NWA-3100

802.11a/b/g Wireless Access Point

User's Guide

Version 3.60
10/2006
Edition 1

ZyXEL
www.zyxel.com

Manual abstract:

· ZyXEL Web Site Please refer to www.zyxel.com for additional support documentation and product certifications. User Guide Feedback Help us help you. Send all User 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 ZyXEL NWA-3100 User's Guide 3 Document Conventions 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 device. Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations. Syntax Conventions · The NWA-3100 may be referred to as the "ZyXEL Device", the "device", the "product" or the "system" 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". 4 ZyXEL NWA-3100 User's Guide Document Conventions Icons Used in Figures Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device. ZyXEL Device Computer Notebook computer Server DSLAM Firewall Telephone Switch Router ZyXEL NWA-3100 User's Guide 5 Safety Warnings Safety Warnings For your safety, be sure to read and follow all warning notices and instructions. · Do NOT use this device near water, for example, in a wet basement or near a swimming pool.

· Do NOT expose your device to dampness, dust or corrosive liquids. · Do NOT store things on the device. · Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning. · Connect ONLY suitable accessories to the device. · ONLY qualified service personnel should service or disassemble this device. · Make sure to connect the cables to the correct ports. · Place connecting cables carefully so that no one will step on them or stumble over them. · Always disconnect all cables from this device before servicing or disassembling. · Use ONLY an appropriate power adaptor or cord for your device.

· Connect the power adaptor or cord 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 device 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 power outlet. · Do NOT attempt to repair the power adaptor or cord.

Contact your local vendor to order a new one. · Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning. · Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

· If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged. · The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors. · Fuse Warning! Replace a fuse only with a fuse of the same type and rating. This product is recyclable. Dispose of it properly. 6 ZyXEL NWA-3100 User's Guide Safety Warnings ZyXEL NWA-3100 User's Guide 7 Safety Warnings 8 ZyXEL NWA-3100 User's Guide Contents Overview Contents Overview Introduction .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 29 Introducing the ZyXEL Device .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 31 Introducing the Web Configurator ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 39 Tutorial ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 43 The Web Configurator ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 61 System Screens .
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 63 Wireless Configuration .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 67 Wireless Security Configuration .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
81 MBSSID and SSID .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

..... 97 Other Wireless Configuration ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 105 IP Screen .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
....113 Rogue AP .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

...117 Remote Management .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 123 Certificates .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

133 Log Screens .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 151 VLAN .....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.... 157 Maintenance .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 175 SMT and Troubleshooting .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 185 Introducing the SMT .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 187 General Setup .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 191 LAN Setup .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 193 SNMP Configuration .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 195 System Password .....

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
197 System Information and Diagnosis .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
199 Firmware and Configuration File Maintenance .....

.....
.....
.....
.....

.....
.....
.....
.....

.. 205 System Maintenance and Information .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 217 Troubleshooting ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....
.....
.....
..... 223 Appendices and Index ....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
. 227 ZyXEL NWA-3100 User's Guide 9 Contents Overview 10 ZyXEL NWA-3100 User's Guide Table of Contents Table of Contents About This User's Guide
....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
..... 3 Document Conventions...
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
4 Safety Warnings.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
6 Contents Overview .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
9 Table of Contents.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 11 List of Figures ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.....
.....
.....

..... 19 List of Tables...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
25 Part I: Introduction.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 29 Chapter 1 Introducing the ZyXEL Device .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 31 1.1 Introducing the ZyXEL Device ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....

..... 31 1.
2 Applications for the ZyXEL Device .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 31 1.2.1 Access Point ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 31 1.2.

2 AP + Bridge .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 32 1.2.3 Bridge / Repeater .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 33 1.2.4 MBSSID .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 35 1.2.5 Pre-Configured SSID Profiles ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 36 1.3 Ways to Manage the ZyXEL Device .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 36 1.4 Good Habits for Managing the ZyXEL Device ..

.....
.....
.....
.....

.....
.....
.....
.....

..... 36 1.5 LEDs ..
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
37 Chapter 2 Introducing the Web Configurator .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 39 2.1 Accessing the Web Configurator .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 39 2.2 Resetting the ZyXEL Device .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 40 2.2.1 Methods of Restoring Factory-Defaults ...

.....
.....
.....
.....

.....
.....
.....
.....

..... 41 2.3 Navigating the Web Configurator ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 41 Chapter 3 Tutorial ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
43 3.1 How to Configure Multiple Wireless Networks .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 70 5.3.3.1 ATC+WMM from LAN to WLAN .....

.....

.....
.....
.....

.....
.....
.....
.....

..... 70 5.3.3.2 ATC+WMM from WLAN to LAN .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 71 5.3.4 Type Of Service (ToS) .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 71 5.

3.4.1 DiffServ .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 71 5.3.4.2 DSCP and Per-Hop Behavior .....

.....
.....
.....
.....

.....
.....
.....

.....

..... 71 12 ZyXEL NWA-3100 User's Guide Table of Contents 5.
3.5 ToS (Type of Service) and WMM QoS ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 72 5.4 Spanning Tree Protocol (STP) .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 72 5.4.1 Rapid STP ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 72 5.4.2 STP Terminology .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 73 5.4.
3 How STP Works .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 73 5.4.4 STP Port States ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
... 73 5.5 Wireless Screen Overview .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 74 5.6 Configuring Wireless Settings .

.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 74 5.6.1 Access Point Mode ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 74 5.6.
2 Bridge/Repeater Mode .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
76 5.6.3 AP+Bridge Mode ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 80 5.6.4 MBSSID Mode .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
80 Chapter 6 Wireless Security Configuration .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 81 6.1 Wireless Security Overview .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 81 6.

1.1 Encryption .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
..... 81 6.1.2 Restricted Access ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 81 6.
1.3 Hide Identity ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 81 6.1.4 WEP Encryption .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 81 6.
2 802.1x Overview .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
82 6.3 EAP Authentication Overview ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
82 6.4 Introduction to WPA .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
82 6.4.1 User Authentication ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 83 6.4.2 Encryption .....

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
. 83 6.4.3 WPA(2)-PSK Application Example ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 84 6.5 WPA(2) with RADIUS Application Example ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 84 6.
6 Security Modes .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 85 6.7 Wireless Client WPA Supplicants ...
.....

.....
.....
.....
.....

.....
.....
.....

.....

.....
.....
86 6.8 Wireless Security Effectiveness ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 86 6.9 Configuring Security ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 86 6.9.1 Security: WEP ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 87 6.9.2 Security: 802.1x Only .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 88 6.9.3 Security: 802.1x Static 64-bit, 802.
1x Static 128-bit .....
.....
.....

.....
.....
.....
.....

. 89 6.9.4 Security: WPA .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 91 6.9.5 Security: WPA2 or WPA2-MIX .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 92 6.9.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX .
.....

.....
.....
.....
.....

.....
. 93 6.10 Introduction to RADIUS ...
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
... 95 6.11 Configuring RADIUS .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
95 Chapter 7 MBSSID and SSID .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 97 7.1 Wireless LAN Infrastructures ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 97 ZyXEL NWA-3100 User's Guide 13 Table of Contents 7.1.1 MBSSID ..
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
97 7.1.2 Notes on Multiple BSS ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 97 7.1.3 Multiple BSS Example .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 97 7.1.4 Multiple BSS with VLAN Example ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
97 7.1.5 Configuring Multiple BSSs ...
.....

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
. 98 7.2 SSID ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 100 7.2.1 The SSID Screen .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
100 7.2.2 Configuring SSID ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 101 Chapter 8 Other Wireless Configuration .....

.....
.....
.....

.....

.....
.....
.....
.....

.....
.....
.....
..... 105 8.1 Layer-2 Isolation Introduction ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

105 8.2 Configuring Layer-2 Isolation .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 106 8.2.1 Layer-2 Isolation Examples ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 107 8.2.1.1 Layer-2 Isolation Example 1 .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
108 8.2.1.2 Layer-2 Isolation Example 2 .....

.....
.....
.....
.....

.....
.....
.....
.....

..... 108 8.3 Configuring MAC Filter .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 109 8.4 Configuring Roaming .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....111 8.4.
1 Requirements for Roaming .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....112 Chapter 9 IP Screen...
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
113 9.1 Factory Ethernet Defaults ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....113 9.2 TCP/IP Parameters ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
....113 9.
2.1 WAN IP Address Assignment ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
113 9.3 Configuring IP ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....114 Chapter 10 Rogue AP..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
117 10.1 Rogue AP Introduction ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....117 10.2 Rogue AP Examples ..

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

.....
..117 10.2.1 "Honeypot" Attack .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
...118 10.3 Configuring Rogue AP Detection .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
119 10.3.1 Rogue AP: Configuration .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
119 10.3.2 Rogue AP: Friendly AP .....

.....
.....
.....
.....

.....
.....
.....

....

....
.....
.....
.. 120 10.3.3 Rogue AP List ......

....
.....
.....
....

....
.....
.....
....

....
.....
.....
....

.... 121 Chapter 11 Remote Management..
.....
.....
....

....
.....
.....
....

....
.....
.....
....

....
.....
.....
...... 123 11.1 Remote Management Overview ...

....
.....
.....
....

....
.....
.....
....

....
.....
.....
... 123 11.1.1 Remote Management Limitations .....

....
.....
.....
....

....
.....
.....
....

.....
124 11.1.2 System Timeout ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 124 11.2 SSH .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 124 14 ZyXEL NWA-3100 User's Guide Table of Contents 11.3 Telnet ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 124 11.4 Configuring FTP ...
.....
.....

.....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

... 125 11.5 Configuring WWW .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 126 11.6 SNMP .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 128 11.

6.1 Supported MIBs .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
... 129 11.6.
2 SNMP Traps .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 129 11.7 SNMP Traps .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 130 11.

7.1 Configuring SNMP .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 130 Chapter 12 Certificates .
.....
.....
.....

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

.....
... 133 12.1 Certificates Overview .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 133 12.1.1 Advantages of Certificates .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 134 12.2 Self-signed Certificates .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 134 12.3 Verifying a Certificate ....
.....
.....
.....

.....
.....
.....

.....

.....
.....
.....
.....

.....
.....
.... 134 12.
3.1 Checking the Fingerprint of a Certificate on Your Computer .....

.....
.....
.....
..... 134 12.4 Configuration Summary ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 135 12.5 My Certificates ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 135 12.

6 Certificate File Formats .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
137 12.7 Importing a Certificate ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 138 12.8 Creating a Certificate .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 139 12.9 My Certificate Details ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
141 12.10 Trusted CAs .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
. 144 12.11 Importing a Trusted CA's Certificate ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 145 12.12 Trusted CA Certificate Details ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

... 146 Chapter 13 Log Screens .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 151 13.1 Configuring View Log ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 151 13.
2 Configuring Log Settings .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 152 13.3 Example Log Messages ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 154 13.4 Log Commands ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 155 13.4.

1 Configuring What You Want the ZyXEL Device to Log .....
.....
.....
.....

.....
.. 155 13.4.2 Displaying Logs .
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 156 13.5 Log Command Example ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 156 Chapter 14 VLAN .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 157 14.
1 VLAN .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....
.....
.....
..... 157 14.1.1 Management VLAN ID .
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
157 14.1.2 VLAN Tagging .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
. 157 14.2 Configuring VLAN ...
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
..... 158 14.2.1 Wireless VLAN ...
.....
.....
.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
158 ZyXEL NWA-3100 User's Guide 15 Table of Contents 14.2.2 RADIUS VLAN .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 160 14.2.3 Configuring Management VLAN Example ...
.....
.....
.....

.....
.....
.....
.....

..... 161 14.2.
4 Configuring Microsoft's IAS Server Example .....
.....
.....

.....
.....
.....
.....

..... 164 14.2.4.
1 Configuring VLAN Groups .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 164 14.2.4.2 Configuring Remote Access Policies .

.....
.....
.....
.....

.....
.....

.....
..... 165 14.

2.5 Second Rx VLAN ID Example .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 172 14.2.5.1 Second Rx VLAN Setup Example .....

.....
.....
.....
.....

.....
.....
.....
..... 172 Chapter 15 Maintenance ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

175 15.1 Maintenance Overview .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 175 15.2 System Status Screen ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 175 15.2.1 System Statistics .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 176 15.3 Association List ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 177 15.4 Channel Usage .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.....
.....
. 178 15.5 F/W Upload Screen .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 178 15.6 Configuration Screen ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 180 15.6.1 Backup Configuration .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 181 15.6.2 Restore Configuration ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

..... 181 15.

6.3 Back to Factory Defaults .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 182 15.

7 Restart Screen .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 183 Part III: SMT and Troubleshooting.....

.....
.....
.....
.....

.....
.....
.. 185 Chapter 16 Introducing the SMT ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 187 16.1 Connect to your ZyXEL Device Using Telnet ...
.....
.....
.....

.....
.....
.....
.....

.....
.... 187 16.
2 Changing the System Password .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
187 16.3 SMT Menu Overview Example ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 188 16.
4 Navigating the SMT Interface .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
188 16.4.1 System Management Terminal Interface Summary ...
.....
.....

.....
.....
.....
..... 190 Chapter 17 General Setup.

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 191 17.

1 General Setup .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 191 17.1.1 Procedure To Configure Menu 1 .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 191 Chapter 18 LAN Setup....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 193 18.1 LAN Setup ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 193 18.2 TCP/IP Ethernet Setup ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 193 16 ZyXEL NWA-3100 User's Guide Table of Contents Chapter 19 SNMP Configuration ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 195 19.1 SNMP Configuration ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.....
.....
.....

.. 195 Chapter 20 System Password .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 197 20.1 System Password ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 197 Chapter 21 System Information and Diagnosis.
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 199 21.
1 System Status .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.....
.....
.....
.....

.... 199 21.2 System Information .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 200 21.2.1 System Information .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 201 21.

2.2 Console Port Speed .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 202 21.3 Log and Trace ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 202 21.3.1 Viewing Error Log .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 202 21.4 Diagnostic ..
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
... 203 Chapter 22 Firmware and Configuration File Maintenance ..
.....
.....

.....
.....
.....
.....

.....
.....
.... 205 22.
1 Filename Conventions .....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
.....

. 205 22.2 Backup Configuration .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 206 22.
2.1 Backup Configuration Using FTP ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 206 22.2.2 Using the FTP command from the DOS Prompt .....
.....
.....
.....

.....
.....
.....
..... 207 22.2.3 Backup Configuration Using TFTP ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
207 22.2.4 Example: TFTP Command ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 208 22.2.5 Backup Via Console Port .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 209 22.3 Restore Configuration ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 210 22.3.
1 Restore Using FTP .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 210 22.4 Uploading Firmware and Configuration Files ..

.....
.....
.....
.....

.....
.....
.....
.....

.... 210 22.4.1 Firmware Upload ....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
..211 22.4.2 Configuration File Upload .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
..211 22.4.3 Using the FTP command from the DOS Prompt Example .
.....

.....
.....
.....
..... 212 22.4.4 TFTP File Upload ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 213 22.4.5 Example: TFTP Command .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....

.... 213 22.4.6 Uploading Via Console Port ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 213 22.

4.7 Uploading Firmware File Via Console Port .....
.....
.....
.....

.....
.....
.....
.....

. 214 22.4.8 Example Xmodem Firmware Upload Using HyperTerminal .....
.....
.....
.....

..... 214 22.4.
9 Uploading Configuration File Via Console Port .....
.....
.....

.....
.....
.....
.....

.... 215 22.4.10 Example Xmodem Configuration Upload Using HyperTerminal ....
.....
.....
.....

... 215 Chapter 23 System Maintenance and Information .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 217 ZyXEL NWA-3100 User's Guide 17 Table of Contents 23.1 Command Interpreter Mode .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 217 23.1.1 Command Syntax ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 218 23.1.2 Command Usage .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 218 23.1.
3 Brute-Force Password Guessing Protection .....

.....
.....
.....
.....

.....
.....
... 218 23.1.
3.1 Configuring Brute-Force Password Guessing Protection: Example .....

.... 218 23.2 Time and Date Setting .....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
. 219 23.2.1 Resetting the Time ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 220 23.3 Remote Management Setup ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 220 23.3.

1 Telnet .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 220 23.3.

2 FTP .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

220 23.3.3 Web .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 220 23.3.4 Remote Management Setup .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 220 23.3.5 Remote Management Limitations ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 222 23.4 System Timeout ..
.....
.....

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

.... 222 Chapter 24 Troubleshooting.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

223 24.1 Power, Hardware Connections, and LEDs .....
.....
.....
.....

.....
.....
.....
.....

.....
. 223 24.2 ZyXEL Device Access and Login ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 223 24.3 Internet Access ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....
.....
.....
..... 225 Part IV: Appendices and Index .
.....
.....
.....
.....
.....
.....
.....
..... 227 Appendix A Product Specifications..
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
..... 229 Appendix B Setting up Your Computer's IP Address.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
..... 233 Appendix C IP Address Assignment Conflicts.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
..... 245 Appendix D Wireless LANs .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....
... 249 Appendix E Indoor Installation Recommendations..
.....
.....

.....
.....
.....
.....

.....
.....
. 259 Appendix F Pop-up Windows, JavaScripts and Java Permissions ....
.....

.....
.....
.....
.... 261 Appendix G IP Addresses and Subnetting .....

.....
.....
.....
.....

.....
.....
.....
.....

..... 267 Appendix H Text File Based Auto Configuration .
.....
.....
.....

.....
.....
.....
.....

.....
.....
275 Appendix I Legal Information.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 283 Appendix J Customer Support .....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
.... 287 Index.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 291 18 ZyXEL NWA-3100 User's Guide List of Figures List of Figures Figure 1 Access Point Application .

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 32 Figure 2 AP+Bridge Application .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 33 Figure 3 Bridge Application .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
34 Figure 4 Repeater Application .....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....

.....
.....
.....
.....

.. 34 Figure 5 Multiple BSSs .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 35 Figure 6 LEDs .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 37 Figure 7 Change Password Screen .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 40 Figure 8 Replace Certificate Screen ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 40 Figure 9 The MAIN MENU Screen of the Web Configurator .
.....

.....
.....
.....
.....

.....
.....
.....
..... 41 Figure 10 Tutorial: Example MBSSID Setup .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 44 Figure 11 Tutorial: Wireless LAN: Before .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

45 Figure 12 Tutorial: Wireless LAN: Change Mode .....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
... 45 Figure 13 Tutorial: WIRELESS > SSID .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 46 Figure 14 Tutorial: VoIP SSID Profile Edit .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 47 Figure 15 Tutorial: VoIP Security .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 48 Figure 16 Tutorial: VoIP Security Profile Edit .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 48 Figure 17 Tutorial: VoIP Security: Updated .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 49 Figure 18 Tutorial: Activate VoIP Profile .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 49 Figure 19 Tutorial: Guest Edit .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 50 Figure 20 Tutorial: Guest Security Profile Edit .....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.....
.....
... 50 Figure 21 Tutorial: Guest Security: Updated .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 51 Figure 22 Tutorial: Layer 2 Isolation .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 51 Figure 23 Tutorial: Activate Guest Profile ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 52 Figure 24 Tutorial: Wireless Network Example ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 53 Figure 25 Tutorial: Friendly AP (Before Data Entry) ..
.....
.....

.....
.....
.....
.....
.....
.....
.....
.....
..... 54 Figure 26 Tutorial: Friendly AP (After Data Entry) ...
.....
.....
.....
.....
.....
.....
.....
.....
.....
... 55 Figure 27 Tutorial: Configuration ..
.....
.....
.....
.....
.....
.....
.....
.....
.....
..... 55 Figure 28 Tutorial: Warning ....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.. 56 Figure 29 Tutorial: Save Friendly AP list .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 56 Figure 30 Tutorial: Periodic Rogue AP Detection ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

56 Figure 31 Tutorial: Log Settings .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
57 Figure 32 System General Setup .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 63 Figure 33 Password. ..
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
64 Figure 34 Time Setting .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 65 Figure 35 Basic Service set ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 67 Figure 36 Extended Service Set .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

... 68 Figure 37 DiffServ: Differentiated Service Field .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 72 Figure 38 Wireless: Access Point .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 75 ZyXEL NWA-3100 User's Guide 19 List of Figures Figure 39 Bridging Example ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 77 Figure 40 Bridge Loop: Two Bridges Connected to Hub ....
.....
.....

.....
.....
.....
.....

.....

.....
.....
... 77 Figure 41 Bridge Loop: Bridge Connected to Wired LAN .....

.....
.....
.....
.....

.....
.....
.....
.....

.... 78 Figure 42 Wireless: Bridge/Repeater .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
78 Figure 43 Wireless: AP+Bridge .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 80 Figure 44 EAP Authentication .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

..... 82 Figure 45 WPA(2)-PSK Authentication ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 84 Figure 46 WPA(2) with RADIUS Application Example ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 85 Figure 47 Security .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 87 Figure 48 Security: WEP .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 88 Figure 49 Security: 802.1x Only .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
89 Figure 50 Security: 802.1x Static 64-bit, 802.1x Static 128-bit .....

.....
.....
.....
.....

.....
.....
.....
.... 90 Figure 51 Security: WPA .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 91 Figure 52 Security:WPA2 or WPA2-MIX .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....

92 Figure 53 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX .....
.....
.....
.....

.....
.....
.....
.....

. 94 Figure 54 RADIUS .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 95 Figure 55 Multiple BSS with VLAN Example ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 98 Figure 56 Wireless: Multiple BSS ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 98 Figure 57 SSID ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 101 Figure 58 Configuring SSID ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
..... 102 Figure 59 Layer-2 Isolation Application .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 106 Figure 60 Layer-2 Isolation Configuration Screen ....
.....
.....

.....
.....
.....
.....

.....

.....
.....
.....

. 107 Figure 61 Layer-2 Isolation Example .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 108 Figure 62 Layer-2 Isolation Example 1 ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 108 Figure 63 Layer-2 Isolation Example 2 ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 109 Figure 64 MAC Address Filter .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

....
....
.....
.110 Figure 65 Roaming Example ....
....
....
.....
.....
....
....
.....
.....
....
....
.....
.....
....
.........111 Figure 66 Roaming .
.....
.....
....
....
.....
.....
....
....
.....
.....
....
....
.....
.....
....
....
.....
..112 Figure 67 IP Setup ...
....
....
.....
.....
....
....
.....
.....
....
....
.....
.....
....
....
.....
.....
......114 Figure 68 Rogue AP: Example ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
118 Figure 69 "Honeypot" Attack .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....119 Figure 70 ROGUE AP > Configuration .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 120 Figure 71 ROGUE AP > Friendly AP ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
..... 121 Figure 72 ROGUE AP > Rogue AP ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 122 Figure 73 Secure and Insecure Remote Management ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
123 Figure 74 SSH Communication Example .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 124 Figure 75 Remote Management: Telnet .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 125 Figure 76 Remote Management: FTP ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 126 Figure 77 Remote Management: WWW ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 127 Figure 78 SNMP Management Model ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 128 Figure 79 Remote Management: SNMP .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 131 Figure 80 Certificates on Your Computer .....

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
..... 134 Figure 81 Certificate Details ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 135 20 ZyXEL NWA-3100 User's Guide List of Figures Figure 82 My Certificates ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 136 Figure 83 My Certificate Import ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 138 Figure 84 My Certificate Create .....
.....
.....

.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 139 Figure 85 My Certificate Details .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 142 Figure 86 Trusted CAs .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 144 Figure 87 Trusted CA Import ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

... 146 Figure 88 Trusted CA Details .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 147 Figure 89 View Log .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 151 Figure 90 Log Settings .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 152 Figure 91 WIRELESS VLAN .....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 159 Figure 92 RADIUS VLAN .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 160 Figure 93 Management VLAN Configuration Example .....

.....
.....
.....
.....

.....
.....
.....
.....

.... 162 Figure 94 VLAN-Aware Switch - Static VLAN .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 162 Figure 95 VLAN-Aware Switch .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
162 Figure 96 VLAN-Aware Switch - VLAN Status .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 163 Figure 97 VLAN Setup ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 163 Figure 98 New Global Security Group ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 165 Figure 99 Add Group Members .....

.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 165 Figure 100 New Remote Access Policy for VLAN Group ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
166 Figure 101 Specifying Windows-Group Condition .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
166 Figure 102 Adding VLAN Group .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 167 Figure 103 Granting Permissions and User Profile Screens ....

.....
.....
.....
.....

.....
.....
.....

..... 167 Figure 104 Authentication Tab Settings .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 168 Figure 105 Encryption Tab Settings .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 168 Figure 106 Connection Attributes Screen ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 169 Figure 107 RADIUS Attribute Screen ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 169 Figure 108 802 Attribute Setting for Tunnel-Medium-Type ....

.....
.....
.....
.....

.....
.....
.....
.....

.. 170 Figure 109 VLAN ID Attribute Setting for Tunnel-Pvt-Group-ID .....
.....
.....
.....

.....
.....
.....
.....

170 Figure 110 VLAN Attribute Setting for Tunnel-Type .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 171 Figure 111 Completed Advanced Tab ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 171 Figure 112 Second Rx VLAN ID Example ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 172 Figure 113 Configuring SSID: Second Rx VLAN ID Example ..

.....
.....

.....
.....

.....
.....
.....
.....

173 Figure 114 System Status .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 175 Figure 115 System Status: Show Statistics ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 176 Figure 116 Association List ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 177 Figure 117 Channel Usage .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 178 Figure 118 Firmware Upload ..
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
179 Figure 119 Firmware Upload In Process .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 179 Figure 120 Network Temporarily Disconnected .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 180 Figure 121 Firmware Upload Error ..
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 180 Figure 122 Configuration .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 181 Figure 123 Configuration Upload Successful .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 182 Figure 124 Network Temporarily Disconnected ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
182 ZyXEL NWA-3100 User's Guide 21 List of Figures Figure 125 Configuration Upload Error .....
.....
.....

.....
.....
.....

.....

.....
.....
.....
.....

.....
.....
.. 182 Figure 126 Reset Warning Message ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 183 Figure 127 Restart Screen ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 183 Figure 128 Login Screen .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
187 Figure 129 Menu 23 System Password .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 187 Figure 130 SMT Main Menu ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 189 Figure 131 Menu 1 General Setup .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 191 Figure 132 Menu 3 LAN Setup .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
193 Figure 133 Menu 3.2 TCP/IP Setup .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 193 Figure 134 Menu 22 SNMP Configuration .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 195 Figure 135 Menu 23 System Password .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
197 Figure 136 Menu 24 System Maintenance .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 199 Figure 137 Menu 24.1 System Maintenance: Status ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 200 Figure 138 Menu 24.2 System Information and Console Port Speed .

.....
.....
.....
.....

.....
.....
.... 201 Figure 139 Menu 24.
2.1 System Information: Information .....

.....
.....
.....
.....

.....
.....
.....
..... 201 Figure 140 Menu 24.2.

2 System Maintenance: Change Console Port Speed .....
.....
.....
.....

..... 202 Figure 141 Menu 24.3 System Maintenance: Log and Trace ..
.....
.....
.....

.....
.....
.....
.....

.....
. 203 Figure 142 Sample Error and Information Messages ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 203 Figure 143 Menu 24.4 System Maintenance: Diagnostic ...

.....
.....
.....
.....

.....

.....
.....
.....

..... 203 Figure 144 Menu 24.5 Backup Configuration ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 206 Figure 145 FTP Session Example .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 207 Figure 146 System Maintenance: Backup Configuration ..
.....

.....
.....
.....
.....

.....
.....
.....
..... 209 Figure 147 System Maintenance: Starting Xmodem Download Screen ...

.....
.....
.....
.....

.....
.... 209 Figure 148 Backup Configuration Example .
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....

.....
.... 209 Figure 149 Successful Backup Confirmation Screen .
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 209 Figure 150 Menu 24.

6 Restore Configuration .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 210 Figure 151 Menu 24.7 System Maintenance: Upload Firmware ...

.....
.....
.....
.....

.....
.....
.....
.....211 Figure 152 Menu 24.7.1 System Maintenance: Upload System Firmware ..

.....
.....
.....
.....

.....
.211 Figure 153 Menu 24.7.2 System Maintenance: Upload System Configuration File ..
.....
.....

.....
.. 212 Figure 154 FTP Session Example ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 212 Figure 155 Menu 24.7.1 as seen using the Console Port ..

.....
.....
.....
.....

.....
.....
.....
.....

..... 214 Figure 156 Example Xmodem Upload ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 214 Figure 157 Menu 24.
7.2 as seen using the Console Port ....
.....

.....
.....
.....
.....

.....
.....
.....
... 215 Figure 158 Example Xmodem Upload .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 215 Figure 159 Menu 24 System Maintenance .....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
.....

.. 217 Figure 160 Valid CI Commands .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
218 Figure 161 Menu 24.10 System Maintenance: Time and Date Setting .....

.....
.....
.....
.....

..... 219 Figure 162 Menu 24.
11 Remote Management Control .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 221 Figure 163 WIndows 95/98/Me: Network: Configuration .

.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 234 Figure 164 Windows 95/98/Me: TCP/IP Properties: IP Address .....
.....
.....
.....

.....
.....
.....
.....

235 Figure 165 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....
.....
.....
.....

.....
.....
. 236 Figure 166 Windows XP: Start Menu ....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 237 Figure 167 Windows XP: Control Panel ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 237 22 ZyXEL NWA-3100 User's Guide List of Figures Figure 168 Windows XP: Control Panel: Network Connections: Properties .....
.....
.....
.....

.....
.. 238 Figure 169 Windows XP: Local Area Connection Properties ...
.....
.....

.....
.....
.....
.....

.....
.....
238 Figure 170 Windows XP: Advanced TCP/IP Settings .....
.....

.....
.....
.....
.....

.....
.....
.....
..... 239 Figure 171 Windows XP: Internet Protocol (TCP/IP) Properties .

.....
.....
.....
.....

.....
.....
.....
..... 240 Figure 172 Macintosh OS 8/9: Apple Menu ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 241 Figure 173 Macintosh OS 8/9: TCP/IP ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 241 Figure 174 Macintosh OS X: Apple Menu .....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 242 Figure 175 Macintosh OS X: Network ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 243 Figure 176 IP Address Conflicts: Case A .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 245 Figure 177 IP Address Conflicts: Case B ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
246 Figure 178 IP Address Conflicts: Case C .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 246 Figure 179 IP Address Conflicts: Case D .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 247 Figure 180 Peer-to-Peer Communication in an Ad-hoc Network ....

.....
.....
.....
.....

.....
.....
.....
... 249 Figure 181 Basic Service Set .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 250 Figure 182 Infrastructure WLAN .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.....
.....
.....

. 251 Figure 183 RTS/CTS .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 252 Figure 184 Pop-up Blocker .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

261 Figure 185 Internet Options: Privacy .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
262 Figure 186 Internet Options: Privacy .....
.....
.....

.....
.....
.....

.....
.....
.....
.....
.....
263 Figure 187 Pop-up Blocker Settings .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
. 263 Figure 188 Internet Options: Security .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
264 Figure 189 Security Settings - Java Scripting .....
.....
.....
.....
.....
.....
.....
.....
.....
..... 265 Figure 190 Security Settings - Java ...
.....
.....
.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 265 Figure 191 Java (Sun) .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 266 Figure 192 Network Number and Host ID .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 268 Figure 193 Subnetting Example: Before Subnetting .....

.....
.....
.....
.....

.....
.....
.....
.....

..... 270 Figure 194 Subnetting Example: After Subnetting .
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
..... 271 Figure 195 Text File Based Auto Configuration ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 275 Figure 196 Configuration File Format .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 277 Figure 197 WEP Configuration File Example .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 278 Figure 198 802.1X Configuration File Example .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 279 Figure 199 WPA-PSK Configuration File Example .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 279 Figure 200 WPA Configuration File Example ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 280 Figure 201 wlan Configuration File Example .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 281 ZyXEL NWA-3100 User's Guide 23 List of Figures 24 ZyXEL NWA-3100 User's Guide List of Tables List of Tables Table 1 LEDs ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 37 Table 2 Tutorial: Example Information .....

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
.....

... 44 Table 3 Tutorial: Rogue AP Example Information .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 53 Table 4 Tutorial: Friendly AP Information .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

54 Table 5 System General Setup .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
63 Table 6 Password .....

.....
.....
.....
.....

.....
.....
.....

.....

.....
.....
.....
.....

.....
.....
.....
.....

64 Table 7 Time Setting .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 65 Table 8 WMM QoS Priorities ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 69 Table 9 Typical Packet Sizes .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 70 Table 10 Automatic Traffic Classifier Priorities .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 70 Table 11 ATC + WMM Priority Assignment (LAN to WLAN) ..
.....

.....
.....
.....
.....

.....
.....
.....
.... 71 Table 12 ATC + WMM Priority Assignment (WLAN to LAN) .....

.....
.....
.....
.....

.....
.....
.....
.....

71 Table 13 ToS and IEEE 802.1d to WMM QoS Priority Level Mapping .....
.....
.....
.....

.....
.....
.....
. 72 Table 14 STP Path Costs .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.... 73 Table 15 STP Port States .
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.. 73 Table 16 Wireless: Access Point ...
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.... 75 Table 17 Wireless: Bridge/Repeater .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
. 79 Table 18 Security Modes ....
.....
.....
.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
85 Table 19 Wireless Security Levels .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

86 Table 20 Security .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 87 Table 21 Security: WEP ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.. 88 Table 22 Security: 802.1x Only ..
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

... 89 Table 23 Security: 802.1x Static 64-bit, 802.1x Static 128-bit .....
.....
.....
.....

.....
.....
.....
.....

..... 90 Table 24 Security: WPA .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
91 Table 25 Security: WPA2 or WPA2-MIX .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 92 Table 26 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX ....

.....
.....
.....
.....
.....
.....
.. 94 Table 27 RADIUS ...
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
..... 95 Table 28 Wireless: Multiple BSS ...
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
99 Table 29 SSID .....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....
.....
.....
..... 101 Table 30 Configuring SSID .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 102 Table 31 Layer-2 Isolation Configuration .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 107 Table 32 MAC Address Filter ....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
...110 Table 33 Private IP Address Ranges ..
.....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
.....113 Table 34 IP Setup ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....114 Table 35 ROGUE AP > Configuration ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
120 Table 36 ROGUE AP > Friendly AP .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 121 Table 37 ROGUE AP > Rogue AP .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 122 Table 38 Remote Management Overview ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 123 ZyXEL NWA-3100 User's Guide 25 List of Tables Table 39 Remote Management: Telnet .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
125 Table 40 Remote Management: FTP .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 126 Table 41 Remote Management: WWW .....

.....
.....
.....
.....

.....

.....
.....
.....

.....
.....
.....
..... 127 Table 42 SNMP Traps .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 129 Table 43 SNMP Interface Index to Physical Port Mapping .....
.....
.....
.....

.....
.....
.....
.....

..... 130 Table 44 Remote Management: SNMP ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 131 Table 45 My Certificates ...
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....

.....
.....
.....
.....

.....
136 Table 46 My Certificate Import .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
138 Table 47 My Certificate Create .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.. 139 Table 48 My Certificate Details ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 142 Table 49 Trusted CAs .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 145 Table 50 Trusted CA Import ...
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

146 Table 51 Trusted CA Details .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.. 147 Table 52 View Log .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
..... 151 Table 53 Log Settings .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 153 Table 54 System Maintenance Logs .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 154 Table 55 ICMP Notes ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 154 Table 56 Sys log .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.... 155 Table 57 Log Categories and Available Settings .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
155 Table 58 WIRELESS VLAN .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 159 Table 59 RADIUS VLAN ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....

.....
.....
.....

..... 161 Table 60 Standard RADIUS Attributes ....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
... 164 Table 61 System Status ..
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 175 Table 62 System Status: Show Statistics ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
176 Table 63 Association List .....
.....

.....
.....
.....
.....

.....
.....
.....

.....

.....
.....
.....
.....

.....
.. 177 Table 64 Channel Usage ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 178 Table 65 Firmware Upload .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.... 179 Table 66 Restore Configuration .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 181 Table 67 SMT Menus Overview .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 188 Table 68 Main Menu Commands ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
... 189 Table 69 Main Menu Summary .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 190 Table 70 Menu 1 General Setup ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
..... 191 Table 71 Menu 3.2 TCP/IP Setup ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 194 Table 72 Menu 22 SNMP Configuration ...
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 195 Table 73 Menu 24.1 System Maintenance: Status ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 200 Table 74 Menu 24.2.1 System Maintenance: Information ...
.....
.....
.....

.....
.....
.....
.....

.....
.... 201 Table 75 Menu 24.
4 System Maintenance Menu: Diagnostic .....
.....

.....
.....
.....
.....

.....
.....
.. 204 Table 76 Filename Conventions ...
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

... 206 Table 77 General Commands for Third Party FTP Clients .....
.....
.....
.....

.....
.....
.....
.....

..... 207 Table 78 General Commands for Third Party TFTP Clients .
.....
.....
.....

.....
.....
.....
.....

.....
.. 208 Table 79 Brute-Force Password Guessing Protection Commands ...
.....
.....

.....
.....
.....
.....

..... 218 Table 80 System Maintenance: Time and Date Setting .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
. 219 Table 81 Menu 24.11 Remote Management Control ...
.....

.....

.....
.....
.....

.....
.....
.....
.....

.. 221 26 ZyXEL NWA-3100 User's Guide List of Tables Table 82 Hardware Specifications .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
229 Table 83 Firmware Specifications .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 229 Table 84 Power over Ethernet Injector Specifications .

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 230 Table 85 Power over Ethernet Injector RJ-45 Port Pin Assignments ....
.....
.....

.....
.....
.....
.....

. 231 Table 86 North American Plug Standards .....
.....
.....

.....

.....
.....
.....
.....

.....
.....
.....
.....

... 231 Table 87 European Plug Standards .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 231 Table 88 United Kingdom Plug Standards .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
231 Table 89 Australia and New Zealand Plug Standards .....
.....

.....
.....
.....
.....

.....
.....
.....
..... 231 Table 90 Comparison of EAP Authentication Types ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 256 Table 91 Wireless Security Relational Matrix .
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
257 Table 92 Subnet Masks .....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 268 Table 93 Subnet Masks .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 269 Table 94 Maximum Host Numbers ..
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....

.....
.....
.....
269 Table 95 Alternative Subnet Mask Notation .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 269 Table 96 Subnet 1 .
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 271 Table 97 Subnet 2 ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 272 Table 98 Subnet 3 .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
... 272 Table 99 Subnet 4 ..
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 272 Table 100 Eight Subnets .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.... 272 Table 101 24-bit Network Number Subnet Planning .
.....

.....
.....
.....
.....

.....

.....
.....
.....

..... 273 Table 102 16-bit Network Number Subnet Planning .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. 273 Table 103 Auto Configuration by DHCP .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 276 Table 104 Manual Configuration .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
. 276 Table 105 Configuration via SNMP ....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

... 276 Table 106 Displaying the File Version .....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 277 Table 107 Displaying the File Version .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 277 Table 108 Displaying the Auto Configuration Status .
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 278 ZyXEL NWA-3100 User's Guide 27 List of Tables 28 ZyXEL NWA-3100 User's Guide PART I Introduction Introducing the ZyXEL Device (31) Introducing the Web Configurator (39) Tutorial (43) 29 30 CHAPTER 1 Introducing the ZyXEL Device This chapter introduces the main applications and features of the ZyXEL Device. It also introduces the ways you can manage the ZyXEL Device. 1.1 Introducing the ZyXEL Device Your ZyXEL Device extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. It is highly versatile, supporting up to eight BSSIDs simultaneously.

The Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

Multiple security profiles allow you to easily assign different types of security to groups of users. The ZyXEL Device controls network access with MAC address filtering, rogue AP detection and layer 2 isolation. 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 ZyXEL Device 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 ZyXEL Device The ZyXEL Device can be configured to use the following WLAN operating modes 1 2 3 4 AP AP+Bridge Bridge/Repeater MBSSID Applications for each operating mode are shown below.

1.2.1 Access Point The ZyXEL Device is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyXEL Device is shown as follows. Stations A, B and C can access the wired network through the ZyXEL Devices.

ZyXEL NWA-3100 User's Guide 31 Chapter 1 Introducing the ZyXEL Device Figure 1 Access Point Application 1.2.2 AP + Bridge In AP+Bridge mode, the ZyXEL Device 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 ZyXEL Device is in AP + Bridge mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP.

See Section 5.6.2 on page 76 for more details. Unless specified, the term "security settings" refers to the traffic between the wireless stations and the ZyXEL Device. If you do not enable WDS security in AP + Bridge mode, traffic between APs is not encrypted. 32 ZyXEL NWA-3100 User's Guide Chapter 1 Introducing the ZyXEL Device Figure 2 AP+Bridge Application 1.2.3 Bridge / Repeater The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. In the figure below, the two ZyXEL Devices (A and B) are connected to independent wired networks and have a bridge connection (A can communicate with B) at the same time. A ZyXEL Device in repeater mode (C) has no Ethernet connection.

When the ZyXEL Device is in bridge mode, you should enable STP to prevent bridge loops. When the ZyXEL Device 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. When WDS security is enabled, both APs must use the same pre-shared key. See Section 5.6.2 on page 76 for more details. Once the security settings of the two APs match one another, the WDS connection is made. If you do not enable WDS security in Bridge / Repeater mode, traffic between APs is not encrypted. ZyXEL NWA-3100 User's Guide 33 Chapter 1 Introducing the ZyXEL Device Figure 3 Bridge Application Figure 4 Repeater Application 34 ZyXEL NWA-3100 User's Guide Chapter 1 Introducing the ZyXEL Device 1.2.

4 MBSSID A BSS (Basic Service Set) is the set of devices forming a single wireless network (usually an access point and one or more wireless clients). An SSID (Service Set IDentifier) is the name of a BSS. In MBSSID (Multiple BSS) mode, the ZyXEL Device provides multiple virtual APs, each forming its own BSS and using its own individual SSID profile. You can configure up to sixteen SSID profiles, and have up to eight active at any one time. You can assign different wireless and security settings to each SSID profile.

This allows you to compartmentalize groups of users, set varying access privileges, and prioritize network traffic to and from certain BSSs. To the wireless clients in the network, each SSID appears to be a different access point. As in any wireless network, clients can associate only with the SSIDs for which they have the correct security settings. For example, you might want to set up a wireless network in your office where Internet telephony (Voice over IP, or VoIP) users have priority. You also want a regular wireless network for standard users, as well as a `guest' wireless network for visitors.

In the following figure, VoIP_SSID users have Quality of Service (QoS) priority, SSID03 is the wireless network for standard users, and Guest_SSID is the wireless network for guest users. In this example, the guest user is forbidden access to the wired LAN behind the AP and can access only the Internet. Figure 5 Multiple BSSs ZyXEL NWA-3100 User's Guide 35 Chapter 1 Introducing the ZyXEL Device 1.2.5 Pre-Configured SSID Profiles The ZyXEL Device has two pre-configured SSID profiles. 1 VoIP_SSID. This profile is intended for use by wireless clients requiring the highest QoS (Quality of Service) level for VoIP (Voice over IP) telephony and other applications requiring low latency. The QoS level of this profile is not user-configurable. See Section 5.3.

1 on page 69 for more information on QoS. 2 Guest_SSID. This profile is intended for use by visitors and others who require access to certain resources on the network (an Internet gateway or a network printer, for example) but must not have access to the rest of the network. Layer 2 isolation is enabled (see Section 8.1 on page 105), and QoS is set to NONE. Intra-BSS traffic blocking is also enabled (see Section 5.1.1 on page 67). These fields are all user-configurable. 1.

3 Ways to Manage the ZyXEL Device Use any of the following methods to manage the ZyXEL Device. · Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser. · Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.

· SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device. Use Telnet to access the SMT. · FTP for firmware upgrades and configuration backup and restore. · SNMP.

The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide. 1.4 Good Habits for Managing the ZyXEL Device Do the following things regularly to make the ZyXEL Device 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 ZyXEL Device to its factory default settings.

If you backed up an earlier configuration file, you won't have to totally re-configure the ZyXEL Device; you can simply restore your last configuration. 36 ZyXEL NWA-3100 User's Guide Chapter 1 Introducing the ZyXEL Device 1.

5 LEDs Figure 6 LEDs Table 1 LEDs LABEL 1 LED SYS COLOR Green STATUS On DESCRIPTION The ZyXEL Device is in AP+Bridge or Bridge/Repeater mode, and has successfully established a Wireless Distribution System (WDS) connection. The ZyXEL Device is starting up. Either · The ZyXEL Device is in Access Point or MBSSID mode and is functioning normally. · The ZyXEL Device is in AP+Bridge or Bridge/ Repeater mode and has not established a Wireless Distribution System (WDS) connection. or · The ZyXEL Device is not receiving power. Red Flashing Off ZyXEL NWA-3100 User's Guide 37 Chapter 1 Introducing the ZyXEL Device Table 1 LEDs (continued) LABEL 2 LED ZyAIR COLOR Blue STATUS On DESCRIPTION The ZyXEL Device is receiving power. You can turn the ZyAIR LED off and on using the Web configurator. See Section 5.

6.1 on page 74. The ZyXEL Device is receiving power and transmitting data to or receiving data from its wireless stations. Either · The ZyXEL Device is not receiving power. or · The ZyAIR LED has been disabled.

See Section 5.6.1 on page 74 for how to enable the ZyAIR LED. The ZyXEL Device has a 10 Mbps Ethernet connection. The ZyXEL Device has a 10 Mbps Ethernet connection and is sending or receiving data.

The ZyXEL Device has a 100 Mbps Ethernet connection. The ZyXEL Device has a 100 Mbps Ethernet connection and is sending/receiving data. The ZyXEL Device does not have an Ethernet connection. The ZyXEL Device is receiving power via the POWER socket. The ZyXEL Device is receiving power via the ETHERNET port using Power over Ethernet (PoE). The ZyXEL Device is not receiving power. Blinking Off 3 ETHN Green On Blinking Yellow On Blinking Off 4 POWER Green Red On On Off 38 ZyXEL NWA-3100 User's Guide CHAPTER 2 Introducing the Web Configurator This chapter describes how to access the ZyXEL Device's web configurator and provides an overview of its screens. 2.1 Accessing the Web Configurator 1 Make sure your hardware is properly connected and prepare your computer or computer network to connect to the ZyXEL Device (refer to the Quick Start Guide). 2 Launch your web browser.

3 Type "192.168.1.2" as the URL (default). 4 Type "1234" (default) as the password and click Login. In some versions, the default password appears automatically - if this is the case, click Login. 5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) then click Apply. Alternatively, click Ignore. If you do not change the password, the following screen appears every time you login.

ZyXEL NWA-3100 User's Guide 39 Chapter 2 Introducing the Web Configurator Figure 7 Change Password Screen 6 Click Apply in the Replace Certificate screen to create a certificate using your ZyXEL Device's MAC address that will be specific to this device. Figure 8 Replace Certificate Screen You should now see the MAIN MENU screen. 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 ZyXEL Device if this happens. 2.

2 Resetting the ZyXEL Device 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. 40 ZyXEL NWA-3100 User's Guide Chapter 2 Introducing the Web Configurator 2.

2.1 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 ZyXEL Device is not known. Use the web configurator to restore defaults (refer to Chapter 15 on page 175). Transfer the configuration file to your ZyXEL Device using FTP. See the section on SMT configuration for more information. 2.3 Navigating the Web Configurator The following summarizes how to navigate the web configurator from the MAIN MENU 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 9 The MAIN MENU Screen of the Web Configurator ZyXEL NWA-3100 User's Guide 41 Chapter 2 Introducing the Web Configurator Click the links under ADVANCED to configure advanced features such as SYSTEM (General Setup, Password and Time Zone), 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), CERTIFICATES (My Certificates, Trusted CAs), LOGS (View Logs and Log Settings) and VLAN (Wireless VLAN and RADIUS VLAN). Click MAINTENANCE to view information about your ZyXEL Device or upgrade configuration and firmware files. Maintenance features include Status (Statistics), Association List, Channel Usage, F/W (firmware) Upload, Configuration (Backup, Restore and Default) and Restart. 42 ZyXEL NWA-3100 User's Guide CHAPTER 3 Tutorial This chapter provides step-by-step guidelines showing how to configure your ZyXEL Device for some example scenarios. The first example shows how to create multiple wireless networks, and the second example shows how to use the rogue AP detection feature. 3.1 How to Configure Multiple Wireless Networks In this example, you have been using your ZyXEL Device as an access point for your office network (See your Quick Start Guide for information on how to set up your ZyXEL Device in Access Point mode). Now your network is expanding and you want to make use of the MBSSID feature (see Section 7.1 on page 97) to provide multiple wireless networks.

Each wireless network will cater for a different type of user. You want to make three wireless networks: one standard office wireless network with all the same settings you already have, another wireless network with high Quality of Service (QoS) settings for Voice over IP users, and a guest network that allows visitors to your office to access only the Internet and the network printer. To do this, you will take the following steps: 1 Change the operating mode from Access Point to MBSSID and reactivate the standard network. 2 Configure a wireless network for Voice over IP users. 3 Configure a wireless network for guests to your office.

The following figure shows the multiple networks you want to set up. Your ZyXEL Device is marked Z, the main network router is marked A, and your network printer is marked B. ZyXEL NWA-3100 User's Guide 43 Chapter 3 Tutorial Figure 10 Tutorial: Example MBSSID Setup The standard network (SSID04) has access to all resources.

The VoIP network (VoIP_SSID) has access to all resources and a high Quality of Service (QoS) setting (see Section 5.3 on page 69 for information on QoS). The guest network (Guest_SSID) has access to the Internet and the network printer only, and a low QoS setting. To configure these settings, you need to know the MAC (Media Access Control) addresses of the devices you want to allow users of the guest network to access. The following table shows the addresses used in this example. Table 2 Tutorial: Example Information Network router (A) MAC address Network printer (B) MAC address 00:AA:00:AA:00:AA AA:00:AA:00:AA:00 3.1.1 Change the Operating Mode Log in to the ZyXEL Device (see Section 2.1 on page 39). Click WIRELESS > Wireless. The Wireless screen appears. In this example, the ZyXEL Device is set to Access Point operating mode, and is currently using the SSID04 profile.

44 ZyXEL NWA-3100 User's Guide Chapter 3 Tutorial Figure 11 Tutorial: Wireless LAN: Before Select MBSSID from the Operating Mode drop-down list box. The screen displays as follows. Figure 12 Tutorial: Wireless LAN: Change Mode This Select SSID Profile table allows you to activate or deactivate SSID profiles. Your wireless network was previously using the SSID04 profile, so select SSID04 in one of the Profile list boxes (number 3 in this example). ZyXEL NWA-3100 User's Guide 45 Chapter 3 Tutorial Select the Index box for the entry and click Apply to activate the profile. Your standard wireless network (SSID04) is now accessible to your wireless clients as before. You do not need to configure anything else for your standard network. 3.1.2 Configure the VoIP Network Next, click WIRELESS > SSID.

The following screen displays. Note that the SSID04 SSID profile (the standard network) is using the security01 security profile. You cannot change this security profile without changing the standard network's parameters, so when you set up security for the VoIP_SSID and Guest_SSID profiles you will need to set different security profiles. Figure 13 Tutorial: WIRELESS > SSID 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.

46 ZyXEL NWA-3100 User's Guide Chapter 3 Tutorial Figure 14 Tutorial: VoIP SSID Profile Edit · Choose a new SSID for the VoIP network. In this example, enter VOIP_SSID_Example. Note that although the SSID changes, the SSID profile name (VoIP_SSID) remains the same as before. · Select Enable from the Hide Name (SSID) list box. You want only authorized company employees to use this network, so there is no need to broadcast the SSID to wireless clients scanning the area.

· The standard network (SSID04) is currently using the security01 profile, so use a different profile for the VoIP network. If you used the security01 profile, anyone who could access the standard network could access the VoIP wireless network. Select security02 from the Security field. · Leave all the other fields at their defaults and click Apply. 3.1.2.1 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. ZyXEL NWA-3100 User's Guide 47 Chapter 3 Tutorial Figure 15 Tutorial: VoIP Security 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 16 Tutorial: VoIP Security Profile Edit · Change the Name field to "VoIP_Security" to make it easier to remember and identify. · In this example, you do not have a RADIUS server for authentication, so select WPA2PSK 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". 48 ZyXEL NWA-3100 User's Guide Chapter 3 Tutorial · 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 17 Tutorial: VoIP Security: Updated 3.

1.2.2 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 and click Apply.

Figure 18 Tutorial: Activate VoIP Profile 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. 3.1.3 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 8.1 on page 105), and "intra-BSS traffic blocking" means that the client cannot access other clients on the same wireless network (see Section 5.1.1 on page 67). Click WIRELESS > SSID. Select Guest_SSID's entry in the list and click Edit. The following screen appears. ZyXEL NWA-3100 User's Guide 49 Chapter 3 Tutorial Figure 19 Tutorial: Guest Edit · Choose a new SSID for the guest network. In this example, enter Guest_SSID_Example.

Note that although the SSID changes, the SSID profile name (Guest_SSID) remains the same as before. · Select Disable from the Hide Name (SSID) list box. This makes it easier for guests to configure their own computers' wireless clients to your network's settings. · The standard network (SSID04) is already using the security01 profile, and the VoIP network is using the security02 profile (renamed VoIP_Security) so select the security03 profile from the Security field. · Leave all the other fields at their defaults and click Apply. 3.1.3.1 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 20 Tutorial: Guest Security Profile Edit · Change the Name field to "Guest_Security" to make it easier to remember and identify. 50 ZyXEL NWA-3100 User's Guide Chapter 3 Tutorial · Select WPA-PSK in the Security Mode field. WPA-PSK provides strong security that is supported by most wireless clients. Even though your Guest_SSID clients do not have access to sensitive information on the network, you should not leave the network without security.

An attacker could still cause damage to the network or intercept unsecured communications. · Enter the PSK you want to use in your network in the Pre Shared Key field. In this example, the PSK is "ThisismyGuestWPApre-sharedkey". · Click Apply.

The WIRELESS > Security screen displays. Ensure that the Profile Name for entry 3 displays "Guest_Security" and that the Security Mode is WPA-PSK. Figure 21 Tutorial: Guest Security: Updated 3.1.3.2 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 22 Tutorial: Layer 2 Isolation Enter the MAC addresses 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.

3.1.3.3 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. ZyXEL NWA-3100 User's Guide 51 Chapter 3 Tutorial Figure 23 Tutorial: Activate Guest Profile Your Guest wireless network is now ready to use. 3.1.4 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 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 screen, and ensure that layer 2 isolation is enabled in the Guest_SSID profile screen. 3.2 How to Set Up and Use Rogue AP Detection This example shows you how to configure the rogue AP detection feature on the ZyXEL Device.

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 ZyXEL Device to send out e-mail alerts whenever it detects a rogue wireless access point. See Chapter 10 on page 117 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. 52 ZyXEL NWA-3100 User's Guide Chapter 3 Tutorial Your wireless network operates in an office building. It consists of four access points (all ZyXEL Devices) 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 24 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 ZyXEL Devices 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 Access Point A Access Point B Access Point C Access Point D IP ADDRESS 192.168.

1.1 192.168.1.2 192.168.1.3 192.168.1.

4 MAC ADDRESS 00:AA:00:AA:00:AA AA:00:AA:00:AA:00 A0:0A:A0:0A:A0:0A 0A:A0:0A:A0:0A:A0 ZyXEL NWA-3100 User's Guide 53 Chapter 3 Tutorial Table 3 Tutorial: Rogue AP Example Information DEVICE File / Mail Server E Access Point 1 IP ADDRESS 192.168.1.25 UNKNOWN MAC ADDRESS N/A AF:AF:AF:FA:FA:FA The ZyXEL Device 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, if possible. 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 2 3 4 5 Set up and save a friendly AP list. Activate periodic Rogue AP Detection.

Set up e-mail alerts. Configure your other access points. Test the setup. 3.2.

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 25 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. Table 4 Tutorial: Friendly AP Information MAC ADDRESS 00:AA:00:AA:00:AA AA:00:AA:00:AA:00 DESCRIPTION My Access Point _A_ My Access Point _B_ 54 ZyXEL NWA-3100 User's Guide Chapter 3 Tutorial Table 4 Tutorial: Friendly AP Information MAC ADDRESS A0:0A:A0:0A:A0:0A 0A:A0:0A:A0:0A:A0 AF:AF:AF:FA:FA:FA DESCRIPTION My Access Point _C_ My Access Point _D_ Coffee Shop Access Point _1_ 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 26 Tutorial: Friendly AP (After Data Entry) 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 27 Tutorial: Configuration 4 Click Export.

If a window similar to the following appears, click Save. ZyXEL NWA-3100 User's Guide 55 Chapter 3 Tutorial Figure 28 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 24 on page 53). The default filename is "Flist". Figure 29 Tutorial: Save Friendly AP list 3.2.2 Activate Periodic Rogue AP Detection Take the following steps to activate rogue AP detection on the first of your ZyXEL Devices. 1 In the ROGUE AP > Configuration screen, select Yes from the Activate Rogue AP Period Detection field. Figure 30 Tutorial: Periodic Rogue AP Detection 56 ZyXEL NWA-3100 User's Guide Chapter 3 Tutorial 2 In the Period (min.) field, enter how often you want the ZyXEL Device to scan for rogue APs.
You can have the ZyXEL Device scan anywhere from once every ten minutes to once every hour. In this example, enter "10". 3 Click Apply. 3.2.
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 email inbox whenever a rogue AP is discovered in your wireless network's coverage area. 1 Click LOGS > Log Settings. The following screen appears. Figure 31 Tutorial: Log Settings · In this example, your mail server's IP address is 192.168.
1.25. Enter this IP address in the Mail Server field. · Enter a subject line for the alert e-mails in the Mail Subject field. Choose a subject that is eye-catching and identifies the access point - in this example, "ALERT_Access_Point_A". · Enter the email address to which you want alerts to be sent (myname@myfirm.com, in this example). ZyXEL NWA-3100 User's Guide 57 Chapter 3 Tutorial · In the Send Immediate Alert section, select the events you want to trigger immediate emails. Ensure that Rogue AP is selected. · Click Apply.

3.2.4 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 53 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.
2.2 on page 56. 5 Set up e-mail logs as in Section 3.2.3 on page 57, but change the Mail Subject field so you can tell which AP the alerts come from ("ALERT_Access_Point_B", etc.) 3.2.5 Test the Setup Next, test your setup to ensure it is correctly configured. · Log into each AP's Web configurator and click ROGUE AP > Rogue AP. Click Refresh.

If any of the MAC addresses from Table 4 on page 54 appear in the list, the friendly AP function may be incorrectly configured - check the ROGUE AP > Friendly AP screen. If any entries appear in the rogue AP list that are not in Table 4 on page 54, 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 ZyXEL Device. · 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 ZyXEL Devices in turn while the network is running. Either wait for at least ten minutes (to ensure the ZyXEL Device performs a scan in that time) or login to the ZyXEL Device's Web configurator and click ROGUE AP > Rogue AP > Refresh to have the ZyXEL Device 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. 58 ZyXEL NWA-3100 User's Guide Chapter 3 Tutorial · Check your e-mail.
You should have received at least one e-mail alert (your other ZyXEL Devices may also have sent alerts, depending on their proximity and the output power of your "rogue" AP). ZyXEL NWA-3100 User's Guide 59 Chapter 3 Tutorial 60 ZyXEL NWA-3100 User's Guide PART II The Web Configurator System Screens (63) Wireless Configuration (67) Wireless Security Configuration (81) MBSSID and SSID (97) Other Wireless Configuration (105) IP Screen (113) Rogue AP (117) Remote Management (123) Certificates (133) Log Screens (151) VLAN (157) Maintenance (175) 61 62 CHAPTER 4.1 System Overview This section provides information on general system setup. 4 System Screens 4.2 Configuring General Setup Click SYSTEM > General.
Figure 32 System General Setup The following table describes the labels in this screen. Table 5 System General Setup LABEL General Setup System Name Type a descriptive name to identify the ZyXEL Device in the Ethernet network. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. This is not a required field.
Leave this field blank or enter the domain name here if you know it. Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). DESCRIPTION Domain Name Administrator Inactivity Timer System DNS Servers ZyXEL NWA-3100 User's Guide 63 Chapter 4 System Screens Table 5 System General Setup LABEL First DNS Server Second DNS Server Third DNS Server DESCRIPTION Select From DHCP if your DHCP server dynamically assigns DNS server information (and the ZyXEL Device's Ethernet IP address). The field to the right displays the (read-only) DNS server IP address that the DHCP assigns.