	24	26	S2				
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	-	-	-	-	-	-	U	-	-	-	-	-	-	-	-	-	0:08:27	Static
5	5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	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 139 on page 251](#).

- 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 143 VLAN Setup

Wireless VLAN | RADIUS VLAN

VIRTUAL LAN Setup

Enable VIRTUAL LAN

Wireless VIRTUAL LAN Setup

Management VLAN ID: (1 - 4094) Native VLAN

VLAN Mapping Table

Index	Name	SSID	VLAN ID	Second Rx VLAN ID
1	VoIP_SSID	VOIP_SSID_Example	<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.

20.3.3 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 79 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 Name you enter in the NWA's VLAN > RADIUS VLAN screen or the number. See Figure 155 on page 261 .

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.

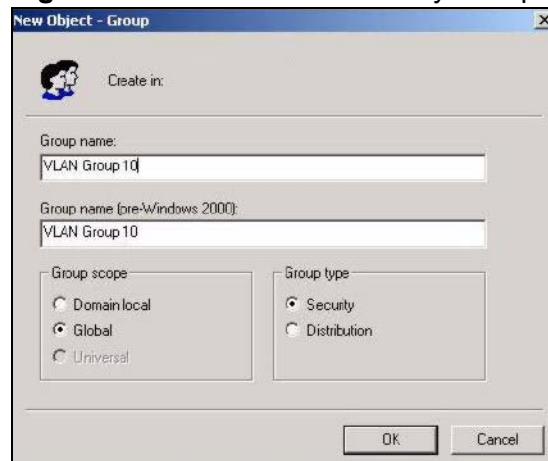
20.3.3.1 Configuring VLAN Groups

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 144 New Global Security Group

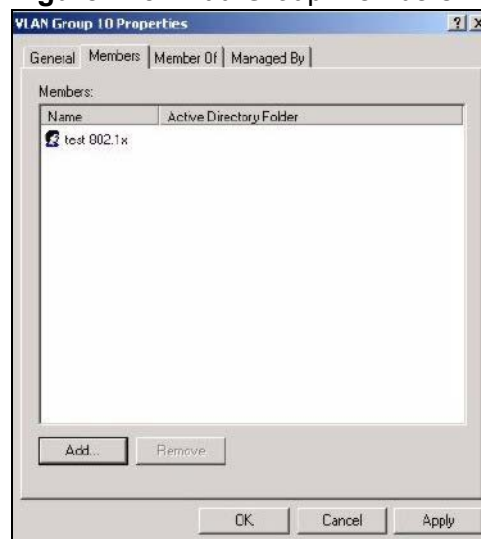


- 2 In **VLAN Group ID Properties**, click the **Members** tab.

Note: 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 145 Add Group Members

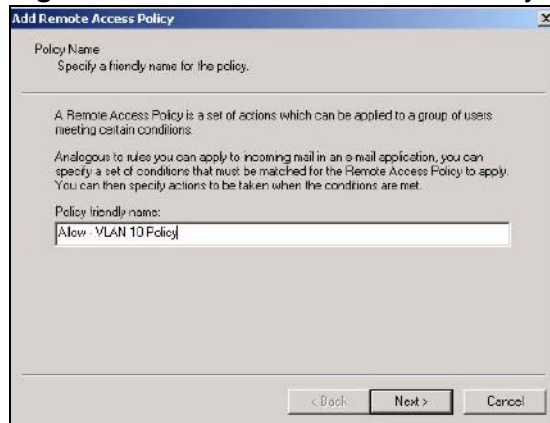


20.3.3.2 Configuring Remote Access Policies

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 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**.

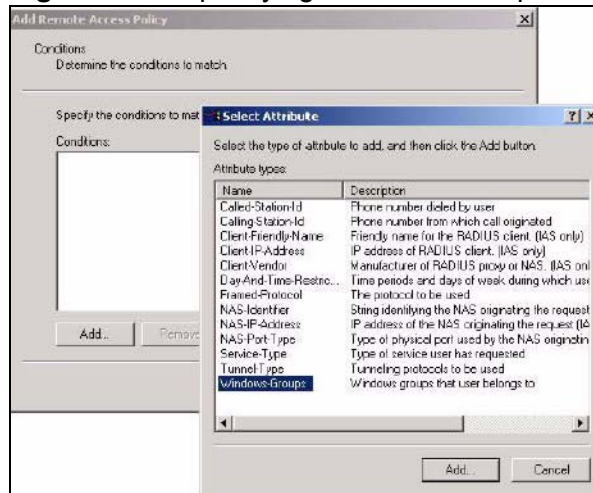
Figure 146 New Remote Access Policy for VLAN Group



- 2 The **Conditions** window displays. Select **Add** to add a condition for this policy to act on.

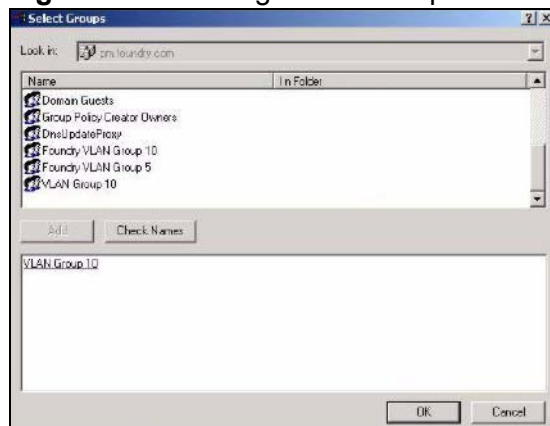
- 3 In the **Select Attribute** screen, click **Windows-Groups** and the **Add** button.

Figure 147 Specifying Windows-Group Condition



- 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.

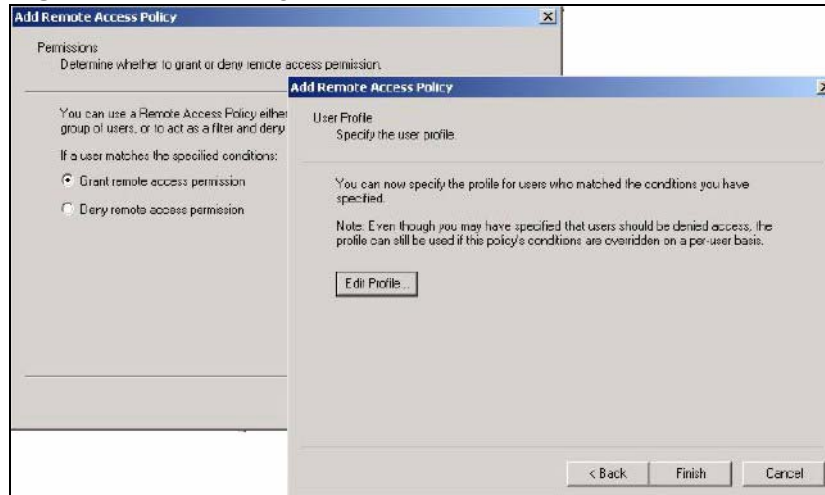
Figure 148 Adding VLAN Group



- 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 149 Granting Permissions and User Profile Screens

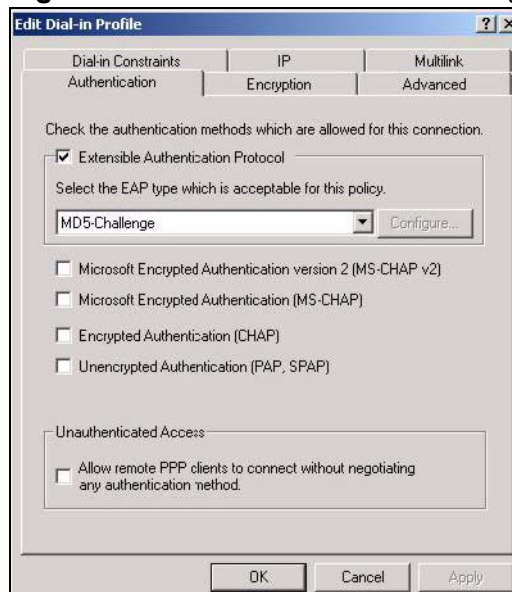


7 The **Edit Dial-in Profile** screen displays. Click the **Authentication** tab and select the **Extensible Authentication Protocol** check box.

7a Select an EAP type depending on your authentication needs from the drop-down list box.

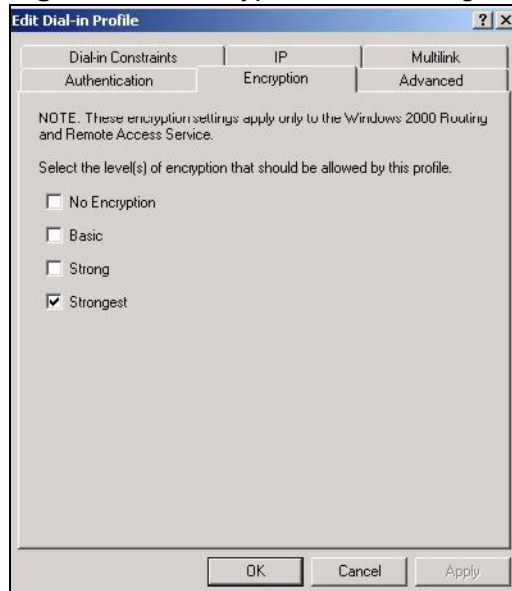
7b Clear the check boxes for all other authentication types listed below the drop-down list box.

Figure 150 Authentication Tab Settings



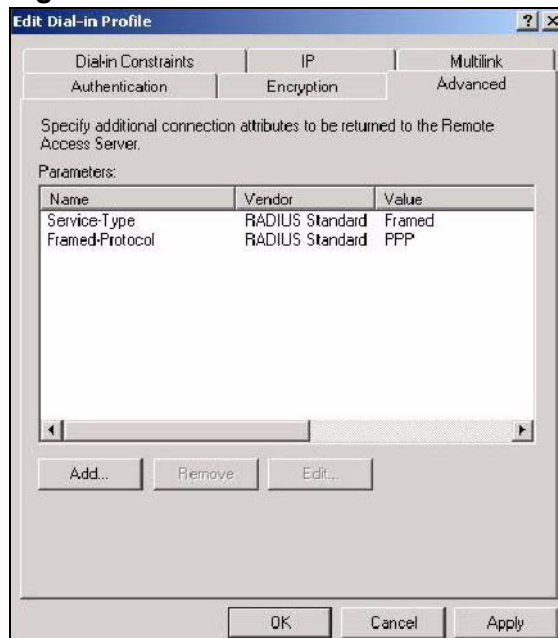
- 8 Click the **Encryption** tab. Select the **Strongest** encryption option. This step is not required for EAP-MD5, but is performed as a safeguard.

Figure 151 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 152 Connection Attributes Screen



11 The RADIUS Attribute screen displays. From the list, three RADIUS attributes will be added:

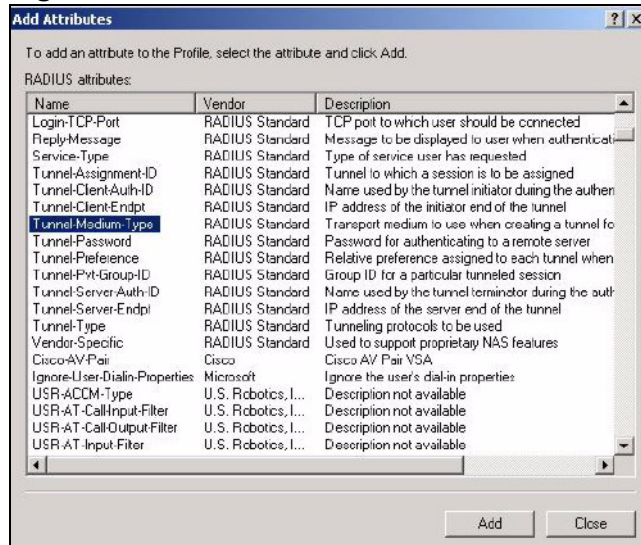
- Tunnel-Medium-Type
- Tunnel-Pvt-Group-ID
- Tunnel-Type

11a Click the **Add** button

11b Select **Tunnel-Medium-Type**

11c Click the **Add** button.

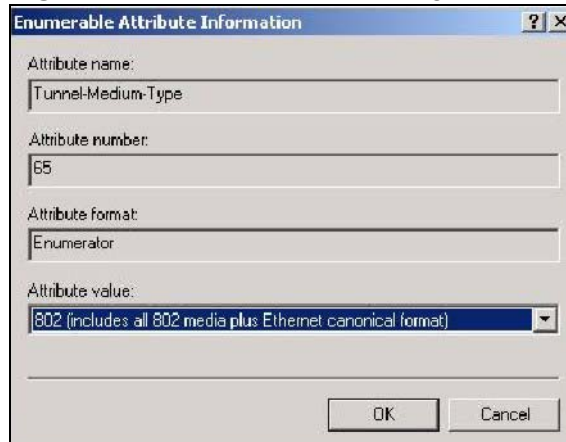
Figure 153 RADIUS Attribute Screen



12 The **Enumerable Attribute Information** screen displays. Select the **802** value from the **Attribute value** drop-down list box.

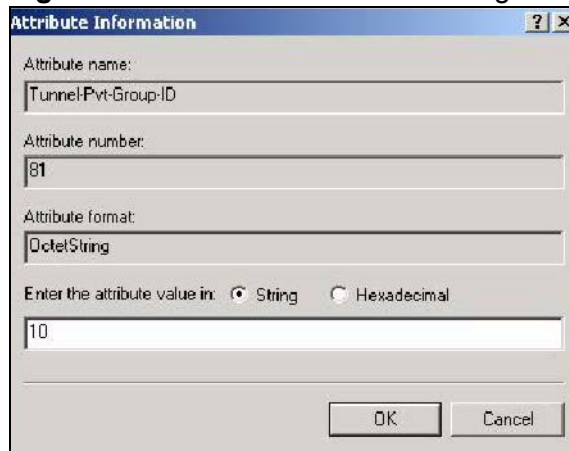
Click **OK**.

Figure 154 802 Attribute Setting for Tunnel-Medium-Type



- 13 Return to the **RADIUS Attribute Screen** shown as [Figure 153 on page 260](#).
 - 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 155 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: TunnelPvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Enter the attribute value in: String Hexadecimal
- Value field: 10
- Buttons: OK, Cancel

- 15 Return to the **RADIUS Attribute Screen** shown as [Figure 153 on page 260](#).
 - 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 156 VLAN Attribute Setting for Tunnel-Type

Enumerable Attribute Information

Attribute name:
Tunnel-Type

Attribute number:
64

Attribute format:
Enumerator

Attribute value:
Virtual LANs (VLAN)

OK Cancel

17 Return to the **RADIUS Attribute Screen** shown as [Figure 153 on page 260](#).

17a Click the **Close** button.

17b The completed **Advanced** tab configuration should resemble the following screen.

Figure 157 Completed Advanced Tab

Allow - VLAN Group 10 Properties

Settings

Policy names:

Specify the condition:
Windows-Groups in

Add...

If a user matches th
 Grant remote c
 Deny remote c
 Access will be
 is overridden c

Edit Profile...

Edit Dial-in Profile

Dial-in Constraints | IP | Multlink
 Authentication | Encryption | Advanced

Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Framed-Protocol	RADIUS Standard	PPP
Tunnel-Medium-Type	RADIUS Standard	802 (includes all 802 m
Tunnel-Priv-Group-ID	RADIUS Standard	10
Tunnel-Type	RADIUS Standard	Virtual LANs (VLAN)

Add... Remove Edit...

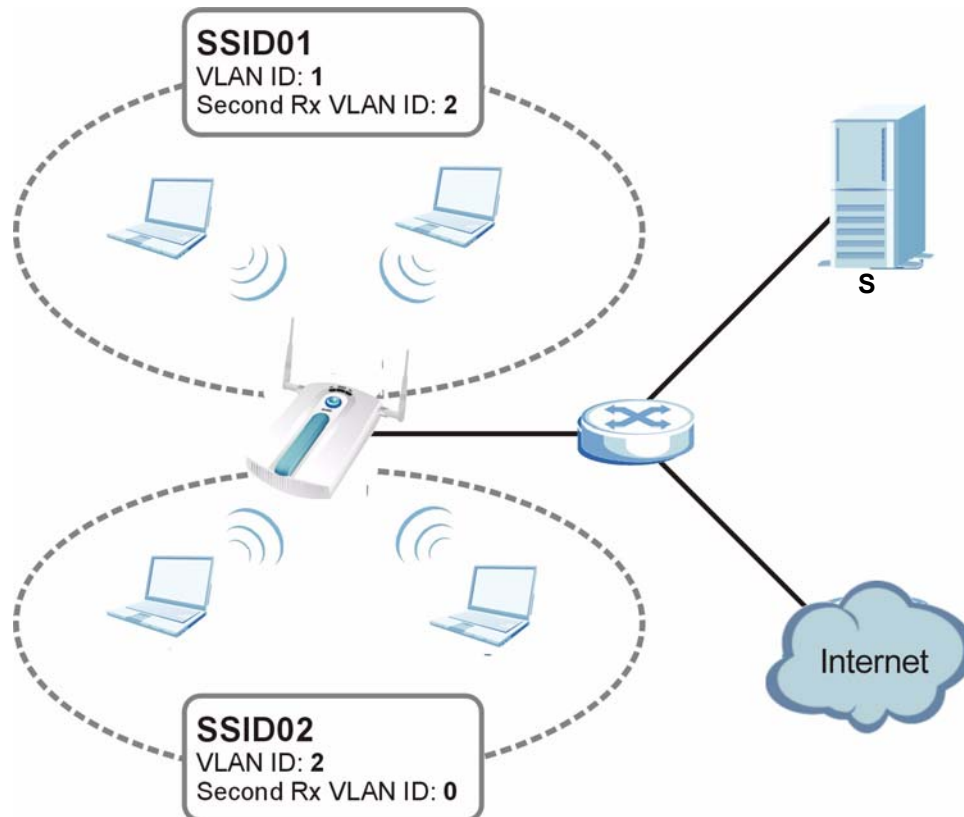
OK Cancel Apply

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.

20.3.4 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 158 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.

20.3.4.1 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 20.3.2 on page 250](#)).

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 159 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) Native VLAN

VLAN Mapping Table

Index	Name	SSID	VLAN ID	Second Rx VLAN ID
1	VoIP_SSID	VOIP_SSID_Example	<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 (AP) 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.

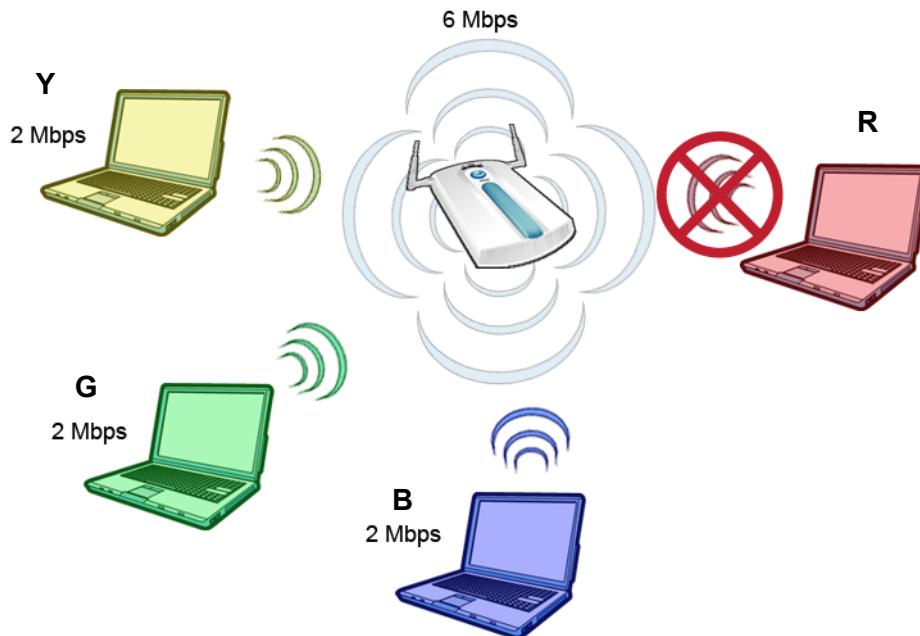
- **Load balancing by traffic level** limits the number of connections to the NWA based on maximum bandwidth available.

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 configured 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 on 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 160 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 161 Load Balancing

The following table describes the labels in this screen

Table 80 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 NWA 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"> • Low - Up to 6 Mbps before it becomes overloaded. • Medium - Up to 13 Mbps before it becomes overloaded. • High - Up to 20 Mbps before it becomes overloaded.

Table 80 Load Balancing

FIELD	DESCRIPTION
Dissociate station when overloaded	<p>Select Enable to “kick” connections to the AP when it becomes overloaded. If you set this option to Disable, 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 determined automatically by the NWA and is as follows:</p> <ul style="list-style-type: none"> • Idle Timeout - Devices that have been idle the longest will be kicked first. If none of the connected devices are idle, then the priority shifts to signal strength. • Signal Strength - Devices with the weakest signal strength will be kicked first. <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.

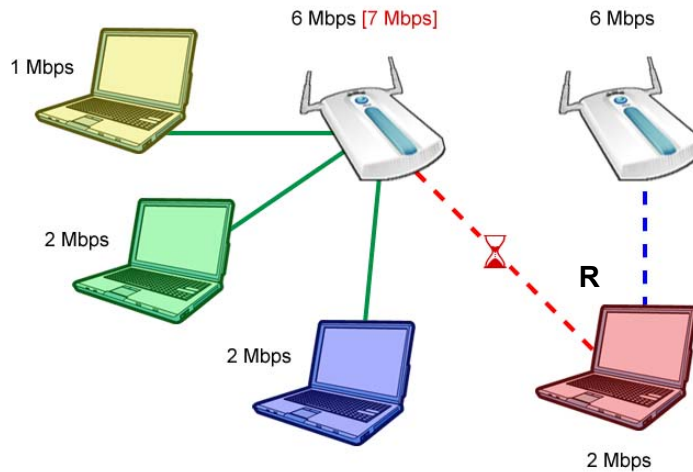
21.2.1 Disassociating and Delaying Connections

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 is lowered or the client connection is picked up by another AP. If the client is picked up by another AP then the original AP cannot resume the connection.

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

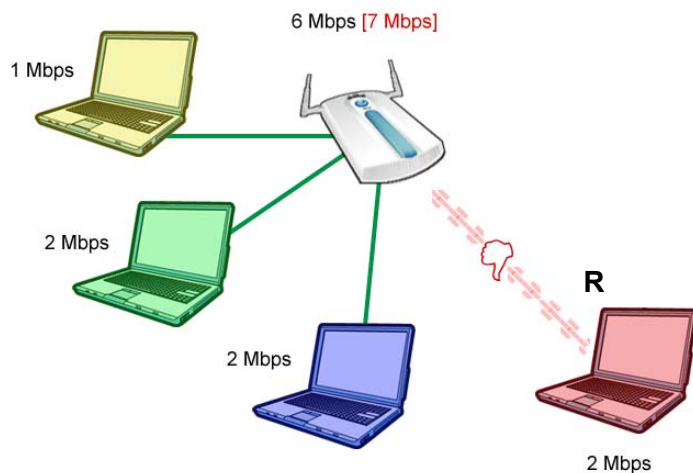
can afford the bandwidth for it or the red laptop is picked up by a different AP that has bandwidth to spare.

Figure 162 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 163 Kicking a Connection



Connections are kicked based on 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

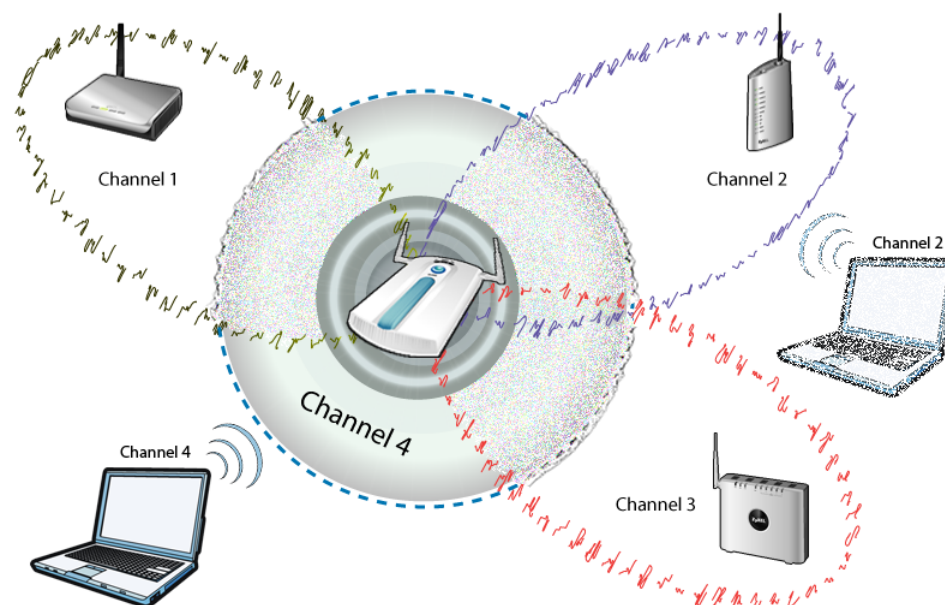
22.1 Overview

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 (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of cross-channel interference.

Figure 164 An example of cross-channel interference



In this example, if the NWA attempts to broadcast on **channels 1, 6, or 11** 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 165 DCS

The following table describes the labels in this screen

Table 81 DCS

FIELD	DESCRIPTION
Dynamic Channel Selection	Select this to either Enable or Disable 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 or a channel with markedly lower interference. This is set to 720 minutes by default.

Table 81 DCS

FIELD	DESCRIPTION
DCS Sensitivity Level	<p>Select the NWA's sensitivity level toward other channels. Options are High, Medium, and Low.</p> <p>Generally, as long as the area in which your NWA is located has minimal interference from other devices you can set the DCS Sensitivity Level to Low. This means that the NWA has a very broad tolerance.</p> <p>If you are not sure about the number and location of any other devices in the region, set the level to Medium just to be safe. The NWA's tolerance for interference is relatively narrow.</p> <p>On the other hand, if you know there are numerous other devices in the region, you should set the level to High to keep the cross-interference to a minimum. In this case, the NWA's tolerance for interference is quite draconian.</p> <p>Note: The higher the sensitivity level, the more frequently the NWA switches channels. As a consequence, anyone connected to the NWA will experience more frequent disconnects and reconnects.</p>
DCS Client Aware	<p>Select Enable to have the NWA wait until all connected clients have disconnected before switching channels.</p> <p>If you select Disable 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.</p>
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 Enable to allow the NWA to broadcast on unused radar channels. If you select Disable to turn the feature off. See Section 8.3.2 on page 145 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 276](#)) to monitor your NWA. Note that these labels are READ-ONLY and are meant to be used for diagnostic purposes.
- Use the **Association List** screen ([Section 23.5 on page 278](#)) to view the wireless stations that are currently associated with the NWA.
- Use the **Channel Usage** screen ([Section 23.6 on page 279](#)) 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 280](#)) to upload the latest firmware for your NWA.
- Use the **Configuration** screen ([Section 23.8 on page 282](#)) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use **Restart** screen ([Section 23.9 on page 284](#)) to reboot the NWA without turning the power off.

23.3 What You Need To Know

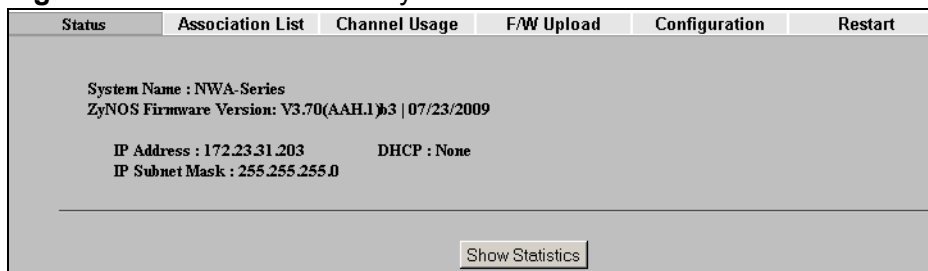
The following terms and concepts may help as you read through this chapter.

Find firmware at 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 166 Maintenance > System Status



The following table describes the labels in this screen.

Table 82 Maintenance > System Status

LABEL	DESCRIPTION
System Name	This is the System Name you can configure in the SYSTEM > General 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 - Client or None .
Show Statistics	Click Show Statistics to see the NWA performance statistics such as number of packets sent and number of packets received for each port.

23.4.1 Show 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 167 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 83 Maintenance > System Status: Show Statistics

LABEL	DESCRIPTION
Port	This is the Ethernet port (LAN) or wireless LAN adaptor (WLAN1 or WLAN2).
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.
WLAN1	This section displays only when wireless LAN adaptor WLAN1 is in AP + Bridge or Bridge / Repeater mode.

Table 83 Maintenance > System Status: Show Statistics

LABEL	DESCRIPTION
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 Up or Down .
TxPkts	This is the number of transmitted packets on the wireless bridge.
RxPkts	This is the number of received packets on the wireless bridge.
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 168 Association List

Status	Association List	Channel Usage	F/W Upload	Configuration	Restart
WLAN1 Stations					
#	MAC Address	Association Time	SSID	Signal	
WLAN2 Stations					
#	MAC Address	Association Time	SSID	Signal	
Refresh					

The following table describes the labels in this screen.

Table 84 Association List

LABEL	DESCRIPTION
WLAN1 / WLAN2 Stations	
Index	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the NWA.
SSID	This field displays the SSID to which the wireless station is associated.

Table 84 Association List

LABEL	DESCRIPTION
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.
Link No	This field displays the index number of a bridge connection on the WDS.
MAC Address	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 (TKIP or AES) or not (None).
Refresh	Click Refresh 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 169 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>BrcmAP0</td> <td>02:10:18:01:00:12</td> <td>1</td> <td>76 %</td> <td>Infra</td> </tr> <tr> <td>ZyXEL_MIS</td> <td>00:19:CB:4B:22:0F</td> <td>1</td> <td>100 %</td> <td>Infra, WEP</td> </tr> <tr> <td>BrcmAP0</td> <td>00:19:CB:F6:61:5C</td> <td>1</td> <td>60 %</td> <td>Infra</td> </tr> <tr> <td>ZyXEL_MIS_WPA</td> <td>06:19:CB:4B:22:0F</td> <td>1</td> <td>100 %</td> <td>Infra, WPA2-MIX</td> </tr> <tr> <td>ZyXEL_Guest</td> <td>0A:19:CB:4B:22:0F</td> <td>1</td> <td>100 %</td> <td>Infra, WPA2-MIX</td> </tr> <tr> <td>PQA-3232-P870HW-51A V2</td> <td>00:19:CB:55:55:89</td> <td>1</td> <td>54 %</td> <td>Infra</td> </tr> <tr> <td>pqa-3260-p2602hwl</td> <td>00:13:49:F5:1A:13</td> <td>3</td> <td>66 %</td> <td>Infra, WEP</td> </tr> <tr> <td>PQA-3261</td> <td>00:A0:C5:F4:38:95</td> <td>4</td> <td>70 %</td> <td>Infra</td> </tr> </tbody> </table>	SSID	MAC Address	Channel	Signal	Network Mode	BrcmAP0	02:10:18:01:00:12	1	76 %	Infra	ZyXEL_MIS	00:19:CB:4B:22:0F	1	100 %	Infra, WEP	BrcmAP0	00:19:CB:F6:61:5C	1	60 %	Infra	ZyXEL_MIS_WPA	06:19:CB:4B:22:0F	1	100 %	Infra, WPA2-MIX	ZyXEL_Guest	0A:19:CB:4B:22:0F	1	100 %	Infra, WPA2-MIX	PQA-3232-P870HW-51A V2	00:19:CB:55:55:89	1	54 %	Infra	pqa-3260-p2602hwl	00:13:49:F5:1A:13	3	66 %	Infra, WEP	PQA-3261	00:A0:C5:F4:38:95	4	70 %	Infra			
SSID	MAC Address	Channel	Signal	Network Mode																																														
BrcmAP0	02:10:18:01:00:12	1	76 %	Infra																																														
ZyXEL_MIS	00:19:CB:4B:22:0F	1	100 %	Infra, WEP																																														
BrcmAP0	00:19:CB:F6:61:5C	1	60 %	Infra																																														
ZyXEL_MIS_WPA	06:19:CB:4B:22:0F	1	100 %	Infra, WPA2-MIX																																														
ZyXEL_Guest	0A:19:CB:4B:22:0F	1	100 %	Infra, WPA2-MIX																																														
PQA-3232-P870HW-51A V2	00:19:CB:55:55:89	1	54 %	Infra																																														
pqa-3260-p2602hwl	00:13:49:F5:1A:13	3	66 %	Infra, WEP																																														
PQA-3261	00:A0:C5:F4:38:95	4	70 %	Infra																																														
Refresh																																																		

The following table describes the labels in this screen.

Table 85 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	This refers to your wireless LAN infrastructure (refer to the Wireless LAN chapter) and security setup.
Refresh	Click Refresh 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 170 Maintenance > F/W Upload

The screenshot shows a web interface with a navigation bar at the top containing the following tabs: Status, Association List, Channel Usage, F/W Upload (which is highlighted), Configuration, and Restart. Below the navigation bar is a section titled "Firmware Upload". The main content area 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 is a "File Path:" label followed by a text input field and a "Browse..." button. At the bottom of the form is an "Upload" button.

The following table describes the labels in this screen.

Table 86 Maintenance > F/W Upload

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

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

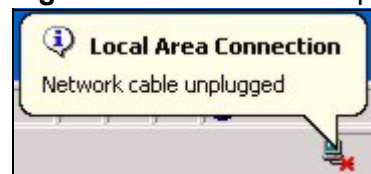
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the NWA again.

Figure 171 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.

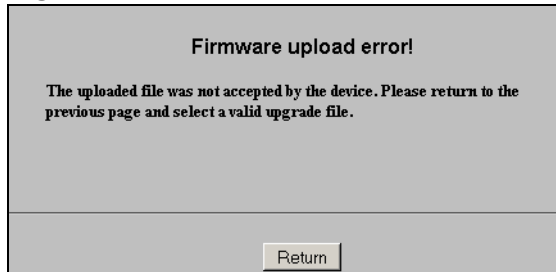
Figure 172 Network Temporarily Disconnected



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.

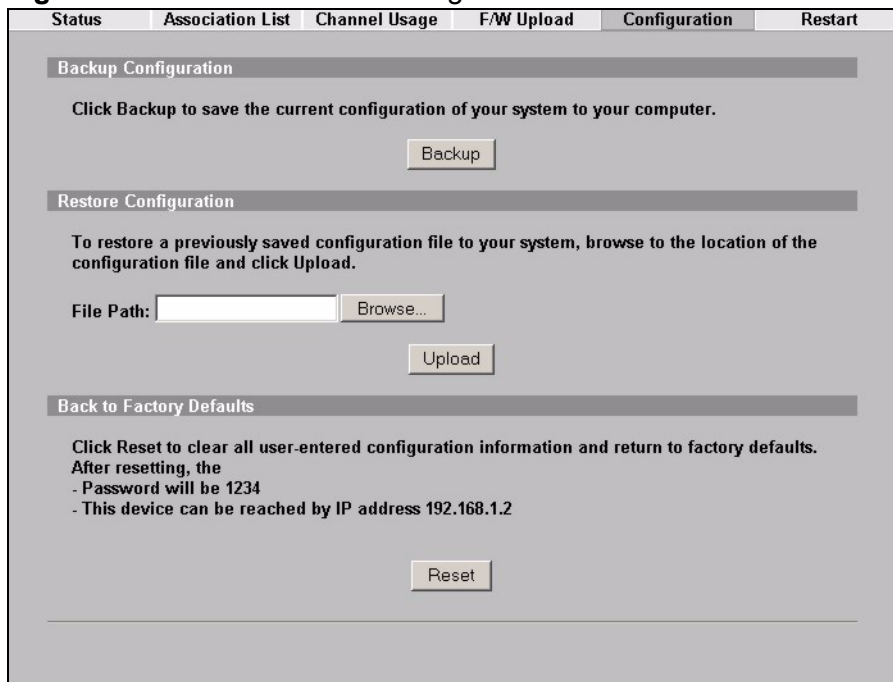
Figure 173 Firmware Upload Error



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 174 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.

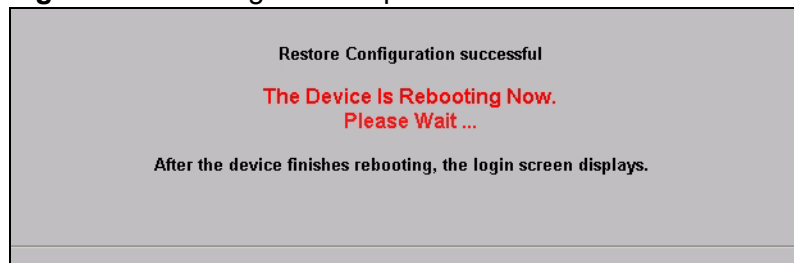
Table 87 Restore Configuration

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

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

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

Figure 175 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 176 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.

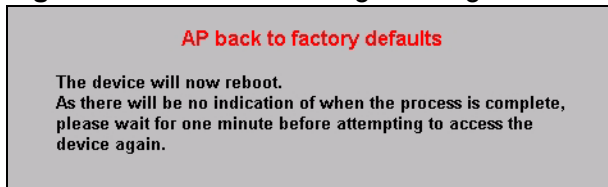
Figure 177 Configuration Upload Error



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 178 Reset Warning Message



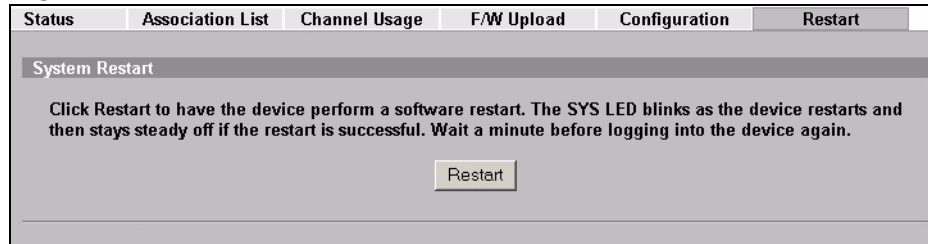
You can also press the **RESET** button to reset your NWA to its factory default settings. Refer to [Section 2.3 on page 38](#) for more information.

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 179 Restart Screen



PART III

Troubleshooting and Specifications

Troubleshooting (289)

Product Specifications (297)

Troubleshooting

24.1 Overview

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

- [Power, Hardware Connections, and LEDs](#)
- [NWA Access and Login](#)
- [AP Management Modes](#)
- [Internet Access](#)
- [Wireless Router/AP Troubleshooting](#)

24.2 Power, Hardware Connections, and LEDs

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

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

One of the LEDs does not behave as expected.

- Make sure you understand the normal behavior of the LED. See [Section 1.7 on page 34](#).
- Check the hardware connections. See the Quick Start Guide.

- Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- Disconnect and re-connect the power adaptor to the NWA.
- If the problem continues, contact the vendor.

24.3 NWA Access and Login

I forgot the IP address for the NWA.

- The default IP address is **192.168.1.2**.
- If you changed the IP address and have forgotten it, you might get the IP address of the NWA by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter "**cmd**", and then enter "**ipconfig**". The IP address of the **Default Gateway** might be the IP address of the NWA (it depends on the network), so enter this IP address in your Internet browser. You can also use the following methods to access the web configurator:
 - If you know your NWA's System Name, enter it in your browser's URL bar. The default System Name is **NWA-Series**. See [Section 7.2 on page 111](#) for information on locating and changing the NWA's System Name.

Note: If you changed the **System Name**, and want to log into the NWA using the **System Name**, you should enter a name not longer than 15 alphanumeric characters.

- If you know your NWA's MAC (Media Access Control) address, enter its last six characters in your browser's URL bar, in the format **zyxelXX:XX:XX**, where **XX:XX:XX** represents the MAC address characters. The MAC address is usually printed on a label on the NWA.

Note: The NWA has two MAC addresses; one for the wired interface (LAN, or Local Area Network) and one for the wireless interface (WLAN, or Wireless Local Area Network). Use the LAN MAC address when accessing the NWA over the wired network, and use the WLAN MAC address when accessing the NWA over the wireless interface.

- If this does not work, you have to reset the device to its factory defaults. See [Section 2.3 on page 38](#).

I forgot the password.

- The default password is **1234**.
- If this does not work, you have to reset the device to its factory defaults. See [Section 2.3 on page 38](#).

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

- Make sure you are using the correct IP address.
 - The default IP address is 192.168.1.2.
 - If you changed the IP address, 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](#).
- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.7 on page 34](#).
- Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 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.
- Reset the device to its factory defaults, and try to access the NWA with the default IP address. See your Quick Start Guide.
- If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

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

I can see the **Login** screen, but I cannot log in to the NWA.

- 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.
- You cannot log in to the web configurator while someone is using 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.

- Disconnect and re-connect the power adaptor or cord to the NWA.
- If this does not work, you have to reset the device to its factory defaults. See [Section 2.3 on page 38](#).

I cannot access the NWA via the console port.

- Check to see if the NWA is connected to your computer's console port.
- Check to see if the communications program is configured correctly. The communications software should be configured as follows:
 - VT100 terminal emulation.
 - 9,600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
 - No parity, 8 data bits, 1 stop bit, data flow set to none.

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.

The Web Configurator keeps logging out.

- 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.
- Change the time out value in the **System > General** screen to have more time between automatic logouts when the Web Configurator is idle.

24.4 AP Management Modes

The primary controller AP cannot connect to the secondary controller AP.

The controllers need to have static IP addresses in the same network. Make sure you set the IP addresses in the **IP** screen.

The secondary controller AP's wireless profiles do not appear in my wireless network.

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. Thus, you will not see any of the secondary controller AP's wireless profiles in your wireless network.

The controller AP cannot detect some of the APs in the network.

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

The configuration updates I applied to the controller AP are not taking effect.

- If you have both primary and secondary controller APs in the network, note that you can only configure one at a time. 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.
- 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.
- The managed APs may be turned off or out of range while you were updating their profiles. The changes will take effect when the managed APs are turned on or are within range again.

Can the controller AP update managed APs that are turned off.

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.

24.5 Internet Access

I cannot access the Internet.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 24.2 on page 289](#).
- Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 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.
- Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 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.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.7 on page 34](#).
- Reboot the NWA.
- If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.7 on page 34](#). If the NWA is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- Check the signal strength. If the signal is weak, try moving the NWA closer to the AP (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).
- Reboot the NWA.
- If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

24.6 Wireless Router/AP Troubleshooting

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

- Make sure the wireless LAN is enabled on the NWA
- Make sure the wireless adapter on the wireless station is working properly.
- Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the NWA.
- Make sure your computer (with a wireless adapter installed) is within the transmission range of the NWA.
- Check that both the NWA and your wireless station are using the same wireless and wireless security settings.
- Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the NWA.
- Make sure you allow the NWA to be remotely accessed through the WLAN interface. Check your remote management settings.

Some clients cannot connect to or keep on getting disconnected from the NWA's wireless network.

- Check if you have **Load Balancing** enabled. Wireless load balancing is the process whereby you limit the number of connections allowed on an wireless access point (AP) or you limit the amount of wireless traffic transmitted and received on it.
- 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.

Product Specifications

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

Table 88 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 89 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 90 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 91 Other Specifications

Approvals	<p>Radio</p> <ul style="list-style-type: none"> • USA: FCC Part 15C 15.247 FCC Part 15E 15.407 FCC OET65 • EU: ETSI EN 300 328 V1.7.1 ETSI EN 301 893 V1.2.3 • Taiwan: DGT LP0002 • Canada: Industry Canada RSS-210 • Australia: AS/NZS 4268 <p>EMC/ EMI</p> <ul style="list-style-type: none"> • USA: FCC Part 15 Subpart B • EU: EN 301 489-17 V1.2.1: 08-2002 EN 55022:2006 • Canada: ICES-003 • Australia: AS/NZS CISPR22 <p>EMC/ EMS</p> <ul style="list-style-type: none"> • EU: EN 301 489-1 V1.5.1: 11-2004 <p>Environmental</p> <ul style="list-style-type: none"> • 2002/95/EC (RoHS) Restriction of Hazardous Substances Directive • 2002/96/EC (WEEE) Waste Electrical and Electronic Equipment Directive • European Parliament and Council Directive 94/62/EC of 20 December 1994 on packaging and packaging waste
-----------	--

Compatible ZyXEL Antennas

At the time of writing, you can use the following antennas in your NWA.

Table 92 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 93 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

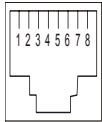
Power over Ethernet (PoE) Specifications

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

Table 94 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Table 95 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
(305)

Wireless LANs (331)

Pop-up Windows, JavaScripts and Java
Permissions (347)

Importing Certificates (355)

IP Addresses and Subnetting (381)

Text File Based Auto Configuration (391)

Legal Information (399)

Index (403)

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:

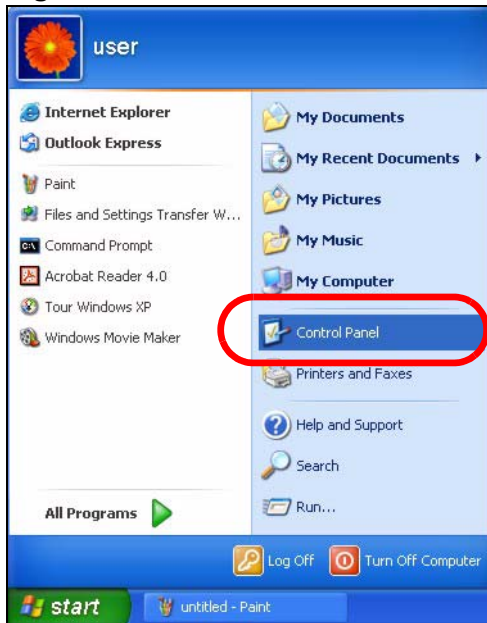
- [Windows XP/NT/2000](#) on [page 305](#)
- [Windows Vista](#) on [page 309](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 313](#)
- [Mac OS X: 10.5](#) on [page 316](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 320](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 325](#)

Windows XP/NT/2000

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

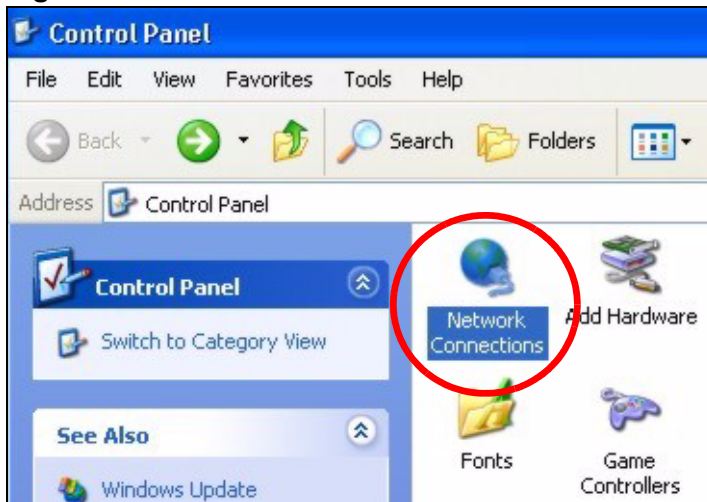
- 1 Click **Start > Control Panel**.

Figure 180 Windows XP: Start Menu



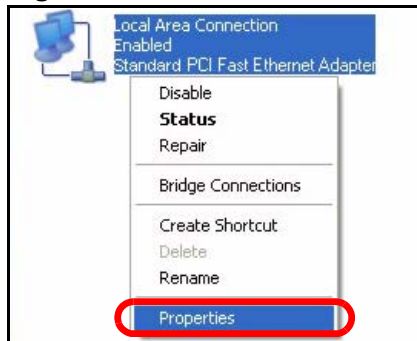
- 2 In the **Control Panel**, click the **Network Connections** icon.

Figure 181 Windows XP: Control Panel



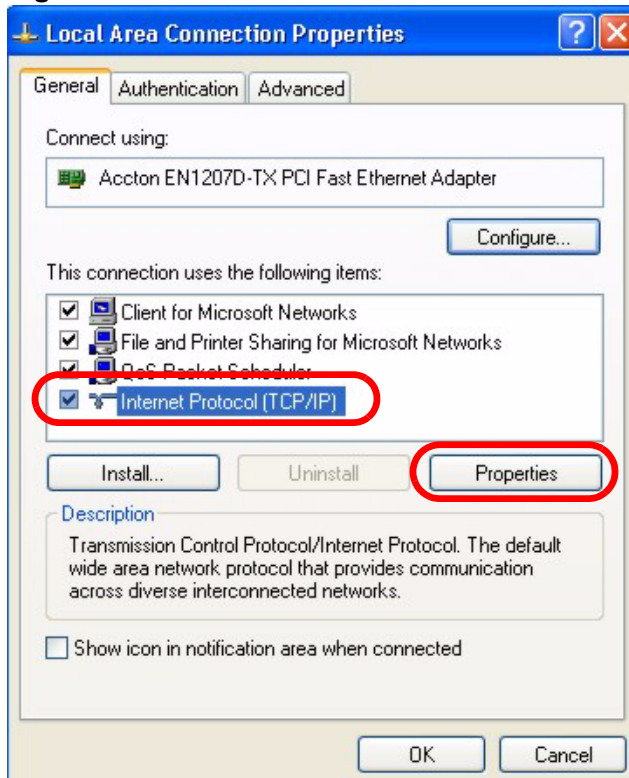
- 3 Right-click **Local Area Connection** and then select **Properties**.

Figure 182 Windows XP: Control Panel > Network Connections > Properties



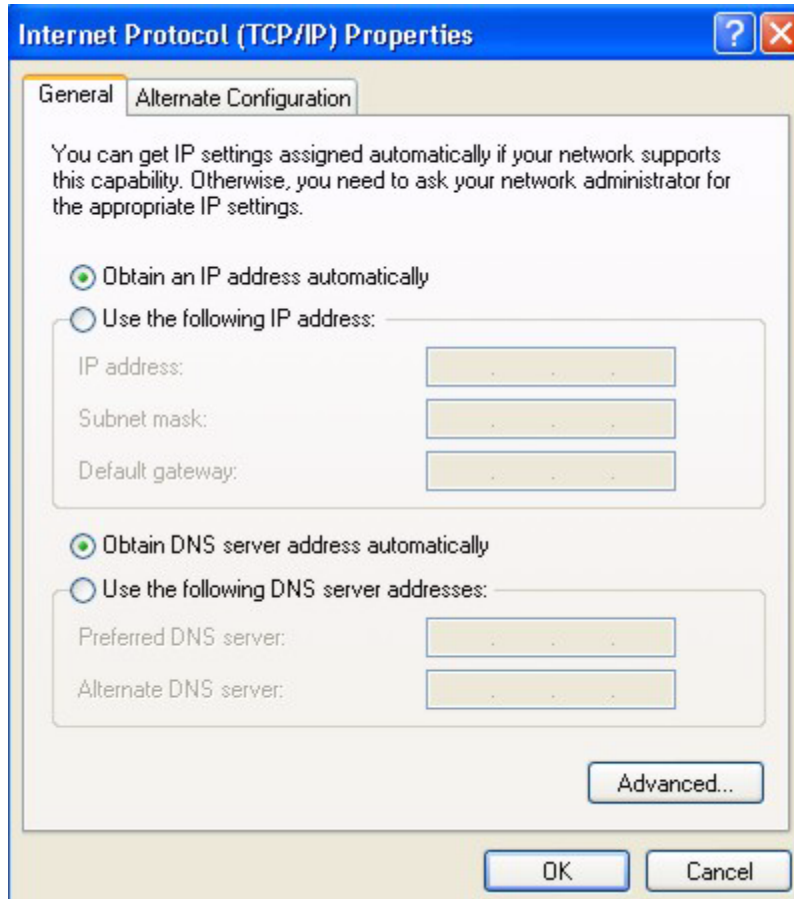
- 4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 183 Windows XP: Local Area Connection Properties



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

Figure 184 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].

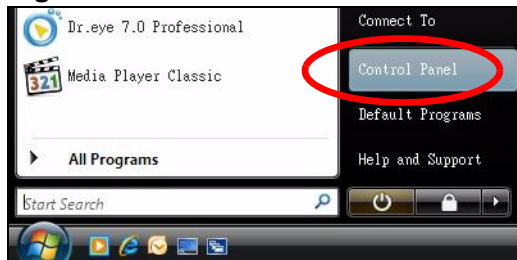
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

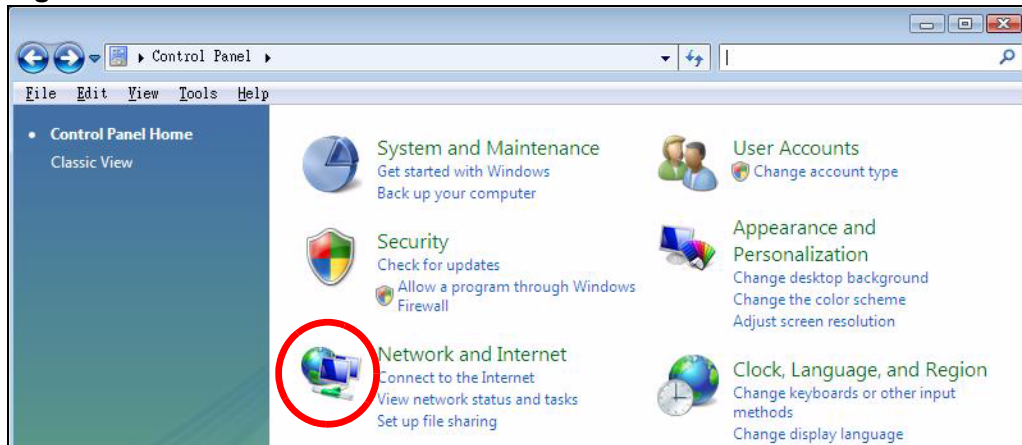
- 1 Click **Start > Control Panel**.

Figure 185 Windows Vista: Start Menu



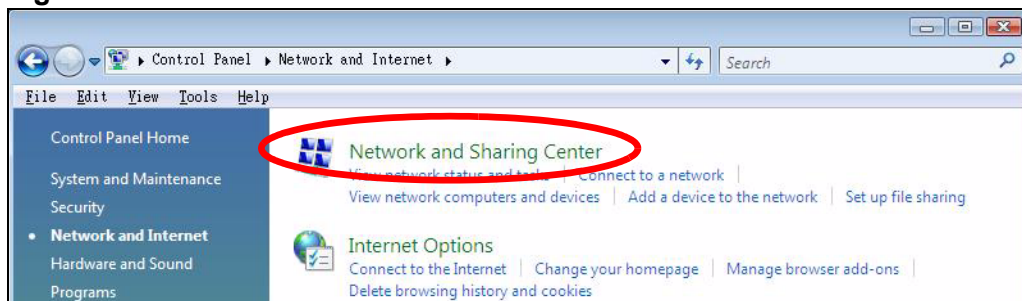
- 2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 186 Windows Vista: Control Panel



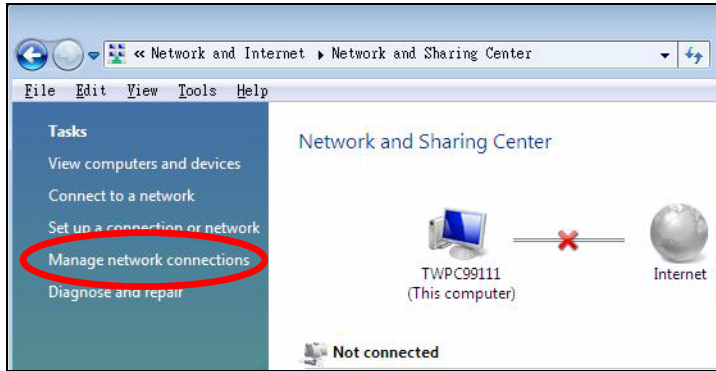
- 3 Click the **Network and Sharing Center** icon.

Figure 187 Windows Vista: Network And Internet



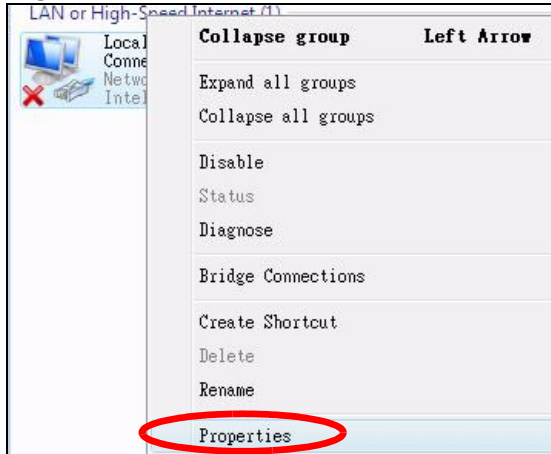
- 4 Click **Manage network connections**.

Figure 188 Windows Vista: Network and Sharing Center



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

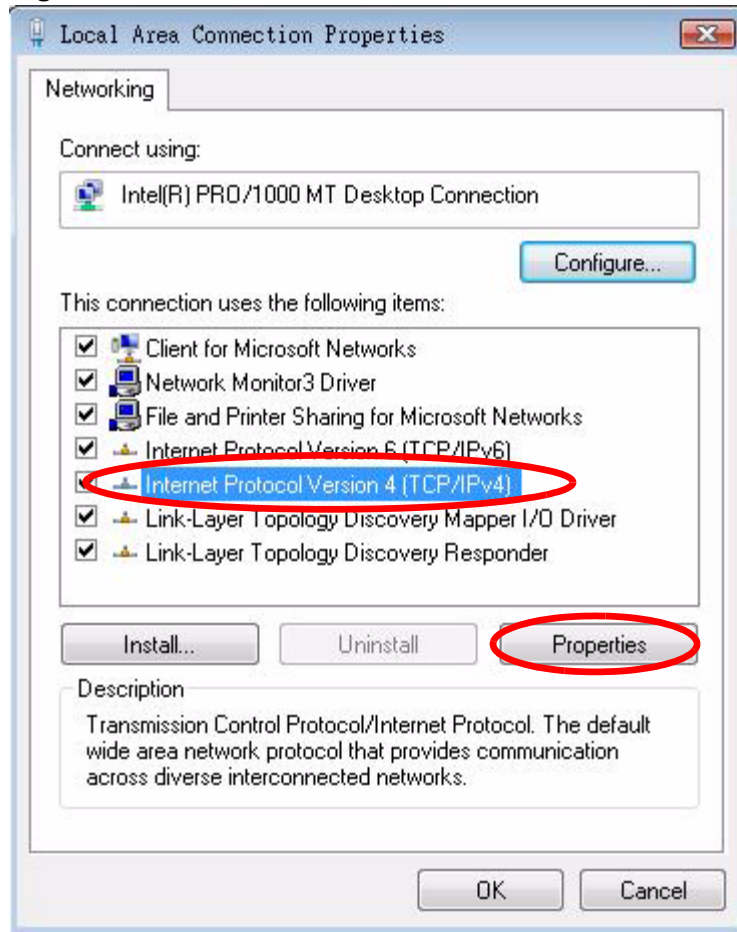
Figure 189 Windows Vista: Network and Sharing Center



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

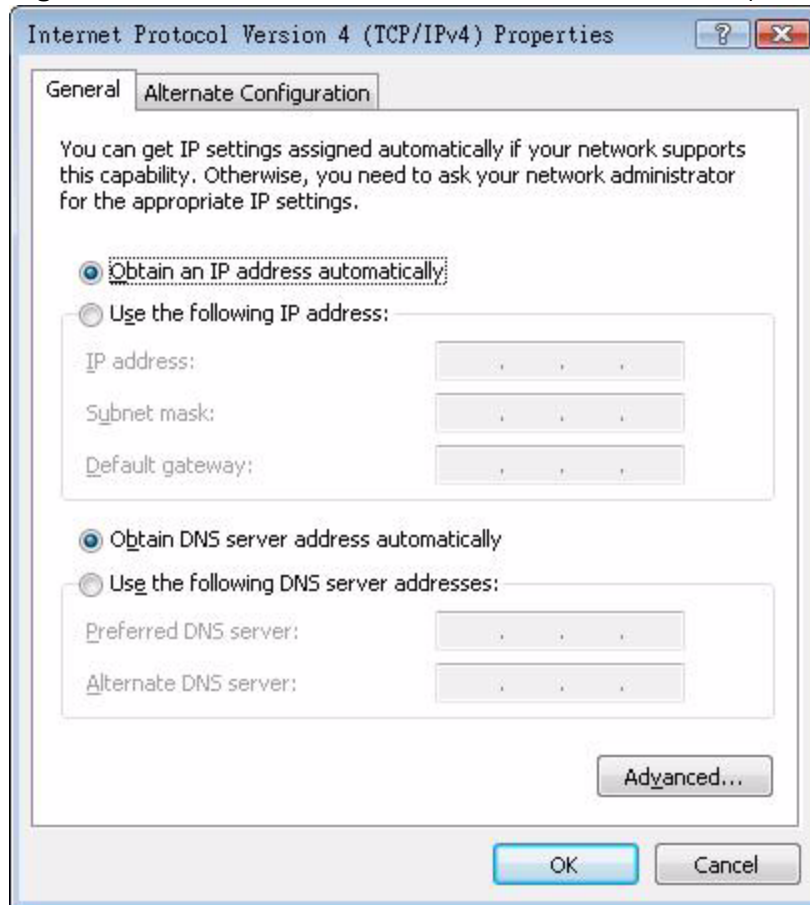
- 6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 190 Windows Vista: Local Area Connection Properties



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

Figure 191 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].

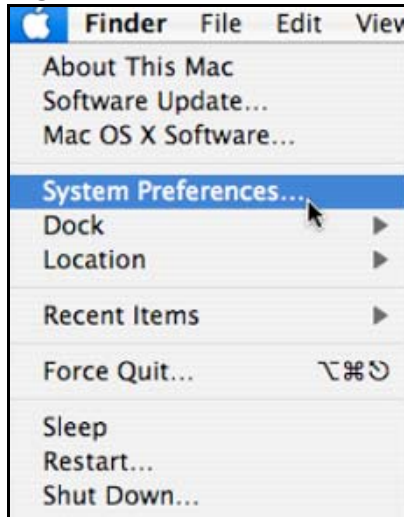
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

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 192 Mac OS X 10.4: Apple Menu



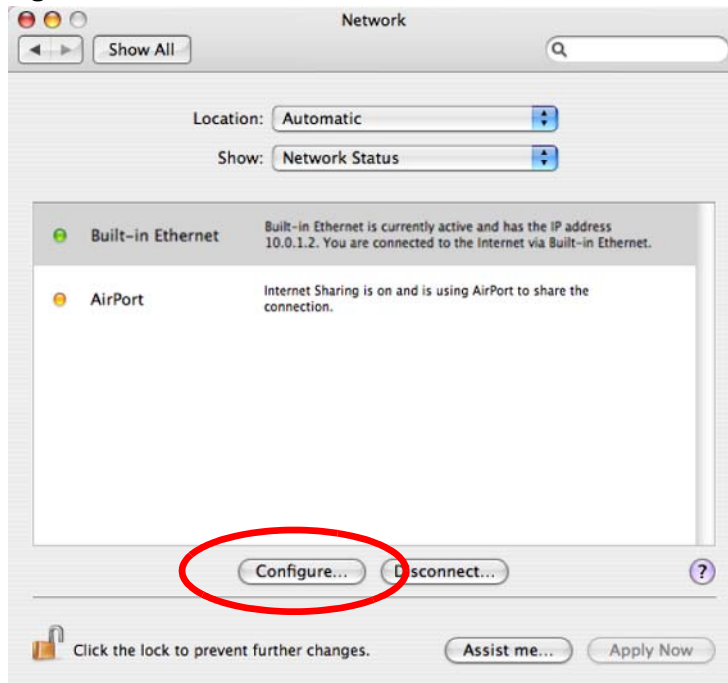
- 2 In the **System Preferences** window, click the **Network** icon.

Figure 193 Mac OS X 10.4: System Preferences



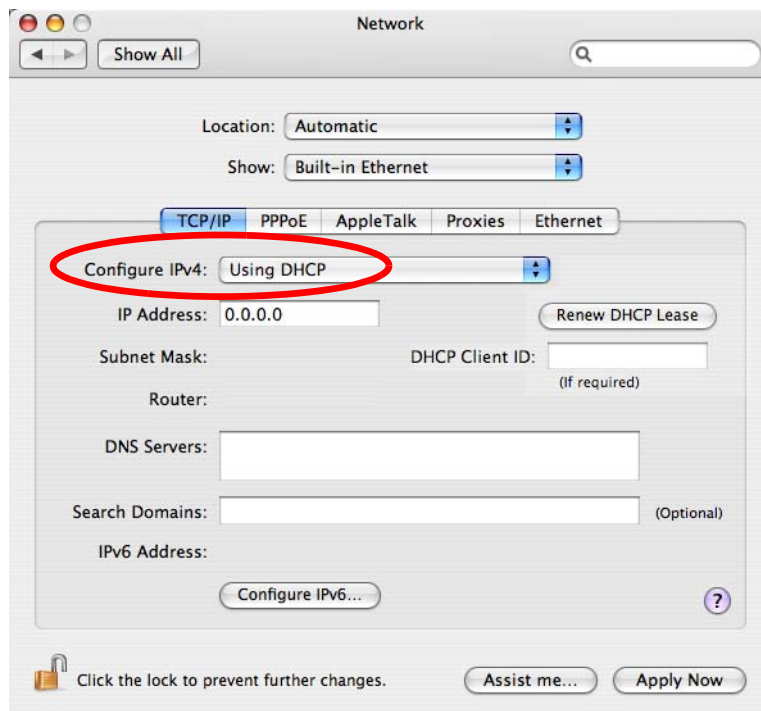
- 3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.

Figure 194 Mac OS X 10.4: Network Preferences



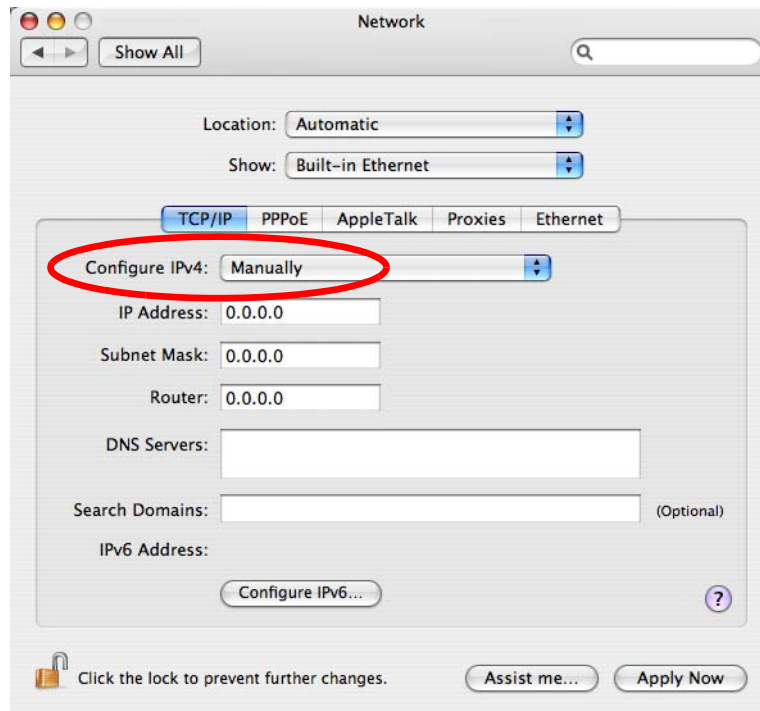
- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 195 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.

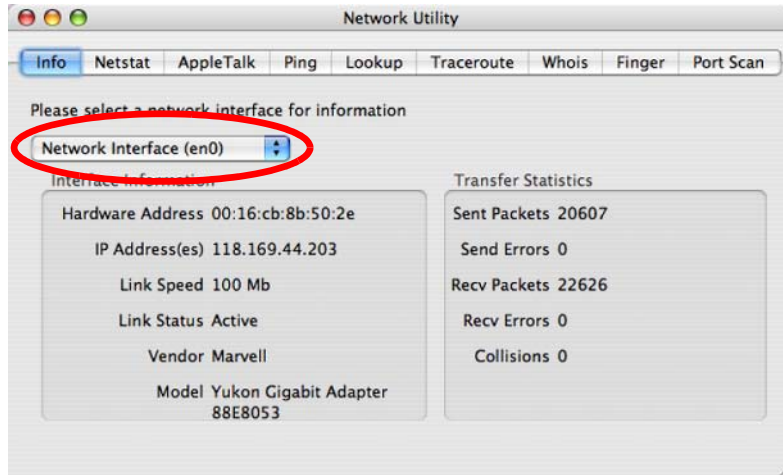
Figure 196 Mac OS X 10.4: Network Preferences > Ethernet



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 197 Mac OS X 10.4: Network Utility

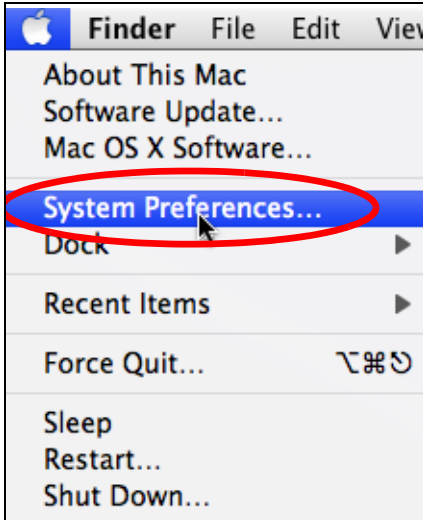


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

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

Figure 198 Mac OS X 10.5: Apple Menu



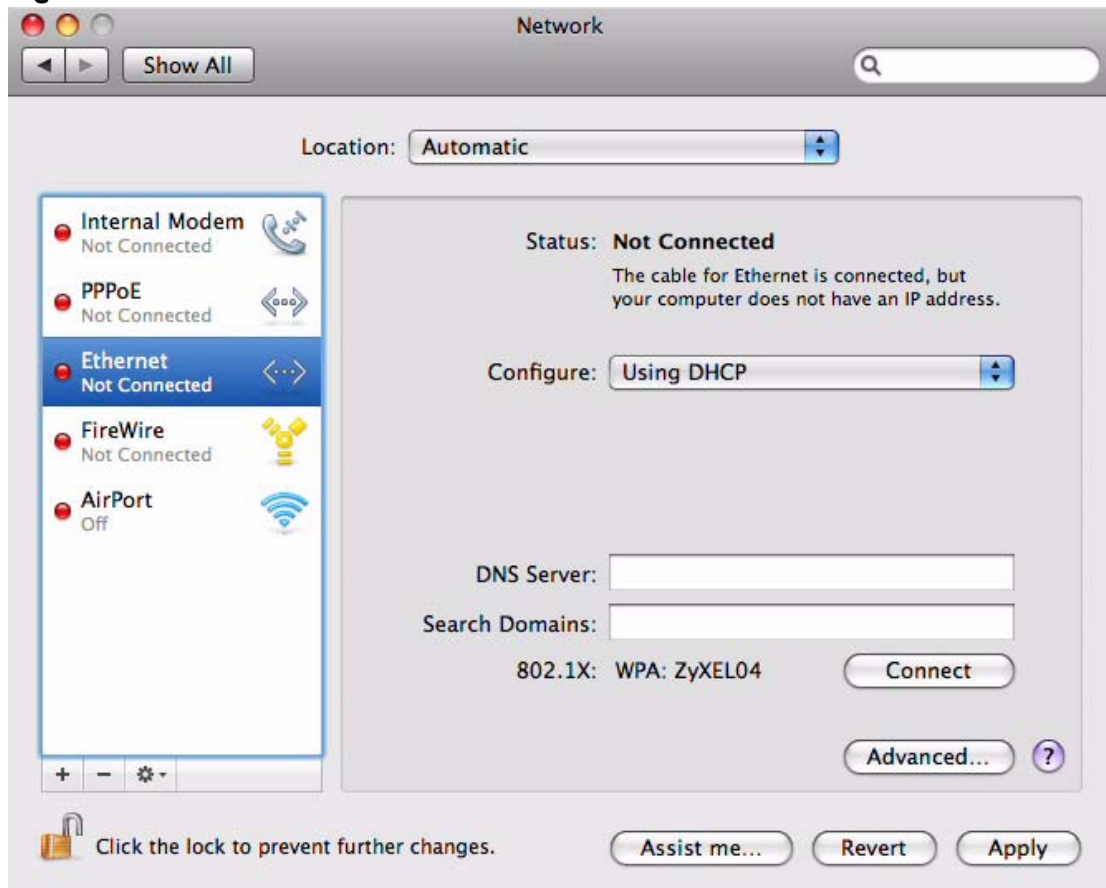
- 2 In **System Preferences**, click the **Network** icon.

Figure 199 Mac OS X 10.5: Systems Preferences



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

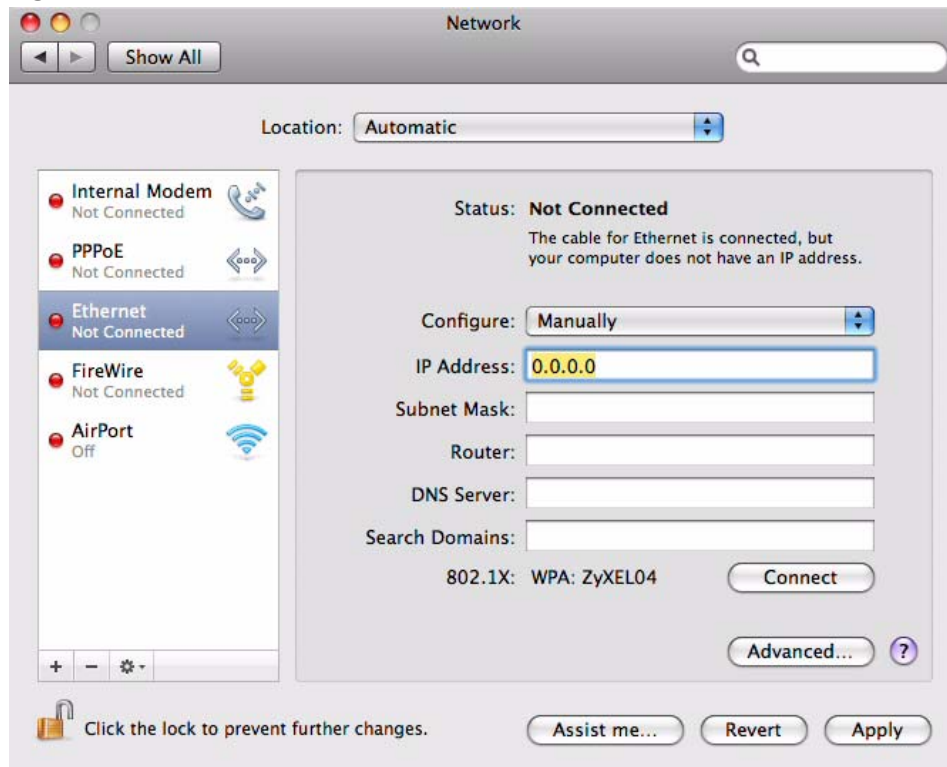
Figure 200 Mac OS X 10.5: Network Preferences > Ethernet



- 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 201 Mac OS X 10.5: Network Preferences > Ethernet

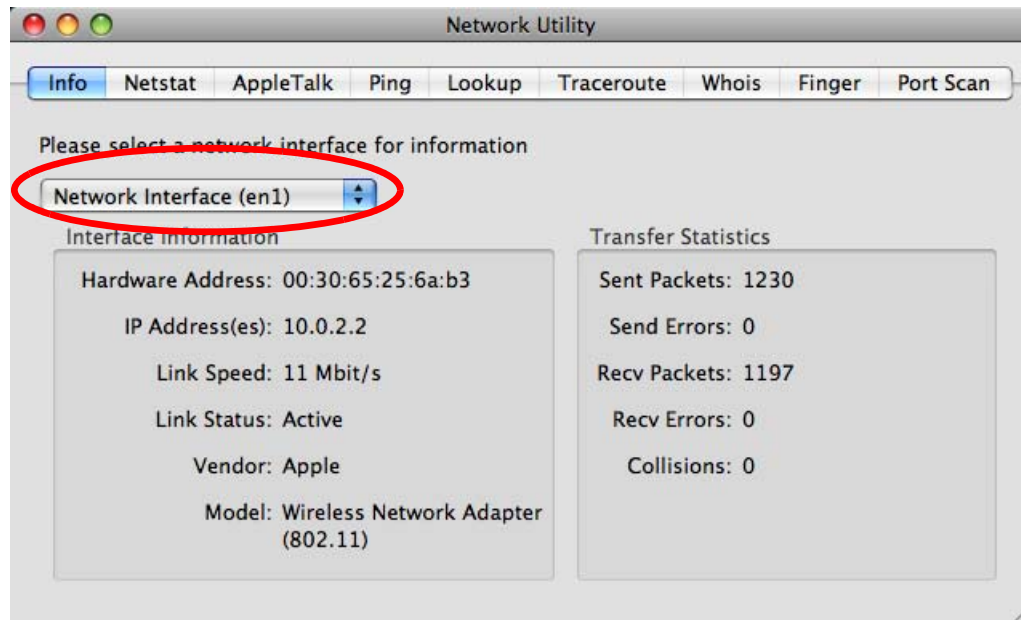


- 6 Click **Apply** and close the window.

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 202 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

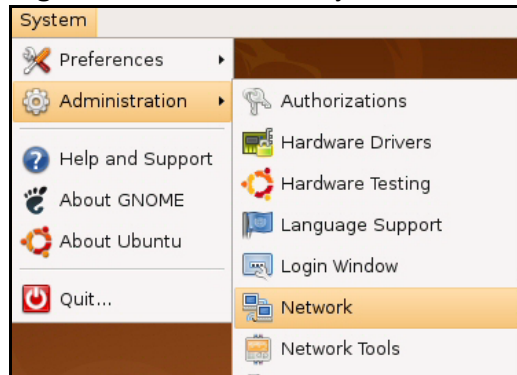
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following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

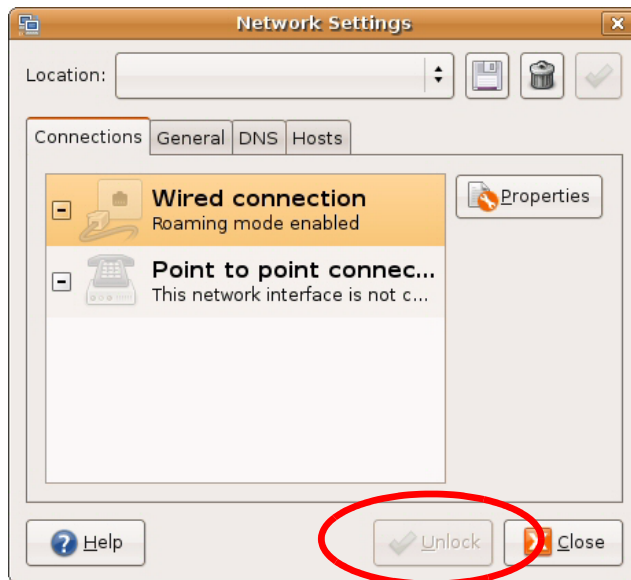
- 1 Click **System > Administration > Network**.

Figure 203 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 204 Ubuntu 8: Network Settings > Connections



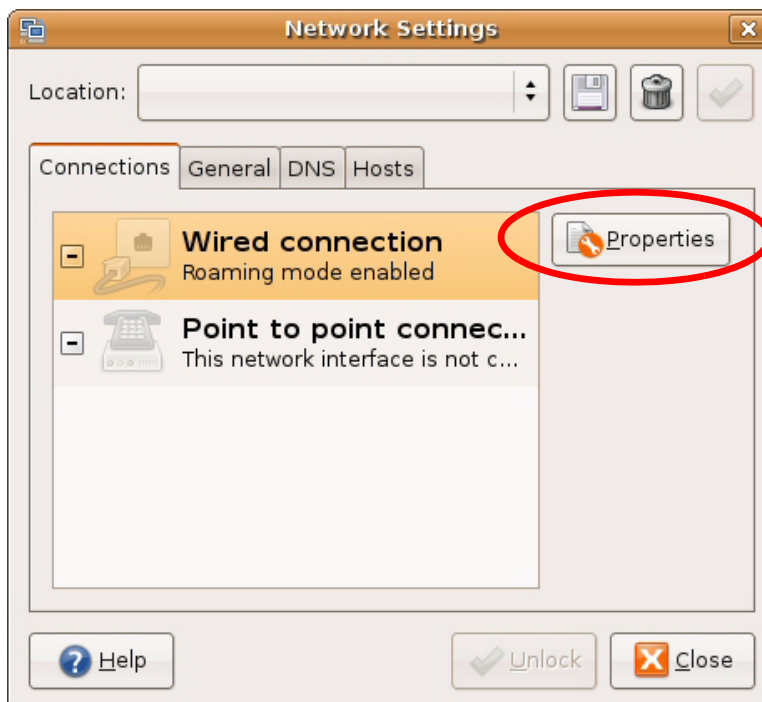
- 3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 205 Ubuntu 8: Administrator Account Authentication



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

Figure 206 Ubuntu 8: Network Settings > Connections



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

Figure 207 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 208 Ubuntu 8: Network Settings > DNS



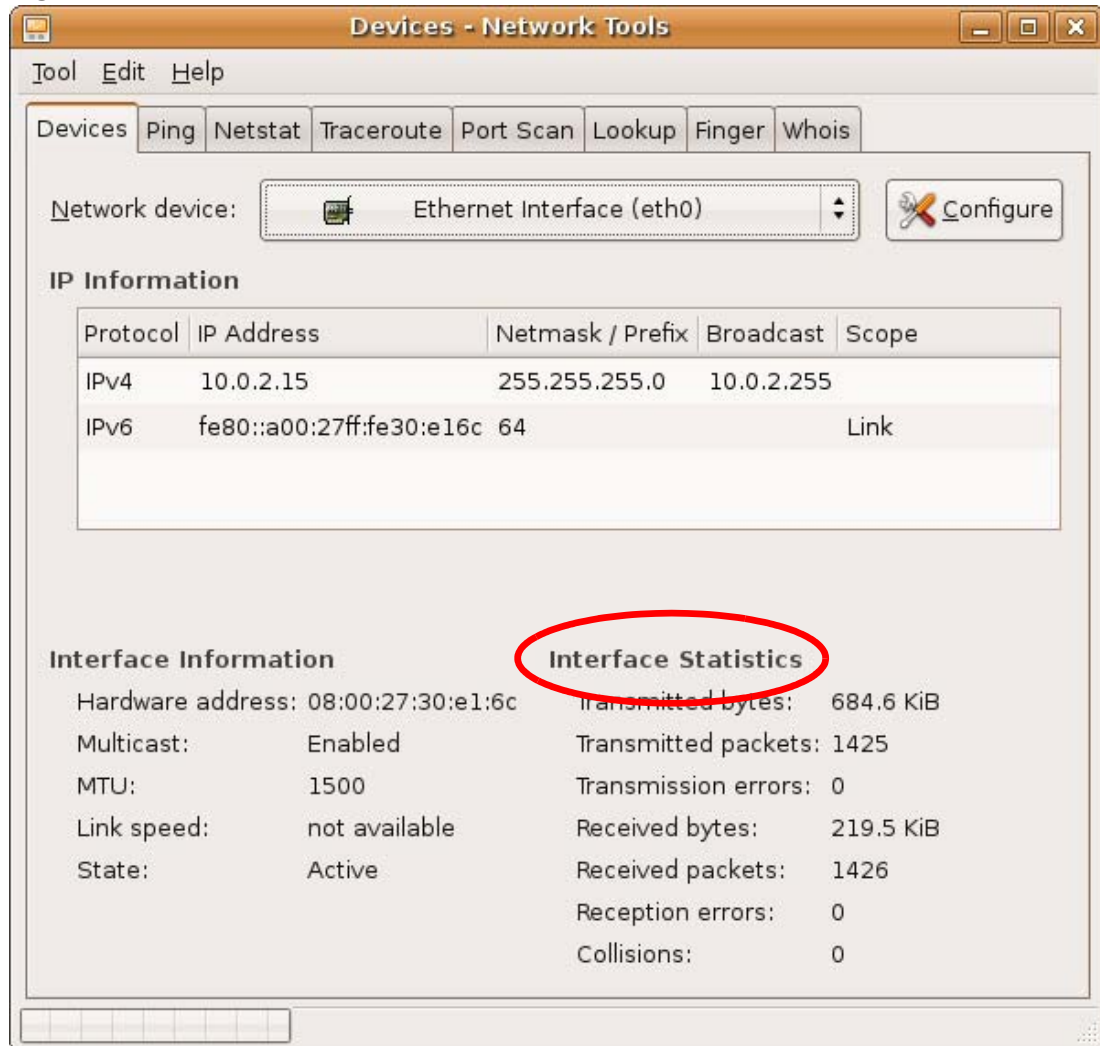
- 8 Click the **Close** button to apply the changes.

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 209 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

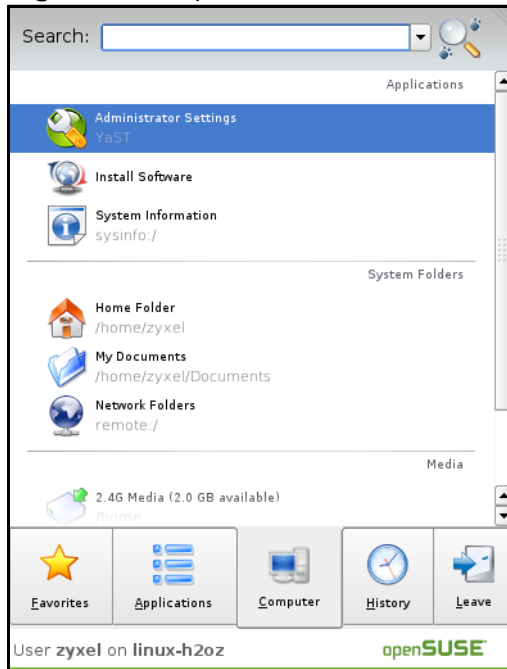
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following 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 210 openSUSE 10.3: K Menu > Computer Menu



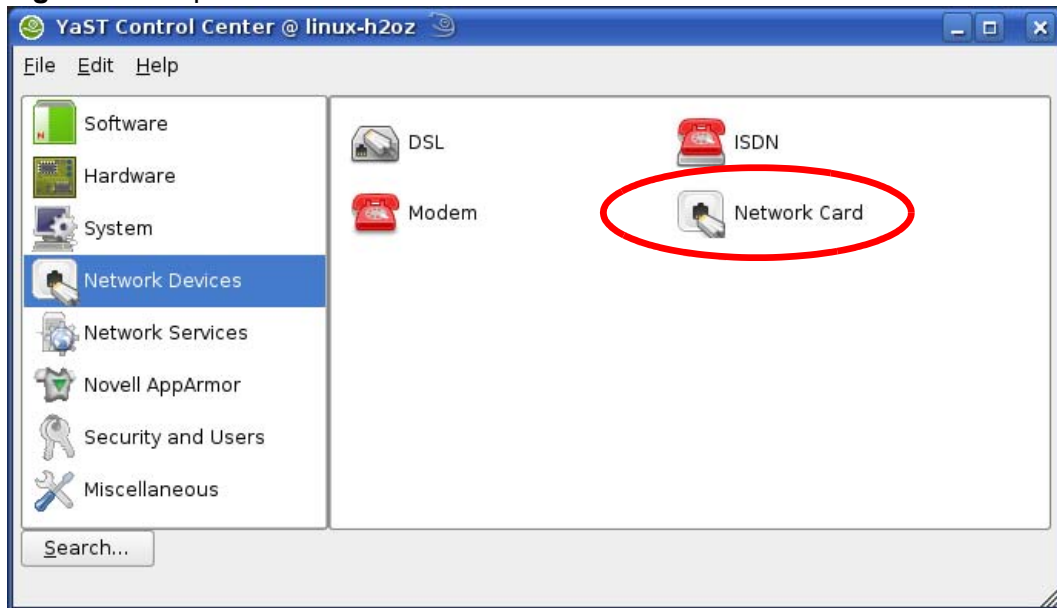
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 211 openSUSE 10.3: K Menu > Computer Menu



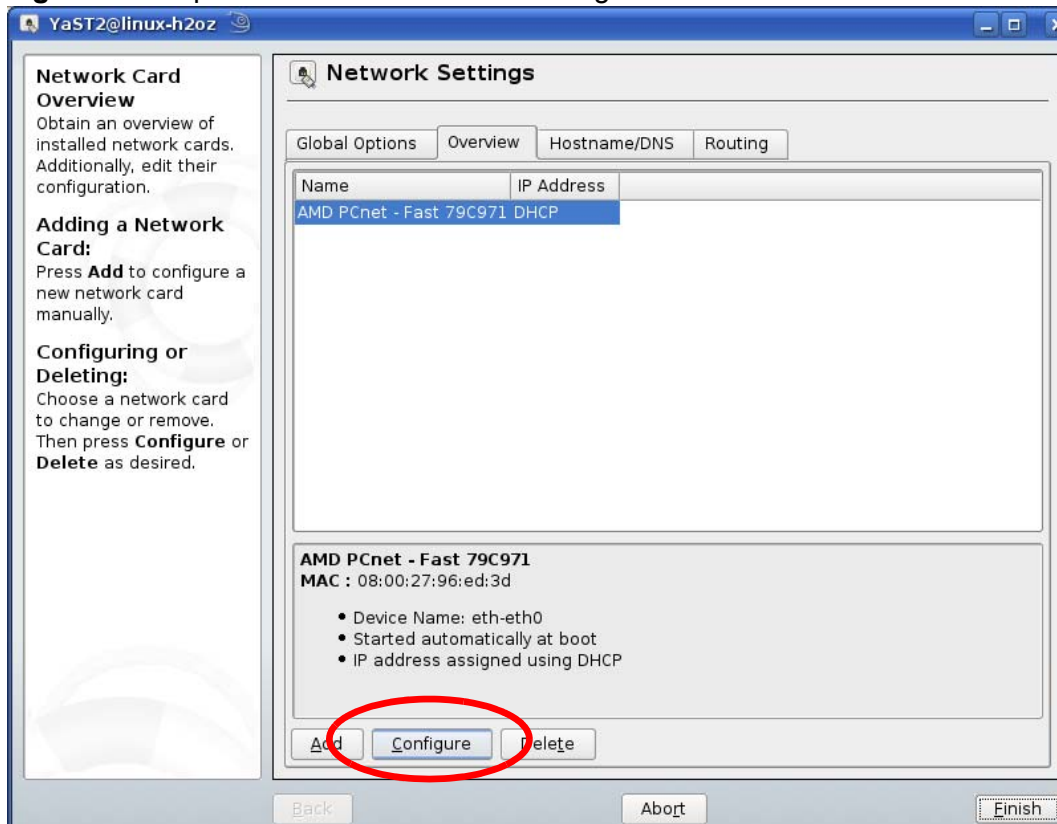
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 212 openSUSE 10.3: YaST Control Center



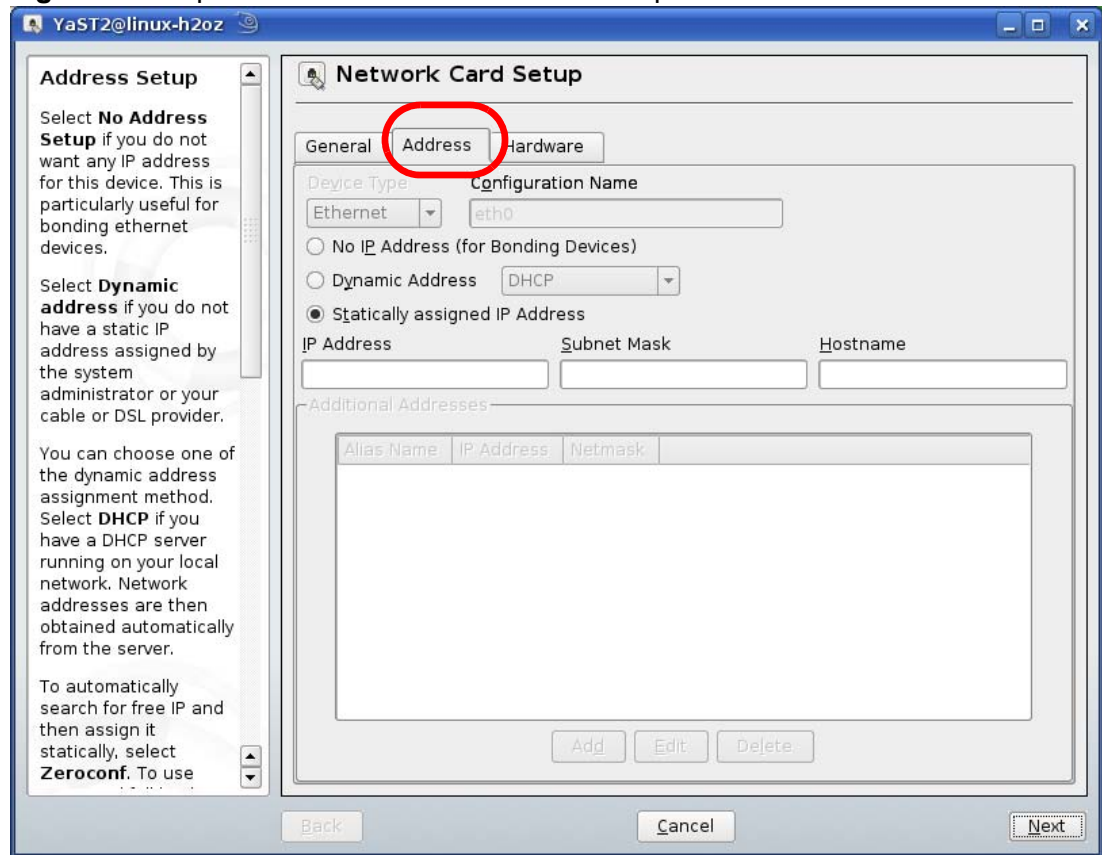
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 213 openSUSE 10.3: Network Settings



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

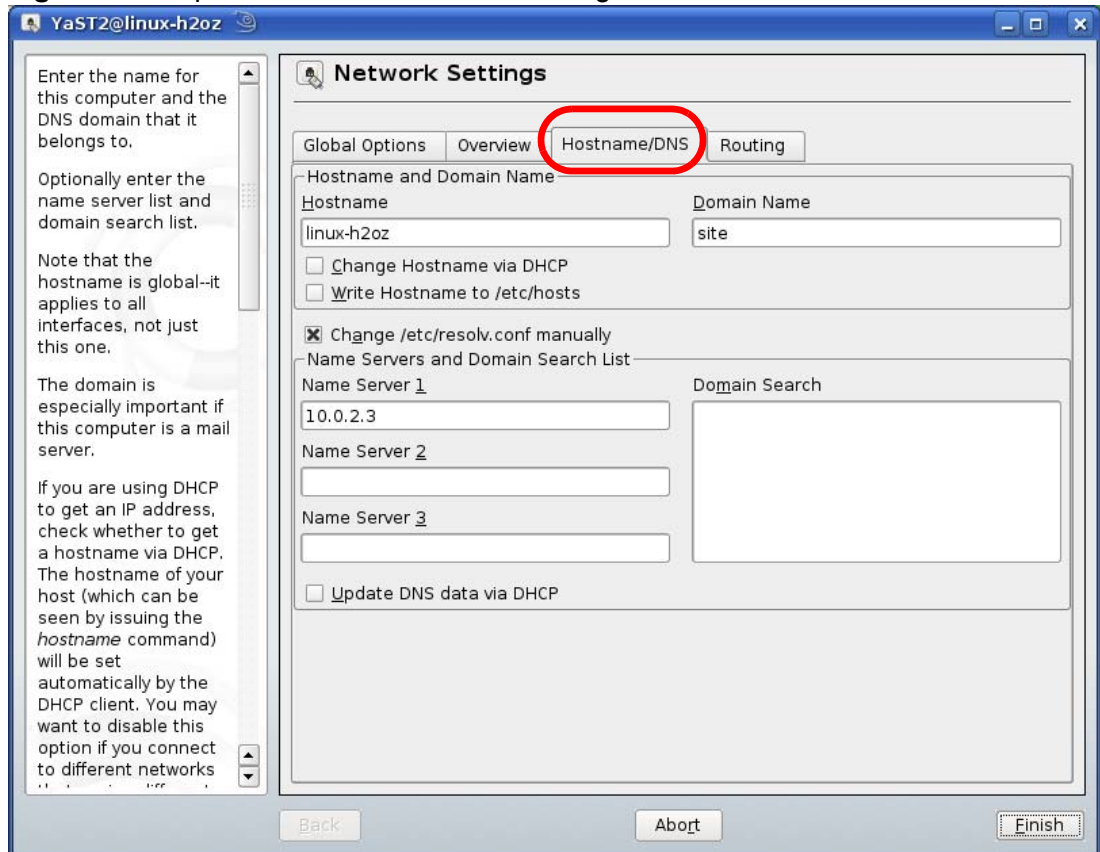
Figure 214 openSUSE 10.3: Network Card Setup



- 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 215 openSUSE 10.3: Network Settings

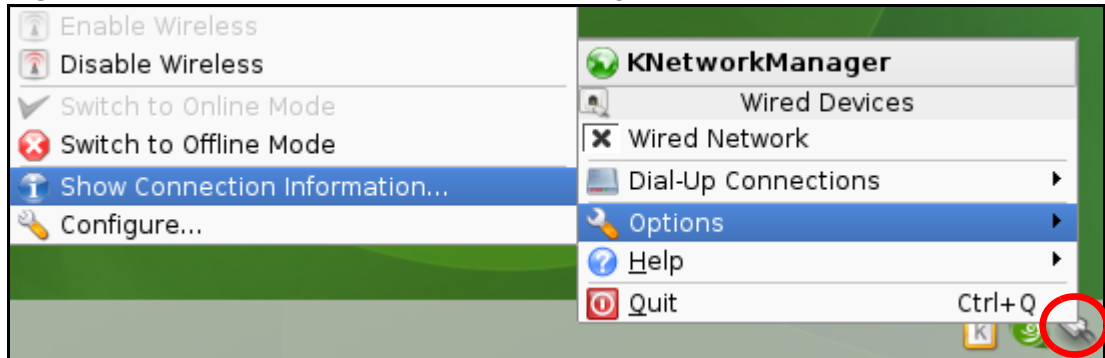


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

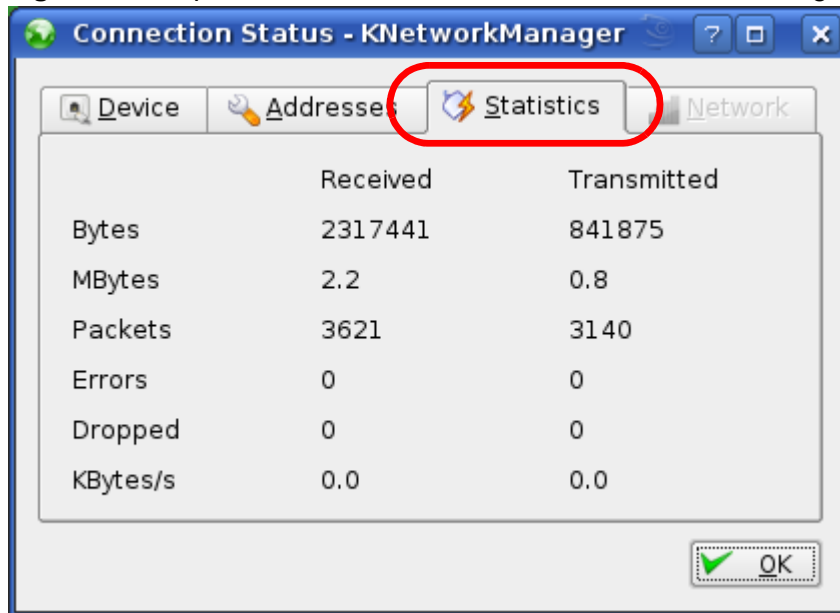
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 216 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 217 openSUSE: Connection Status - KNetwork Manager



Wireless LANs

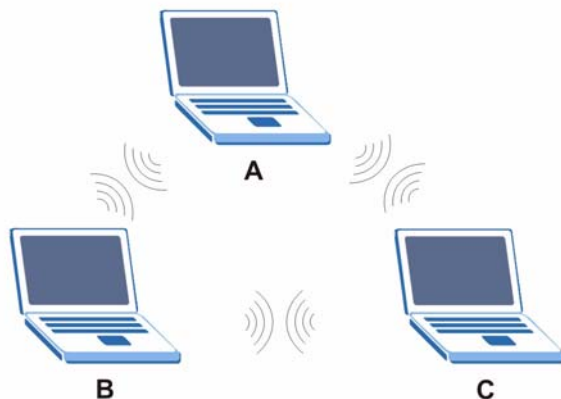
Wireless LAN Topologies

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



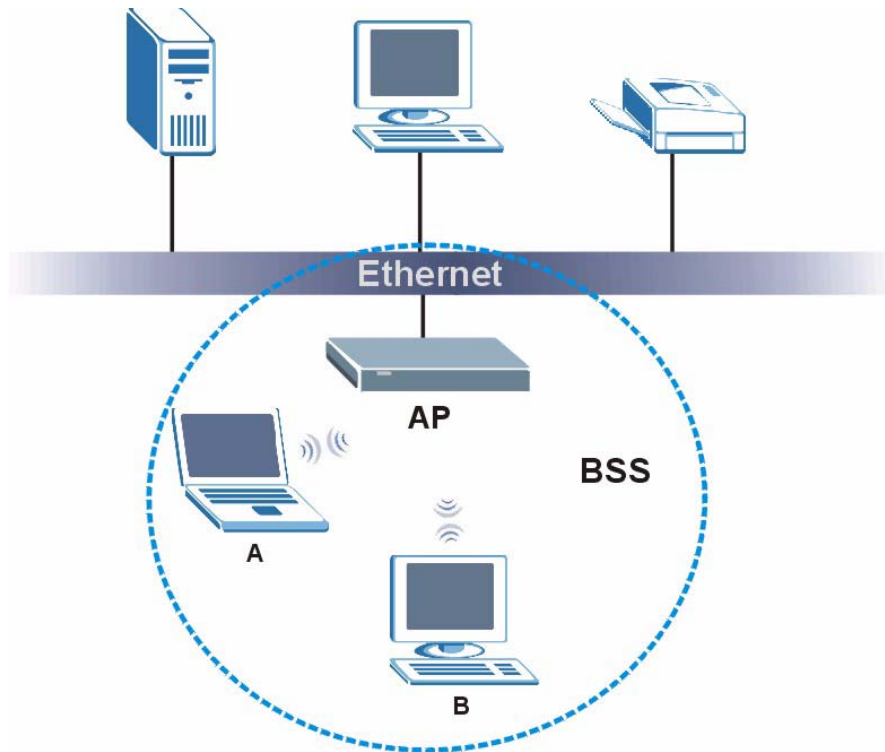
BSS

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 219 Basic Service Set



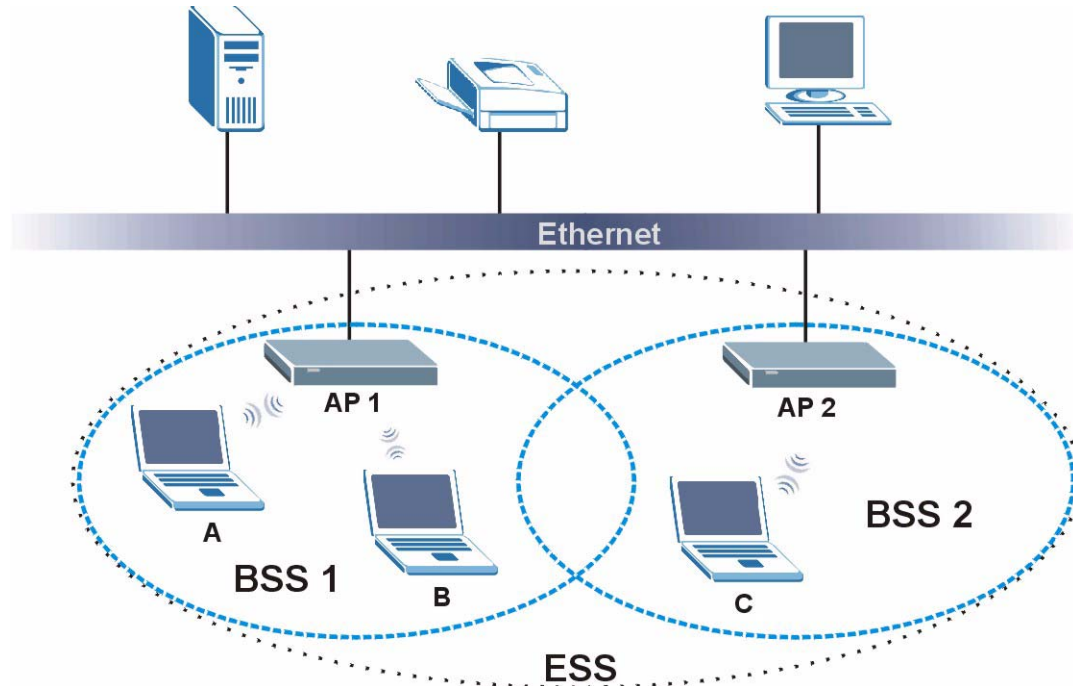
ESS

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 220 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.

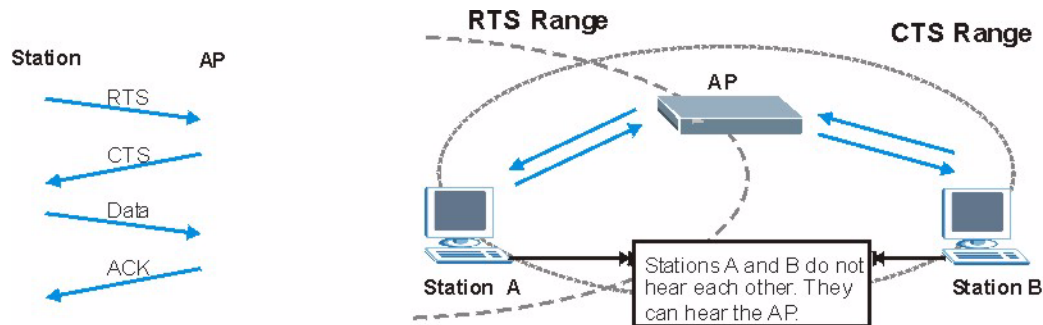
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel 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 221 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 96 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 97 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 98 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.

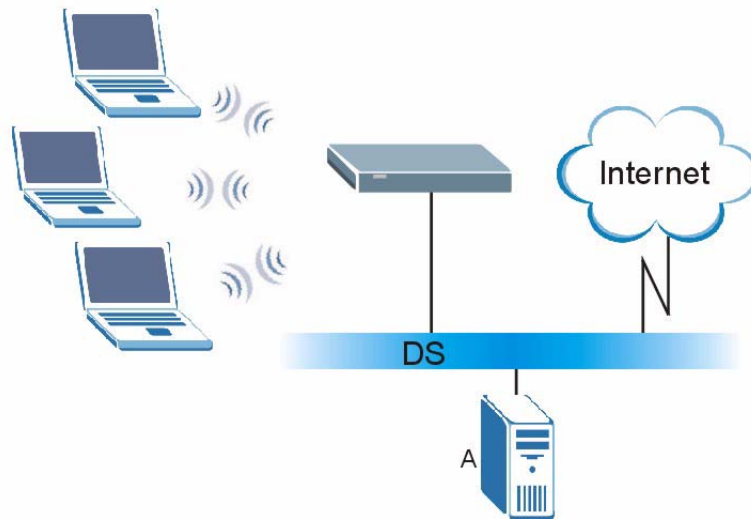
WPA(2) with RADIUS Application Example

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 222 WPA(2) with RADIUS Application Example



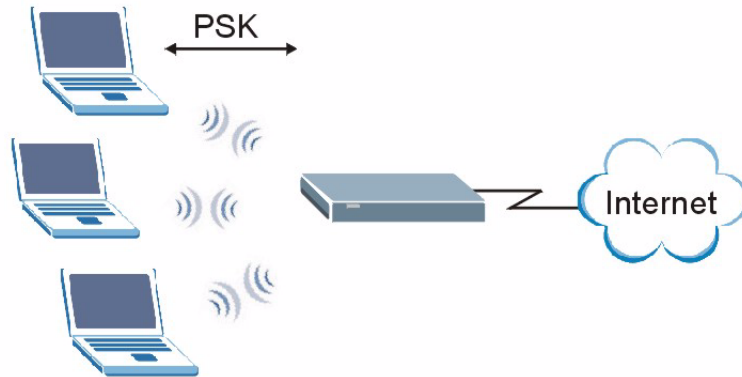
WPA(2)-PSK Application Example

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 223 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 99 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

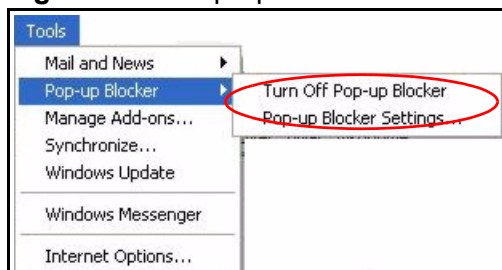
You may have to disable pop-up blocking to log into your device.

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**.

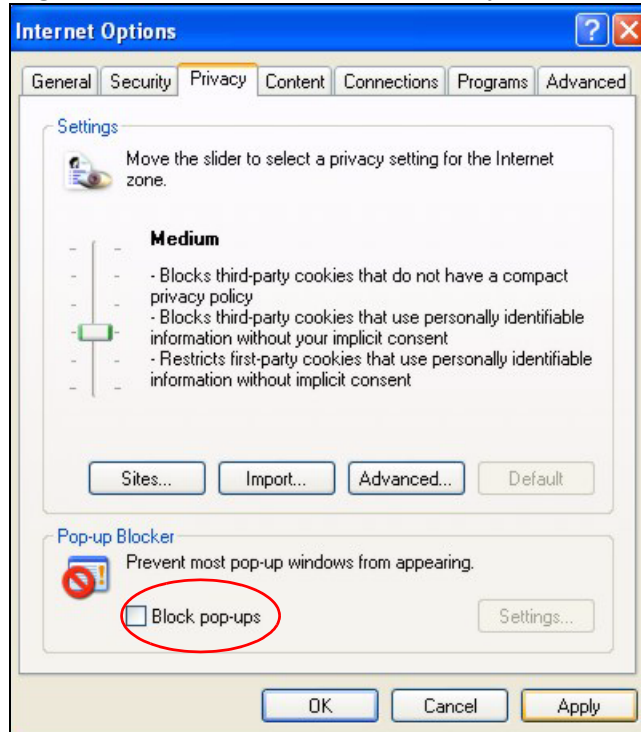
Figure 224 Pop-up Blocker



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 225 Internet Options: Privacy



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

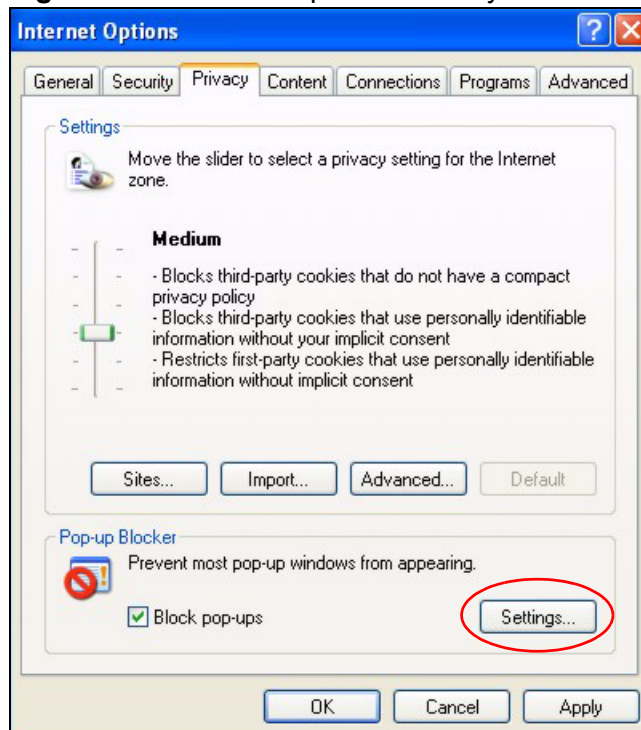
Enable pop-up Blockers with Exceptions

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.

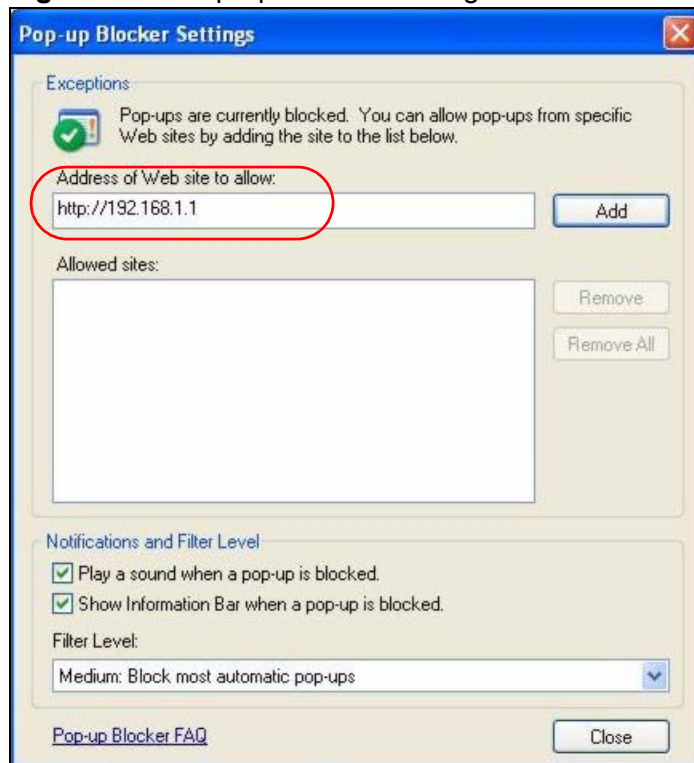
Figure 226 Internet Options: Privacy



- 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 227 Pop-up Blocker Settings



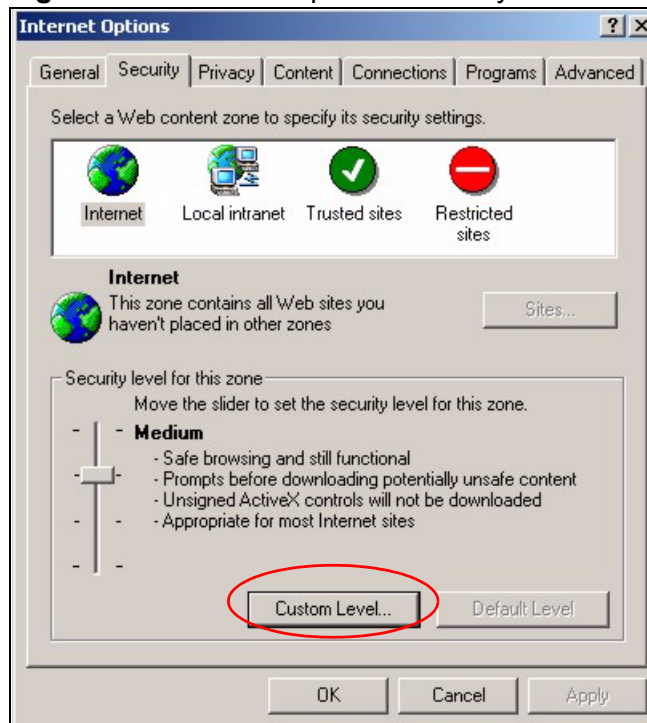
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

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.

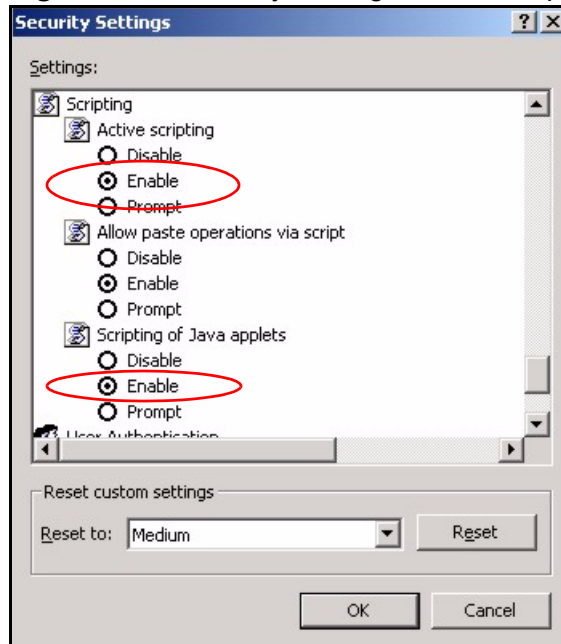
Figure 228 Internet Options: Security



- 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 229 Security Settings - Java Scripting

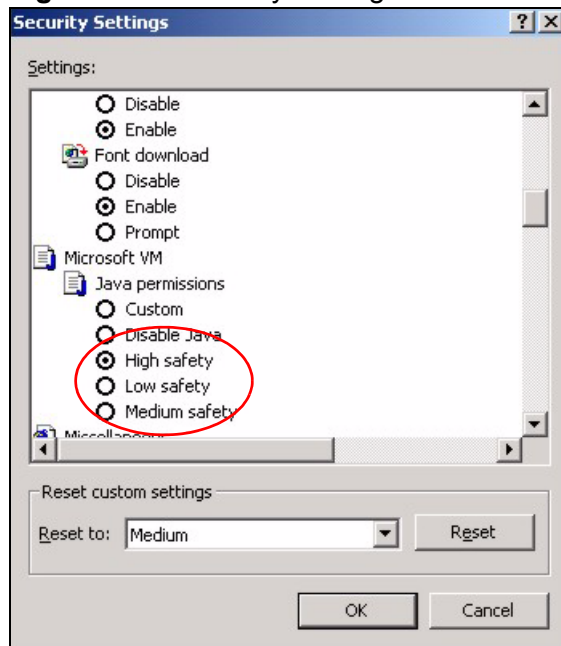


Java Permissions

- 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 230 Security Settings - Java

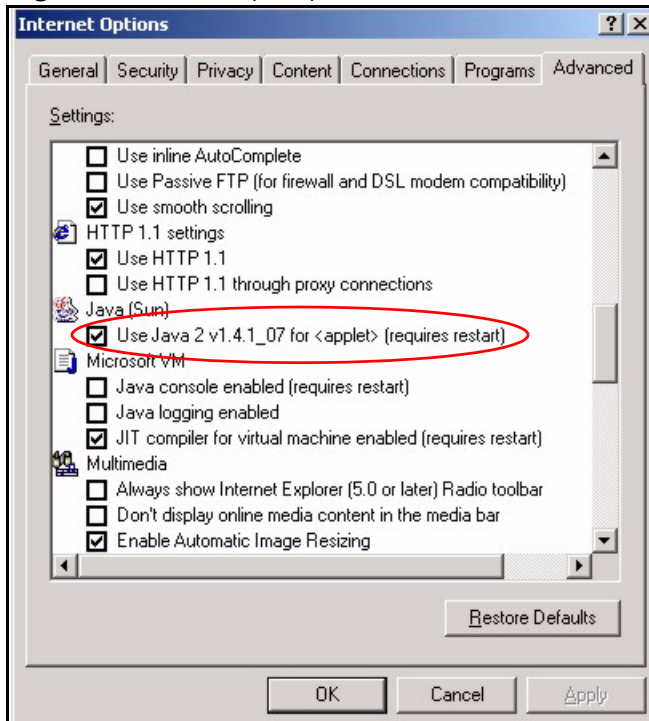


JAVA (Sun)

- 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 231 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:

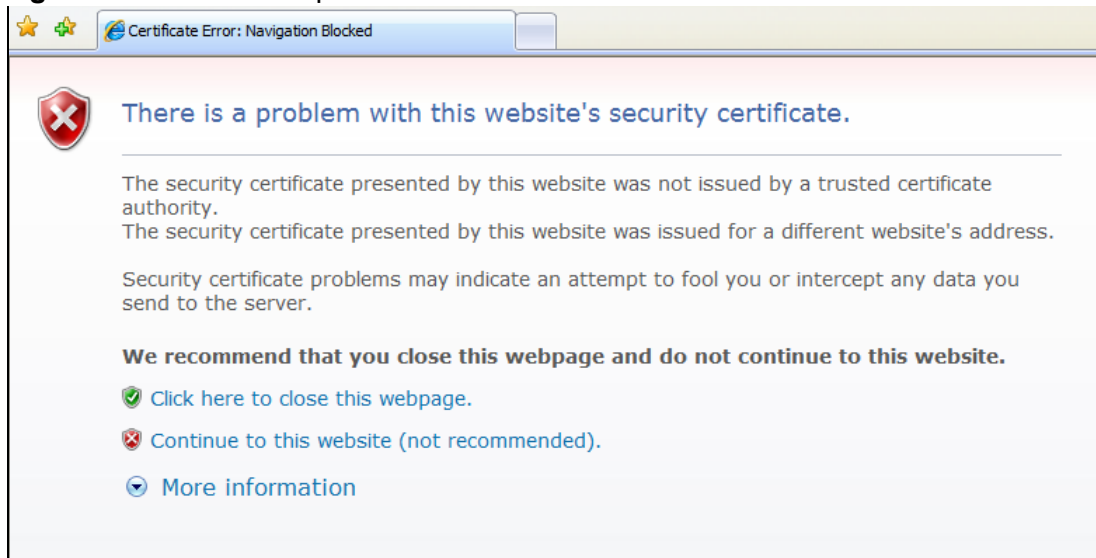
- Internet Explorer on [page 355](#)
- Firefox on [page 364](#)
- Opera on [page 369](#)
- Konqueror on [page 376](#)

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 232 Internet Explorer 7: Certification Error



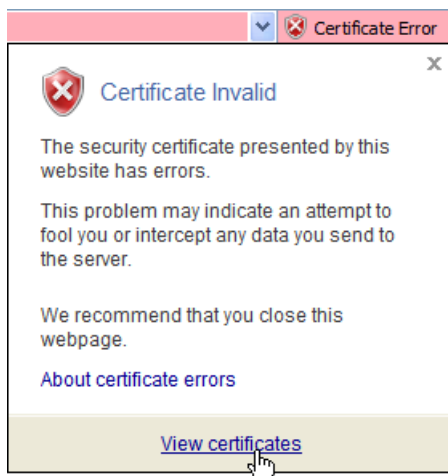
- 2 Click **Continue to this website (not recommended)**.

Figure 233 Internet Explorer 7: Certification Error



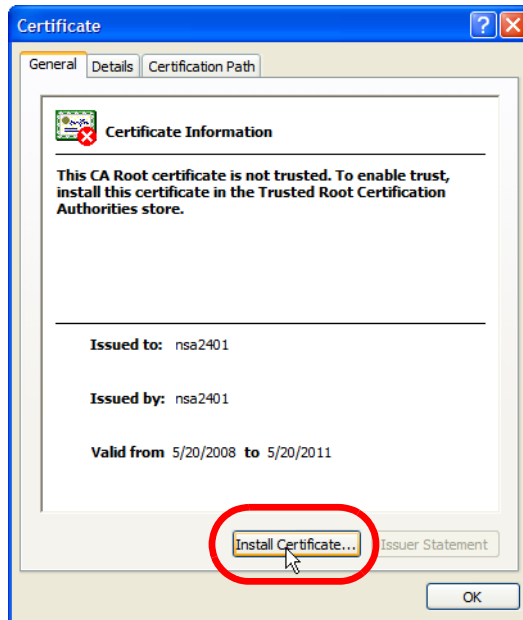
- 3 In the **Address Bar**, click **Certificate Error > View certificates**.

Figure 234 Internet Explorer 7: Certificate Error



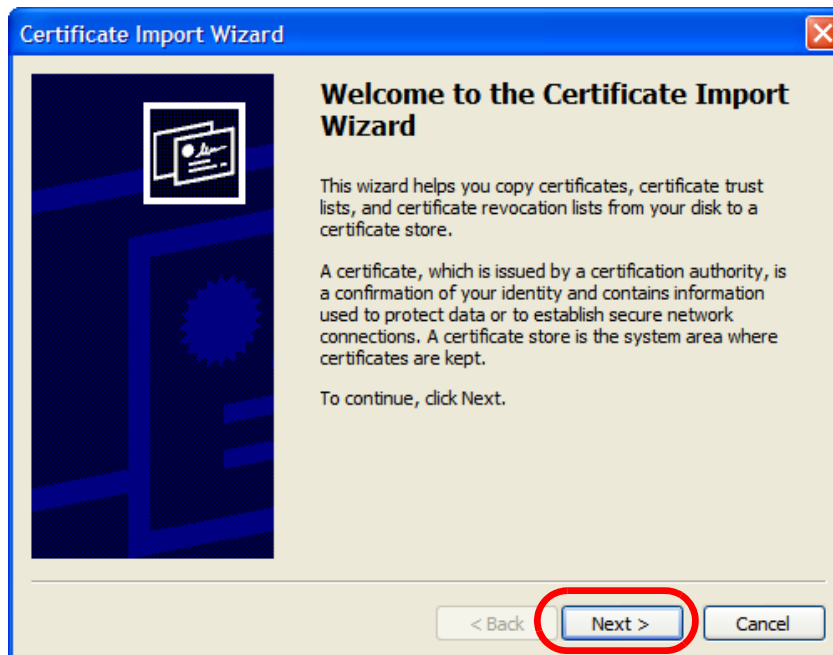
- 4 In the **Certificate** dialog box, click **Install Certificate**.

Figure 235 Internet Explorer 7: Certificate



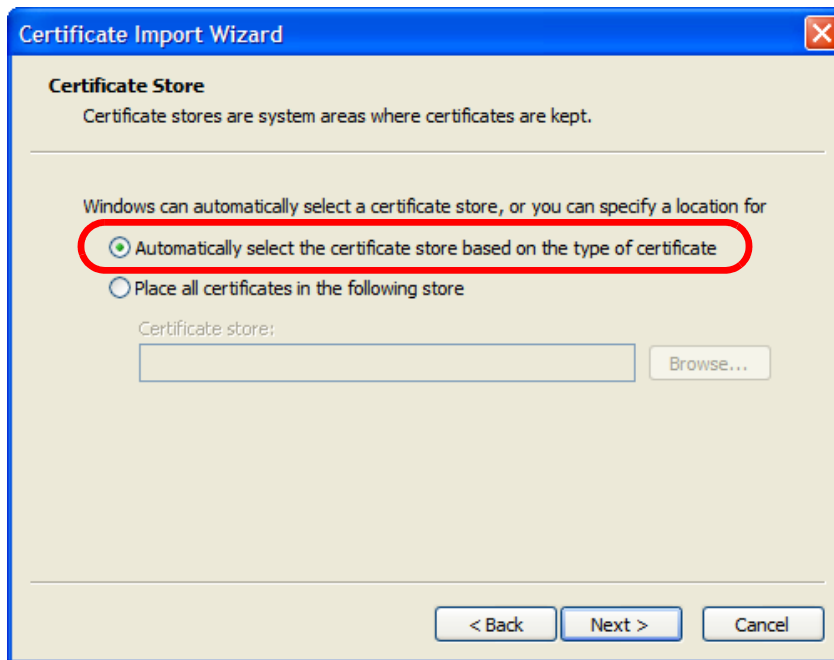
- 5 In the **Certificate Import Wizard**, click **Next**.

Figure 236 Internet Explorer 7: Certificate Import Wizard



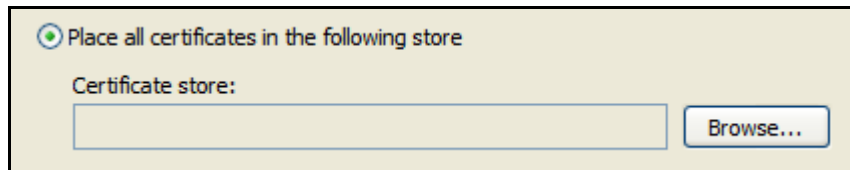
- 6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

Figure 237 Internet Explorer 7: Certificate Import Wizard



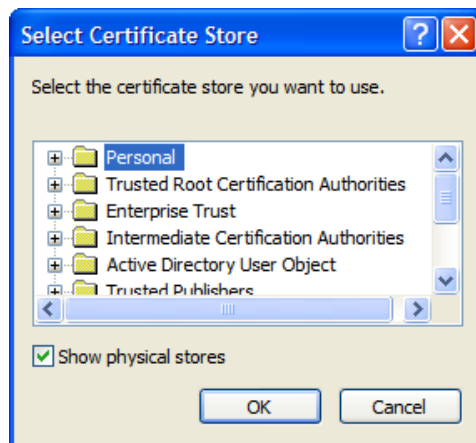
- 7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

Figure 238 Internet Explorer 7: Certificate Import Wizard



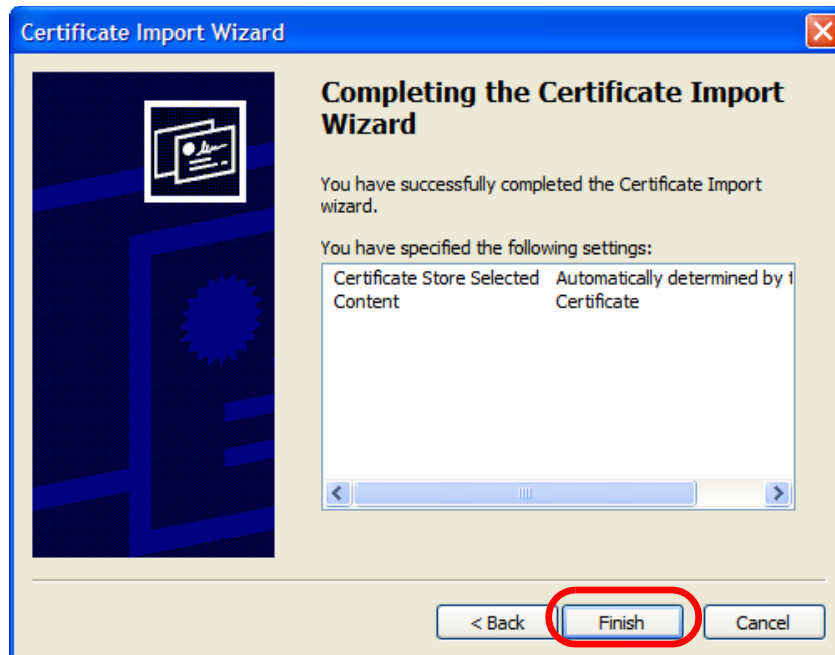
- 8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

Figure 239 Internet Explorer 7: Select Certificate Store



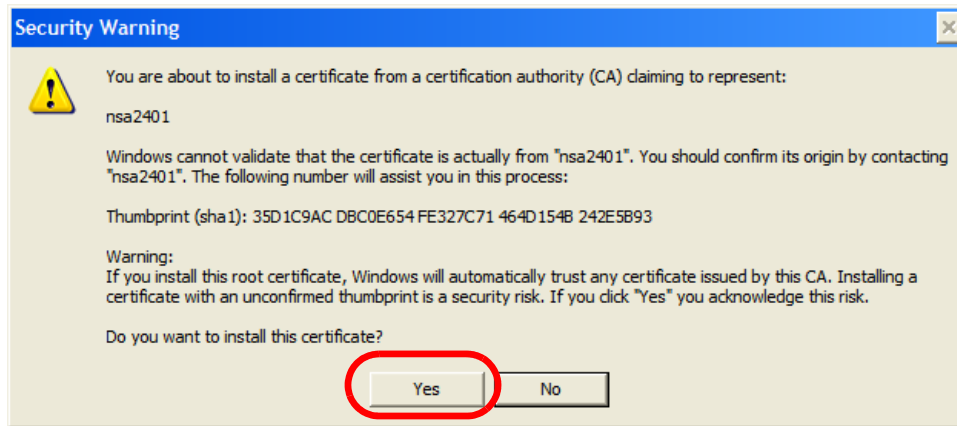
- 9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

Figure 240 Internet Explorer 7: Certificate Import Wizard



- 10 If you are presented with another **Security Warning**, click **Yes**.

Figure 241 Internet Explorer 7: Security Warning



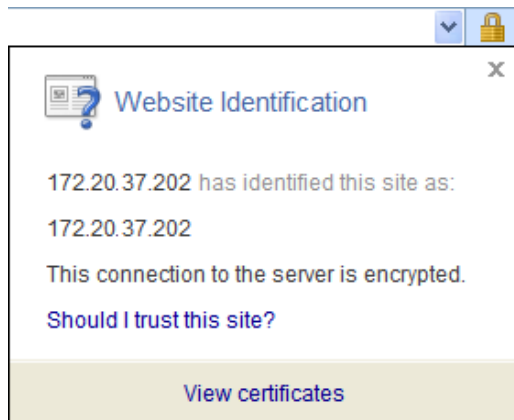
- 11 Finally, click **OK** when presented with the successful certificate installation message.

Figure 242 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 243 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.

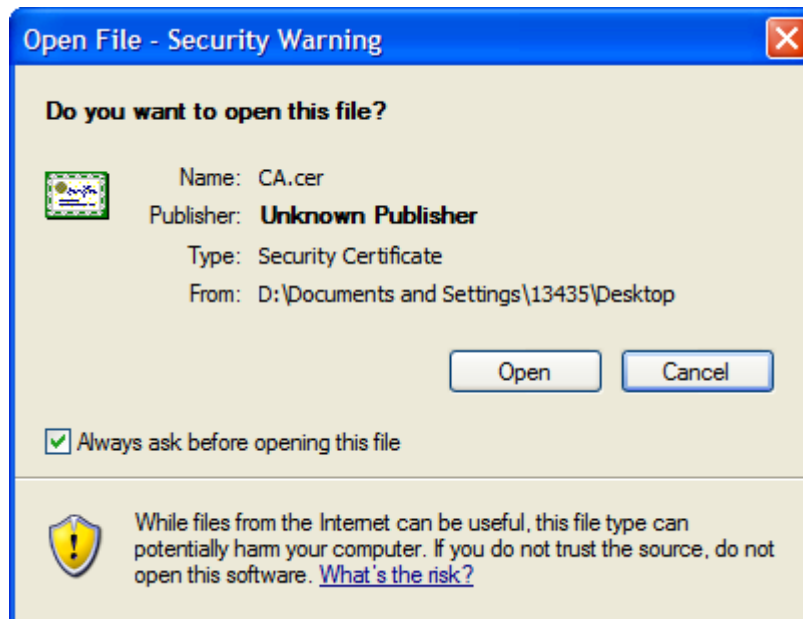
- 1 Double-click the public key certificate file.

Figure 244 Internet Explorer 7: Public Key Certificate File



- 2 In the security warning dialog box, click **Open**.

Figure 245 Internet Explorer 7: Open File - Security Warning



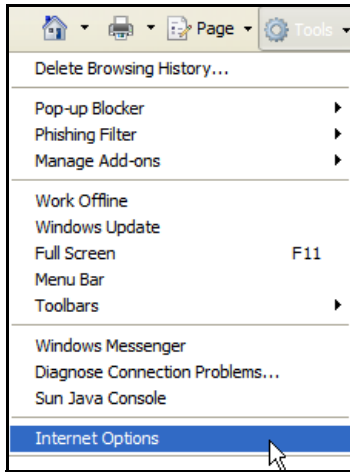
- 3 Refer to steps 4-12 in the Internet Explorer procedure beginning on [page 355](#) to complete the installation process.

Removing a Certificate in Internet Explorer

This section shows you how to remove a public key certificate in Internet Explorer 7.

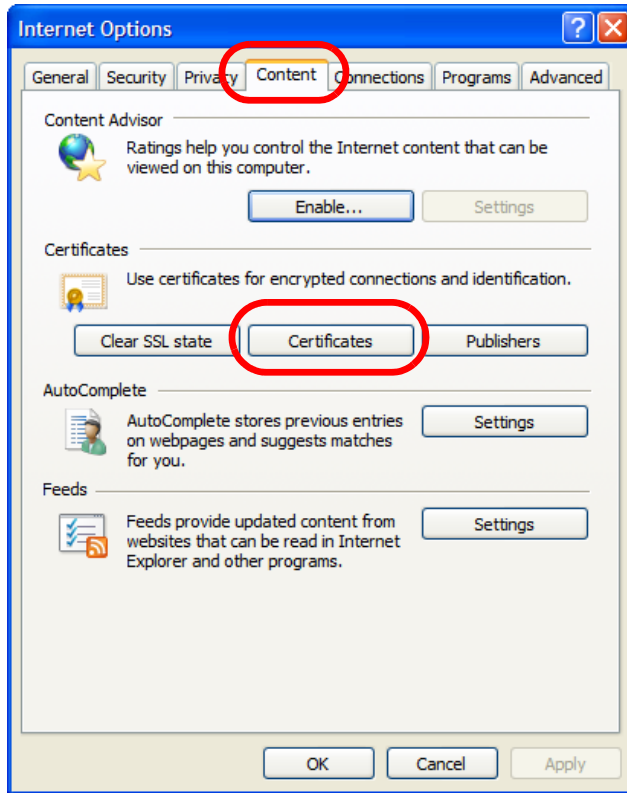
- 1 Open **Internet Explorer** and click **Tools > Internet Options**.

Figure 246 Internet Explorer 7: Tools Menu



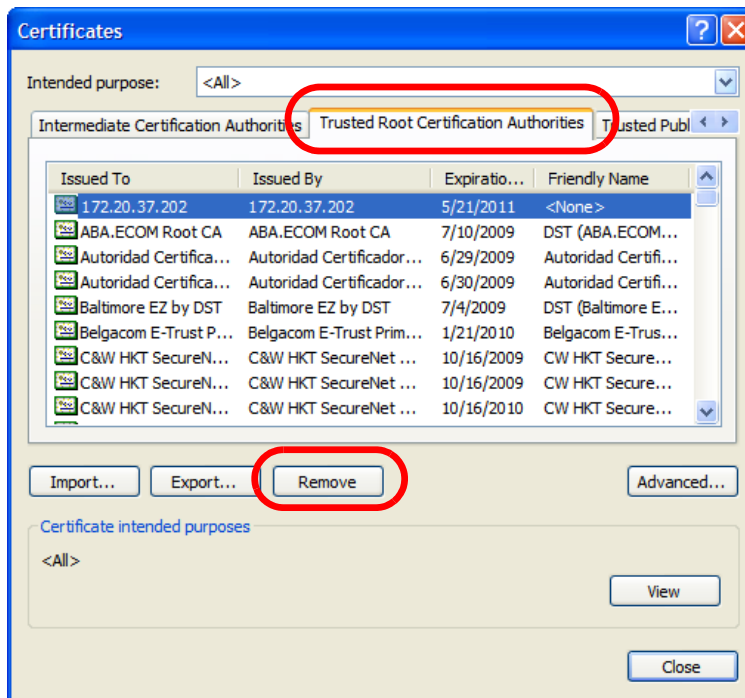
- 2 In the **Internet Options** dialog box, click **Content > Certificates**.

Figure 247 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 248 Internet Explorer 7: Certificates



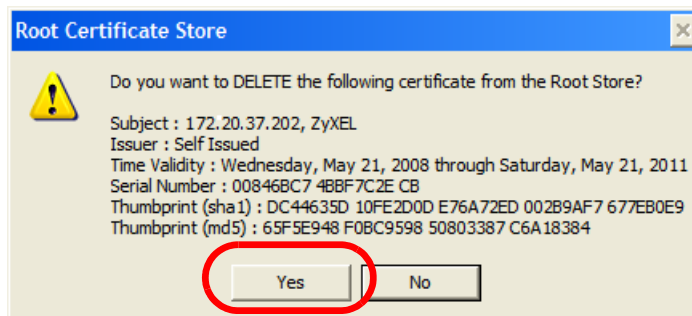
- 4 In the **Certificates** confirmation, click **Yes**.

Figure 249 Internet Explorer 7: Certificates



- 5 In the **Root Certificate Store** dialog box, click **Yes**.

Figure 250 Internet Explorer 7: Root Certificate Store



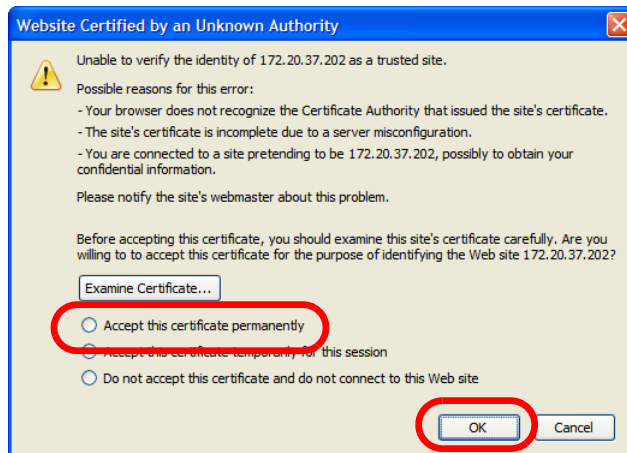
- 6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

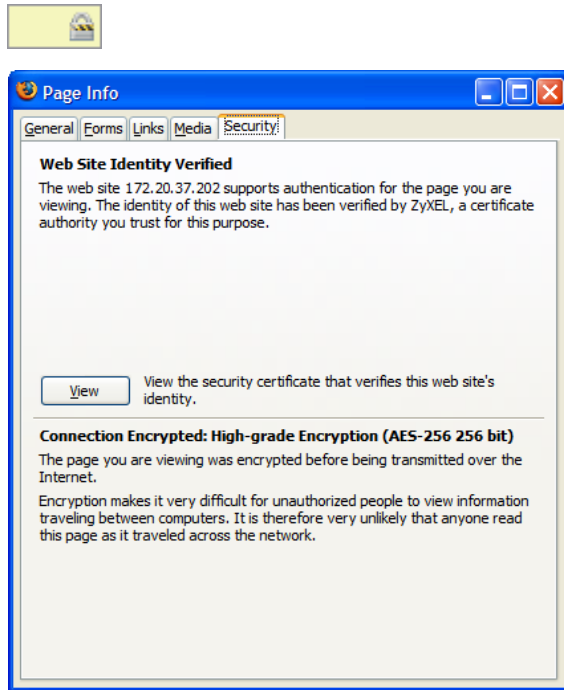
- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Select **Accept this certificate permanently** and click **OK**.

Figure 251 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 252 Firefox 2: Page Info

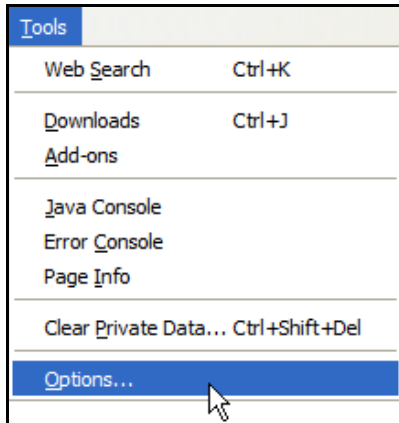


Installing a Stand-Alone Certificate File in Firefox

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.

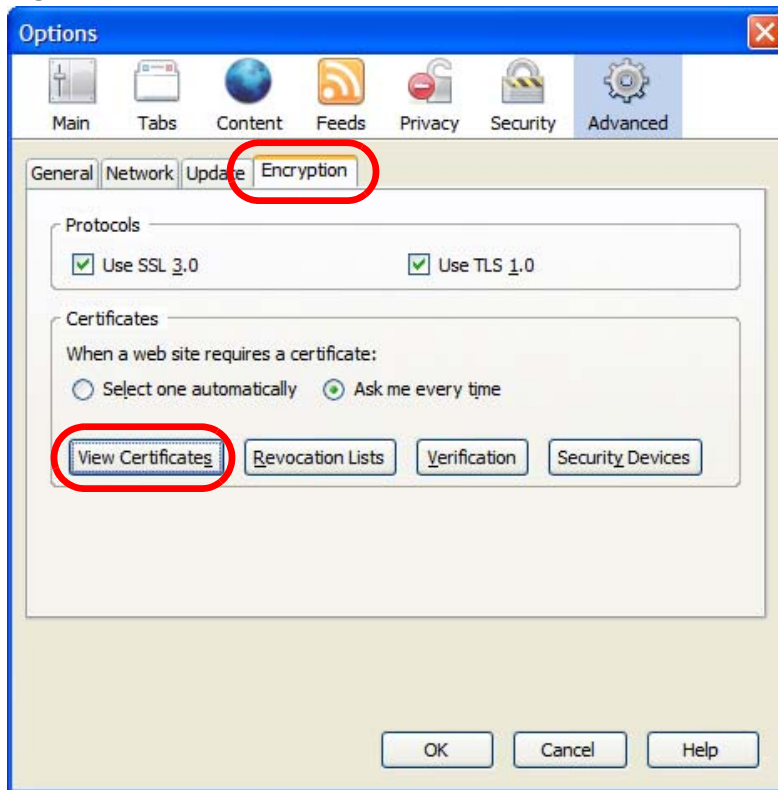
- 1 Open **Firefox** and click **Tools > Options**.

Figure 253 Firefox 2: Tools Menu



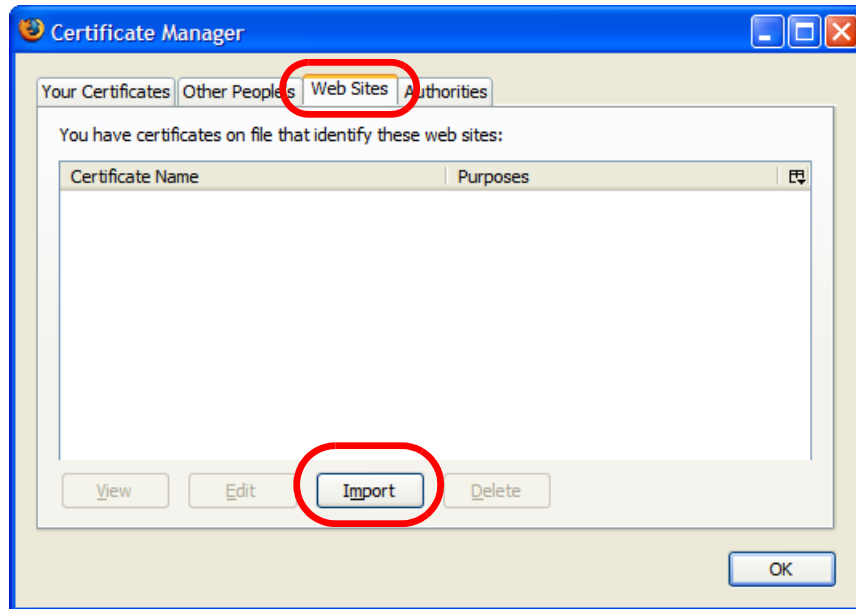
- 2 In the **Options** dialog box, click **Advanced > Encryption > View Certificates**.

Figure 254 Firefox 2: Options



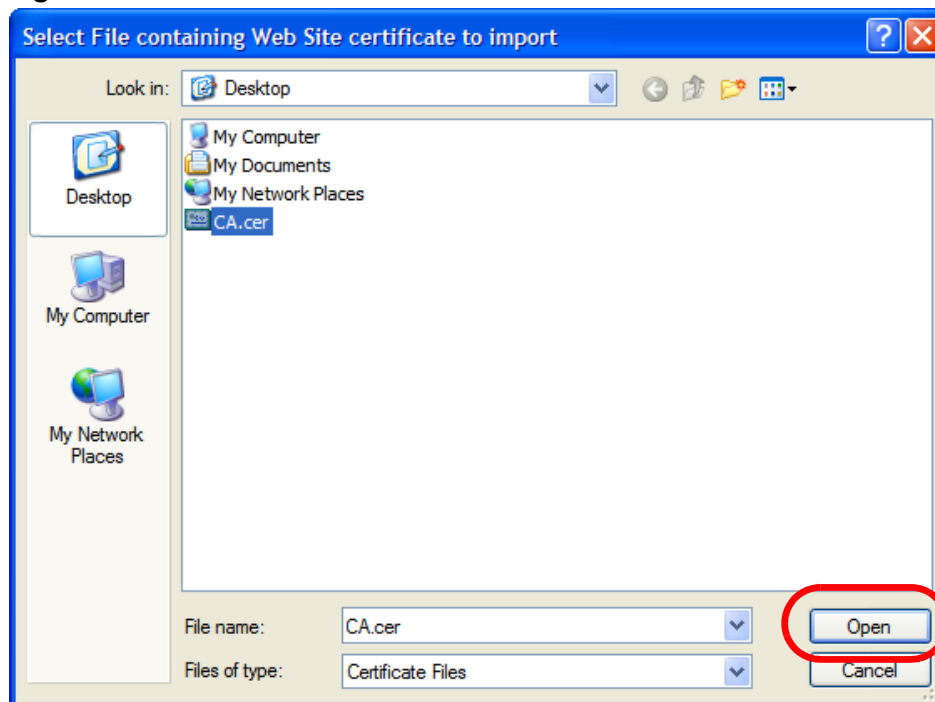
- 3 In the **Certificate Manager** dialog box, click **Web Sites > Import**.

Figure 255 Firefox 2: Certificate Manager



- 4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

Figure 256 Firefox 2: Select File



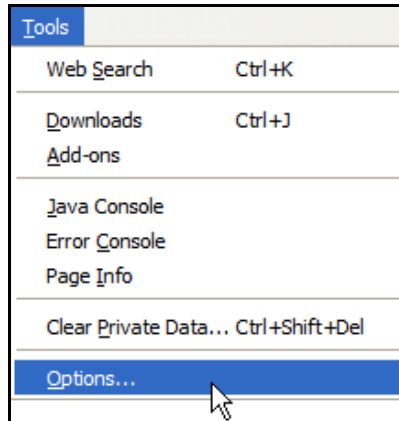
- 5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

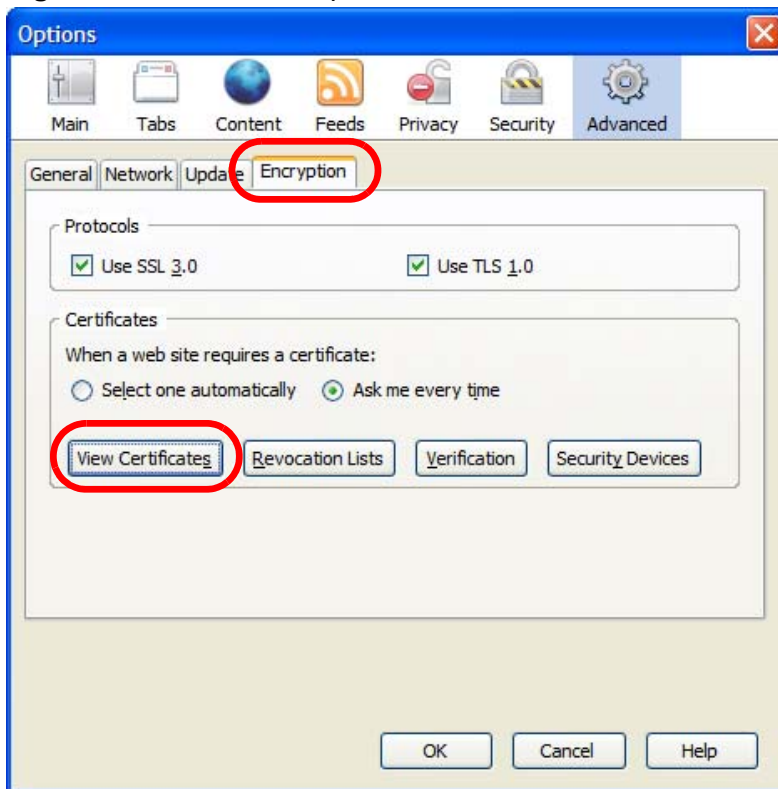
- 1 Open **Firefox** and click **Tools > Options**.

Figure 257 Firefox 2: Tools Menu



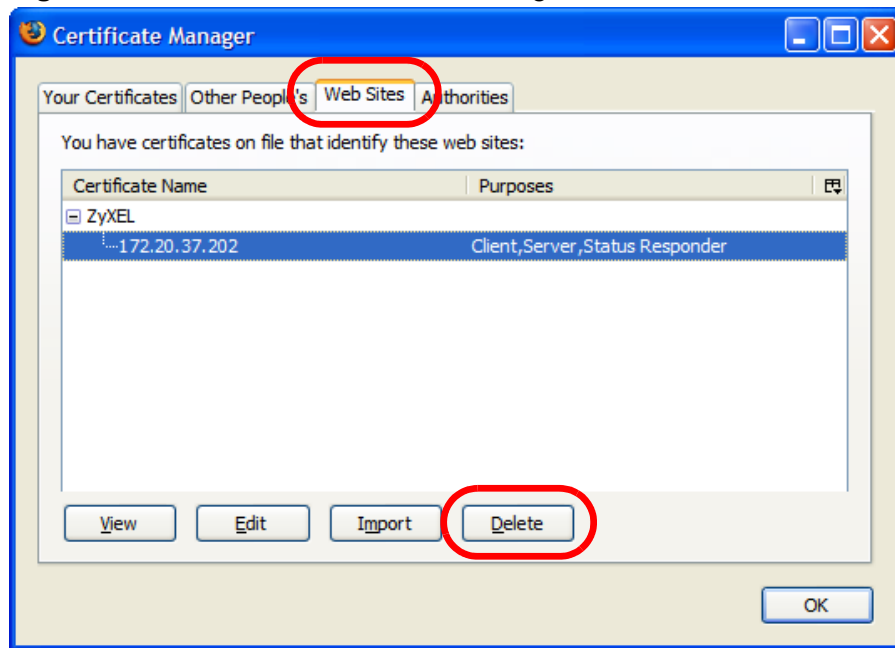
- 2 In the **Options** dialog box, click **Advanced > Encryption > View Certificates**.

Figure 258 Firefox 2: Options



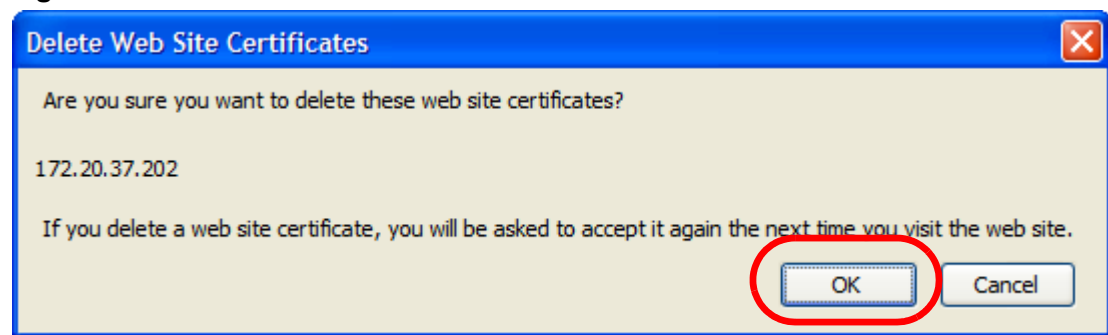
- 3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

Figure 259 Firefox 2: Certificate Manager



- 4 In the **Delete Web Site Certificates** dialog box, click **OK**.

Figure 260 Firefox 2: Delete Web Site Certificates



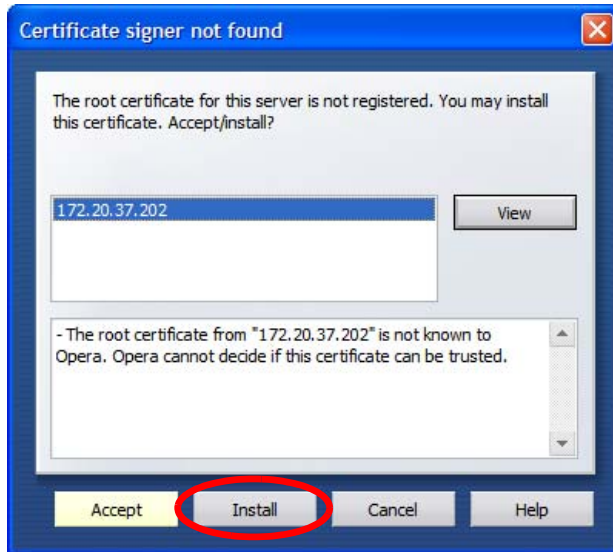
- 5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

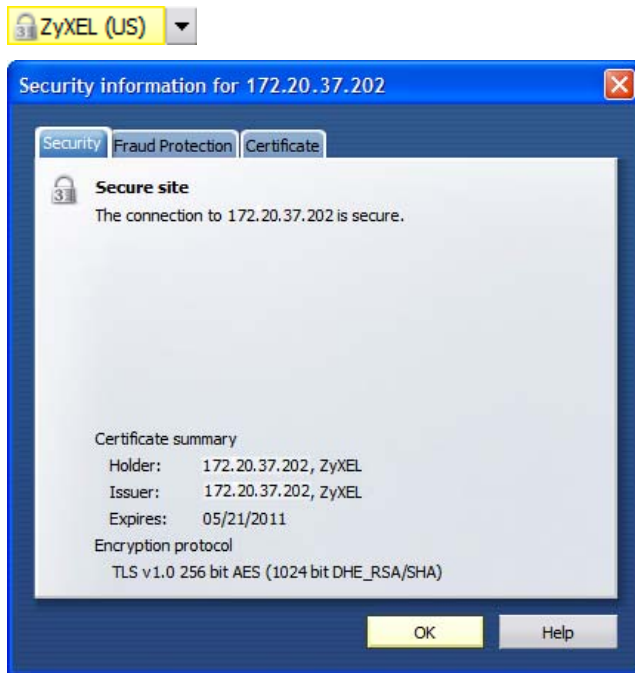
- 1 If your device's web configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Click **Install** to accept the certificate.

Figure 261 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 262 Opera 9: Security information

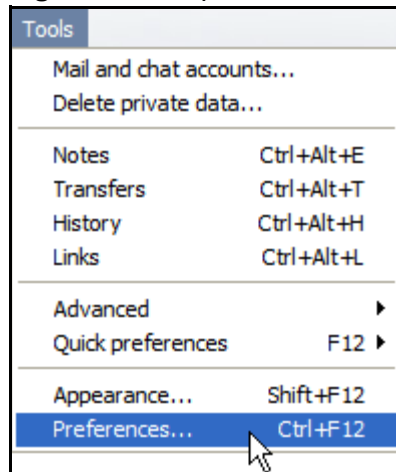


Installing a Stand-Alone Certificate File in Opera

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.

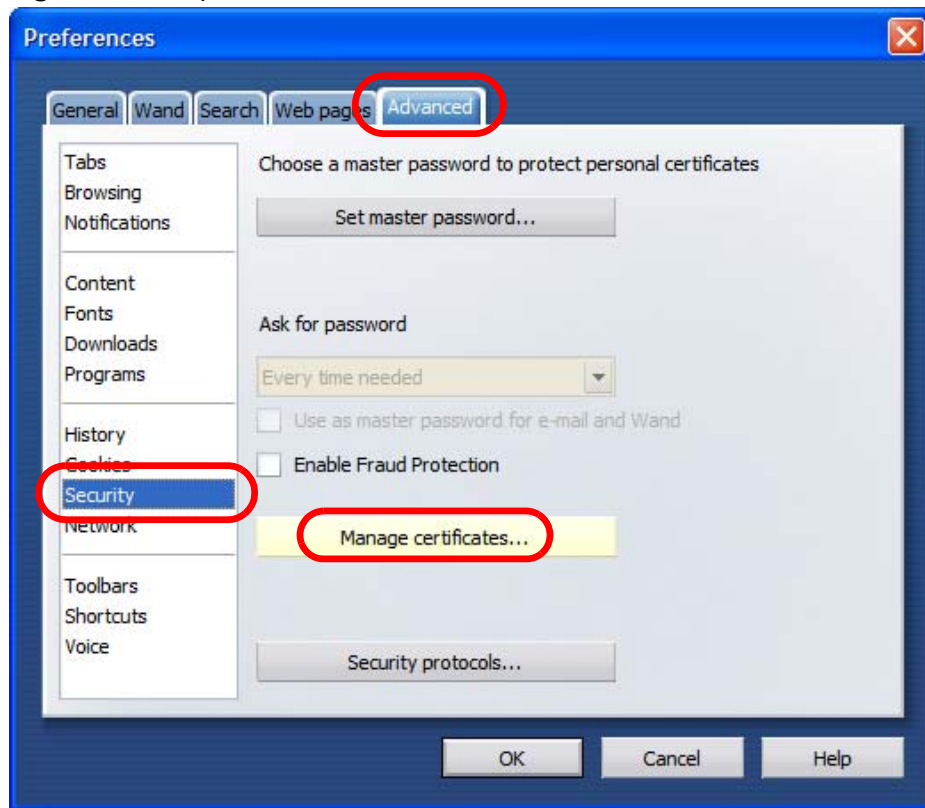
- 1 Open **Opera** and click **Tools > Preferences**.

Figure 263 Opera 9: Tools Menu



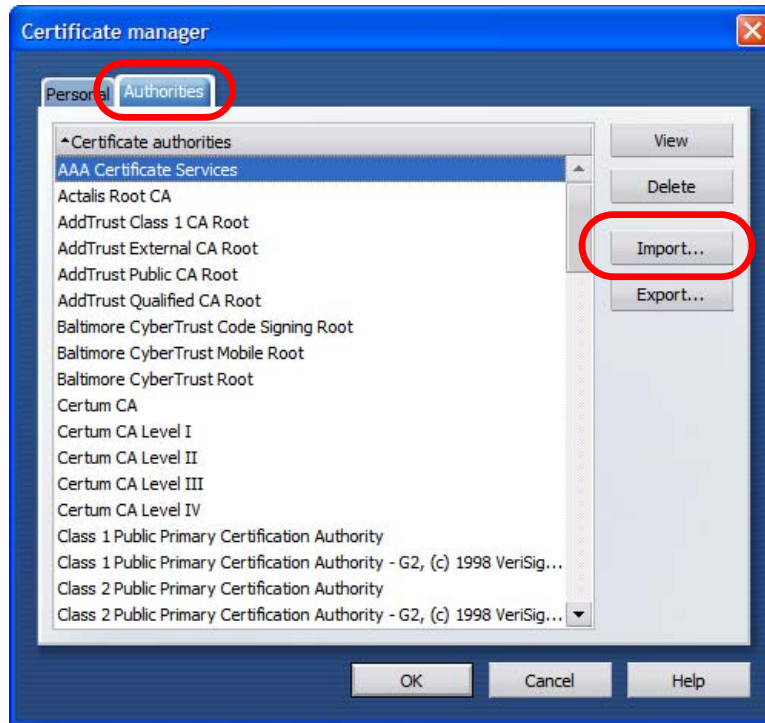
- 2 In **Preferences**, click **Advanced** > **Security** > **Manage certificates**.

Figure 264 Opera 9: Preferences



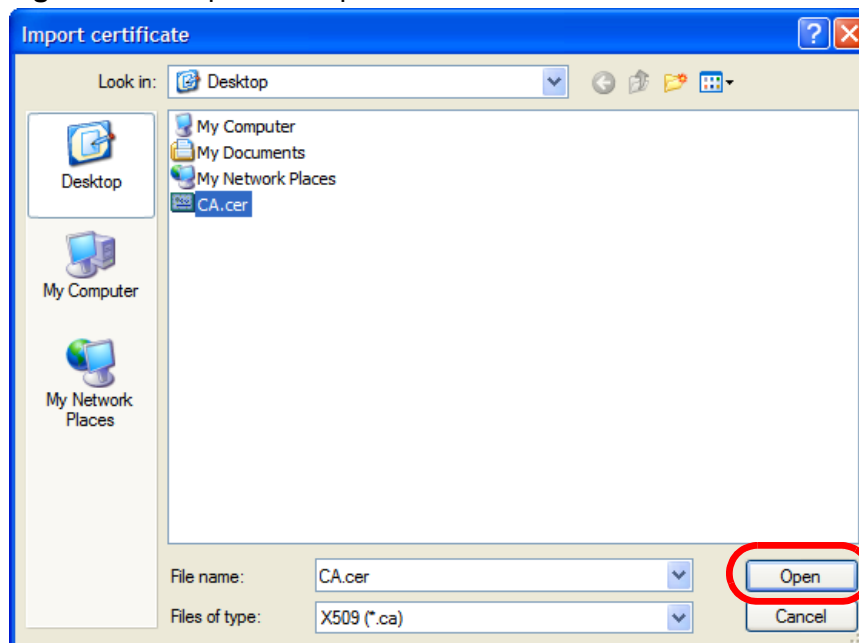
- 3 In the **Certificates Manager**, click **Authorities > Import**.

Figure 265 Opera 9: Certificate manager



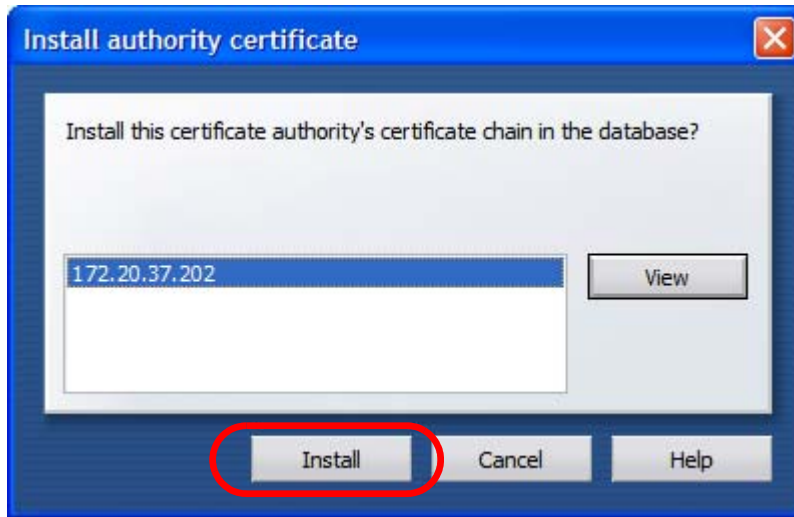
- 4 Use the **Import certificate** dialog box to locate the certificate and then click **Open**.

Figure 266 Opera 9: Import certificate



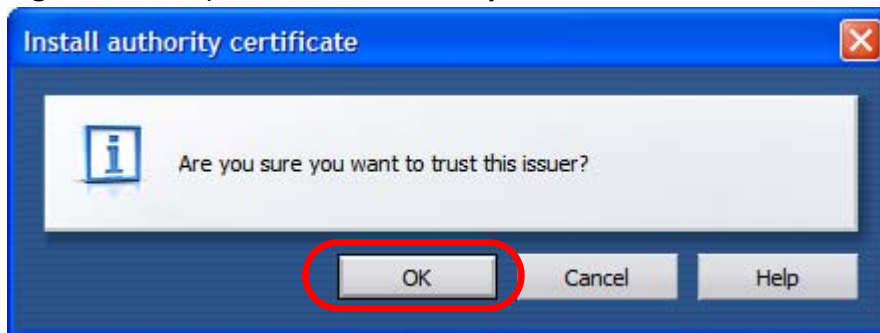
- 5 In the **Install authority certificate** dialog box, click **Install**.

Figure 267 Opera 9: Install authority certificate



- 6 Next, click **OK**.

Figure 268 Opera 9: Install authority certificate



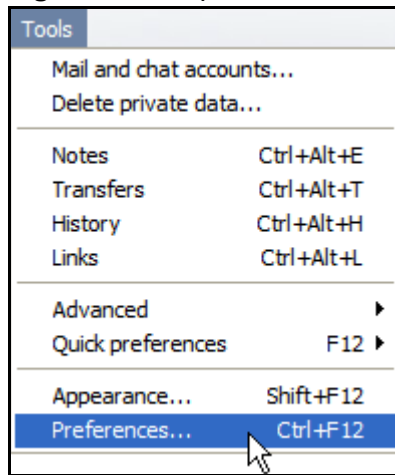
- 7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

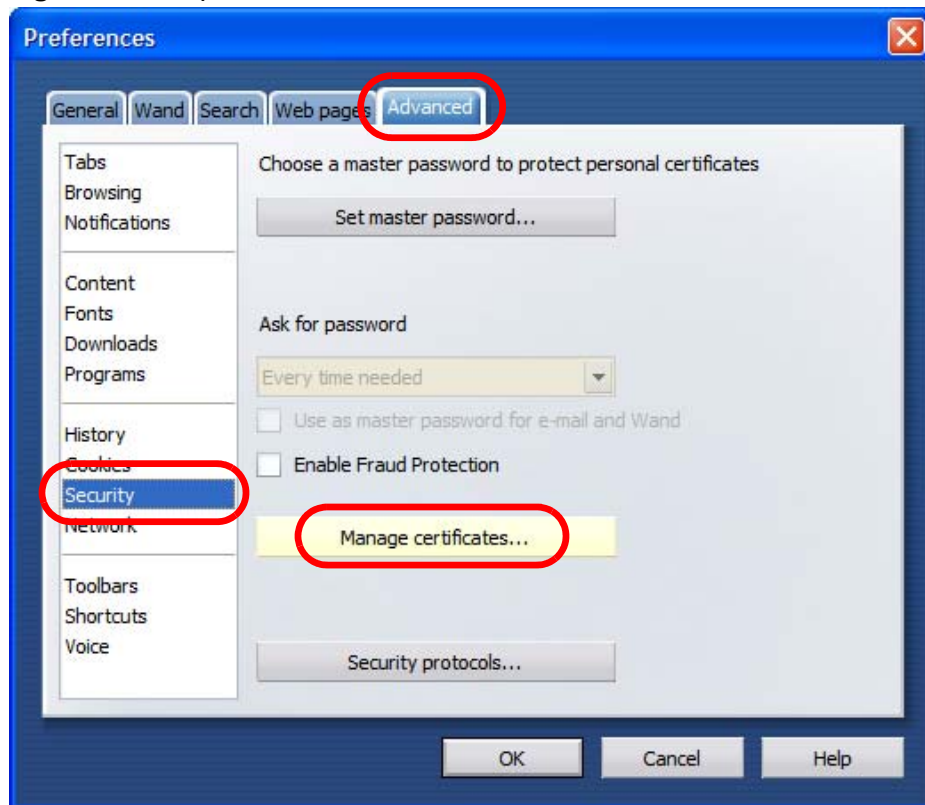
- 1 Open **Opera** and click **Tools > Preferences**.

Figure 269 Opera 9: Tools Menu



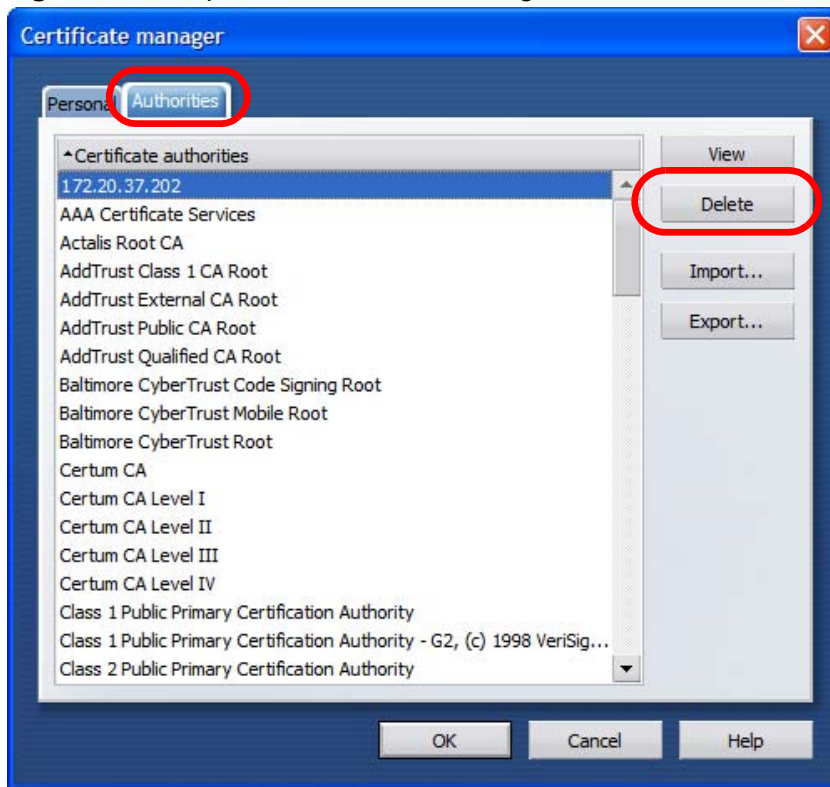
- 2 In **Preferences, Advanced > Security > Manage certificates**.

Figure 270 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 271 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 272 Konqueror 3.5: Server Authentication



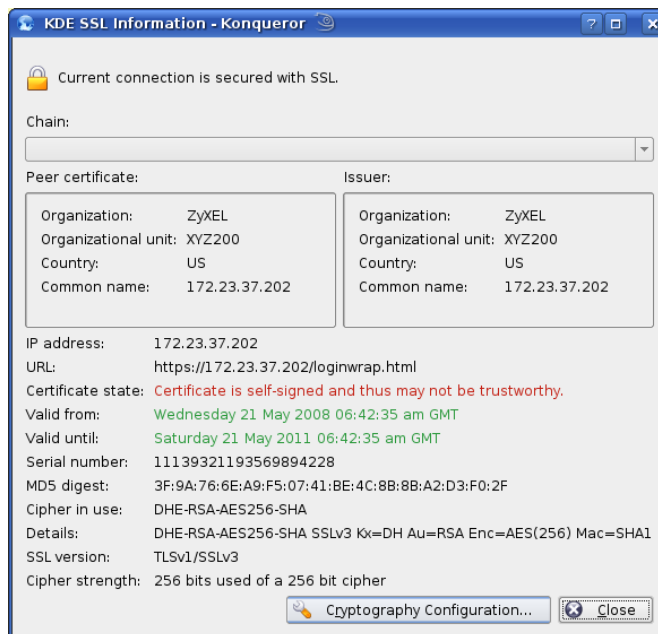
- 3 Click **Forever** when prompted to accept the certificate.

Figure 273 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 274 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 275 Konqueror 3.5: Public Key Certificate File



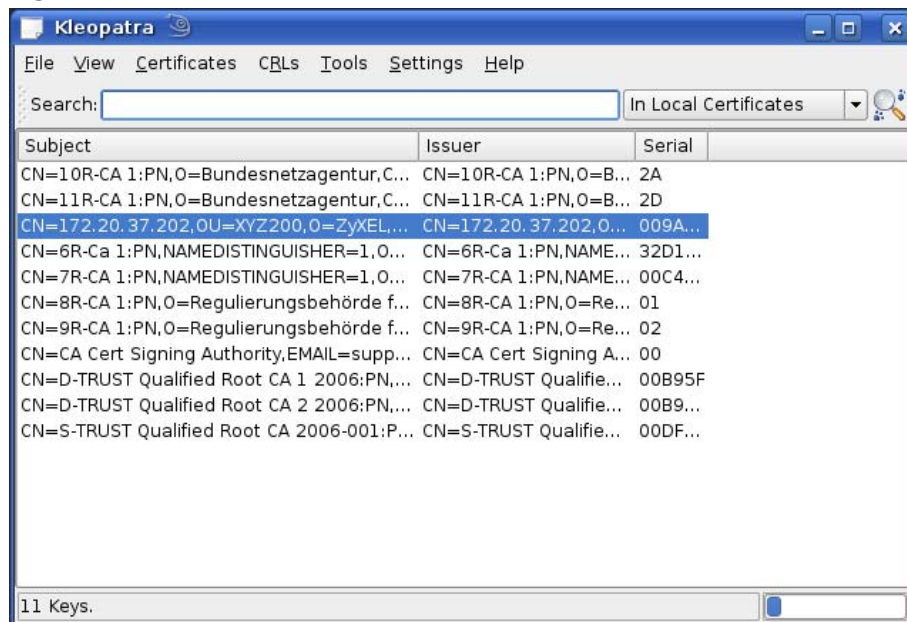
- 2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

Figure 276 Konqueror 3.5: Certificate Import Result



The public key certificate appears in the KDE certificate manager, **Kleopatra**.

Figure 277 Konqueror 3.5: Kleopatra



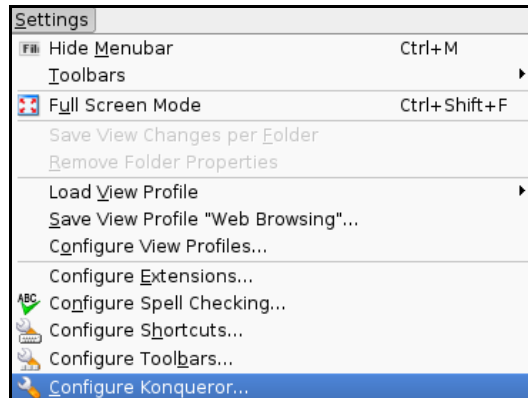
- 3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

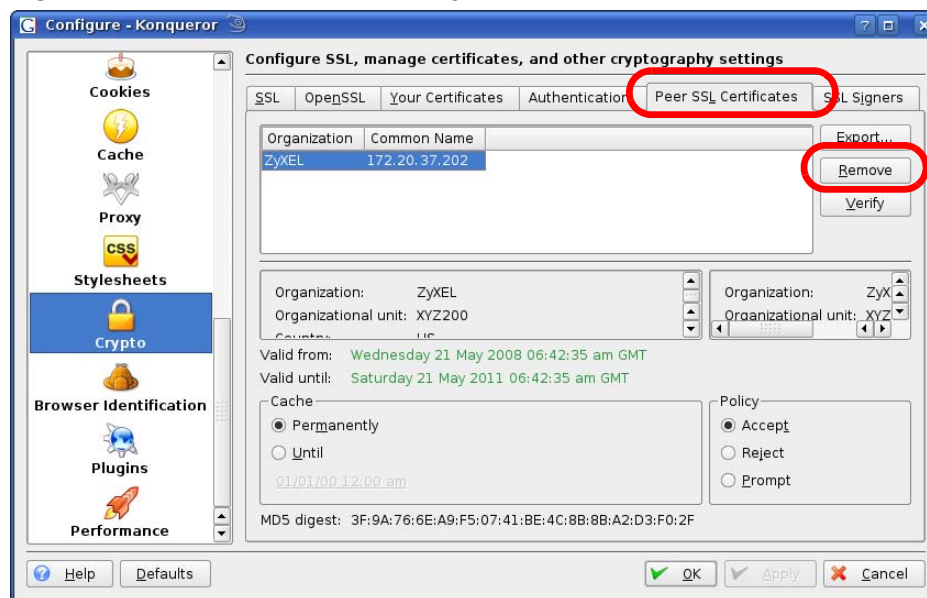
- 1 Open **Konqueror** and click **Settings > Configure Konqueror**.

Figure 278 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 279 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.

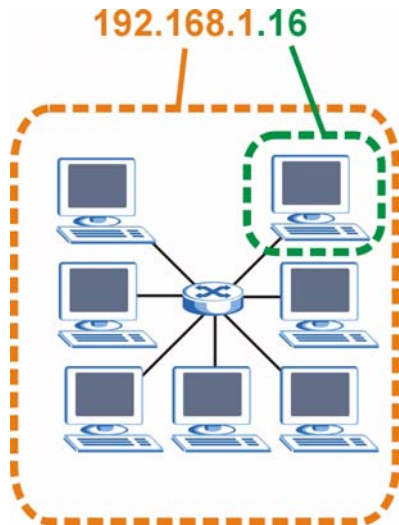
Structure

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 280 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 100 Subnet Masks

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

Table 100 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
Network Number	11000000	10101000	00000001	
Host ID				00000010

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

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

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

Table 101 Subnet Masks

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

Network Size

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

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

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

Table 102 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 103 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

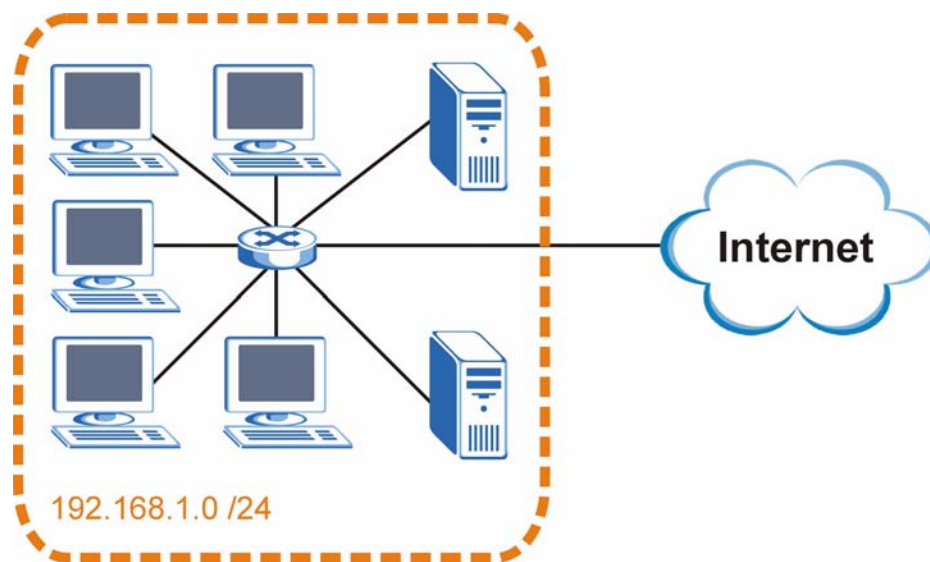
Subnetting

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 281 Subnetting Example: Before Subnetting

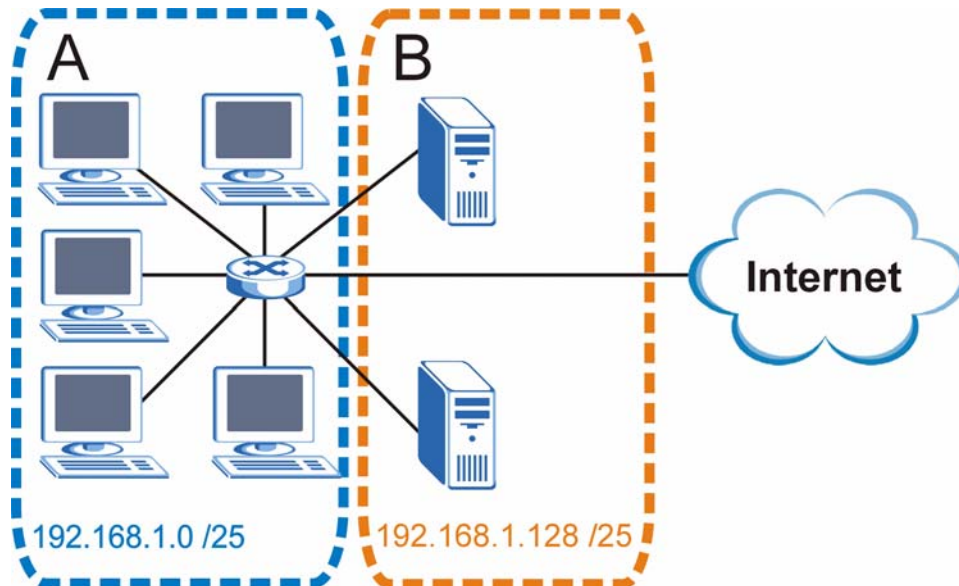


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 282 Subnetting Example: After Subnetting



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

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

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

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

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

Table 104 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 105 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 106 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 107 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 107 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 108 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 109 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 110 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*.

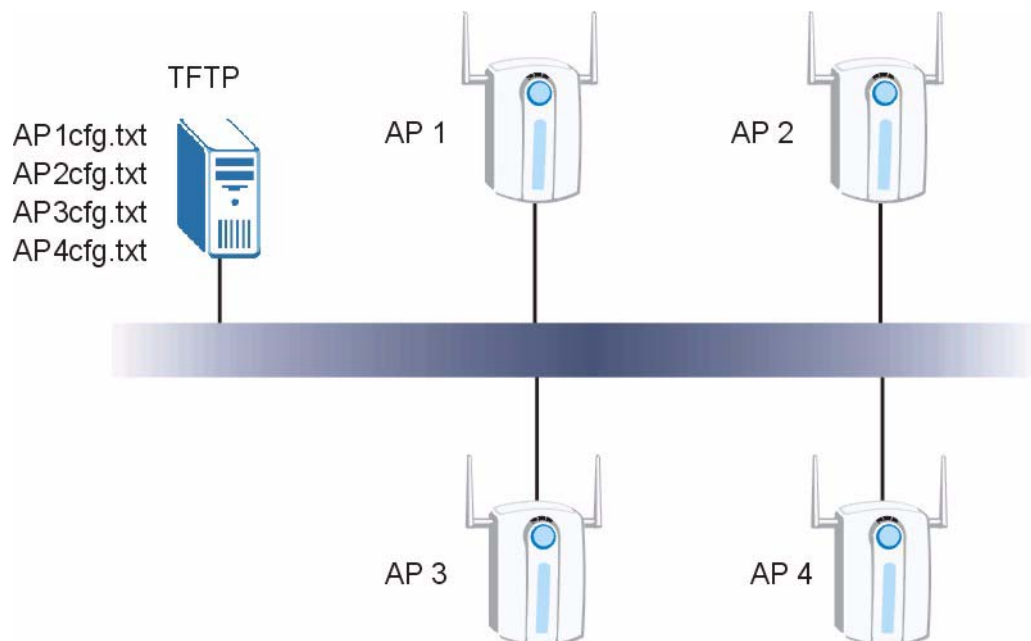
Text File Based Auto Configuration

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 283 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 111 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 112 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 113 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 114 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 115 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 284 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 116 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 285 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 286 802.1X 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 287 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 288 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 289 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.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

A

access [24](#)
 access point [24](#)
 access privileges [29](#)
 address [110](#)
 address assignment [110, 185](#)
 address filtering [23](#)
 administrator authentication on RADIUS [117](#)
 Advanced Encryption Standard
 See AES.
 AES [341](#)
 alternative subnet mask notation [384](#)
 antenna [297, 298](#)
 directional [346](#)
 gain [345](#)
 omni-directional [346](#)
 AP [23, 24, 25, 28, 333](#)
 AP (access point) [122](#)
 AP+Bridge [24](#)
 AP/Bridge [28](#)
 applications [24](#)
 Access Point [24](#)
 AP/Bridge [28](#)
 Bridge/Repeater [25](#)
 MBSSID [28](#)
 ATC [149, 150](#)
 ATC+WMM [149](#)
 ATM [150](#)
 authentication server [23](#)
 auto configuration [391](#)
 auto configuration status [394](#)

B

backup [282](#)
 Basic Service Set [120](#)
 see BSS

bridge [25, 28](#)
 Bridge Protocol Data Units (BPDUs) [140](#)
 Bridge/Repeater [24, 25](#)
 BSS [28, 29, 331](#)
 BSSID [23](#)

C

CA [233, 339](#)
 CAPWAP [87, 89, 93](#)
 Certificate Authority
 See CA.
 certificates [211](#)
 CA [233](#)
 thumbprint algorithms [234](#)
 thumbprints [234](#)
 verifying fingerprints [234](#)
 Certification Authority. See CA.
 certifications [399](#)
 notices [401](#)
 viewing [401](#)
 channel [24, 122, 333](#)
 interference [333](#)
 Class of Service (CoS) [152](#)
 command interface [32](#)
 configuration [23](#)
 configuration file
 examples [395](#)
 format [393](#)
 configuration file rules [394](#)
 Control and Provisioning of Wireless Access
 Points
 See CAPWAP
 copyright [399](#)
 CoS [152](#)
 CTS (Clear to Send) [334](#)

D

default [284](#)
DFS [141](#)
Differentiated Services [153](#)
DiffServ [152](#)
DiffServ Code Point (DSCP) [153](#)
DiffServ Code Points [153](#)
DiffServ marking rule [153](#)
dimensions [297](#)
disclaimer [399](#)
Distribution System [120](#)
DS field [153](#)
DSCPs [153](#)
DTLS [31](#), [87](#)
dual wireless modules [23](#)
Dynamic Frequency Selection [141](#)
dynamic WEP key exchange [340](#)

E

EAP authentication [338](#)
encryption [28](#), [341](#)
ESS [120](#), [332](#)
ESS IDentification [121](#)
ESSID [295](#)
Extended Service Set [120](#)
 see ESS
Extended Service Set IDentification [122](#), [126](#),
 [133](#), [138](#)

F

FCC interference statement [399](#)
file version [393](#)
filtering [23](#)
firmware file
 maintenance [276](#)
fragmentation threshold [335](#)
friendly AP list [189](#), [191](#)
FTP [32](#), [197](#)
 restrictions [197](#)

G

general setup [111](#)
guest SSID [30](#)

H

hidden node [333](#)
honeypot attack [189](#)
host [113](#)
host ID [110](#)
humidity [297](#), [298](#)

I

IANA [110](#), [390](#)
IBSS [331](#)
IEEE 802.11g [335](#)
IEEE 802.1x [23](#)
in-band management [250](#)
Independent Basic Service Set [280](#)
 see IBSS
initialization vector (IV) [341](#)
installation [23](#)
interference [24](#)
internal authentication server [23](#)
Internal RADIUS Server Setting Screen [210](#)
Internet Assigned Numbers Authority
 See IANA
Internet telephony [29](#)
IP address [110](#), [185](#), [298](#)
IPSec VPN capability [298](#)
isolation [23](#)

L

LAN [278](#)
layer-2 isolation [23](#), [30](#)
LEDs [34](#)
log descriptions [240](#)

logs [235](#)

M

MAC address [23](#), [174](#), [179](#)

MAC address filter action [181](#)

MAC filter [30](#)

MAC filtering [299](#)

maintenance [23](#)

management [23](#)

Management Information Base (MIB) [207](#)

Management Mode

 CAPWAP and DHCP [88](#)

 CAPWAP and IP Subnets [88](#)

 managed AP [88](#)

 standalone mode [87](#)

management VLAN [250](#)

managing the device

 good habits [32](#)

 using FTP. See FTP.

 using Telnet. See command interface.

 using the command interface. See command interface.

mask [110](#)

max age [140](#)

MBSSID [24](#), [28](#)

Message Integrity Check (MIC) [341](#)

mobile access [23](#)

mode [24](#)

N

NAT [389](#)

network [23](#)

network access [23](#)

network bridge [25](#)

network number [110](#)

network traffic [23](#)

O

operating mode [24](#)

out-of-band management [250](#)

P

Pairwise Master Key (PMK) [341](#), [343](#)

password [298](#)

path cost [140](#)

Per-Hop Behavior [153](#)

PHB (Per-Hop Behavior) [153](#)

PoE [302](#)

power specification [297](#)

power specifications [297](#), [302](#)

preamble mode [335](#)

pre-configured profiles [30](#)

priorities [150](#)

prioritization [23](#)

private IP address [110](#), [185](#)

private networks [110](#)

product registration [402](#)

PSK [341](#)

Q

QoS [23](#), [149](#)

Quick Start Guide [37](#)

R

radio [24](#)

RADIUS [337](#)

 message types [337](#)

 messages [337](#)

 shared secret key [338](#)

rapid STP [139](#)

reauthentication time [161](#), [163](#), [164](#), [165](#), [166](#)

registration

 product [402](#)

- related documentation [3](#)
- remote management limitations [196](#)
- repeater [25](#)
- reset button [297](#)
- restore [283](#)
- RF interference [24](#)
- roaming [141](#)
 - requirements [143](#)
- rogue AP [23](#), [189](#), [190](#), [191](#)
- root bridge [140](#)
- RTS (Request To Send) [334](#)
 - threshold [333](#), [334](#)

S

- safety warnings [7](#)
- security [25](#)
- security profiles [23](#)
- server [23](#)
- Service Set [122](#), [126](#), [133](#), [138](#)
- Service Set Identifier
 - see SSID
- SNMP [299](#)
 - MIBs [207](#)
 - traps [207](#)
- specifications [302](#)
- SSID [28](#)
- SSID profile [146](#)
 - pre-configured [29](#)
- SSID profiles [29](#), [30](#)
- STP [139](#)
- STP - how it works [140](#)
- STP (Spanning Tree Protocol) [298](#)
- STP path costs [140](#)
- STP port states [141](#)
- STP terminology [140](#)
- subnet [381](#)
- subnet mask [110](#), [298](#), [382](#)
- subnetting [385](#)
- syntax conventions [5](#)
- system name [111](#)
- system timeout [198](#)

T

- tagged VLAN example [250](#)
- telnet [198](#)
- temperature [297](#), [298](#)
- Temporal Key Integrity Protocol (TKIP) [341](#)
- text file based auto configuration [299](#), [391](#)
- TFTP restrictions [197](#)
- time-sensitive [23](#)
- ToS [152](#)
- trademarks [399](#)
- traffic security [23](#)
- Type of Service [152](#)

U

- use [23](#)

V

- Virtual Local Area Network [245](#)
- VLAN [245](#), [265](#), [271](#)
- VoIP [23](#), [29](#), [149](#)
- VoIP SSID [30](#)

W

- warranty [401](#)
 - note [402](#)
- wcfg command [395](#)
- WDS [25](#), [26](#), [28](#)
- web configurator [23](#), [37](#), [39](#)
- WEP [23](#)
- WEP encryption [159](#)
- Wi-Fi Multimedia QoS [149](#)
- Wi-Fi Protected Access [23](#), [340](#)
- wired network [23](#), [24](#), [25](#)
- wireless channel [295](#)
- wireless client WPA supplicants [342](#)
- Wireless Distribution System (WDS) [28](#)

- wireless Internet connection [24](#)
- wireless LAN [295](#)
- wireless modules (dual) [23](#)
- wireless security [29](#), [155](#), [295](#), [336](#)
- WLAN
 - interference [333](#)
 - security parameters [344](#)
- WLAN interface [24](#)
- WMM [149](#)
- WPA [23](#), [340](#)
 - key caching [342](#)
 - pre-authentication [342](#)
 - user authentication [342](#)
 - vs WPA-PSK [341](#)
 - wireless client supplicant [342](#)
 - with RADIUS application example [342](#)
- WPA2 [23](#), [340](#)
 - user authentication [342](#)
 - vs WPA2-PSK [341](#)
 - wireless client supplicant [342](#)
 - with RADIUS application example [342](#)
- WPA2-Pre-Shared Key [340](#)
- WPA2-PSK [340](#), [341](#)
 - application example [343](#)
- WPA-PSK [341](#)
 - application example [343](#)

