

User's Guide

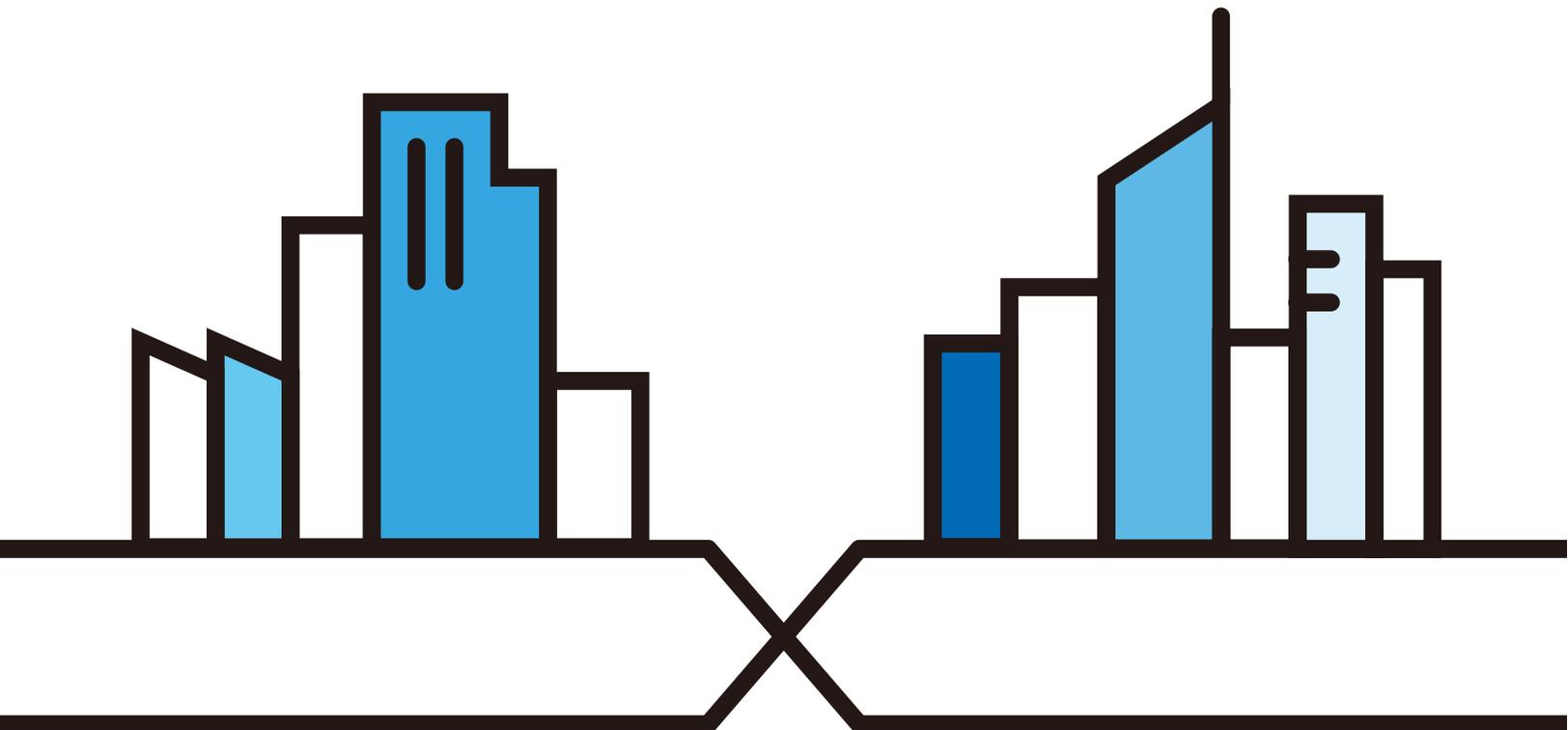
VMG/XMG Series

DSL Router

Default Login Details

| | |
|----------------|----------------------|
| LAN IP Address | http://192.168.1.1 |
| Login | admin |
| Password | See the device label |

Version 5.13 Edition 2, 10/2018



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the managed device

- More Information

Go to **support.zyxel.com** to find other information on the Zyxel Device.



Contents Overview

| | |
|---|-----------|
| User's Guide | 16 |
| Introducing the Zyxel Device | 17 |
| The Web Configurator | 34 |
| Quick Start | 42 |
| Tutorials | 48 |
| Technical Reference | 80 |
| Connection Status Screens | 81 |
| Broadband | 93 |
| Wireless | 121 |
| Home Networking | 151 |
| Routing | 168 |
| Quality of Service (QoS) | 176 |
| Network Address Translation (NAT) | 195 |
| Dynamic DNS Setup | 213 |
| IGMP/MLD | 217 |
| Vlan Group | 220 |
| Interface Grouping | 222 |
| USB Service | 227 |
| Home Connectivity | 233 |
| Firewall | 235 |
| MAC Filter | 244 |
| Parental Control | 246 |
| Scheduler Rule | 252 |
| Certificates | 254 |
| Voice | 261 |
| Log | 291 |
| Traffic Status | 294 |
| VoIP Status | 298 |
| ARP Table | 301 |
| Routing Table | 303 |
| Multicast Status | 305 |
| xDSL Statistics | 307 |
| WLAN Station Status | 309 |
| Cellular Statistics | 311 |
| System | 313 |
| User Account | 314 |
| Remote Management | 317 |

| | |
|---------------------------|------------|
| SNMP | 320 |
| Time Settings | 323 |
| E-mail Notification | 325 |
| Log Setting | 327 |
| Firmware Upgrade | 331 |
| Backup Restore | 334 |
| Diagnostic | 337 |
| Troubleshooting | 343 |
| Appendices | 349 |

Table of Contents

| | |
|---|-----------|
| Contents Overview | 3 |
| Table of Contents | 5 |
| | |
| Part I: User's Guide..... | 16 |
| | |
| Chapter 1 | |
| Introducing the Zyxel Device | 17 |
| 1.1 Overview | 17 |
| 1.1.1 Internet Access | 18 |
| 1.1.2 G.fast | 18 |
| 1.1.3 Ethernet WAN | 19 |
| 1.1.4 Triple Play | 19 |
| 1.1.5 WAN Priority | 20 |
| 1.1.6 Wireless Access | 20 |
| 1.1.7 Zyxel Device's USB Support | 21 |
| 1.1.8 VoIP Features | 22 |
| 1.2 Ways to Manage the Zyxel Device | 22 |
| 1.3 Good Habits for Managing the Zyxel Device | 23 |
| 1.4 Hardware | 23 |
| 1.5 LEDs (Lights) | 24 |
| 1.5.1 Using the WLAN and WPS Buttons | 32 |
| 1.5.2 The RESET Button | 33 |
| | |
| Chapter 2 | |
| The Web Configurator..... | 34 |
| 2.1 Overview | 34 |
| 2.1.1 Accessing the Web Configurator | 34 |
| 2.2 Web Configurator Layout | 36 |
| 2.2.1 Settings Icon | 36 |
| 2.2.2 Widget Icon | 41 |
| | |
| Chapter 3 | |
| Quick Start..... | 42 |
| 3.1 Overview | 42 |
| 3.2 Quick Start Setup | 42 |
| 3.3 Time Zone | 42 |
| 3.4 Internet | 43 |

3.4.1 Internet Status 43

3.4.2 Successful Internet Connection 44

3.4.3 Unsuccessful Internet Connection 44

3.4.4 Incorrect Internet Information 45

3.4.5 Encapsulation 45

3.4.6 Internet Information Input 46

3.5 Quick Start Setup-Wireless 46

3.6 Quick Start Setup-Finish 47

Chapter 4

Tutorials48

4.1 Overview 48

4.2 Setting Up an ADSL PPPoE Connection 48

4.3 Setting Up a Secure Wireless Network 51

 4.3.1 Configuring the Wireless Network Settings 51

 4.3.2 Using WPS 54

 4.3.3 Without WPS 58

4.4 Setting Up Multiple Wireless Groups 59

4.5 Using the File Sharing Feature 63

 4.5.1 Set Up File Sharing 63

 4.5.2 Access Your Shared Files From a Computer 65

4.6 Using the Media Server Feature 65

 4.6.1 Configuring the Zyxel Device 66

 4.6.2 Using Windows Media Player 66

 4.6.3 Using a Digital Media Adapter 68

4.7 Configuring Static Route for Routing to Another Network 69

4.8 Configuring QoS Queue and Class Setup 72

4.9 Access the Zyxel Device Using DDNS 76

 4.9.1 Registering a DDNS Account on www.dyndns.org 76

 4.9.2 Configuring DDNS on Your Zyxel Device 77

 4.9.3 Testing the DDNS Setting 77

4.10 Configuring the MAC Address Filter 78

4.11 Access Your Shared Files From a Computer 79

Part II: Technical Reference 80

Chapter 5

Connection Status Screens81

5.1 The Connection Status Screen 81

 5.1.1 The Connectivity Screen 81

 5.1.2 The System Info Screen 82

5.1.3 The Wi-Fi Settings Screen 84
 5.1.4 The Guest Wi-Fi Settings Screen 86
 5.1.5 The LAN Screen 88
 5.1.6 The Parental Control Screen 89

Chapter 6

Broadband.....93

6.1 Overview 93
 6.1.1 What You Can Do in this Chapter 93
 6.1.2 What You Need to Know 94
 6.1.3 Before You Begin 97
 6.2 The Broadband Screen 97
 6.2.1 Add/Edit Internet Connection 99
 6.3 The Cellular Backup Screen 107
 6.4 The Broadband Advanced Screen 113
 6.5 Technical Reference 115

Chapter 7

Wireless121

7.1 Wireless Overview 121
 7.1.1 What You Can Do in this Chapter 121
 7.1.2 What You Need to Know 121
 7.2 The Wireless General Settings Screen 122
 7.2.1 No Security 124
 7.2.2 More Secure (WPA(2)-PSK) 124
 7.3 The Guest/More AP Screen 125
 7.3.1 The Edit Guest/More AP Screen 126
 7.4 The MAC Authentication Screen 129
 7.5 The WPS Screen 131
 7.6 The WMM Screen 132
 7.7 The Others Screen 133
 7.8 The Channel Status Screen 136
 7.9 The MESH Screen 136
 7.10 Technical Reference 138
 7.10.1 Wireless Network Overview 138
 7.10.2 Additional Wireless Terms 140
 7.10.3 Wireless Security Overview 140
 7.10.4 Signal Problems 142
 7.10.5 BSS 142
 7.10.6 MBSSID 143
 7.10.7 Preamble Type 143
 7.10.8 WiFi Protected Setup (WPS) 144

| | |
|--|------------|
| Chapter 8 | |
| Home Networking | 151 |
| 8.1 Home Networking Overview | 151 |
| 8.1.1 What You Can Do in this Chapter | 151 |
| 8.1.2 What You Need To Know | 152 |
| 8.1.3 Before You Begin | 153 |
| 8.2 The LAN Setup Screen | 153 |
| 8.3 The LAN Static DHCP Screen | 157 |
| 8.4 The UPnP Screen | 159 |
| 8.4.1 Turning On UPnP in Windows 7 Example | 160 |
| 8.5 The LAN Additional Subnet Screen | 161 |
| 8.6 The STB Vendor ID Screen | 163 |
| 8.7 The Wake on LAN Screen | 163 |
| 8.8 The TFTP Server Name Screen | 164 |
| 8.9 Technical Reference | 165 |
| 8.9.1 LANs, WANs and the Zyxel Device | 165 |
| 8.9.2 DHCP Setup | 165 |
| 8.9.3 DNS Server Addresses | 166 |
| 8.9.4 LAN TCP/IP | 166 |
| | |
| Chapter 9 | |
| Routing | 168 |
| 9.1 Overview | 168 |
| 9.2 The Routing Screen | 168 |
| 9.2.1 Add/Edit Static Route | 169 |
| 9.3 The DNS Route Screen | 171 |
| 9.3.1 The DNS Route Add Screen | 171 |
| 9.4 The Policy Route Screen | 172 |
| 9.4.1 Add/Edit Policy Route | 173 |
| 9.5 The RIP Screen | 174 |
| | |
| Chapter 10 | |
| Quality of Service (QoS) | 176 |
| 10.1 QoS Overview | 176 |
| 10.1.1 What You Can Do in this Chapter | 176 |
| 10.2 What You Need to Know | 177 |
| 10.3 The Quality of Service General Screen | 178 |
| 10.4 The Queue Setup Screen | 180 |
| 10.4.1 Adding a QoS Queue | 181 |
| 10.5 The QoS Classification Setup Screen | 182 |
| 10.5.1 Add/Edit QoS Class | 183 |
| 10.6 The QoS Shaper Setup Screen | 187 |
| 10.6.1 Add/Edit a QoS Shaper | 188 |

| | |
|--|------------|
| 10.7 The QoS Policer Setup Screen | 188 |
| 10.7.1 Add/Edit a QoS Policer | 189 |
| 10.8 Technical Reference | 190 |
| Chapter 11 | |
| Network Address Translation (NAT) | 195 |
| 11.1 NAT Overview | 195 |
| 11.1.1 What You Can Do in this Chapter | 195 |
| 11.1.2 What You Need To Know | 195 |
| 11.2 The Port Forwarding Screen | 196 |
| 11.2.1 Add/Edit Port Forwarding | 198 |
| 11.3 The Port Triggering Screen | 200 |
| 11.3.1 Add/Edit Port Triggering Rule | 202 |
| 11.4 The DMZ Screen | 204 |
| 11.5 The ALG Screen | 204 |
| 11.6 The Address Mapping Screen | 205 |
| 11.6.1 Add/Edit Address Mapping Rule | 206 |
| 11.7 The NAT Sessions Screen | 207 |
| 11.8 Technical Reference | 208 |
| 11.8.1 NAT Definitions | 208 |
| 11.8.2 What NAT Does | 209 |
| 11.8.3 How NAT Works | 210 |
| 11.8.4 NAT Application | 210 |
| Chapter 12 | |
| Dynamic DNS Setup | 213 |
| 12.1 DNS Overview | 213 |
| 12.1.1 What You Can Do in this Chapter | 213 |
| 12.1.2 What You Need To Know | 213 |
| 12.2 The DNS Entry Screen | 214 |
| 12.2.1 Add/Edit DNS Entry | 214 |
| 12.3 The Dynamic DNS Screen | 215 |
| Chapter 13 | |
| IGMP/MLD | 217 |
| 13.1 IGMP/MLD Overview | 217 |
| 13.1.1 What You Need To Know | 217 |
| 13.2 The IGMP/MLD Screen | 217 |
| Chapter 14 | |
| Vlan Group | 220 |
| 14.1 Overview | 220 |
| 14.1.1 What You Can Do in this Chapter | 220 |

| | |
|--|------------|
| 14.2 The Vlan Group Screen | 220 |
| 14.2.1 Add/Edit a VLAN Group | 221 |
| Chapter 15 | |
| Interface Grouping | 222 |
| 15.1 Interface Grouping Overview | 222 |
| 15.1.1 What You Can Do in this Chapter | 222 |
| 15.2 The Interface Grouping Screen | 222 |
| 15.2.1 Interface Group Configuration | 224 |
| 15.2.2 Interface Grouping Criteria | 225 |
| Chapter 16 | |
| USB Service | 227 |
| 16.1 USB Service Overview | 227 |
| 16.1.1 What You Can Do in this Chapter | 227 |
| 16.1.2 What You Need To Know | 227 |
| 16.1.3 Before You Begin | 228 |
| 16.2 The File Sharing Screen | 228 |
| 16.2.1 The Add New Share Screen | 230 |
| 16.2.2 The Add New User Screen | 231 |
| 16.3 The Media Server Screen | 231 |
| Chapter 17 | |
| Home Connectivity | 233 |
| 17.1 Home Connectivity Overview | 233 |
| 17.2 The Home Connectivity Screen | 233 |
| Chapter 18 | |
| Firewall | 235 |
| 18.1 Firewall Overview | 235 |
| 18.1.1 What You Can Do in this Chapter | 235 |
| 18.1.2 What You Need to Know | 236 |
| 18.2 The Firewall Screen | 236 |
| 18.3 The Protocol Screen | 237 |
| 18.3.1 Add New/Edit Protocol Entry | 238 |
| 18.4 The Access Control Screen | 239 |
| 18.4.1 Add/Edit an ACL Rule | 240 |
| 18.5 The DoS Screen | 242 |
| Chapter 19 | |
| MAC Filter | 244 |
| 19.1 MAC Filter Overview | 244 |
| 19.2 The MAC Filter Screen | 244 |

| | |
|---|------------|
| Chapter 20 | |
| Parental Control | 246 |
| 20.1 Parental Control Overview | 246 |
| 20.2 The Parental Control Screen | 246 |
| 20.2.1 Add/Edit a Parental Control Profile | 247 |
| Chapter 21 | |
| Scheduler Rule | 252 |
| 21.1 Scheduler Rule Overview | 252 |
| 21.2 The Scheduler Rule Screen | 252 |
| 21.2.1 Add/Edit a Schedule Rule | 252 |
| Chapter 22 | |
| Certificates | 254 |
| 22.1 Certificates Overview | 254 |
| 22.1.1 What You Can Do in this Chapter | 254 |
| 22.2 What You Need to Know | 254 |
| 22.3 The Local Certificates Screen | 254 |
| 22.3.1 Create Certificate Request | 255 |
| 22.3.2 View Certificate Request | 256 |
| 22.4 The Trusted CA Screen | 257 |
| 22.4.1 View Trusted CA Certificate | 258 |
| 22.4.2 Import Trusted CA Certificate | 259 |
| Chapter 23 | |
| Voice | 261 |
| 23.1 Voice Overview | 261 |
| 23.1.1 What You Can Do in this Chapter | 261 |
| 23.1.2 What You Need to Know About VoIP | 261 |
| 23.2 Before You Begin | 262 |
| 23.3 The SIP Account Screen | 262 |
| 23.3.1 The SIP Account Add/Edit Screen | 263 |
| 23.4 The SIP Service Provider Screen | 267 |
| 23.4.1 The SIP Service Provider Add/Edit Screen | 268 |
| 23.5 The Phone Device Screen | 272 |
| 23.5.1 The Phone Device Edit Screen | 273 |
| 23.6 The Phone Region Screen | 274 |
| 23.7 The Call Rule Screen | 275 |
| 23.8 The Call History Screen | 276 |
| 23.9 The Call Summary Screen | 277 |
| 23.10 Technical Reference | 278 |
| 23.10.1 Quality of Service (QoS) | 286 |
| 23.10.2 Phone Services Overview | 286 |

| | |
|--|------------|
| Chapter 24 | |
| Log | 291 |
| 24.1 Log Overview | 291 |
| 24.1.1 What You Can Do in this Chapter | 291 |
| 24.1.2 What You Need To Know | 291 |
| 24.2 The System Log Screen | 292 |
| 24.3 The Security Log Screen | 292 |
| Chapter 25 | |
| Traffic Status | 294 |
| 25.1 Traffic Status Overview | 294 |
| 25.1.1 What You Can Do in this Chapter | 294 |
| 25.2 The WAN Status Screen | 294 |
| 25.3 The LAN Status Screen | 295 |
| 25.4 The NAT Status Screen | 296 |
| Chapter 26 | |
| VoIP Status | 298 |
| 26.1 VoIP Status Overview | 298 |
| Chapter 27 | |
| ARP Table | 301 |
| 27.1 ARP Table Overview | 301 |
| 27.1.1 How ARP Works | 301 |
| 27.2 ARP Table Screen | 302 |
| Chapter 28 | |
| Routing Table | 303 |
| 28.1 Routing Table Overview | 303 |
| 28.2 The Routing Table Screen | 303 |
| Chapter 29 | |
| Multicast Status | 305 |
| 29.1 Multicast Status Overview | 305 |
| 29.2 The IGMP Status Screen | 305 |
| 29.3 The MLD Status Screen | 306 |
| Chapter 30 | |
| xDSL Statistics | 307 |
| 30.1 xDSL Statistics Overview | 307 |
| Chapter 31 | |
| WLAN Station Status | 309 |

| | |
|---|------------|
| 31.1 WLAN Station Status Overview | 309 |
| Chapter 32 | |
| Cellular Statistics | 311 |
| 32.1 Cellular Statistics Overview | 311 |
| 32.2 The Cellular Statistics Screen | 311 |
| Chapter 33 | |
| System..... | 313 |
| 33.1 System Overview | 313 |
| 33.2 The System Screen | 313 |
| Chapter 34 | |
| User Account..... | 314 |
| 34.1 User Account Overview | 314 |
| 34.2 The User Account Screen | 314 |
| 34.2.1 The User Account Add/Edit Screen | 315 |
| Chapter 35 | |
| Remote Management..... | 317 |
| 35.1 Remote Management Overview | 317 |
| 35.2 The MGMT Services Screen | 317 |
| 35.3 The Trust Domain Screen | 318 |
| 35.4 The Add Trust Domain Screen | 319 |
| Chapter 36 | |
| SNMP | 320 |
| 36.1 SNMP Overview | 320 |
| 36.2 The SNMP Screen | 321 |
| Chapter 37 | |
| Time Settings..... | 323 |
| 37.1 Time Settings Overview | 323 |
| 37.2 The Time Screen | 323 |
| Chapter 38 | |
| E-mail Notification | 325 |
| 38.1 E-mail Notification Overview | 325 |
| 38.2 The Email Notification Screen | 325 |
| 38.2.1 Email Notification Edit | 326 |
| Chapter 39 | |
| Log Setting | 327 |

| | |
|--|------------|
| 39.1 Logs Setting Overview | 327 |
| 39.2 The Log Settings Screen | 327 |
| 39.2.1 Example E-mail Log | 329 |
| Chapter 40 | |
| Firmware Upgrade | 331 |
| 40.1 Firmware Upgrade Overview | 331 |
| 40.2 The Firmware Screen | 331 |
| Chapter 41 | |
| Backup Restore | 334 |
| 41.1 Backup Restore Overview | 334 |
| 41.2 The Backup Restore Screen | 334 |
| 41.3 The Reboot Screen | 336 |
| Chapter 42 | |
| Diagnostic | 337 |
| 42.1 Diagnostic Overview | 337 |
| 42.1.1 What You Can Do in this Chapter | 337 |
| 42.2 What You Need to Know | 337 |
| 42.3 Ping & TraceRoute & Nslookup | 338 |
| 42.4 The 802.1ag (CFM) Screen | 339 |
| 42.5 The 802.3ah (OAM) Screen | 340 |
| 42.6 The OAM Ping Screen | 341 |
| Chapter 43 | |
| Troubleshooting | 343 |
| 43.1 Power, Hardware Connections, and LEDs | 343 |
| 43.2 Zyxel Device Access and Login | 344 |
| 43.3 Internet Access | 345 |
| 43.4 Wireless Internet Access | 347 |
| 43.5 USB Device Connection | 348 |
| 43.6 UPnP | 348 |
| Part III: Appendices | 349 |
| Appendix A Customer Support | 350 |
| Appendix B Wireless LANs | 356 |
| Appendix C IPv6 | 369 |
| Appendix D Services | 377 |

Appendix E Legal Information 381

Index389

PART I

User's Guide

CHAPTER 1

Introducing the Zyxel Device

1.1 Overview

The Zyxel Device is a wireless VDSL router and Gigabit Ethernet gateway.

Zyxel Device refers to these models as outlined below.

- VMG1312-B10D
- VMG3312-T20A
- VMG3625-T20A
- VMG3925-B10B
- VMG3925-B10C
- XMG3927-B50A
- VMG3927-Bx0A
- VMG8823-Bx0B
- VMG8825-Bx0A
- VMG8924-B10D

The following table describes the feature differences of the Zyxel Device by model.

Table 1 Zyxel Device Comparison Table

| | VMG1312-B10D | VMG3312-T20A | VMG3625-T20A | VMG3925-B10B | VMG3925-B10C |
|------------------------|--------------|--------------|--------------|--------------|--------------|
| Gigabit Ethernet Ports | - | V | V | V | V |
| 2.4G WLAN | V | V | V | V | V |
| 5G WLAN | - | - | V | V | V |
| G.fast | - | - | - | - | - |
| VoIP | - | - | - | - | - |

Table 2 Zyxel Device Comparison Table

| | XMG3927-B50A | VMG3927-BX0A | VMG8823-BX0B | VMG8825-BX0A | VMG8924-B10D |
|------------------------|--------------|--------------|--------------|--------------|--------------|
| Gigabit Ethernet Ports | V | V | V | V | V |
| 2.4G WLAN | V | V | V | V | V |
| 5G WLAN | V | V | V | V | V |
| G.fast | V | - | - | - | - |
| VoIP | - | - | V | V | V |

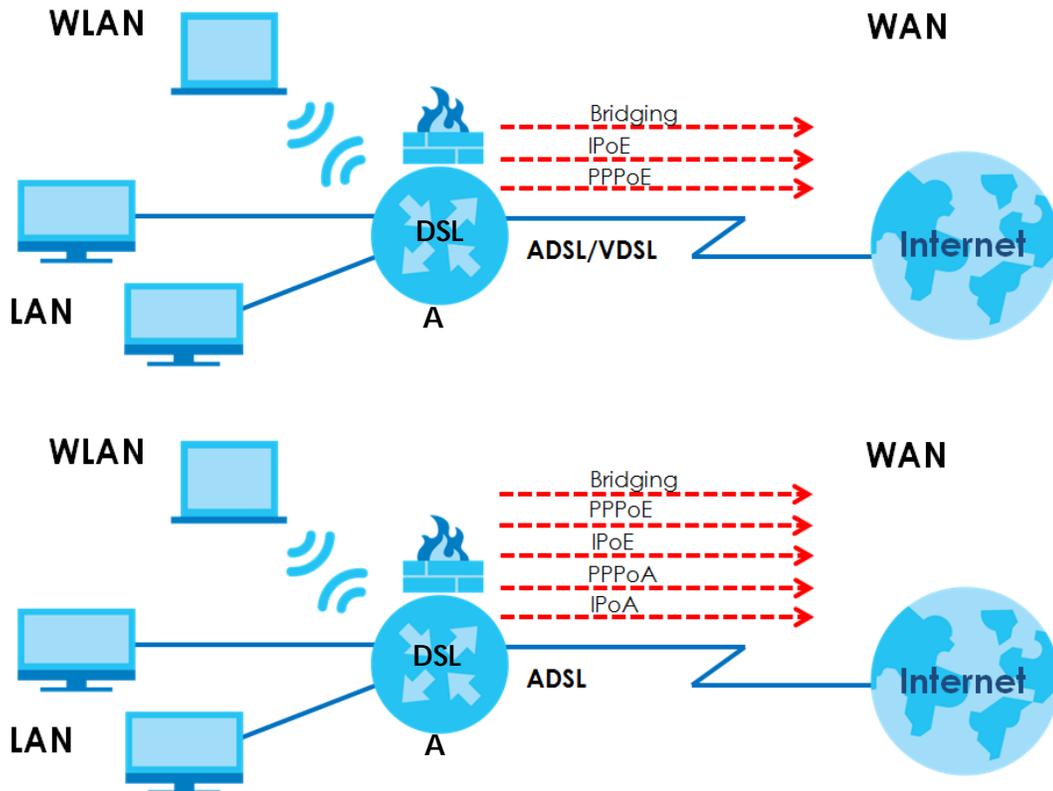
1.1.1 Internet Access

Your Zyxel Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. You can have multiple WAN services over one ADSL or VDSL. The Zyxel Device cannot work in ADSL and VDSL mode at the same time.

Note: The ADSL and VDSL lines share the same WAN (layer-2) interfaces that you configure in the Zyxel Device. Refer to [Section 6.2 on page 97](#) for the **Network Setting > Broadband** screen.

Computers can connect to the Zyxel Device's LAN ports (or wirelessly).

Figure 1 Zyxel Device's Internet Access Application



You can also configure IP filtering on the Zyxel Device for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

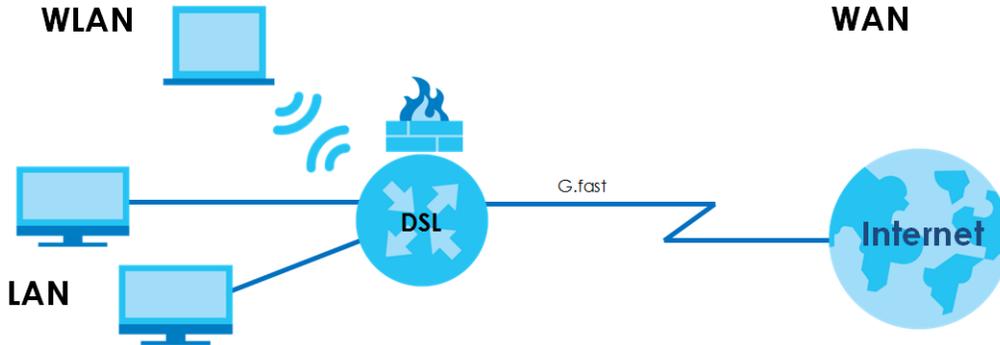
Only use firmware for your Zyxel Device's specific model. Refer to the label on the bottom of your Zyxel Device.

1.1.2 G.fast

You can have gigabit Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack for G.fast.

G.FAST is the acronym for Fast Access to Subscriber Terminals, and the letter G stands for the ITU-T G series of recommendations. G.fast is a technology providing gigabit speeds over traditional copper twisted-pair wires. G.fast applies Fiber-To-The-distribution point (FTTdp) structure, which reuses the deployed copper wire for the final meters.

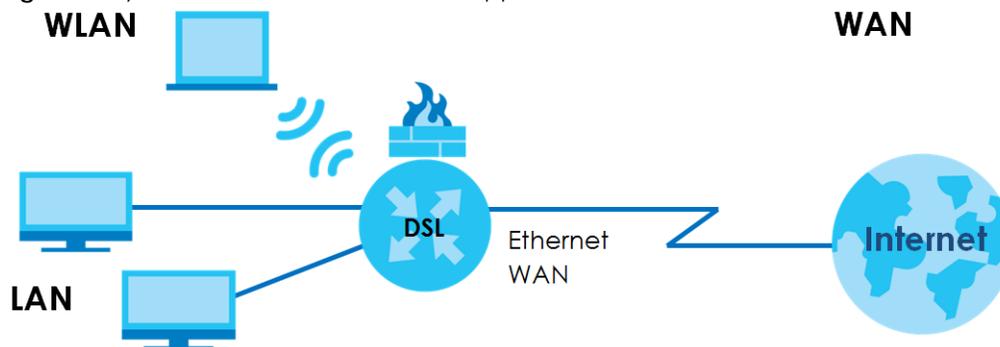
Figure 2 Zyxel Device's Internet Access Application: G.fast



1.1.3 Ethernet WAN

If you prefer not to use a DSL line and you have another broadband modem or router (such as ADSL) available, you can use the Ethernet WAN port and then connect it to the broadband modem or router. This way, you can access the Internet via an Ethernet connection and still use the QoS, Firewall and parental control functions on the Zyxel Device.

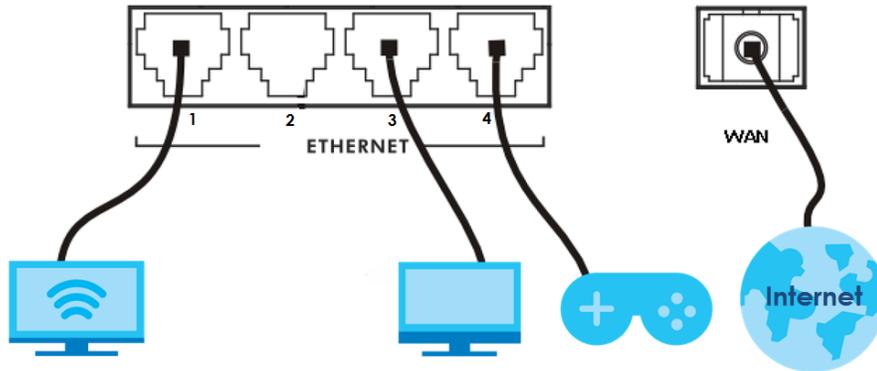
Figure 3 Zyxel Device's Internet Access Application: Ethernet WAN



1.1.4 Triple Play

The ISP may provide "triple play" service to the Zyxel Device. This allows you to take advantage of "triple play" services such as Voice over IP telephony, and streaming video/audio media all at the same time, with no noticeable loss in bandwidth.

Figure 4 Triple Play Example



1.1.5 WAN Priority

The WAN connection priority is as follows:

- 1 Ethernet WAN
 - 2 G.fast/DSL
 - 3 Cellular WAN (3G/4G)
- See [Section 1.1.7 on page 21](#) for more information about Cellular backup.

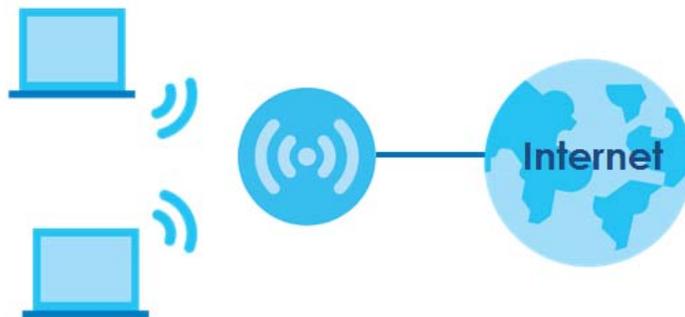
1.1.6 Wireless Access

The Zyxel Device is a wireless Access Point (AP) for IEEE 802.11b/g/n/a/ac wireless clients, such as notebook computers, iPads, smartphones, etc. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables.

Your Zyxel Device supports Wi-Fi Protected Setup (WPS), which allows you to quickly set up a wireless network with strong security.

See [Section 1.5.1 on page 32](#) for more information about how to set up a wireless network with WLAN and WPS buttons.

Figure 5 Wireless Access Example



1.1.7 Zyxel Device's USB Support

The USB port of the Zyxel Device is used for cellular WAN backup, file-sharing, and media server.

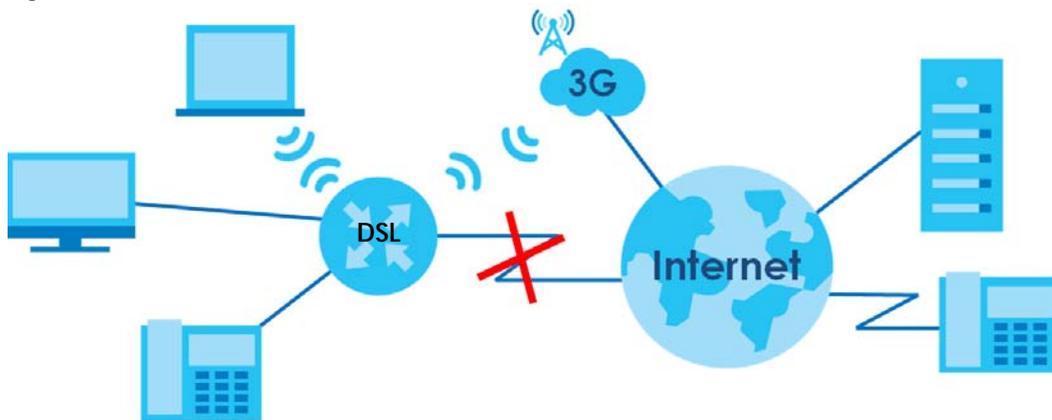
Cellular WAN (3G/4G) Backup

Connect a supported cellular USB dongle with an active SIM card to the USB port. This adds a second WAN interface and allows the Zyxel Device to wirelessly access the Internet via a cellular network. The cellular WAN connection is a backup in case the DSL connection fails.

To set up a cellular connection, click **Network > Broadband > Cellular Backup**.

To update the supported cellular USB dongle list, download the latest WWAN package from the Zyxel website and upload it to the Zyxel Device using the **Maintenance > Firmware Upgrade** screen.

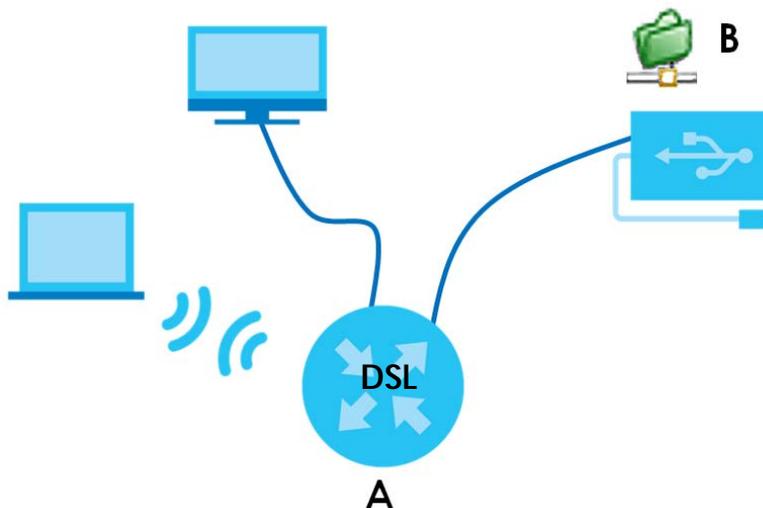
Figure 6 Internet Access Application: Cellular WAN



File Sharing

Use the built-in USB 3.0 port to share files on a USB memory stick or a USB hard drive (B). Use FTP to access the files on the USB device.

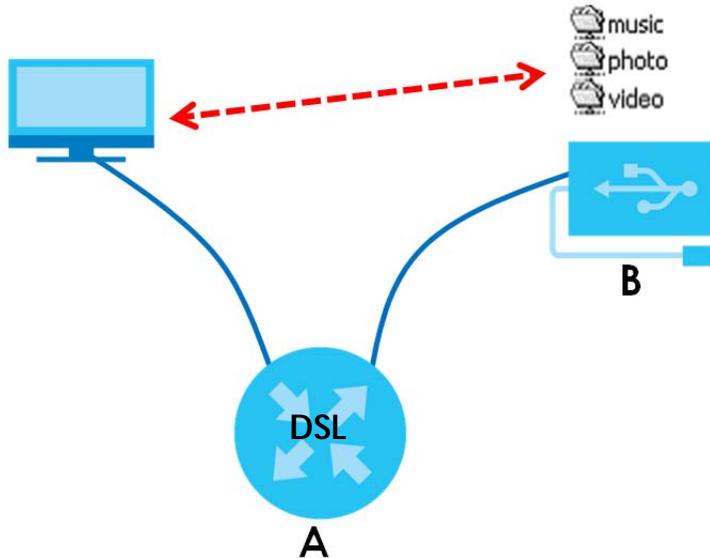
Figure 7 USB File Sharing Application



Media Server

You can also use the Zyxel Device as a media server. This lets anyone on your network play video, music, and photos from a USB device (B) connected to the Zyxel Device's USB port (without having to copy them to another computer).

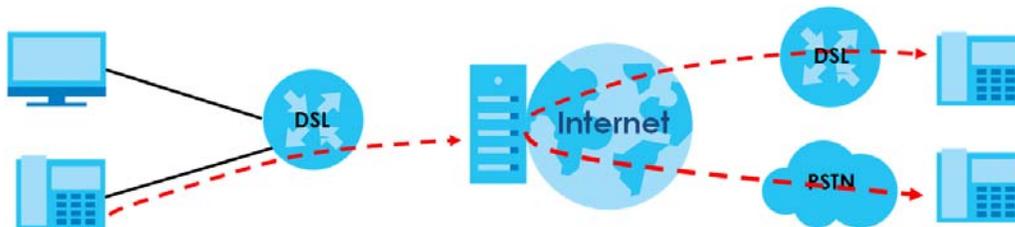
Figure 8 USB Media Server Application



1.1.8 VoIP Features

You can register up to 2 SIP (Session Initiation Protocol) accounts and use the Zyxel Device to make and receive VoIP telephone calls:

Figure 9 Zyxel Device's VoIP Features



Calls via a VoIP service provider - the Zyxel Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

1.2 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.
- FTP. Use FTP for firmware upgrades and configuration backup/restore.

1.3 Good Habits for Managing the Zyxel Device

Do the following things regularly to make the Zyxel Device more secure and to manage the Zyxel Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Zyxel Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Zyxel Device. You could simply restore your last configuration.

1.4 Hardware

Refer to the Zyxel Device's Quick Start Guides to see the product drawings and how to make the hardware connections.

The following table describes the items on the panels.

Table 3 Panel Ports and Buttons

| LABEL | DESCRIPTION |
|-----------------|--|
| WLAN | Press the WLAN button for more than one second to enable the wireless function. |
| WPS | Press the WPS button for more than one second to quickly set up a secure wireless connection between the device and a WPS-compatible client. |
| USB | The USB port is used for cellular WAN backup, file-sharing, media server, and print server. |
| DSL | Connect a RJ-11 cable to the DSL port for Internet access. |
| PHONE1 ~ PHONE2 | Connect analog phones to the phone ports to make phone calls. |
| LAN1 ~ LAN4 | Connect computers or other Ethernet devices to Ethernet ports for Internet access. |
| WAN | Connect an Ethernet cable to the Ethernet WAN port for Internet access. |
| Power | Connect the power cable can press the power button to start the device. |
| Reset | Press the button to return the Zyxel Device to the factory defaults. |

1.5 LEDs (Lights)

None of the LEDs are on if the Zyxel Device is not receiving power.

Table 4 VMG1312-B10D LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|-------------|-------|----------|--|
| POWER | Green | On | The Zyxel Device is receiving power and ready for use. |
| | | Blinking | The Zyxel Device is self-testing. |
| | Red | On | The Zyxel Device detected an error while self-testing, or there is a device malfunction. |
| | | Off | The Zyxel Device is not receiving power. |
| DSL | Green | On | The DSL line is up. |
| | | Blinking | The Zyxel Device is initializing the DSL line. |
| | | Off | The DSL line is down. |
| INTERNET | Green | On | The Zyxel Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The Zyxel Device is sending or receiving IP traffic. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | Red | On | The Zyxel Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| ETHERNET1~4 | Green | On | The Zyxel Device has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the LAN at 10/100 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the LAN. |
| WLAN/WPS | Green | On | The wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with wireless clients. |
| | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a wireless client. |
| | | Off | The wireless network is not activated. |
| USB | Green | On | The Zyxel Device recognizes a USB connection through the USB slot. |
| | | Blinking | The Zyxel Device is sending/receiving data to/from the USB device connected to it. |
| | | Off | The Zyxel Device does not detect a USB connection through the USB slot. |

Table 5 VMG3312-T20A LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|-------|-------|----------|--|
| POWER | Green | On | The Zyxel Device is receiving power and ready for use. |
| | | Blinking | The Zyxel Device is self-testing. |
| | Red | On | The Zyxel Device detected an error while self-testing, or there is a device malfunction. |
| | | Off | The Zyxel Device is not receiving power. |

Table 5 VMG3312-T20A LED Descriptions (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|-------------|--------|---------------|--|
| ETHERNET1~4 | Green | On | The Zyxel Device has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the LAN at 10/100 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the LAN. |
| WLAN | Green | On | The wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with wireless clients. |
| WPS | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a wireless client. |
| | | Off | The wireless network is not activated. |
| DSL | Green | On | The VDSL line is up. |
| | | Blinking | The Zyxel Device is initializing the VDSL line. |
| | | Off | The DSL line is down. |
| | Orange | On | The ADSL line is up. |
| | | Slow Blinking | The Zyxel Device is detecting carrier signals. |
| | | Fast Blinking | The Zyxel Device is initializing the VDSL line. |
| WAN | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the WAN at 10/100/1000 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the WAN. |
| INTERNET | Green | On | The Zyxel Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server). PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The VMG is sending or receiving IP traffic. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | Red | On | The VMG attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| USB | Green | On | The Zyxel Device recognizes a USB connection through the USB slot. |
| | | Blinking | The Zyxel Device is sending/receiving data to/from the USB device connected to it. |
| | | Off | The Zyxel Device does not detect a USB connection through the USB slot. |

Table 6 VMG3625-T20A LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|-------|-------|----------|--|
| POWER | Green | On | The Zyxel Device is receiving power and ready for use. |
| | | Blinking | The Zyxel Device is self-testing. |
| | Red | On | The Zyxel Device detected an error while self-testing, or there is a device malfunction. |
| | | Blinking | The Zyxel Device is upgrading firmware. |
| | | Off | The Zyxel Device is not receiving power. |

Table 6 VMG3625-T20A LED Descriptions (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|-------------|--------|---------------|--|
| DSL | Green | On | The VDSL line is up. |
| | | Blinking | The Zyxel Device is initializing the VDSL line. |
| | | Off | The DSL line is down. |
| | Orange | On | The ADSL line is up. |
| | | Slow Blinking | The Zyxel Device is detecting carrier signals. |
| | | Fast Blinking | The Zyxel Device is initializing the ADSL line. |
| INTERNET | Green | On | The Zyxel Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server). PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The VMG is sending or receiving IP traffic. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | Red | On | The VMG attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| WAN | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the WAN at 10/100/1000 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the WAN. |
| ETHERNET1~4 | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the LAN at 10/100 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the LAN. |
| WLAN | Green | On | The wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with wireless clients. |
| | | Off | The wireless network is not activated or down. |
| | Orange | Blinking | The Zyxel Device is setting up a WPS connection with a 2.4 GHz or 5 GHz wireless client. |
| USB | Green | On | The Zyxel Device recognizes a USB connection through the USB slot. |
| | | Blinking | The Zyxel Device is sending/receiving data to/from the USB device connected to it. |
| | | Off | The Zyxel Device does not detect a USB connection through the USB slot. |

Table 7 VMG3925-B10B LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|-------|-------|----------|--|
| Power | Green | On | The Zyxel Device is receiving power and ready for use. |
| | | Blinking | The Zyxel Device is self-testing. |
| | Red | On | The Zyxel Device detected an error while self-testing, or there is a device malfunction. |
| | | Off | The Zyxel Device is not receiving power. |

Table 7 VMG3925-B10B LED Descriptions (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|---------------|--------|----------|--|
| DSL | Green | On | The VDSL line is up. |
| | | Blinking | The Zyxel Device is initializing the VDSL line. |
| | Orange | On | The ADSL line is up. |
| | | Blinking | The Zyxel Device is initializing the ADSL line. |
| | | Off | The DSL line is down. |
| Internet | Green | On | The Zyxel Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The Zyxel Device is sending or receiving IP traffic. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | Red | On | The Zyxel Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| Ethernet WAN | Green | On | The Zyxel Device has a successful 1000 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the WAN at 1000 Mbps. |
| | Orange | On | The Zyxel Device has a successful 10/100 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the WAN at 10/100 Mbps. |
| | | Off | There is no Ethernet connection on the WAN. |
| LAN1~4 | Green | On | The Zyxel Device has a successful 1000 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the LAN at 1000 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the LAN. |
| 2.4G WLAN/WPS | Green | On | The 2.4 GHz wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with 2.4 GHz wireless clients. |
| | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a 2.4 GHz wireless client. |
| | | Off | The 2.4 GHz wireless network is not activated. |
| 5G WLAN/WPS | Green | On | The 5 GHz wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with 5 GHz wireless clients. |
| | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a 5 GHz wireless client. |
| | | Off | The 5 GHz wireless network is not activated. |
| USB1 | Green | On | The Zyxel Device recognizes a USB connection through the USB1 slot. |
| | | Blinking | The Zyxel Device is sending/receiving data to /from the USB device connected to it. |
| | | Off | The Zyxel Device does not detect a USB connection through the USB1 slot. |

Table 8 VMG3925-B10C LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|-------------------|-------|-----------------|--|
| Power | Green | On | The Zyxel Device is receiving power and ready for use. |
| | | Blinking | The Zyxel Device is self-testing. |
| | Red | On | The Zyxel Device detected an error while self-testing, or there is a device malfunction. |
| | | Blinking | The Zyxel Device is uploading firmware. |
| | | Off | The Zyxel Device is not receiving power. |
| DSL | Green | On | The VDSL line is up. |
| | | Blinking (slow) | The Zyxel Device is looking for a VDSL line. |
| | | Blinking (fast) | The Zyxel Device is initializing the VDSL line. |
| | Amber | On | The ADSL line is up. |
| | | Blinking (slow) | The Zyxel Device is looking for an ADSL line. |
| | | Blinking (fast) | The Zyxel Device is initializing the ADSL line. |
| | | Off | The DSL line is down. |
| Internet | Green | On | The Zyxel Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The Zyxel Device is sending or receiving IP traffic. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | Red | On | The Zyxel Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| WAN | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the WAN at 10/100/1000 Mbps. |
| | | Off | There is no Ethernet connection on the WAN. |
| LAN1~4 | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the LAN at 10/100/1000 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the LAN. |
| 2.4G WLAN/ WPS | Green | On | The 2.4 GHz wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with 2.4 GHz wireless clients. |
| | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a 2.4 GHz wireless client. |
| | | Off | The 2.4 GHz wireless network is not activated. |
| 5G WLAN/ WPS | Green | On | The 5 GHz wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with 5 GHz wireless clients. |
| | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a 5 GHz wireless client. |
| | | Off | The 5 GHz wireless network is not activated. |

Table 8 VMG3925-B10C LED Descriptions (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|-----|-------|----------|---|
| USB | Green | On | The Zyxel Device recognizes a USB connection through the USB1 slot. |
| | | Blinking | The Zyxel Device is sending/receiving data to /from the USB device connected to it. |
| | | Off | The Zyxel Device does not detect a USB connection through the USB1 slot. |

Table 9 XMG3927-B50A/VMG3927-BX0A/VMG8825-BX0A LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|---------------|-------|--|---|
| POWER | Blue | On | The Zyxel Device is receiving power and ready for use. |
| | | Blinking | The Zyxel Device is self-testing. |
| | Red | On | The Zyxel Device detected an error while self-testing, or there is a device malfunction. |
| | | Blinking | The Zyxel Device is uploading firmware. |
| | Off | The Zyxel Device is not receiving power. | |
| WAN | Blue | On | One of the following connections is up. <ul style="list-style-type: none"> • ADSL • G.fast • VDSL • Ethernet connection on the WAN. |
| | | Blinking (slow) | The ADSL/G.fast/VDSL link is down, and the Zyxel Device is looking for an ADSL/G.fast/VDSL link. |
| | | Blinking (fast) | The Zyxel Device is initializing the ADSL/G.fast/VDSL link. |
| | | Off | There is no Ethernet connection on the WAN. |
| INTERNET | Blue | On | Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The Zyxel Device is sending or receiving IP traffic. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | Red | On | The Zyxel Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| ETHERNET1~4 | Blue | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the LAN at 10/100/1000 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the LAN. |
| 2.4G WLAN/WPS | Blue | On | The 2.4 GHz wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with 2.4 GHz wireless clients. |
| | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a 2.4 GHz wireless client. |
| | | Off | The 2.4 GHz wireless network is not activated. |
| 5G WLAN/WPS | Blue | On | The 5 GHz wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with 5 GHz wireless clients. |
| | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a 5 GHz wireless client. |
| | | Off | The 5 GHz wireless network is not activated. |

Table 10 VMG8823-BX0B LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|----------|--------|---------------|--|
| Power | Green | On | The Zyxel Device is receiving power and ready for use. |
| | | Blinking | The Zyxel Device is self-testing. |
| | Red | On | The Zyxel Device detected an error while self-testing, or there is a device malfunction. |
| | | Blinking | The VMG is upgrading firmware. |
| | | Off | The Zyxel Device is not receiving power. |
| DSL | Green | On | The VDSL line is up. |
| | | Slow Blinking | The Zyxel Device is detecting carrier signals. |
| | | Fast Blinking | The Zyxel Device is initializing the VDSL line. |
| | Orange | On | The ADSL line is up. |
| | | Slow Blinking | The Zyxel Device is detecting carrier signals. |
| | | Fast Blinking | The Zyxel Device is initializing the ADSL line. |
| | | Off | The DSL line is down. |
| Internet | Green | On | The Zyxel Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The Zyxel Device is sending or receiving IP traffic. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | Red | On | The Zyxel Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| WAN | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the WAN at 10/100/1000 Mbps. |
| | | Off | There is no Ethernet connection on the WAN. |
| LAN1~4 | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the LAN at 10/100/1000 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the LAN. |
| WLAN/WPS | Green | On | The 2.4 GHz or 5 GHz wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with 2.4 GHz or 5 GHz wireless clients. |
| | Amber | Blinking | The Zyxel Device is setting up a WPS connection with a 2.4 GHz or 5 GHz wireless client. |
| | | Off | The 2.4 GHz or 5 GHz wireless network is not activated. |

Table 10 VMG8823-BX0B LED Descriptions (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|-------------------|--------|----------|---|
| Phone1, Phone2 | Green | On | A SIP account is registered for the phone port. |
| | | Blinking | A telephone connected to the phone port has its receiver off of the hook or there is an incoming call. |
| | Orange | On | A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account. |
| | | Blinking | A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account. |
| | | Off | The phone port does not have a SIP account registered. |
| USB | Green | On | The Zyxel Device recognizes a USB connection through the USB slot. |
| | | Blinking | The Zyxel Device is sending/receiving data to /from the USB device connected to it. |
| | | Off | The Zyxel Device does not detect a USB connection through the USB slot. |

Table 11 VMG8924-B10D LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|----------|--------|---------------|--|
| Power | Green | On | The Zyxel Device is receiving power and ready for use. |
| | | Blinking | The Zyxel Device is self-testing. |
| | Red | On | The Zyxel Device detected an error while self-testing, or there is a device malfunction. |
| | | Blinking | The VMG is upgrading firmware. |
| | | Off | The Zyxel Device is not receiving power. |
| DSL | Green | On | The VDSL line is up. |
| | | Slow Blinking | The Zyxel Device is detecting carrier signals. |
| | | Fast Blinking | The Zyxel Device is initializing the VDSL line. |
| | Orange | On | The ADSL line is up. |
| | | Slow Blinking | The Zyxel Device is detecting carrier signals. |
| | | Fast Blinking | The Zyxel Device is initializing the ADSL line. |
| | | Off | The DSL line is down. |
| Internet | Green | On | The Zyxel Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up. |
| | | Blinking | The Zyxel Device is sending or receiving IP traffic. |
| | | Off | There is no Internet connection or the gateway is in bridged mode. |
| | Red | On | The Zyxel Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. |
| WAN | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection on the WAN. |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the WAN at 10/100/1000 Mbps. |
| | | Off | There is no Ethernet connection on the WAN. |

Table 11 VMG8924-B10D LED Descriptions (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|-------------------|--------|----------|---|
| LAN1~4 | Green | On | The Zyxel Device has a successful 10/100/1000 Mbps Ethernet connection with a device on the Local Area Network (LAN). |
| | | Blinking | The Zyxel Device is sending or receiving data to/from the LAN at 10/100/1000 Mbps. |
| | | Off | The Zyxel Device does not have an Ethernet connection with the LAN. |
| WLAN/WPS | Green | On | The 2.4 GHz or 5 GHz wireless network is activated. |
| | | Blinking | The Zyxel Device is communicating with 2.4 GHz or 5 GHz wireless clients. |
| | Orange | Blinking | The Zyxel Device is setting up a WPS connection with a 2.4 GHz or 5 GHz wireless client. |
| | | Off | The 2.4 GHz or 5 GHz wireless network is not activated. |
| Phone1, Phone2 | Green | On | A SIP account is registered for the phone port. |
| | | Blinking | A telephone connected to the phone port has its receiver off of the hook or there is an incoming call. |
| | Orange | On | A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account. |
| | | Blinking | A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account. |
| | | Off | The phone port does not have a SIP account registered. |
| USB | Green | On | The Zyxel Device recognizes a USB connection through the USB slot. |
| | | Blinking | The Zyxel Device is sending/receiving data to /from the USB device connected to it. |
| | | Off | The Zyxel Device does not detect a USB connection through the USB slot. |

1.5.1 Using the WLAN and WPS Buttons

If the wireless network is turned off, press the **WLAN** button. Check the **WLAN/WPS** LED on the front panel to see if the wireless network is active.

You can also use the **WPS** button to quickly set up a secure wireless connection between the Zyxel Device and a WPS-compatible client by adding one device at a time.

To activate WPS:

- 1 Make sure the **POWER** LED is on and not blinking.
- 2 Press the **WPS** button and release it.
- 3 Press the WPS button on another WPS-enabled device within range of the Zyxel Device. The **WLAN/WPS** LED flashes amber while the Zyxel Device sets up a WPS connection with the other wireless device.
- 4 Once the connection is successfully made, the **WLAN/WPS** LED shines blue or green.

Note: If your Zyxel Device supports both 2.4 GHz and 5 GHz wireless networks, the connection to the 2.4 GHz wireless network has priority.

To turn off the wireless network, press the **WLAN** button. The **WLAN/WPS** LED turns off when the wireless network is off.

See the following table to see how long you need to press the **WLAN** and **WPS** buttons on the Zyxel Device.

Table 12 WLAN and WPA Buttons

| MODEL | WLAN BUTTON | WPS BUTTON |
|--------------|-----------------------|------------------------|
| VMG1312-B10D | One second | Two seconds |
| VMG3312-T20A | More than two seconds | More than five seconds |
| VMG3625-T20A | More than two seconds | More than five seconds |
| VMG3925-B10B | Two seconds | Two seconds |
| VMG3925-B10C | More than two seconds | More than five seconds |
| XMG3927-B50A | More than one second | More than one second |
| VMG3927-Bx0A | More than one second | More than one second |
| VMG8823-Bx0B | More than two seconds | More than five seconds |
| VMG8825-Bx0A | More than one second | More than one second |
| VMG8924-B10D | More than two seconds | More than five seconds |

1.5.2 The RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to the factory default (see the device label), and the LAN IP address will be "192.168.1.1".

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

See the following table to see how long you need to press the **RESET** button on the Zyxel Device.

Table 13 RESET Button

| MODEL | RESET BUTTON |
|--------------|------------------------|
| VMG1312-B10D | One second |
| VMG3312-T20A | Five seconds |
| VMG3625-T20A | Five seconds |
| VMG3925-B10B | Ten seconds |
| VMG3925-B10C | More than five seconds |
| XMG3927-B50A | More than five seconds |
| VMG3927-Bx0A | More than five seconds |
| VMG8823-Bx0B | Five seconds |
| VMG8825-Bx0A | More than five seconds |
| VMG8924-B10D | Five seconds |

CHAPTER 2

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy Zyxel Device setup and management via Internet browser. Use Internet Explorer 8.0 and later versions or Mozilla Firefox 3 and later versions or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

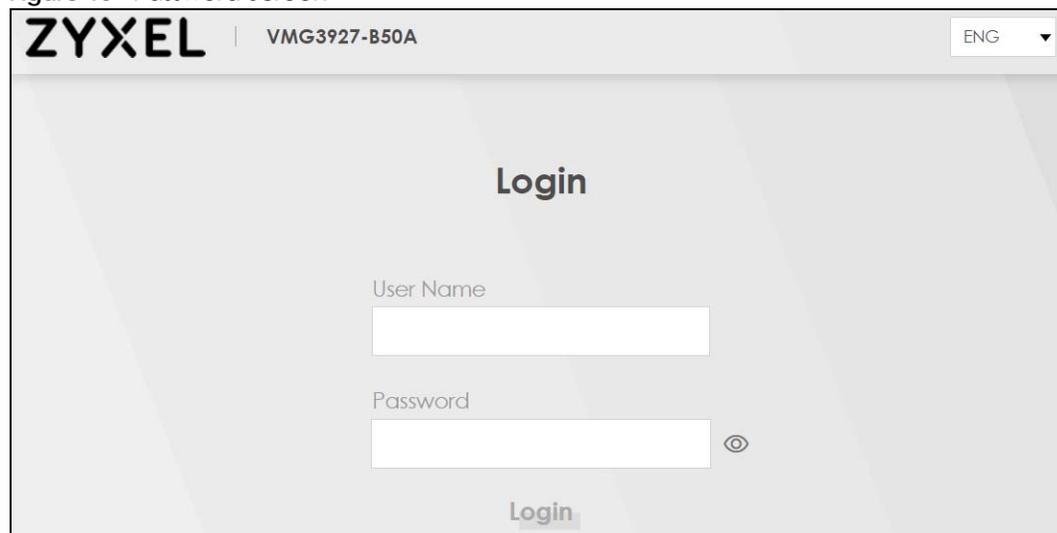
In order to use the web configurator you need to allow:

- Web browser pop-up windows from your Zyxel Device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.1.1 Accessing the Web Configurator

- 1 Make sure your Zyxel Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser. If the Zyxel Device does not automatically re-direct you to the login screen, go to <http://192.168.1.1>.
- 3 A password screen displays. Select the language you prefer.
- 4 To access the administrative web configurator and manage the Zyxel Device, type the default username **admin** and the randomly assigned default password (see the device label) in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 10 Password Screen



The screenshot displays the login interface of a Zyxel web configurator. At the top left, the 'ZYXEL' logo is visible next to the device model 'VMG3927-B50A'. A language selection dropdown menu is set to 'ENG'. The central heading is 'Login'. Below this, there are two text input fields: 'User Name' and 'Password'. To the right of the password field is an eye icon for toggling password visibility. At the bottom center, there is a 'Login' button.

- 5 The following screen displays when you log into the web configurator for the first time. Enter a new password, retype it to confirm, and click **Change password**. If you prefer to use the default password, click **Skip**.

Figure 11 Change Password Screen

ZYXEL | VMG3927-B50A

Password Reset

New Password

Password

Change password
[Skip](#)

- 6 The **Wizard** screen displays when you log into the web configurator for the first time. Use the **Wizard** screens to configure the Zyxel Device's time zone, basic Internet access, and wireless settings. See [Chapter 3 on page 42](#) for more information about the **Wizard** screens.
- 7 The **Connection Status** page appears. Use this screen to configure basic Internet access, wireless settings, and parental control settings.

Figure 12 Connection Status

Connectivity

System Info

| | |
|------------------|--------------------------------|
| Model Name | VMG3927-B50A |
| Firmware Version | V5.13(ABMT.0)b1 |
| System Uptime | 0 days 0 hours 35 mins 12 secs |
| LAN MAC Address | BC:99:11:60:9D:E4 |
| Ethernet WAN | 1000/Full |

WiFi Settings

| Band | WiFi Name | WiFi Password |
|------|------------|---------------|
| 2.4G | Zyxel_9DE5 | |
| 5G | Zyxel_9DE5 | |

Guest WiFi Settings

| Band | WiFi Name | WiFi Password |
|------|-------------------|---------------|
| 2.4G | Zyxel_9DE5_guest1 | |
| 5G | Zyxel_9DE5_guest1 | |

LAN

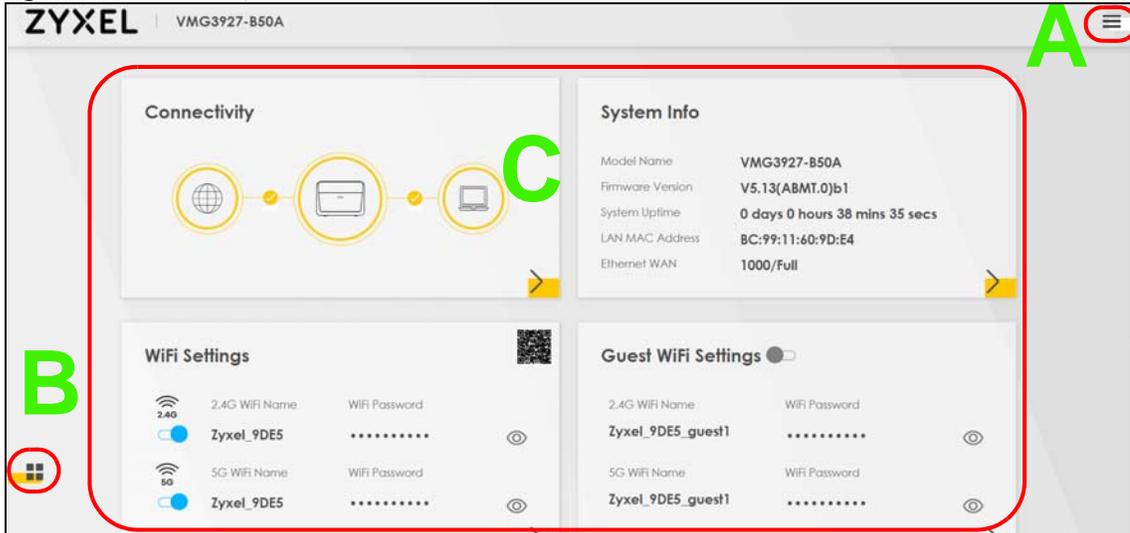
| | |
|------------------|-------------------------------------|
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| IP Address Range | 192.168.1.2 ~ 192.168.1.254 |
| DHCP | <input checked="" type="checkbox"/> |
| Lease Time | 1 days 0 hours 0 mins |

Parental Control

0 profile scheduled

2.2 Web Configurator Layout

Figure 13 Screen Layout



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

- A - Settings Icon (Navigation Panel & Side Bar)
- B - Widget Icon
- C - Main Window

2.2.1 Settings Icon

Click this icon (☰) to see the side bar and navigation panel.

2.2.1.1 Side Bar

The side bar provides some icons on the right hand side.



The icons provide the following functions.

Table 14 Web Configurator Icons in the Title Bar

| ICON | DESCRIPTION |
|--|---|
|  | Wizard: Click this icon to open screens where you can configure the Zyxel Device's time zone, Internet access, and wireless settings. See Chapter 3 on page 42 for more information about the Wizard screens. |
|  | Theme: Click this icon to select a color that you prefer and apply it to the web configurator. Network Temporarily Disconnected  |
|  | Language: Select the language you prefer. |
|  | Restart: Click this icon to reboot the Zyxel Device without turning the power off. |
|  | Logout: Click this icon to log out of the web configurator. |

2.2.1.2 Navigation Panel

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

Note: The menu items on the navigation panel vary among the models. See [Section 1.1 on page 17](#) for more information about the feature differences of the Zyxel Device .

Table 15 Navigation Panel Summary

| LINK | TAB | FUNCTION |
|-------------------|-----------------|--|
| Connection Status | | Use this screen to configure basic Internet access, wireless settings, and parental control settings. This screen also shows the network status of the Zyxel Device and computers/devices connected to it. |
| Network Setting | | |
| Broadband | Broadband | Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections. |
| | Cellular Backup | Use this screen to configure 3G WAN connection. |
| | Advanced | Use this screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions. |

Table 15 Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|-----------------|----------------------|--|
| Wireless | General | Use this screen to configure the wireless LAN settings and WLAN authentication/security settings. |
| | Guest/More AP | Use this screen to configure multiple BSSs on the Zyxel Device. |
| | MAC Authentication | Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the Zyxel Device. |
| | WPS | Use this screen to configure and view your WPS (Wi-Fi Protected Setup) settings. |
| | WMM | Use this screen to enable or disable Wi-Fi MultiMedia (WMM). |
| | Others | Use this screen to configure advanced wireless settings. |
| | Channel Status | Use this screen to scan wireless LAN channel noises and view the results. |
| | MESH | Use this screen to enable or disable Zyxel Mesh (Multy Pro). |
| | | |
| Home Networking | LAN Setup | Use this screen to configure LAN TCP/IP settings, and other advanced properties. |
| | Static DHCP | Use this screen to assign specific IP addresses to individual MAC addresses. |
| | UPnP | Use this screen to turn UPnP and UPnP NAT-T on or off. |
| | Additional Subnet | Use this screen to configure IP alias and public static IP. |
| | STB Vendor ID | Use this screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses. |
| | Wake on LAN | Use this screen to remotely turn on a device on the local network. |
| | TFTP Server Name | Use DHCP option 66 to identify a TFTP server name. |
| Routing | Static Route | Use this screen to view and set up static routes on the Zyxel Device. |
| | DNS Route | Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). |
| | Policy Route | Use this screen to configure policy routing on the Zyxel Device. |
| | RIP | Use this screen to configure Routing Information Protocol to exchange routing information with other routers. |
| QoS | General | Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions. |
| | Queue Setup | Use this screen to configure QoS queues. |
| | Classification Setup | Use this screen to define a classifier. |
| | Shaper Setup | Use this screen to limit outgoing traffic rate on the selected interface. |
| | Policer Setup | Use this screen to configure QoS policers. |
| NAT | Port Forwarding | Use this screen to make your local servers visible to the outside world. |
| | Port Triggering | Use this screen to change your Zyxel Device's port triggering settings. |
| | DMZ | Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen. |
| | ALG | Use this screen to enable or disable SIP ALG. |
| | Address Mapping | Use this screen to change your Zyxel Device's address mapping settings. |
| | Sessions | Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the Zyxel Device. |

Table 15 Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|--------------------|----------------------|---|
| DNS | DNS Entry | Use this screen to view and configure DNS routes. |
| | Dynamic DNS | Use this screen to allow a static hostname alias for a dynamic IP address. |
| IGMP/MLD | IGMP/MLD | Use this screen to configure multicast settings (IGMP for IPv4 and MLD for IPv6 multicast groups) on the WAN. |
| Vlan Group | Vlan Group | Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface. |
| Interface Grouping | Interface Grouping | Use this screen to map a port to a PVC or bridge group. |
| USB Service | File Sharing | Use this screen to enable file sharing via the Zyxel Device. |
| | Media Server | Use this screen to use the Zyxel Device as a media server. |
| | | |
| Home Connectivity | Home Connectivity | Use this screen to enable or disable Wi-Fi auto-configuration. |
| Security | | |
| Firewall | General | Use this screen to configure the security level of your firewall. |
| | Protocol | Use this screen to add Internet services and configure firewall rules. |
| | Access Control | Use this screen to enable specific traffic directions for network services. |
| | Dos | Use this screen to activate protection against Denial of Service (DoS) attacks. |
| MAC Filter | MAC Filter | Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device. |
| Parental Control | Parental Control | Use this screen to block web sites with the specific URL. |
| Scheduler Rule | Scheduler Rule | Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced. |
| Certificates | Local Certificates | Use this screen to view a summary list of certificates and manage certificates and certification requests. |
| | Trusted CA | Use this screen to view and manage the list of the trusted CAs. |
| VoIP | | |
| SIP | SIP Account | Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the Zyxel Device. |
| | SIP Service Provider | Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions, and dialing plan. |
| Phone | Phone | Use this screen to select your location and a call service mode. |
| | Region | Use this screen to select your location and a call service mode. |
| Call Rule | Call Rule | Use this screen to configure speed dial for SIP phone numbers that you call often. |
| Call History | Call History | Use this screen to view a call history list. |
| | Call Summary | Use this screen to view the summary of received, dialed and missed calls. |
| System Monitor | | |

Table 15 Navigation Panel Summary (continued)

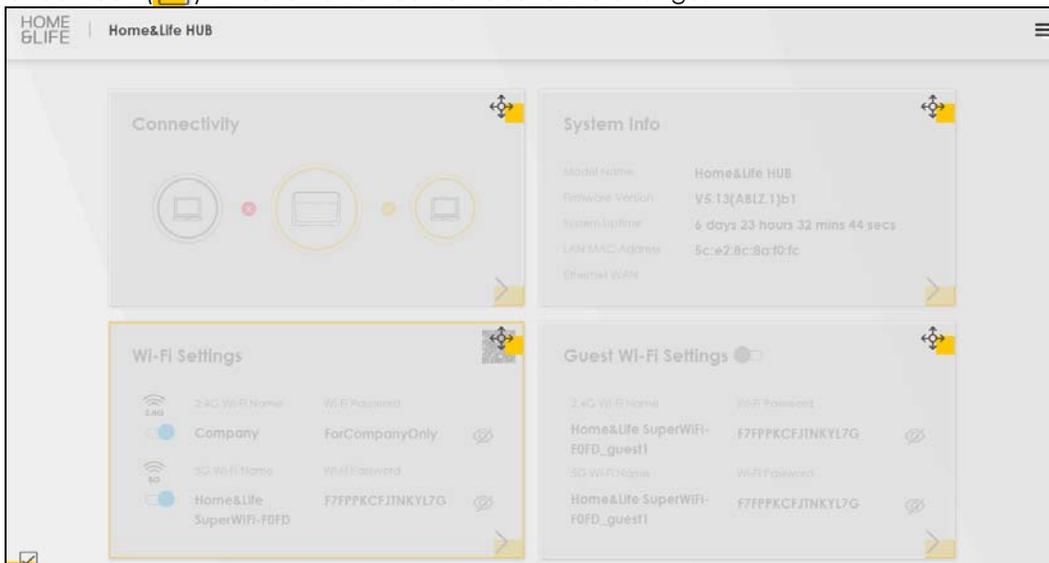
| LINK | TAB | FUNCTION |
|---------------------|---------------------|--|
| Log | System Log | Use this screen to view the status of events that occurred to the Zyxel Device. You can export or e-mail the logs. |
| | Security Log | Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window. Levels include: <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Categories include: <ul style="list-style-type: none"> • Account • Attack • Firewall • MAC Filter |
| Traffic Status | WAN | Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device. |
| | LAN | Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device. |
| | NAT | Use this screen to view NAT statistics for connected hosts. |
| VoIP Status | VoIP Status | Use this screen to view VoIP registration, current call status and phone numbers for the phone ports. |
| ARP table | ARP table | Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection. |
| Routing Table | Routing Table | Use this screen to view the routing table on the Zyxel Device. |
| Multicast Status | IGMP Status | Use this screen to view the status of all IGMP settings on the Zyxel Device. |
| | MLD Status | Use this screen to view the status of all MLD settings on the Zyxel Device. |
| xDSL Statistics | xDSL Statistics | Use this screen to view the VMG's xDSL traffic statistics. |
| WLAN Station Status | WLAN Station Status | Use this screen to view the wireless stations that are currently associated to the Zyxel Device. |
| Cellular Statistics | Cellular Statistics | Use this screen to look at cellular Internet connection status. |
| GPON Status | GPON Status | Use this screen to view real-time SFP (Small Form Factor Pluggable) transceiver information and operating parameters on the SFP port. |
| Maintenance | | |
| System | System | Use this screen to set Device name and Domain name. |
| User Account | User Account | Use this screen to change user password on the Zyxel Device. |
| Remote Management | MGMT Service | Use this screen to enable specific traffic directions for network services. |
| | Trust Domain | Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the Maintenance > Remote Management screen. |
| SNMP | SNMP | Use this screen to configure SNMP (Simple Network Management Protocol) settings. |
| Time | Time | Use this screen to change your Zyxel Device's time and date. |

Table 15 Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|--------------------|---------------------------|--|
| Email Notification | E-mail Notification | Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device. |
| Log Setting | Log Setting | Use this screen to change your Zyxel Device's log settings. |
| Firmware Upgrade | Firmware Upgrade | Use this screen to upload firmware to your Zyxel Device. |
| Backup/Restore | Backup/Restore | Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings. |
| Reboot | Reboot | Use this screen to reboot the Zyxel Device without turning the power off. |
| Diagnostic | Ping&Traceroute &Nslookup | Use this screen to identify problems with the DSL connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems. |
| | 802.1ag | Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports. |
| | 802.3ah | Use this screen to configure link OAM port parameters, |
| | OAM Ping | Use this screen to view information to help you identify problems with the DSL connection. |

2.2.2 Widget Icon

Click this icon () to arrange the screen order. Select a block and hold it to move around. Click the Check icon () in the lower left corner to save the changes.



CHAPTER 3

Quick Start

3.1 Overview

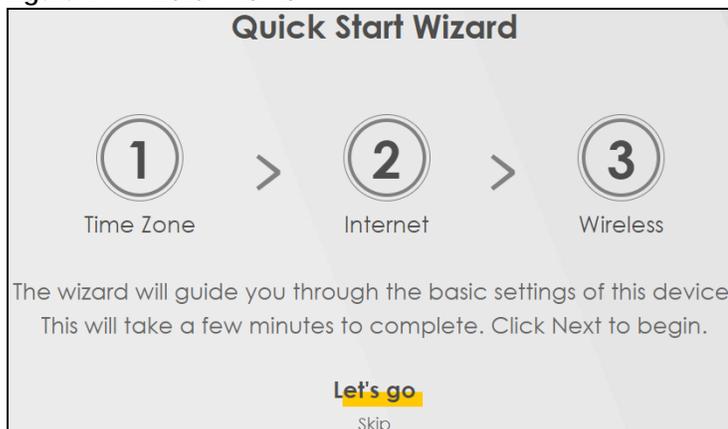
Use the **Wizard** screens to configure the Zyxel Device's time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on [Chapter 4 on page 48](#)) for background information on the features in this chapter.

3.2 Quick Start Setup

You can click the **Wizard** icon in the side bar to open the **Wizard** screens. See [Section 2.2.1.1 on page 36](#) for more information about side bar. After you click the **Wizard** icon, the following screen appears. Click **Let's Go** to proceed with settings on time zone, basic Internet access, and wireless networks. It will take you a few minutes to complete the settings on the **Wizard** screens. You can also click **Skip** to leave the **Wizard** screens.

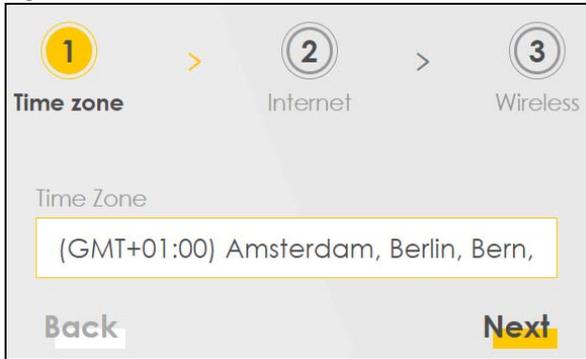
Figure 14 Wizard - Home



3.3 Time Zone

Select the time zone of your location. Click **Next**.

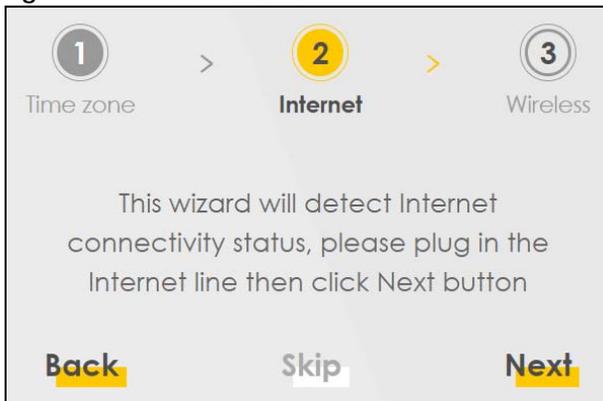
Figure 15 Wizard - Time Zone



3.4 Internet

Connect an Ethernet cable, a DSL cable, or a USB dongle for Internet access. See [Section 1.1.5 on page 20](#) for more information about WAN priority. The Zyxel Device will check the Internet status automatically, and determine your connection type. You can also click **Skip** to pass Internet settings in the **Wizard**.

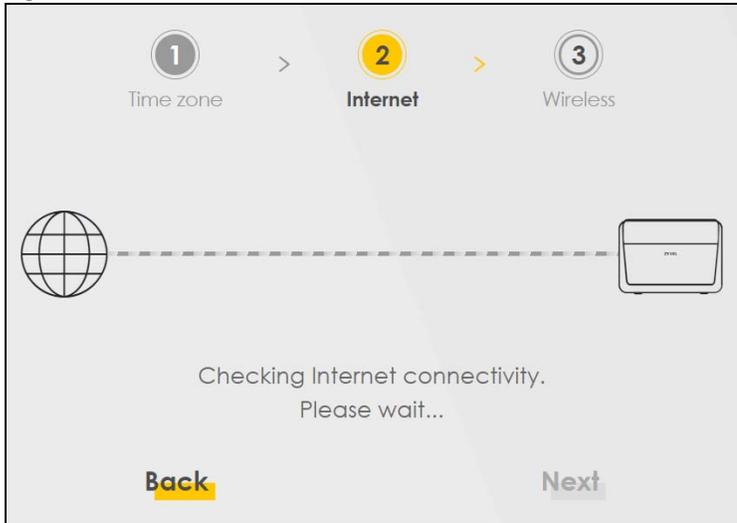
Figure 16 Wizard - Internet



3.4.1 Internet Status

The Zyxel Device is checking the Internet status. Click **Next**.

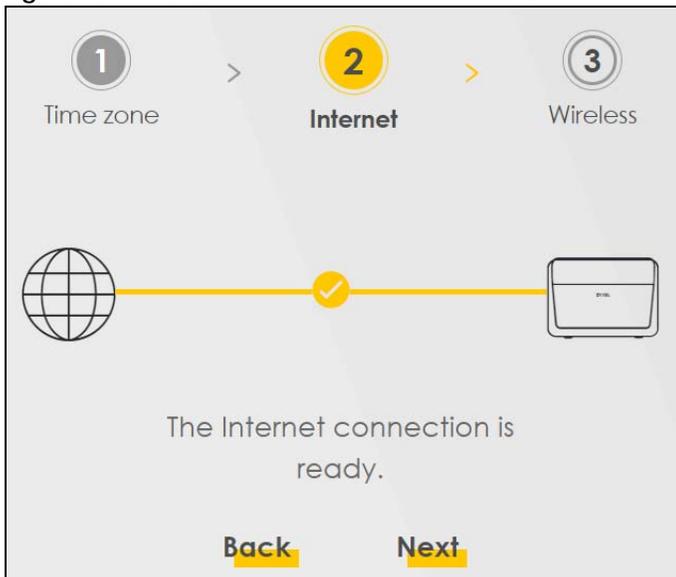
Figure 17 Wizard - Internet Check



3.4.2 Successful Internet Connection

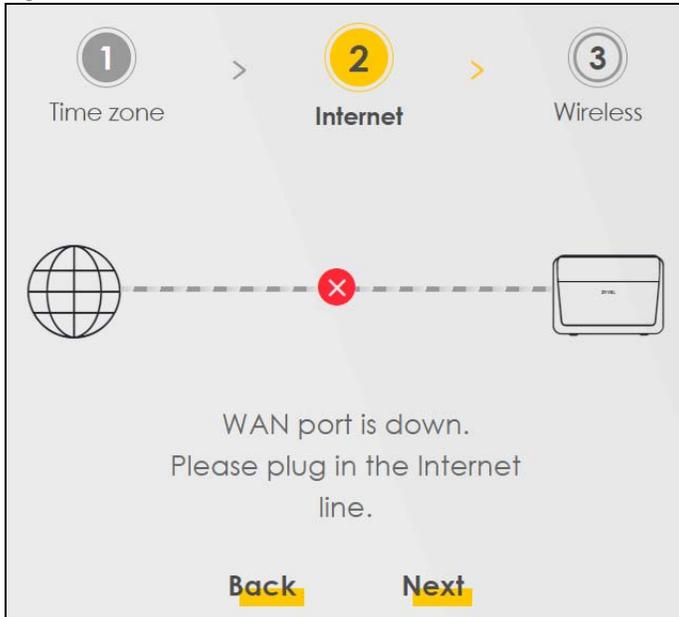
The Zyxel Device has Internet access.

Figure 18 Wizard - Successful WAN Connection



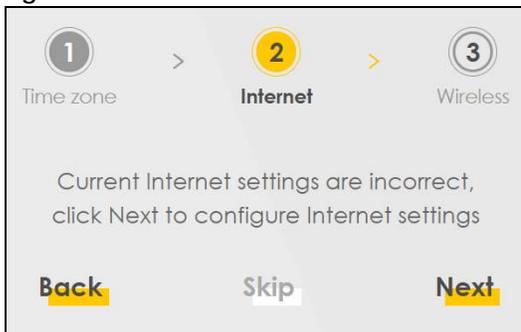
3.4.3 Unsuccessful Internet Connection

The Zyxel Device didn't detect a WAN connection. Connect an Ethernet cable, a DSL cable, or a USB dongle for Internet access if you haven't connected any.

Figure 19 Wizard - WAN Connection is Down

3.4.4 Incorrect Internet Information

The Internet connection information is incorrect. Click **Next** to configure the Internet settings.

Figure 20 Wizard - Incorrect Internet Information

3.4.5 Encapsulation

Select the encapsulation type your ISP uses.

Figure 21 Wizard - Incorrect Internet Information

The screenshot shows a three-step wizard. Step 1 is 'Time zone', step 2 is 'Internet' (highlighted in yellow), and step 3 is 'WiFi'. Below the steps, there is a section for 'Encapsulation' with a dropdown menu currently set to 'IPoE'. At the bottom, there are 'Back' and 'Next' buttons, with 'Next' being highlighted in yellow.

3.4.6 Internet Information Input

Enter your Internet connection information if you select **PPPoE** as the encapsulation method. Click **Next**.

Figure 22 Wizard - Internet Connection Information

The screenshot shows the same three-step wizard. Step 2 'Internet' is highlighted in yellow. The 'Encapsulation' dropdown is now set to 'PPPoE'. Below it, there are three input fields: 'User Name' containing 'benvenuto', and 'Password' which is masked with seven dots. A toggle icon for password visibility is visible on the right side of the password field. The 'Next' button is no longer highlighted.

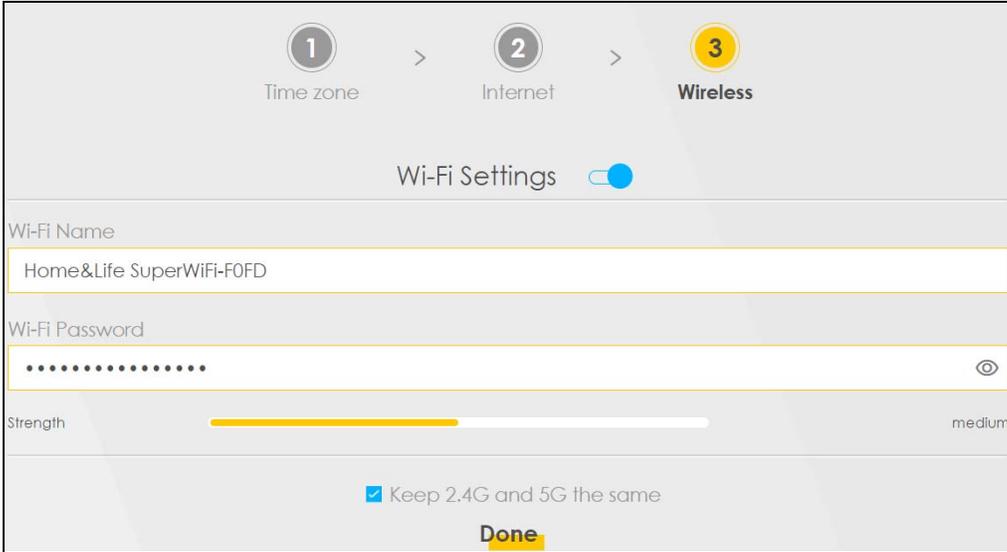
3.5 Quick Start Setup-Wireless

Turn the wireless LAN on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the Zyxel Device.

Click the **Keep 2.4G and 5G the same** check box to use the same SSID for 2.4GHz and 5GHz wireless networks. Otherwise, deselect the check box to have two different SSIDs for 2.4GHz and 5GHz wireless networks. The screen and fields to enter may vary when you select or deselect the check box. Note that you have to disable Zyxel MESH in the **Network > Wireless > MESH** screen to deselect the **Keep 2.4G and 5G the same** check box.

Click **Done**.

Figure 23 Wizard - Wireless



3.6 Quick Start Setup-Finish

Your Zyxel Device saves your settings and attempts to connect to the Internet.

CHAPTER 4

Tutorials

4.1 Overview

This chapter shows you how to use the Zyxel Device's various features.

- [Setting Up an ADSL PPPoE Connection](#), see page 48
- [Setting Up a Secure Wireless Network](#), see page 51
- [Setting Up Multiple Wireless Groups](#), see page 59
- [Using the File Sharing Feature](#), see page 63
- [Using the Media Server Feature](#), see page 65
- [Configuring Static Route for Routing to Another Network](#), see page 69
- [Configuring QoS Queue and Class Setup](#), see page 72
- [Access the Zyxel Device Using DDNS](#), see page 76
- [Configuring the MAC Address Filter](#), see page 78
- [Access Your Shared Files From a Computer](#), see page 79

4.2 Setting Up an ADSL PPPoE Connection

This tutorial shows you how to set up an ADSL Internet connection using the Web Configurator.

If you connect to the Internet through an ADSL connection, use the information from your Internet Service Provider (ISP) to configure the Zyxel Device. Be sure to contact your service provider for any information you need to configure the **Broadband** screens.

- 1 Click **Network Setting > Broadband** to open the following screen. Click **Add New WAN Interface**.

| # | Name | Type | Mode | Encapsulation | 802.1p | 802.1q | IGMP Proxy | NAT | Default Gateway | IPv6 | MLD Proxy | Modify |
|---|--------|------|---------|---------------|--------|--------|------------|-----|-----------------|------|-----------|--------|
| 1 | ADSL | ATM | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |
| 2 | VDSL | PTM | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |
| 3 | ETHWAN | ETH | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |

- 2 In this example, the DSL connection has the following information.

| General | |
|-----------------------|--|
| Name | MyDSLConnection |
| Type | ADSL over ATM |
| Connection Mode | Routing |
| Encapsulation | PPPoE |
| IPv6/IPv4 Mode | IPv4 |
| ATM PVC Configuration | |
| VPI/VCI | 36/48 |
| Encapsulation Mode | LLC/SNAP-Bridging |
| Service Category | UBR without PCR |
| Account Information | |
| PPP User Name | 1234@DSL-Ex.com |
| PPP Password | ABCDEF! |
| Static IP Address | 192.168.1.32 |
| Gateway IP Address | 192.168.1.254 |
| Others | Authentication Method: AUTO PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enabled VLAN: Disabled |

- 3 Enter the **General** and **ATM PVC Configuration** settings as provided above.

Set the **Type** to **ADSL over ATM**.

Choose the **Encapsulation** specified by your DSL service provider. For this example, the service provider requires a username and password to establish Internet connection. Therefore, select **PPPoE** as the WAN encapsulation type.

Set the **IPv4/IPv6 Mode** to **IPv4 Only**.

- 4 Enter the account information provided to you by your DSL service provider.
- 5 Configure this rule as your default Internet connection by selecting the **Apply as Default Gateway** check box. Then select DNS as **Static** and enter the DNS server addresses provided to you, such as **192.168.5.2** (DNS server1)/**192.168.5.1** (DNS server2).
- 6 Leave the rest of the fields to the default settings.
- 7 Click **Apply** to save your settings.

✕

Add New WAN Interface

| | |
|--|---|
| <div style="text-align: right; margin-bottom: 10px;">General <input checked="" type="checkbox"/></div> <p>Name: <input type="text" value="MyDSLConnection"/></p> <p>Type: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="text" value="ADSL over ATM"/></p> <p>Mode: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="text" value="Routing"/></p> <p>Encapsulation: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="text" value="PPPoE"/></p> <p>IPv4/IPv6 Mode: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="text" value="IPv4 Only"/></p> | <div style="text-align: right; margin-bottom: 10px;">PPP Information</div> <p>PPP User Name: <input type="text" value="1234@DSL-Ex.com"/></p> <p>PPP Password: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="password" value="*****"/></p> <p>PPP Connection Trigger: <input checked="" type="radio"/> Auto Connect <input type="radio"/> On Demand</p> <p>PPPoE Passthrough: <input type="checkbox"/></p> |
| <div style="text-align: right; margin-bottom: 10px;">ATM PVC Configuration</div> <p>VPI [0-255]: <input type="text" value="36"/></p> <p>VCI [32-65535]: <input type="text" value="48"/></p> <p>Encapsulation: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="text" value="LLC/SNAP-BRIDGING"/></p> <p>Service Category: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="text" value="UBR Without PCR"/></p> | <div style="text-align: right; margin-bottom: 10px;">VLAN <input type="checkbox"/></div> <p>802.1p: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="text" value="0"/></p> <p>802.1q: <input style="border: none; border-bottom: 1px solid gray; background-color: #f0f0f0; width: 100%;" type="text" value=""/> (1-4094)</p> <div style="text-align: right; margin-bottom: 10px;">MRU/MTU</div> <p>MRU/MTU: <input type="text" value="1492"/></p> |
| <div style="text-align: right; margin-bottom: 10px;">IP Address</div> <p><input type="radio"/> Obtain an IP Address Automatically</p> <p><input checked="" type="radio"/> Static IP Address</p> <p>IP Address: <input type="text" value="192 . 168 . 1 . 32"/></p> <div style="text-align: right; margin-bottom: 10px;">DNS Server</div> <p><input type="radio"/> Obtain DNS Info Automatically</p> <p><input checked="" type="radio"/> Use Following Static DNS Address:</p> <p>Primary DNS Server: <input type="text" value="192 . 168 . 5 . 2"/></p> <p>Secondary DNS Server: <input type="text" value="192 . 168 . 5 . 1"/></p> | <div style="text-align: right; margin-bottom: 10px;">Routing Feature</div> <p>NAT: <input checked="" type="checkbox"/> IGMP Proxy: <input checked="" type="checkbox"/></p> <p>Apply as Default Gateway: <input checked="" type="checkbox"/> Fullcone NAT: <input type="checkbox"/></p> <p>6RD: <input type="checkbox"/></p> |

Cancel Apply

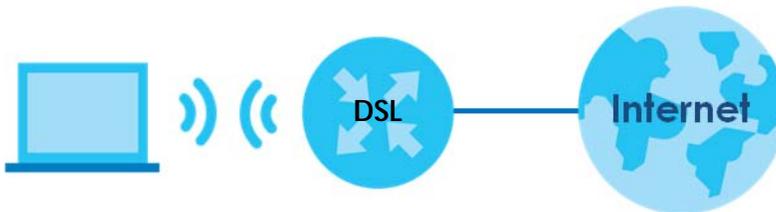
8 You should see a summary of your new DSL connection setup in the **Broadband** screen as follows.

| Broadband | | | | | | | | | | | | |
|--|-----------------|------|---------|---------------|--------|--------|------------|-----|-----------------|------|-----------|--------|
| Broadband Cellular Backup Advanced | | | | | | | | | | | | |
| You can configure the Internet settings of this device. Correct configurations build successful Internet connection. | | | | | | | | | | | | |
| + Add New WAN Interface | | | | | | | | | | | | |
| # | Name | Type | Mode | Encapsulation | 802.1p | 802.1q | IGMP Proxy | NAT | Default Gateway | IPv6 | MLD Proxy | Modify |
| 1 | ADSL | ATM | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |
| 2 | VDSL | PTM | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |
| 3 | ETHWAN | ETH | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |
| 4 | MyDSLConnection | ATM | Routing | PPPoE | N/A | N/A | Y | Y | Y | N | N | |

Try to connect to a website to see if you have correctly set up your Internet connection. Be sure to contact your service provider for any information you need to configure the WAN screens.

4.3 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the Zyxel Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



Thomas has to configure the wireless network settings on the Zyxel Device. Then he can set up a wireless network using WPS ([Section 4.3.2 on page 54](#)) or manual configuration ([Section 4.3.3 on page 58](#)).

4.3.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a wireless network.

| | |
|----------------|-----------------------------|
| SSID | Example |
| Security Mode | WPA2-PSK |
| Pre-Shared Key | DoNotStealMyWirelessNetwork |
| 802.11 Mode | 802.11b/g/n Mixed |

- 1 Click **Network Setting** > **Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see [page 51](#)). Click **Apply**.

Wireless

General | Guest/More AP | MAC Authentication | WPS | WMM | Others | Channel Status | MESH

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than no security to protect your data from unauthorized access or damage via wireless network.

Wireless

Keep 2.4G and 5G wireless network name the same

Wireless Network Setup

Band: 2.4GHz

Wireless:

Channel: Auto Current : 7 / 40 MHz

Bandwidth: 20MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name: Example

Max Clients: 32

Hide SSID ⓘ

Multicast Forwarding

Max. Upstream Bandwidth:

Max. Downstream Bandwidth:

Note

(1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.
 (2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.
 (3) If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.
 (4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID: 5C:E2:8C:8A:F0:FD

Security Level

No Security More Secure (Recommended)

▼

Security Mode: WPA2-PSK

Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password: DoNotStealMyWirelessNetwork

Encryption: AES

Timer: 3600 sec

- 2 Go to the **Wireless > Others** screen and select **802.11b/g/n Mixed** in the **802.11 Mode** field. Click **Apply**.

Wireless

General Guest/More AP MAC Authentication WPS WMM **Others** Channel Status MESH

The configurations below are the advanced wireless settings.

| | |
|-----------------------------|--------------------------|
| RTS/CTS Threshold | 2347 |
| Fragmentation Threshold | 2346 |
| Output Power | 100% |
| Beacon Interval | 100 ms |
| DTIM Interval | 1 ms |
| 802.11 Mode | 802.11b/g/n Mixed |
| 802.11 Protection | Auto |
| Preamble | Long |
| Protected Management Frames | Capable |

Cancel **Apply**

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the ZyXel Device (see [Section 4.3.2 on page 54](#)). He can also use the notebook's wireless client to search for the ZyXel Device (see [Section 4.3.3 on page 58](#)).

4.3.2 Using WPS

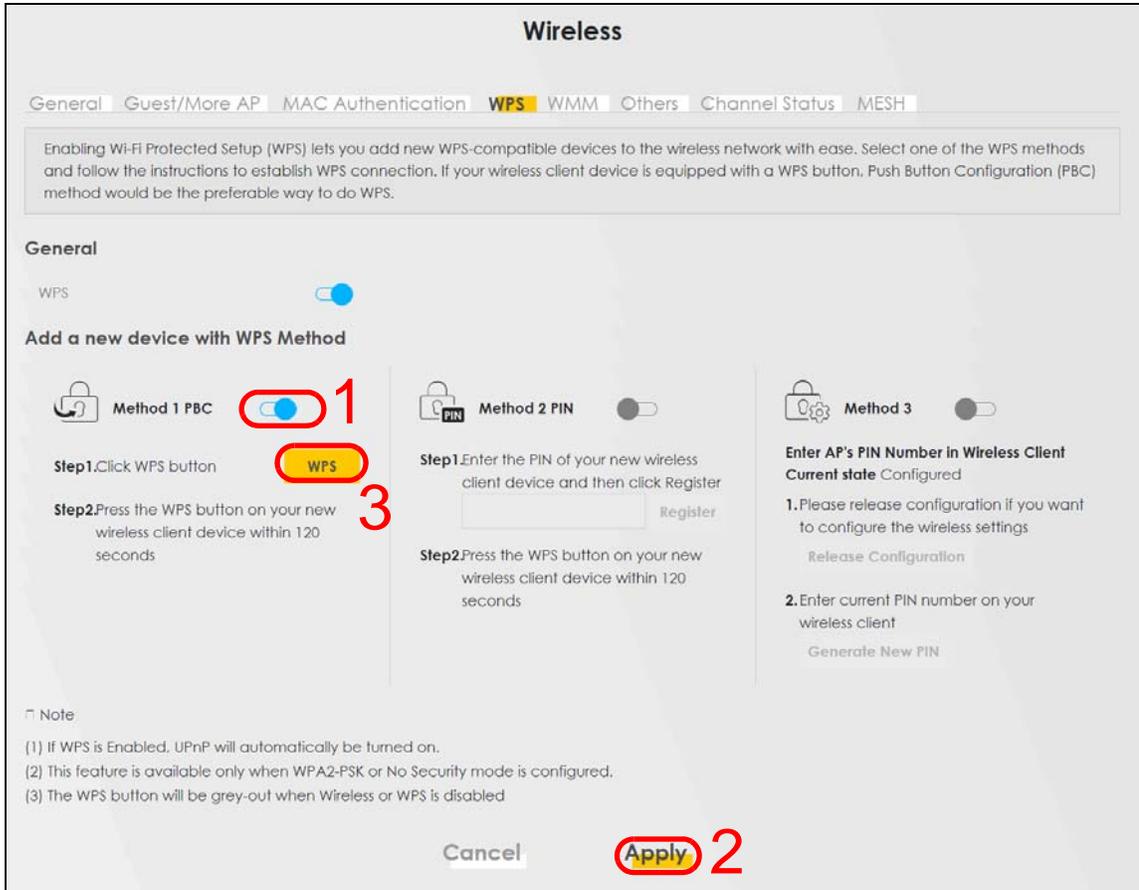
This section gives you an example of how to set up a wireless network using WPS. This example uses the ZyXel Device as the AP and a WPS-enabled Android 4.4.2 smartphone as the wireless client.

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section on page 54](#). This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the ZyXel Device's interface. See [Section on page 56](#). This is the more secure method, since one device can authenticate the other.

Push Button Configuration (PBC)

- 1 Make sure that your ZyXel Device is turned on and your notebook is within the cover range of the wireless signal.
- 2 Push and hold the **WPS** button located on the ZyXel Device's front panel for more than one second. Alternatively, you may log into ZyXel Device's web configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function for method 1 and click **Apply**. Then click the **Connect** button.



Note: Your ZyXel Device has a WPS button located on its side panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The ZyXel Device sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the ZyXel Device securely.

The following figure shows you how to set up wireless network and security by pressing a button on both ZyXel Device and wireless client (the Android 4.4.2 phone in this example).

Figure 24 Example WPS Process: PBC Method

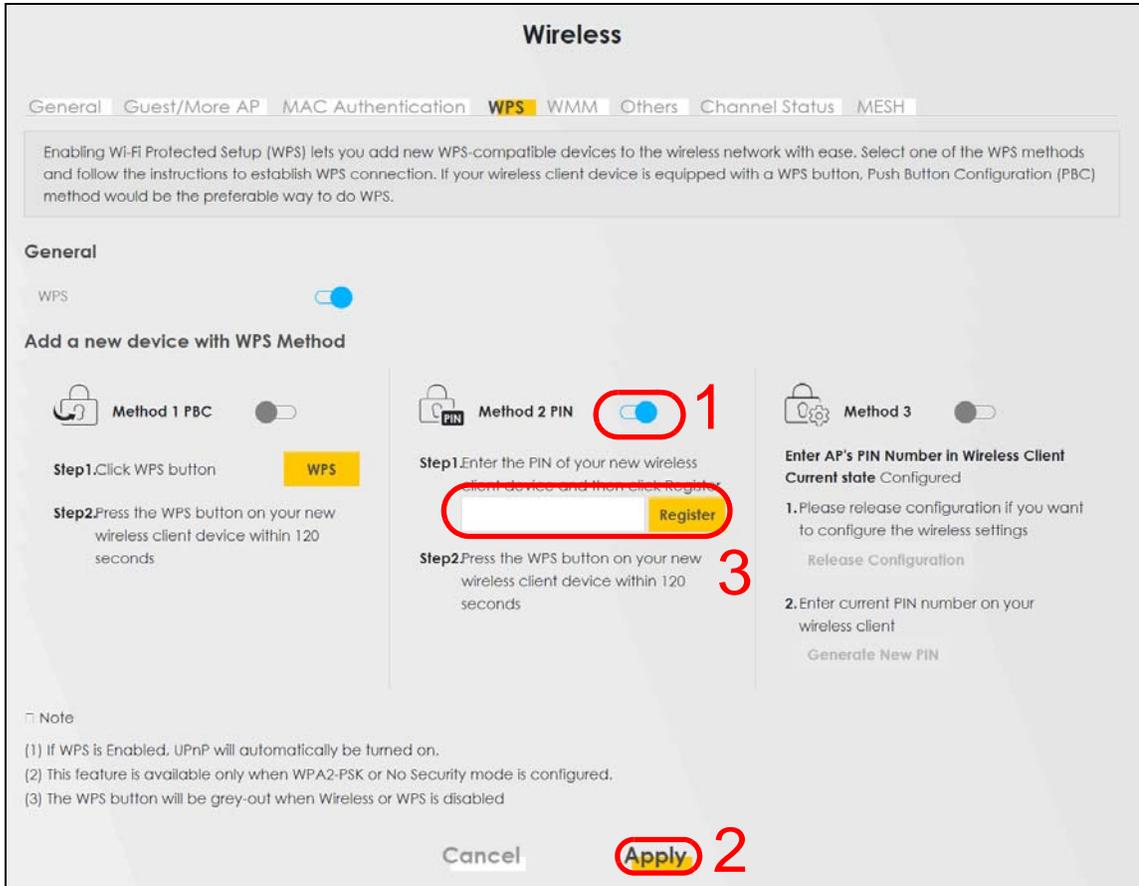
Wireless Client



PIN Configuration

When you use the PIN configuration method, you need to check the client's PIN number and use the Zyxel Device's configuration interface.

- 1 Go to your phone settings and turn on Wi-Fi. Open the Wi-Fi networks list and tap **WPS PIN Entry** to get a PIN number.
- 2 Log into Zyxel Device's web configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function and click **Apply**.



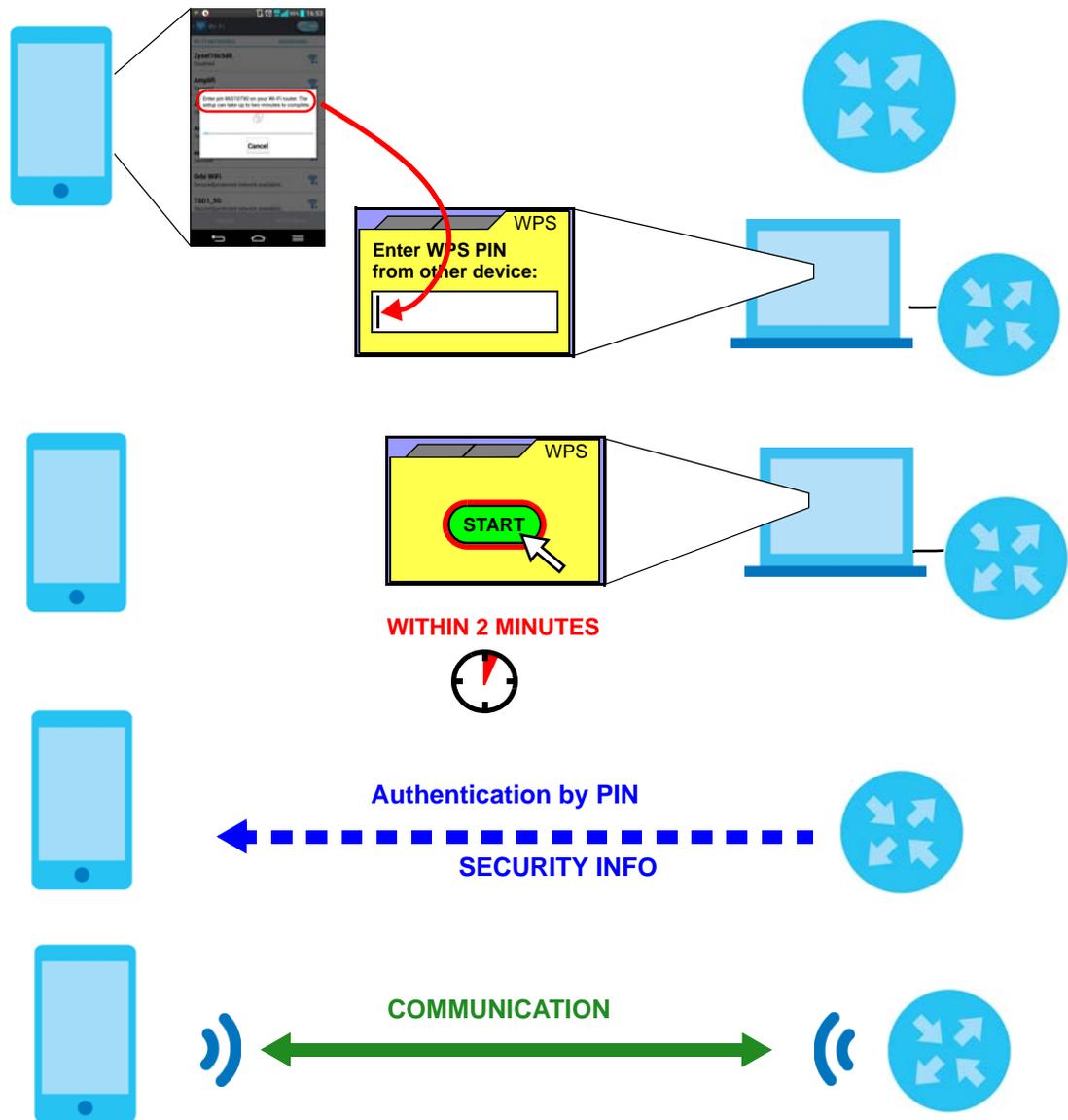
- 3 Enter the PIN number of the wireless client and click the **Register** button. Activate WPS function on the wireless client utility screen within two minutes.

The Zyxel Device authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the Zyxel Device securely.

The following figure shows you how to set up wireless network and security on Zyxel Device and wireless client (Android 4.4.2 smartphone in this example) by using PIN method.

Figure 25 Example WPS Process: PIN Method

Wireless Client



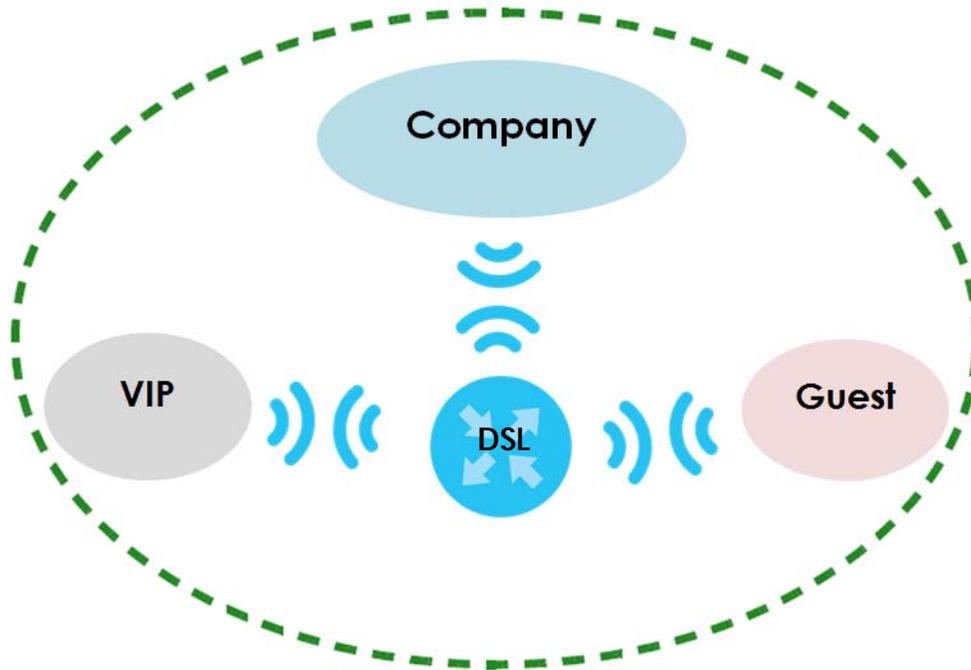
4.3.3 Without WPS

Use the wireless adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish a wireless Internet connection.

Note: The Zyxel Device supports IEEE 802.11b and IEEE 802.11g wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

4.4 Setting Up Multiple Wireless Groups

Company A wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own SSID and security mode.

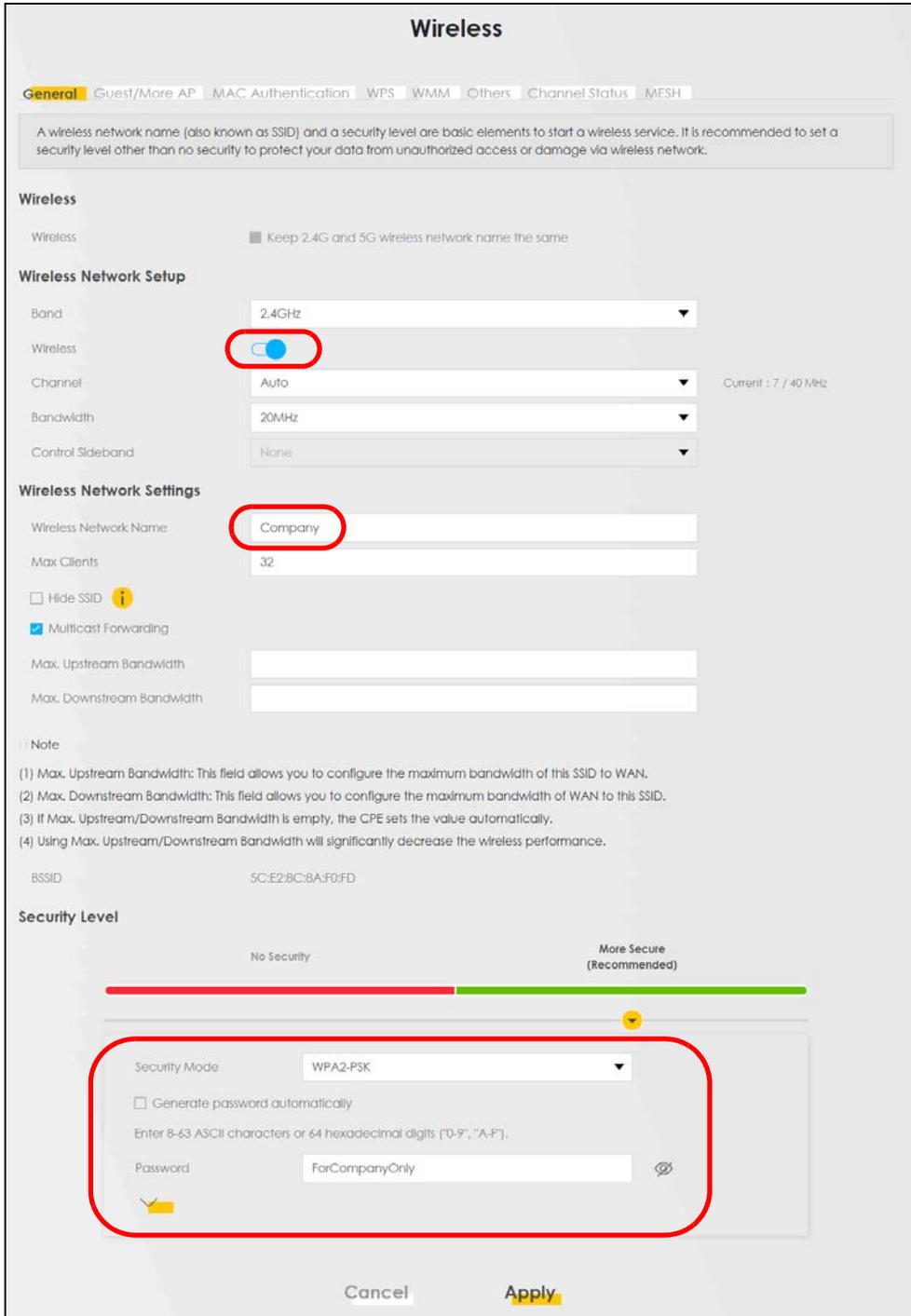


- Employees in Company A will use a general **Company** wireless network group.
- Higher management level and important visitors will use the **VIP** group.
- Visiting guests will use the **Guest** group, which has a different SSID and password.

Company A will use the following parameters to set up the wireless network groups.

| | COMPANY | VIP | GUEST |
|-----------------------|----------------|-------------|-------------|
| SSID | Company | VIP | Guest |
| Security Level | More Secure | More Secure | More Secure |
| Security Mode | WPA2-PSK | WPA2-PSK | WPA2-PSK |
| Pre-Shared Key | ForCompanyOnly | 123456789 | guest123 |

- 1 Click **Network Setting > Wireless** to open the **General** screen. Use this screen to set up the company's general wireless network group. Configure the screen using the provided parameters and click **Apply**.



- 2 Click **Network Setting > Wireless > Guest/More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group.

| # | Status | SSID | Security | Guest WLAN | Modify |
|---|--------|-------------------|---------------|----------------|--------|
| 1 | 🔦 | ZyxeI_9DE5_guest1 | WPA2-Personal | External Guest | ✎ |
| 2 | 🔦 | ZyxeI_9DE5_guest2 | WPA2-Personal | External Guest | ✎ |
| 3 | 🔦 | ZyxeI_9DE5_guest3 | WPA2-Personal | External Guest | ✎ |

- 3 Configure the screen using the provided parameters and click **Apply**.

More AP Edit ✕

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

Wireless Network Setup

Wireless

Security Level

Wireless Network Name

Hide SSID

Guest WLAN

Access Scenario

Max. Upstream Bandwidth

Max. Downstream Bandwidth

Note

(1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.

(2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.

(3) If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

(4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID

SSID Subnet

Security Level

No Security More Secure (Recommended)

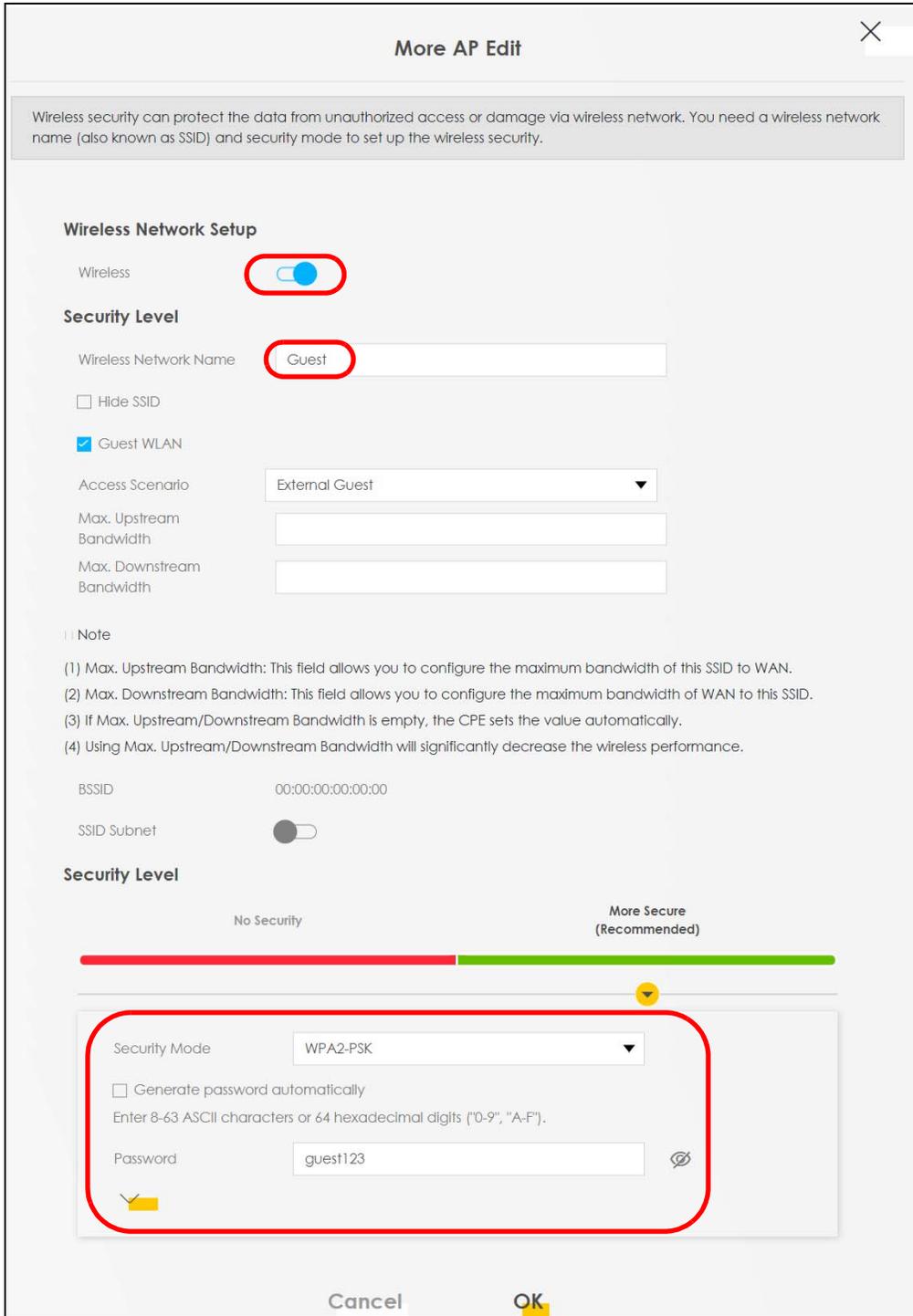
Security Mode

Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password

- 4 In the **Guest/More AP** screen, click the **Edit** icon to configure the third wireless network group. Configure the screen using the provided parameters and click **Apply**.



- 5 Check the status of **VIP** and **Guest** in the **Guest/More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.

| # | Status | SSID | Security | Guest WLAN | Modify |
|---|--------|---------------------------------|---------------|----------------|--------|
| 1 | | Home&Life SuperWiFi-F0FD_guest1 | WPA2-Personal | External Guest | |
| 2 | | VIP | WPA2-Personal | External Guest | |
| 3 | | Guest | WPA2-Personal | External Guest | |

4.5 Using the File Sharing Feature

In this section you can:

- Set up file sharing of your USB device from the Zyxel Device.
- Access the shared files of your USB device from a computer.

4.5.1 Set Up File Sharing

To set up file sharing you need to connect your USB device, enable file sharing and set up your share(s).

Before enabling file sharing in the Zyxel Device, please set up your shares beforehand in the USB.

4.5.1.1 Activate File Sharing

Connect your USB device to the USB port at the side panel of the Zyxel Device.

Click **Network Setting > USB Service > File Sharing**. Enable and click **Apply** to activate the file sharing function. The Zyxel Device automatically adds your USB device to the **Information**.

USB Service

FileSharing MediaServer

The device can share Files from your USB flash drive or disk when you attach it to the USB port. You may Start from deciding which folders in the USB disks to share and which users can access the shared folders.

Information

| Volume | Capacity | Used Space |
|-----------|----------|------------|
| usb1_sda1 | 0 MB | 0 MB |

Server Configuration

File Sharing Services

Share Directory List + Add New Share

| Active | Status | Share Name | Share Path | Share Description | Modify |
|--------|--------|------------|------------|-------------------|--------|
|--------|--------|------------|------------|-------------------|--------|

Account Management + Add New User

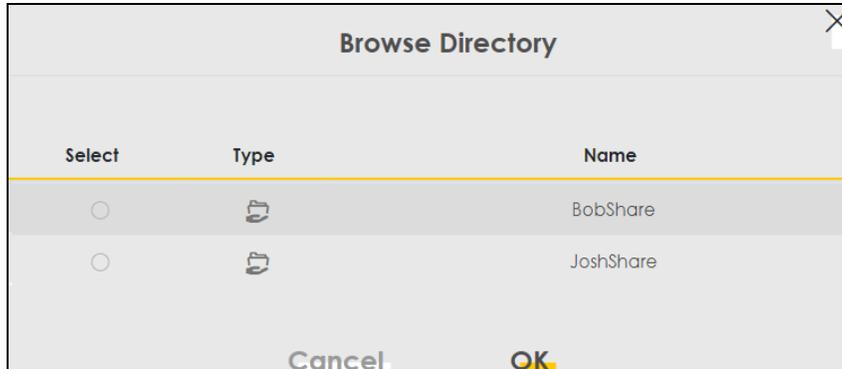
| Status | User Name |
|--------|-----------|
| | admin |

Cancel Apply

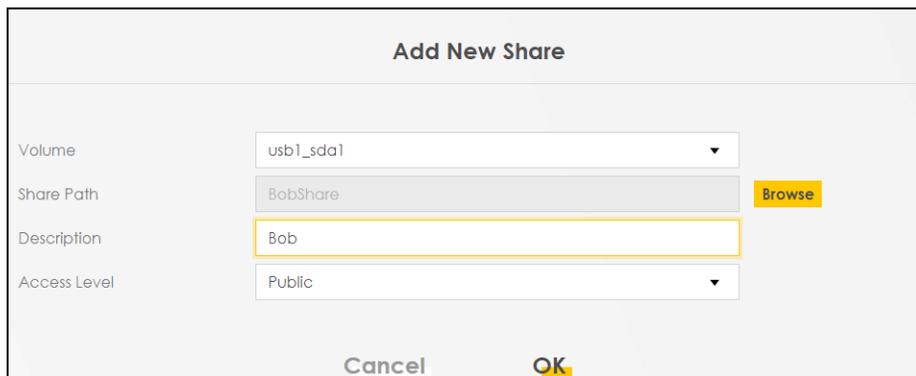
4.5.1.2 Set up File Sharing on Your Zyxel Device

You also need to set up file sharing on your Zyxel Device in order to share files.

- 1 Click **Add New Share** in the **File Sharing** screen to add a new share. Select your USB device from the **Volume** drop-down list box.
- 2 Click **Browse** to browse through all the files on your USB device. Select the folder that you want to add as a share. In this example, select **BobShare**. Click **Apply**



- 3 It's mandatory for you to add a description for the share. Also, if you want the share to be accessed by users connecting to the Zyxel Device, you can select **Public** in **Access Level** or select **Security** to specific users' use only. Please note that you need to create the users' accounts that are eligible to access the secure shares beforehand in **Account Management**, if you want to configure the **Access Level** to **Security**. For detailed information, please refer to the steps below. The **Add Share Directory** screen should look like the following. Click **Apply** to finish.



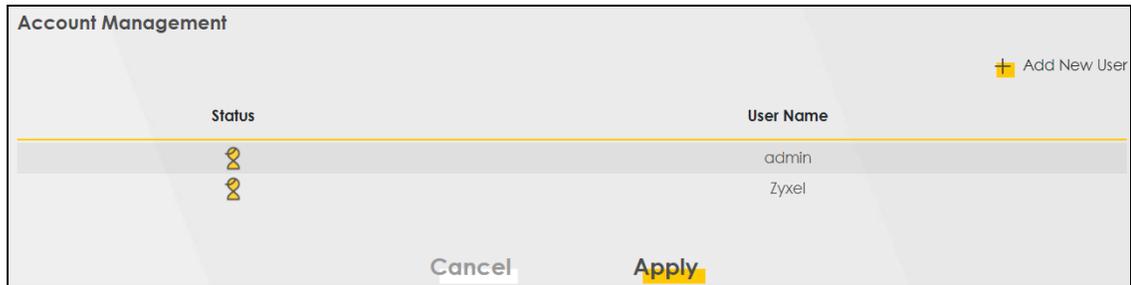
- 4 This sets up the file sharing server. You can see the USB storage device listed in the table below.

| Share Directory List | | | | | | | + Add New Share |
|-------------------------------------|--------|------------|--------------------------|-------------------|--------|--|-----------------|
| Active | Status | Share Name | Share Path | Share Description | Modify | | |
| <input checked="" type="checkbox"/> | | BobShare | /mnt/usb1_sda1/BobShare | Bob | | | |
| <input checked="" type="checkbox"/> | | JoshShare | /mnt/usb1_sda1/JoshShare | Josh | | | |

- 5 If you want specific users only to access the shares, you need to **Add New Users** in **Account Management**. Once you click the **Add New User** button, you'll be directed to the **User Account** screen. To create a user account that can access the secured shares on the USB device, click the **Add New Account** button in the **Maintenance > User Account** screen.

Please see [Chapter 34 on page 314](#), for detailed information about User Account screen.

- 6 After you create a new user account, the screen should look like the following.



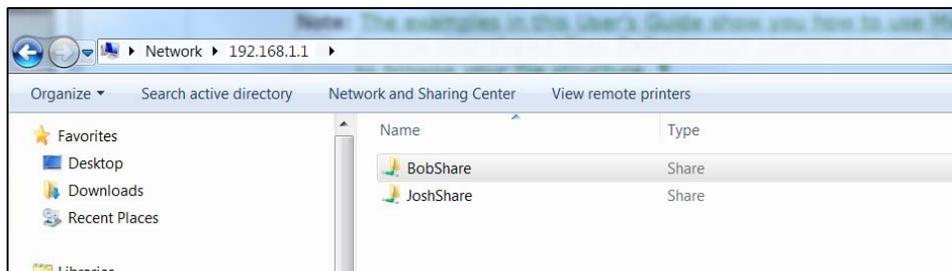
4.5.2 Access Your Shared Files From a Computer

You can use Windows Explorer to access the file storage devices connected to the Zyxel Device.

Note: The examples in this User's Guide show you how to use Microsoft's Windows 7 to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Open Windows Explorer to access **BobShare** using Windows Explorer browser.

In Windows Explorer's Address bar type a double backslash "\\ " followed by the IP address of the Zyxel Device (the default IP address of the Zyxel Device is 192.168.1.1) and press [ENTER]. The share folder **BobShare** is available.



Once you access **BobShare** via your Zyxel Device, you do not have to relogin unless you restart your computer.

4.6 Using the Media Server Feature

Use the media server feature to play files on a computer or on your television (using DMA-2500).

This section shows you how the media server feature works using the following media clients:

- Microsoft (MS) Windows Media Player
Media Server works with Windows 7. Make sure your computer is able to play media files (music, videos and pictures).
- Zyxel DMA-2500, a digital media adapter
You need to set up the DMA-2500 to work with your television (TV). Refer to the DMA-2500 Quick Start Guide for the correct hardware connections.

Before you begin, connect the USB storage device containing the media files you want to play to the USB port of your Zyxel Device.

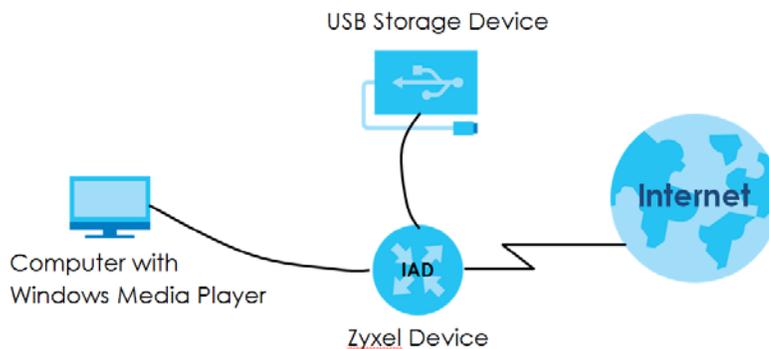
4.6.1 Configuring the Zyxel Device

To use your Zyxel Device as a media server, click **Network Setting > USB Service > Media Server**.

Enable Media Server, select an interface on which you want to enable the media server function, enter the path clients use to access the media files on a USB storage device connected to the Zyxel Device, and click **Apply**. This enables DLNA-compliant media clients to play the video, music and image files in your USB storage device.

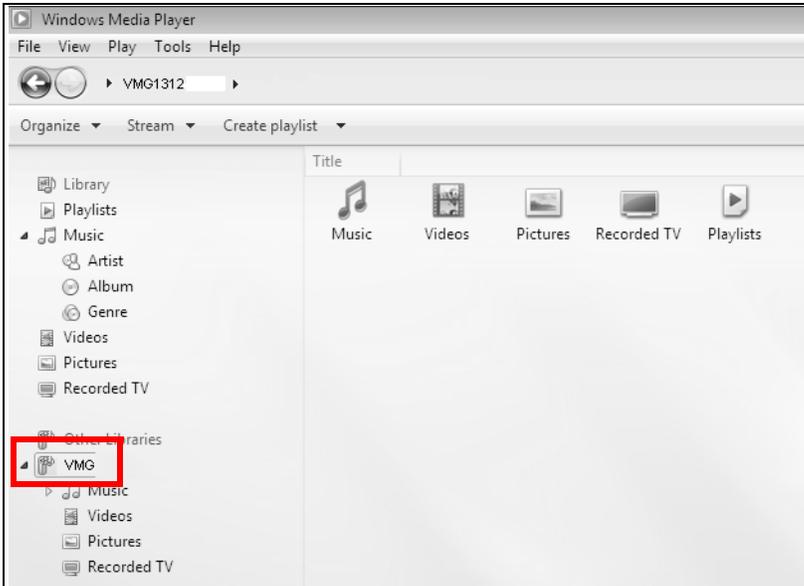
4.6.2 Using Windows Media Player

This section shows you how to play the media files on the USB storage device connected to your Zyxel Device using Windows Media Player.

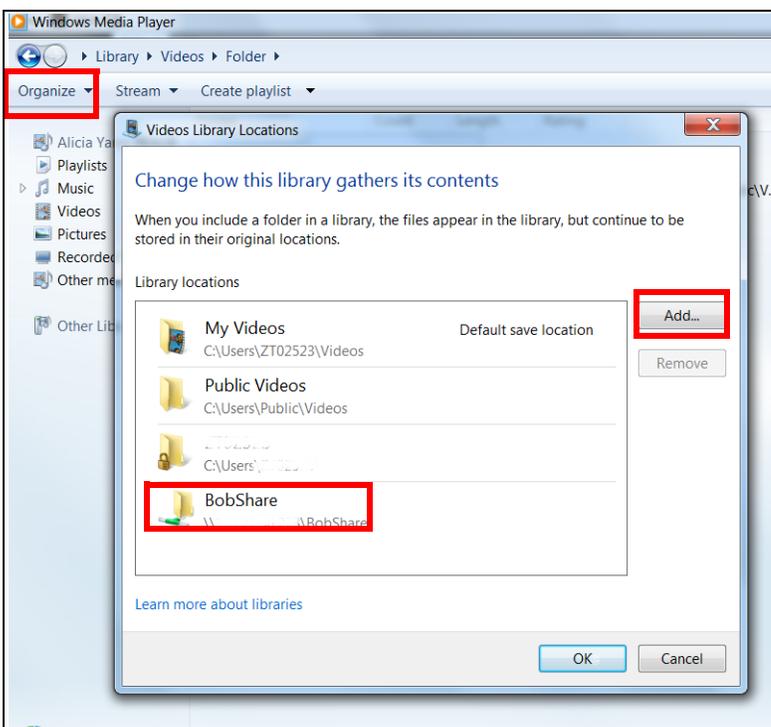


Windows 7

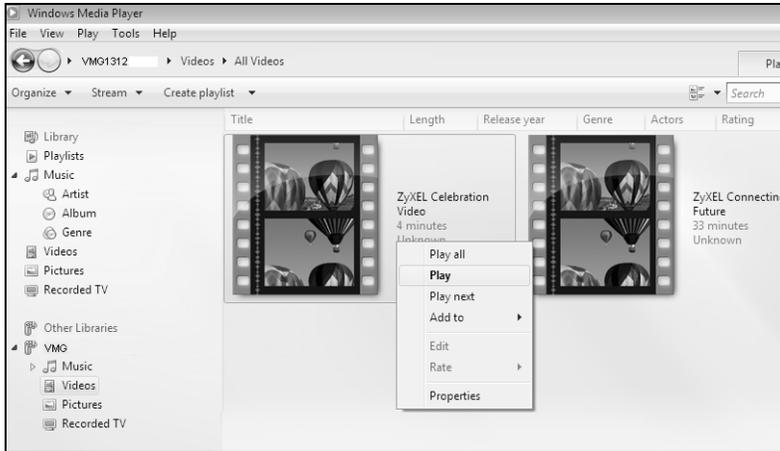
- 1 Open Windows Media Player. It should automatically detect the Zyxel Device.



- 2 If you cannot see the Zyxel Device in the left panel as shown above, go to **Organize > Manage Libraries > Music/Videos/Pictures/Recorded TV > Add > \\192.168.1.1\BobShare**. (Select the folder containing the media you wish to upload to Windows Media Player.)



- 3 In the right panel, you should see a list of files available in the USB storage device.

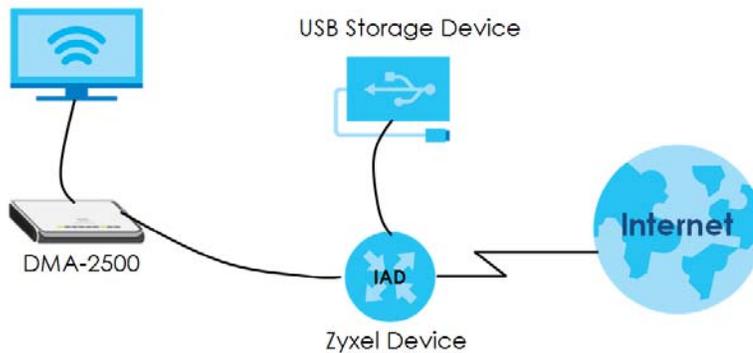


4.6.3 Using a Digital Media Adapter

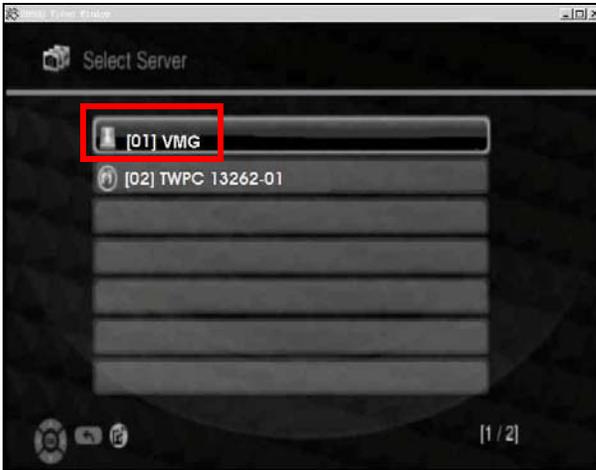
This section shows you how you can use the Zyxel Device with a Zyxel DMA-2500 to play media files stored in the USB storage device in your TV screen.

Note: For this tutorial, your DMA-2500 should already be set up with the TV according to the instructions in the DMA-2500 Quick Start Guide.

- 1 Connect the DMA-2500 to an available LAN port in your Zyxel Device.



- 2 Turn on the TV and wait for the DMA-2500 **Home** screen to appear. Using the remote control, go to **MyMedia** to open the following screen. Select the GPON Device as your media server.



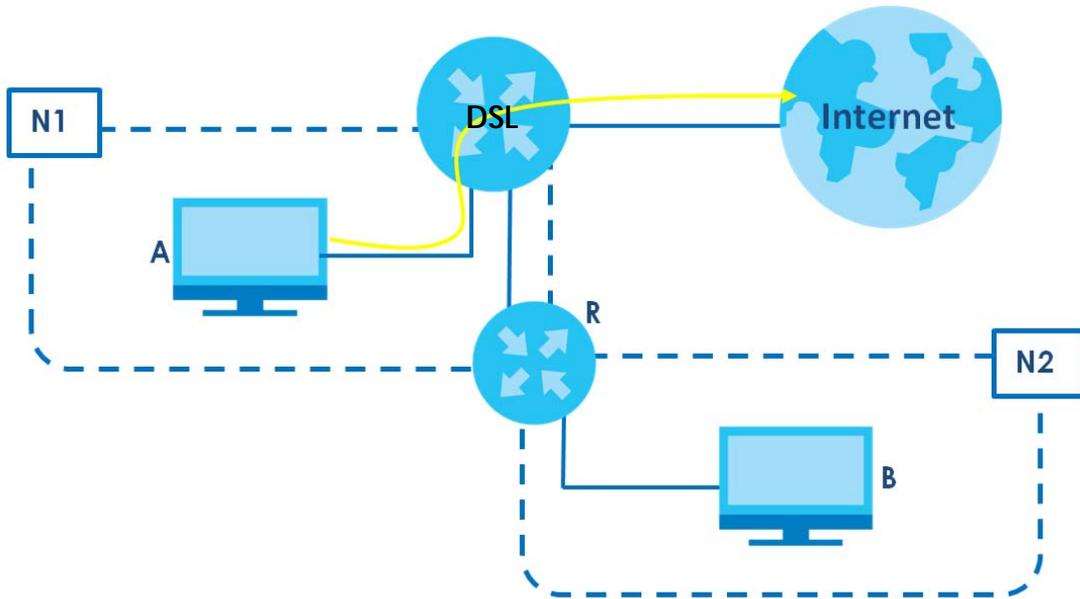
- 3 The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button in the remote control.



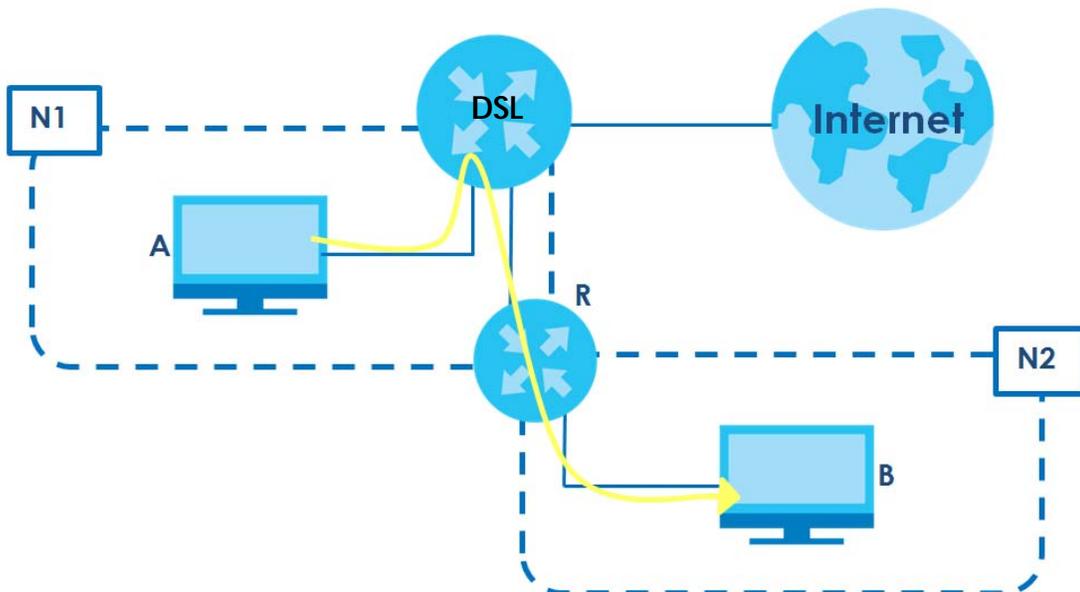
4.7 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Zyxel Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the Zyxel Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the Zyxel Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the Zyxel Device to specify R as the router in charge of forwarding traffic to N2. In this case, the Zyxel Device routes traffic from A to R and then R routes the traffic to B.



This tutorial uses the following example IP settings:

Table 16 IP Settings in this Tutorial

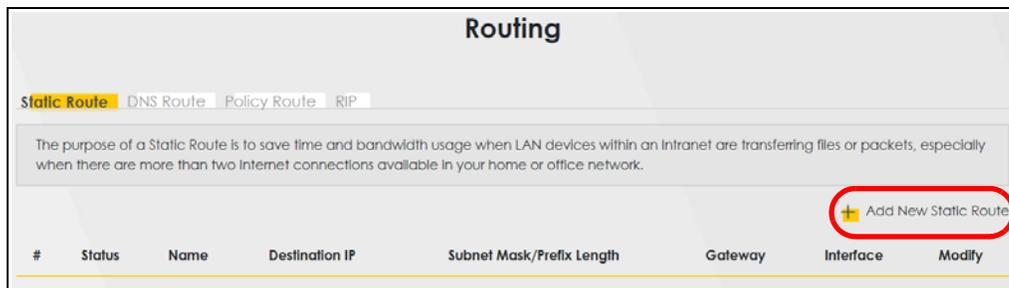
| DEVICE / COMPUTER | IP ADDRESS |
|------------------------|-------------|
| The Zyxel Device's WAN | 172.16.1.1 |
| The Zyxel Device's LAN | 192.168.1.1 |
| IP Type | IPv4 |
| Use Interface | VDSL |

Table 16 IP Settings in this Tutorial

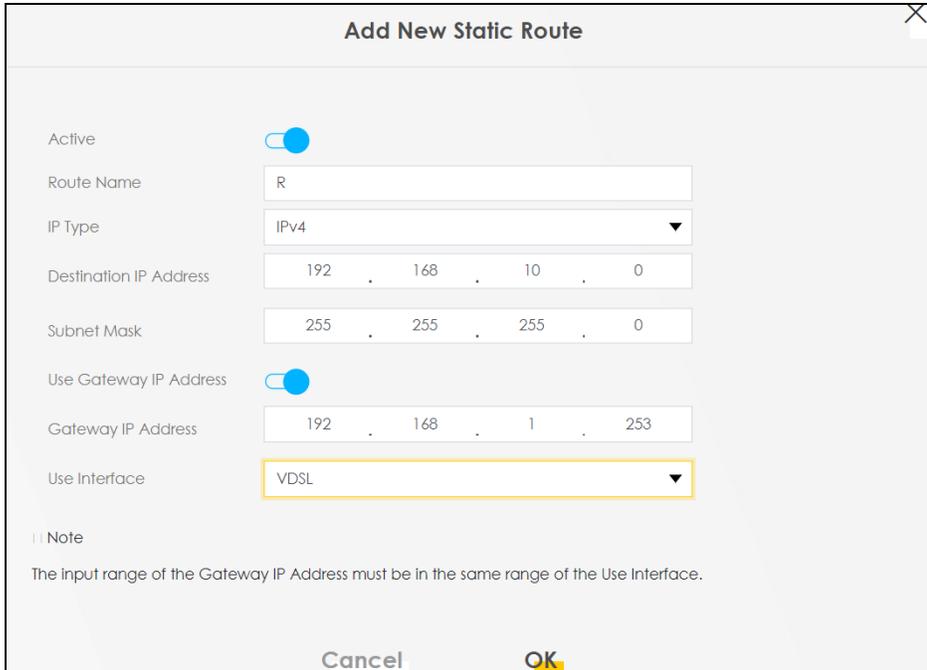
| DEVICE / COMPUTER | IP ADDRESS |
|-------------------|---------------|
| A | 192.168.1.34 |
| R's N1 | 192.168.1.253 |
| R's N2 | 192.168.10.2 |
| B | 192.168.10.33 |

To configure a static route to route traffic from **N1** to **N2**:

- 1 Log into the Zyxel Device's Web Configurator in advanced mode.
- 2 Click **Network Setting > Routing**.
- 3 Click **Add new Static Route** in the **Static Route** screen.



- 4 Configure the **Static Route Setup** screen using the following settings:
 - 4a Click the **Active** button to enable this static route. When the switch turns blue () , the function is enabled. Enter the **Route Name** as **R**.
 - 4b Set **IP Type** to **IPv4**.
 - 4c Type the **Destination IP Address** **192.168.10.0** and **IP Subnet Mask** **255.255.255.0** for the destination, **N2**.
 - 4d Click the **Use Gateway IP Address** button to enable this function. When the switch turns blue () , the function is enabled. Type **192.168.1.253** (**R's N1** address) in the **Gateway IP Address** field.
 - 4e Select **VDSL** as the **Use Interface**.



4a Click **OK**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

4.8 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

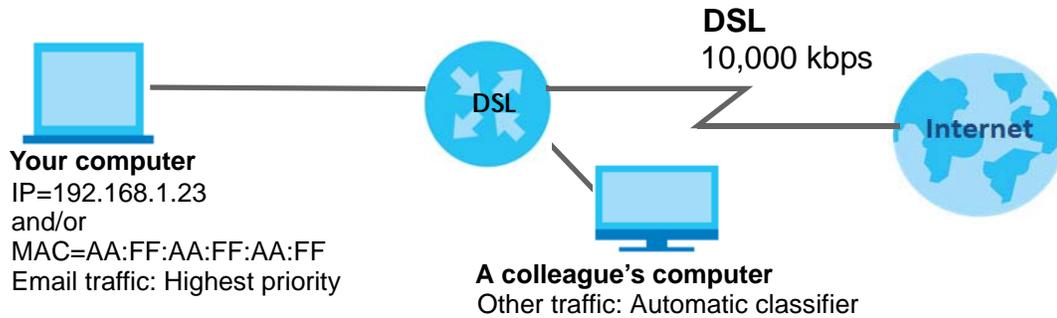
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

- Configure a queue to assign the highest priority queue (1) to e-mail traffic going to the WAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the Zyxel Device.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the Zyxel Device.



- 1 Click **Network Setting > QoS > General** and click the **QoS** button to enable. When the switch turns blue () , the function is enabled. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Zyxel Device automatically determine this figure). Click **Apply**.

QoS

General QueueSetup ClassificationSetup ShaperSetup PolicerSetup

Quality of Service (QoS) defines the traffic priority of Internet services to the home network.

QoS

WAN Managed Upstream Bandwidth (kbps)

LAN Managed Downstream Bandwidth (kbps)

Upstream Traffic Priority Assigned by

Note

(1) You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.

(2) If Upstream Traffic Priority is selected, 8 level strict priority QoS will be applied automatically according to the selected criteria. In this mode, user manually defined QoS will not be applied until Auto-Priority Mapping is disabled.

(3) If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

Cancel **Apply**

- 2 Click **Network > Queue Setup > Add new Queue** to create a new queue. In the screen that opens, click the **Active** field to enable. When the switch turns blue () , the function is enabled. Enter or select the following values:
 - **Name:** E-mail
 - **Interface:** WAN
 - **Priority:** 1 (High)
 - **Weight:** 8
 - **Rate Limit:** 5,000 (kbps)

The screenshot shows a configuration window titled "Add New Queue". It contains the following fields and settings:

| | |
|-------------------|-------------------------------------|
| Active | <input checked="" type="checkbox"/> |
| Name | E-mail |
| Interface | WAN |
| Priority | 1 (highest) |
| Weight | 8 |
| Buffer Management | Drop Tail (DT) |
| Rate Limit | 5000 (kbps) |

At the bottom of the window, there are two buttons: "Cancel" and "OK". The "OK" button is highlighted with a yellow background.

- 3 Click **Network > QoS > Classification Setup > Add new Classification** to create a new class. Select **Enable** in the **Active** field and follow the settings as shown in the screen below.

✕

Add New Classification

Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

Active

Class Name

Classification Order

Step2: Criteria Configuration

Use the configurations below to specify the characteristics of a data flow needed to be managed by this QoS rule

Basic

From Interface

Ether Type

Source

Address Subnet Mask Exclude

Port Range - Exclude

MAC MAC Mask Exclude

Destination

Address Subnet Mask Exclude

Port Range - Exclude

MAC MAC Mask Exclude

Others

Service Exclude

IP protocol Exclude

DHCP Exclude

IP Packet Length - Exclude

DSCP (0-63) Exclude

802.1P Exclude

VLAN ID (1-4094) Exclude

TCP ACK Exclude

Step3: Packet Modification

The content of the packet can be modified by applying the following settings:

DSCP Mark (0-63)

VLAN ID Tag (1-4094)

802.1P Mark

Step4: Class Routing

This module can route a packet to a certain interface according to the class setting

Forward To Interface

Step5: Outgoing Queue Selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN Interface.

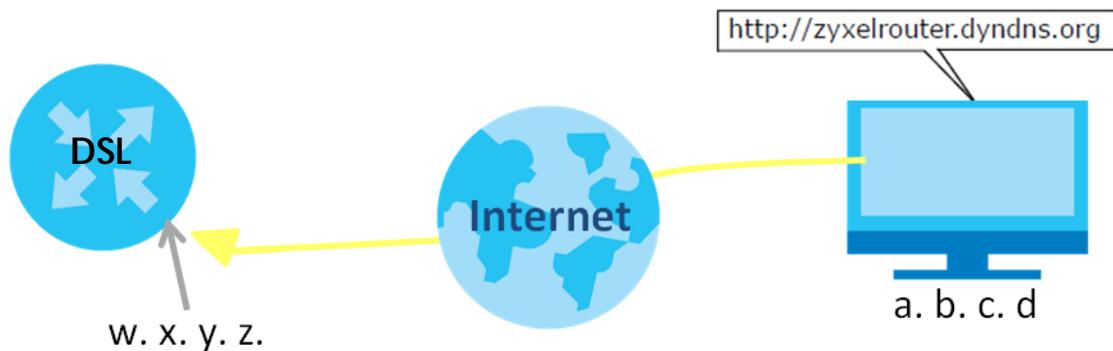
To Queue Index

| | |
|-----------------------|--|
| Class Name | Give a class name to this traffic, such as E-mail in this example. |
| From Interface | This is the interface from which the traffic will be coming from. Select LAN1 for this example. |
| Ether Type | Select IP to identify the traffic source by its IP address or MAC address. |
| IP Address | Type the IP address of your computer - 192.168.1.23 . Type the IP Subnet Mask if you know it. |
| MAC Address | Type the MAC address of your computer - AA:FF:AA:FF:AA:FF . Type the MAC Mask if you know it. |
| To Queue Index | Link this to an item in the Network Setting > QoS > Queue Setup screen, which is the E-mail queue created in this example. |

This maps e-mail traffic coming from port 25 to the highest priority, which you have created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to the **E-mail** queue (see the **Source** fields).

4.9 Access the Zyxel Device Using DDNS

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The Zyxel Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Zyxel Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial covers:

- [Registering a DDNS Account on \[www.dyndns.org\]\(http://www.dyndns.org\)](#)
- [Configuring DDNS on Your Zyxel Device](#)
- [Testing the DDNS Setting](#)

Note: If you have a private WAN IP address, then you cannot use DDNS.

4.9.1 Registering a DDNS Account on www.dyndns.org

- 1 Open a browser and type <http://www.dyndns.org>.
- 2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
- 3 Log into www.dyndns.org using your account.

- 4 Add a new DDNS host name. This tutorial uses the following settings as an example.
 - Hostname: **zyxelrouter.dyndns.org**
 - Service Type: **Host with IP address**
 - IP Address: Enter the WAN IP address that your Zyxel Device is currently using. You can find the IP address on the Zyxel Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the Zyxel Device later.

4.9.2 Configuring DDNS on Your Zyxel Device

Configure the following settings in the **Network Setting > DNS > Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).

DNS

DNS Entry **Dynamic DNS**

Dynamic DNS can update your current dynamic IP into a hostname. Use the settings to set up dynamic DNS information.

Dynamic DNS Setup

Dynamic DNS Enable Disable (Settings are invalid when disable)

Service Provider

Host Name

Username

Password

Enable Wildcard Option

Enable Off Line Option (Only applies to custom DNS)

Dynamic DNS Status

User Authentication Result

Last Updated Time

Current Dynamic IP

Click **Apply**.

4.9.3 Testing the DDNS Setting

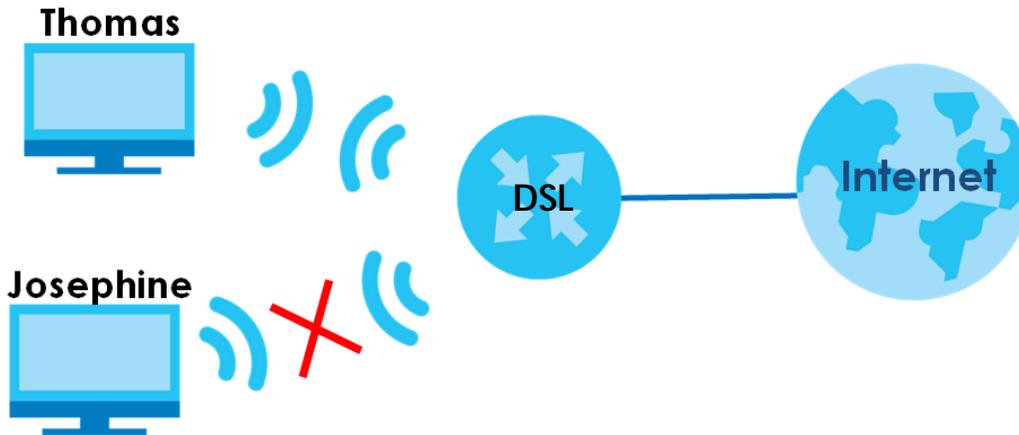
Now you should be able to access the Zyxel Device from the Internet. To test this:

- 1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
- 2 Type **http://zyxelrouter.dyndns.org** and press [Enter].
- 3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

4.10 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the Zyxel Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



- 1 Click **Security > MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.
- 2 Select **Allow**. Click **Add a new setting** to add a new entry. Then enter the host name and MAC address of Thomas' computer in this screen. Click **Apply**.

Mac Filter

Enable MAC filters and add the MAC addresses of LAN client in your home or office network to the following table, if you wish to allow or deny them to access your network. Sometimes, MAC Filter is considered a method to increase the security of your network.

MAC Address Filter Enable Disable (Settings are invalid when disable)

MAC Restrict Mode Allow Deny

+ Add a new setting

| Set | Active | Host Name | MAC Address | Delete |
|-----|-------------------------------------|-----------|-----------------------------|--------|
| 1 | <input checked="" type="checkbox"/> | Thomas | 00 - 24 - 21 - AB - 1F - 0d | 🗑️ |

Note
Only devices listed here are granted access to the network

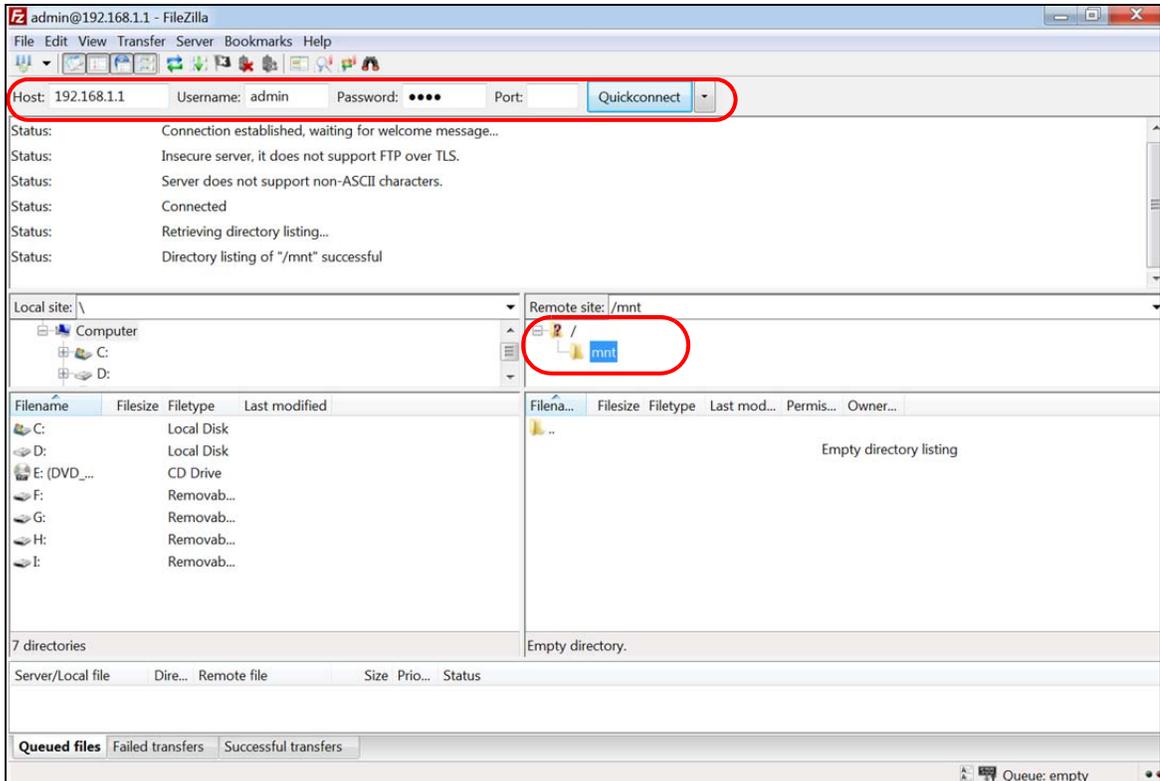
Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the Zyxel Device.

4.11 Access Your Shared Files From a Computer

Here is how to use an FTP program to access a file storage device connected to the Zyxel Device's USB port.

Note: This example uses the FileZilla FTP program to browse your shared files.

- 1 In FileZilla enter the IP address of the Zyxel Device (the default is 192.168.1.1), your account's user name and password and port 21 and click **Quickconnect**. A screen asking for password authentication appears.



- 2 Once you log in the USB device displays in the **mnt** folder.

PART II

Technical Reference

CHAPTER 5

Connection Status Screens

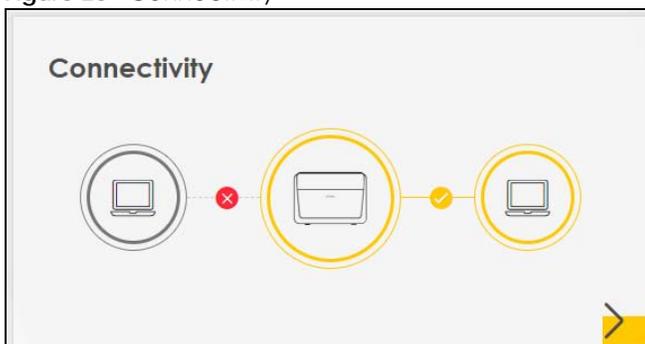
5.1 The Connection Status Screen

After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access, wireless settings, and parental control settings in this screen. It also shows the network status of the Zyxel Device and computers/devices connected to it.

5.1.1 The Connectivity Screen

Use this screen to view the network connection status of the Zyxel Device and its clients.

Figure 26 Connectivity



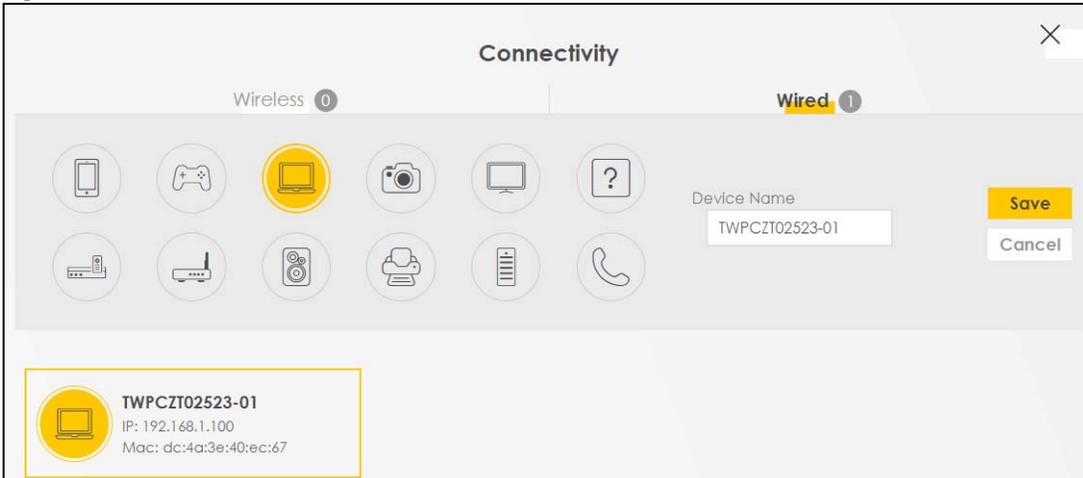
Click the Arrow icon () to view IP addresses and MAC addresses of the wireless and wired devices connected to the Zyxel Device.

Figure 27 Connectivity: Connected Devices



You can change the icon and name of a connected device. Place your mouse within the device block, and an Edit icon () will appear. Click the Edit icon, and you'll see there are several icon choices for you to select. Enter a name in the **Device Name** field for a connected device. Click **Save** to save your changes.

Figure 28 Connectivity: Edit



5.1.2 The System Info Screen

Use this screen to view the basic system information of the Zyxel Device.

Figure 29 System Info



Click the Arrow icon (➤) to view the more information on the status of your firewall and interfaces (WAN, LAN, and WLAN).

Figure 30 System Info: Detailed Information

The screenshot shows the 'System Info' screen with the following details:

- System Info:** Host Name: VMG3927-B50A, Model Name: VMG3927-B50A, Serial number: S184123012004, Firmware Version: V5.13(ABMT.0)b1, System Uptime: 0 days 4 hours 43 mins 32 secs.
- Interface Status:** LAN1 (1000M/Full), LAN2, LAN3, LAN4, WAN (1000M/Full), DSL, 3G(USB), WLAN 2.4G (216 Mbps), WLAN 5G (1733 Mbps).
- WAN Information (Ethernet WAN):** Encapsulation: IPoE, IP Address: 192.168.1.1 (with a 'Release' button), IP Subnet Mask: 255.255.255.0, IPv6 Address: N/A, MAC Address: BC:99:11:60:9D:E8, Primary DNS server: 172.21.5.1, Secondary DNS server: 172.21.6.1, Primary DNSv6 server: N/A, Secondary DNSv6 server: N/A.
- WLAN Information:**
 - 2.4GHz:** MAC Address: BC:99:11:60:9D:E5, Status: On, SSID: Zyxel_9DE5, Channel: Auto(Current 4), Security: WPA2-Personal, 802.11 Mode: 802.11b/g/n Mixed, WPS: On.
 - 5GHz:** MAC Address: BC:99:11:60:9D:E6, Status: On, SSID: Zyxel_9DE5, Channel: Auto(Current 56), Security: WPA2-Personal, 802.11 Mode: 802.11a/n/ac Mixed, WPS: On.
- LAN Information:** IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, IPv6 Link Local Address: fe80::be99:11ff:fe60:9de4, DHCP: Server.
- Security:** Firewall: Medium.

Each field is described in the following table.

Table 17 System Info: Detailed Information

| LABEL | DESCRIPTION |
|--|--|
| Host Name | This field displays the Zyxel Device system name. It is used for identification. |
| Model Name | This shows the model number of your Zyxel Device. |
| Serial Number | This field displays the serial number of the Zyxel Device. |
| Firmware Version | This is the current version of the firmware inside the Zyxel Device. |
| System Up Time | This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (Maintenance > Reboot), or when you reset it. |
| Interface Status | Virtual ports are shown here. You can see the ports in use and their transmission rate. |
| WAN Information (These fields display when you have a WAN connection.) | |

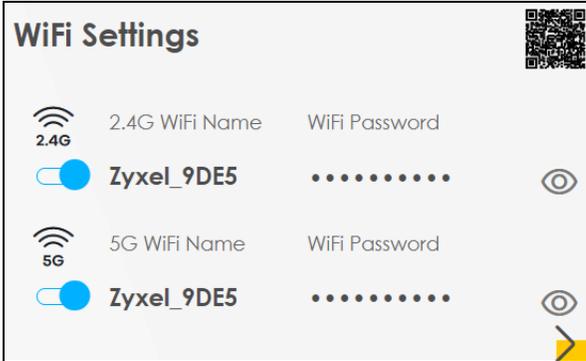
Table 17 System Info: Detailed Information (continued)

| LABEL | DESCRIPTION |
|--------------------------|---|
| Encapsulation | This field displays the current encapsulation method. |
| IP Address | This field displays the current IP address of the Zyxel Device in the WAN. Click the Release button to release the IP address provided by a DHCP server. |
| IP Subnet Mask | This field displays the current subnet mask in the WAN. |
| IPv6 Address | This field displays the current IPv6 address of the Zyxel Device in the WAN. |
| MAC Address | This shows the WAN Ethernet adapter MAC (Media Access Control) Address of your Zyxel Device. |
| Primary DNS server | This field displays the first DNS server address assigned by the ISP. |
| Secondary DNS server | This field displays the second DNS server address assigned by the ISP. |
| Primary DNSv6 server | This field displays the first DNS server IPv6 address assigned by the ISP. |
| Secondary DNSv6 server | This field displays the second DNS server IPv6 address assigned by the ISP. |
| LAN Information | |
| IP Address | This is the current IP address of the Zyxel Device in the LAN. |
| Subnet Mask | This is the current subnet mask in the LAN. |
| IPv6 Link Local Address | This field displays the current link-local address of the Zyxel Device for the LAN interface. |
| DHCP | This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are: Server - The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay - The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. None - The Zyxel Device is not providing any DHCP services to the LAN. |
| Security | |
| Firewall | This displays the firewall's current security level. |
| WLAN 2.4G/5G Information | |
| MAC Address | This shows the wireless adapter MAC (Media Access Control) Address of the wireless interface. |
| Status | This displays whether the WLAN is activated. |
| SSID | This is the descriptive name used to identify the Zyxel Device in a wireless LAN. |
| Channel | This is the channel number used by the wireless interface now. |
| Security | This displays the type of security mode the wireless interface is using in the wireless LAN. |
| 802.11 Mode | This displays the type of 802.11 mode the wireless interface is using in the wireless LAN. |
| WPS | This displays whether WPS is activated on the wireless interface. |

5.1.3 The Wi-Fi Settings Screen

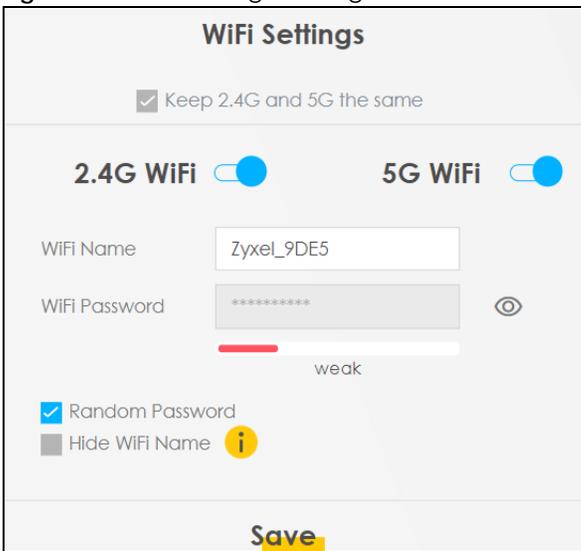
Use this screen to enable or disable the main 2.4 GHz and/or 5 GHz wireless networks. When the switch turns blue () , the function is enabled. Otherwise, it's not. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the main wireless networks.. If you want to show or hide your WiFi passwords, click the Eye icon ().

Figure 31 Wi-Fi Settings



Click the Arrow icon (➤) to configure the SSIDs and/or passwords for your main wireless networks.

Figure 32 Wi-Fi Settings: Configuration



Each field is described in the following table.

Table 18 Wi-Fi Settings: Configuration

| LABEL | DESCRIPTION |
|---------------------------|---|
| Keep 2.4G and 5G the same | <p>Select this and the 2.4 GHz and 5 GHz wireless networks will use the same SSID.</p> <p>Note that you have to disable Zyxel MESH in the Network > Wireless > MESH screen to deselect the Keep 2.4G and 5G the same check box.</p> <p>If you deselect this, the screen will change. You need to assign different SSIDs for the 2.4 GHz and 5 GHz wireless networks.</p>  |
| 2.4G/5G WiFi | Click this switch to enable or disable the 2.4 GHz and/or 5 GHz wireless networks. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Wi-Fi Name | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |
| Wi-Fi Password | <p>If you selected Random Password, this field displays a pre-shared key generated by the Zyxel Device.</p> <p>If you did not select Random Password, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.</p> |
| | Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed  , you'll see the password in plain text. Otherwise, it's hidden. |
| Random Password | Select this option to have the Zyxel Device automatically generate a password. The Wi-Fi Password field will not be configurable when you select this option. |
| Hide Wi-Fi Name | <p>Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.</p> <p>Note: Disable WPS in the Network Setting > Wireless > WPS screen to hide the SSID.</p> |
| Save | Click Save to save your changes. |

5.1.4 The Guest Wi-Fi Settings Screen

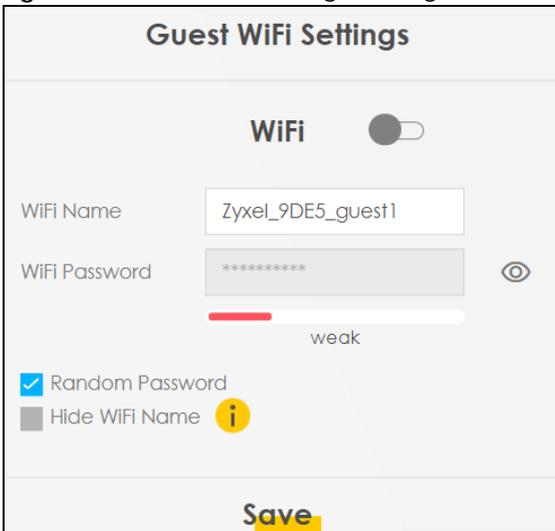
Use this screen to enable or disable the guest 2.4 GHz and/or 5 GHz wireless networks. When the switch turns blue () , the function is enabled. Otherwise, it's not. You can check their SSIDs (WiFi network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click the Eye icon.

Figure 33 Guest Wi-Fi Settings



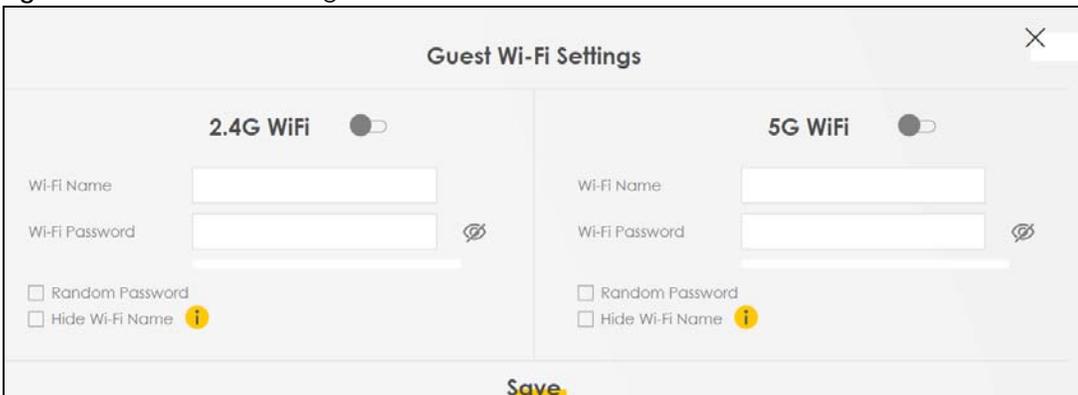
Click the Arrow icon (➔) to configure the SSIDs and/or passwords for your guest wireless networks.

Figure 34 Guest Wi-Fi Settings: Configuration



To assign different SSIDs for the 2.4 GHz and 5 GHz wireless networks, deselect **Keep 2.4G and 5G the same** in the **Wi-Fi Settings** screen, and the **Guest Wi-Fi Settings** screen will change. Note that you have to disable Zyxel MESH in the **Network > Wireless > MESH** screen to deselect the **Keep 2.4G and 5G the same** check box.

Figure 35 Guest Wi-Fi Settings: Different SSIDs



Each field is described in the following table.

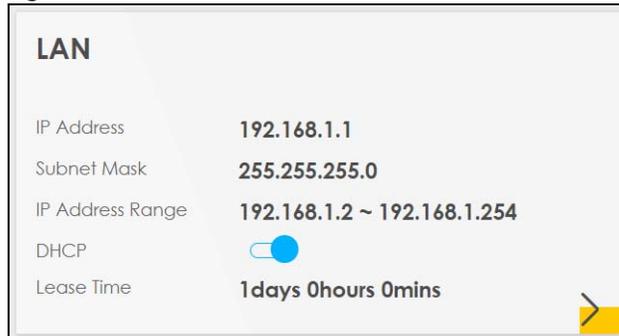
Table 19 Wi-Fi Settings: Configuration

| LABEL | DESCRIPTION |
|----------------------|--|
| WiFi 2.4G/5G WiFi | Click this switch to enable or disable the 2.4 GHz and/or 5 GHz wireless networks. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Wi-Fi Name | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |
| Wi-Fi Password | If you selected Random Password , this field displays a pre-shared key generated by the Zyxel Device. If you did not select Random Password , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. |
| | Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed  , you'll see the password in plain text. Otherwise, it's hidden. |
| Random Password | Select this option to have the Zyxel Device automatically generate a password. The Wi-Fi Password field will not be configurable when you select this option. |
| Hide Wi-Fi Name | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the Network Setting > Wireless > WPS screen to hide the SSID. |
| Save | Click Save to save your changes. |

5.1.5 The LAN Screen

Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device.

Figure 36 LAN



Click the Arrow icon () to configure the LAN IP settings and DHCP setting for your Zyxel Device.

Figure 37 LAN Setup

The screenshot shows a 'LAN' configuration window. It is divided into three main sections:

- LAN IP Setup:** Contains two input fields. 'IP Address' is set to '192 . 168 . 1 . 1' and 'Subnet Mask' is set to '255 . 255 . 255 . 0'.
- IP Addressing Values:** Contains two input fields. 'Beginning IP Address' is set to '192 . 168 . 1 . 2' and 'Ending IP Address' is set to '192 . 168 . 1 . 254'.
- DHCP Server State:** Contains a 'DHCP Server Lease Time' field set to '1' days, '0' hours, and '0' minutes.

A 'Save' button is located at the bottom center of the window.

Each field is described in the following table.

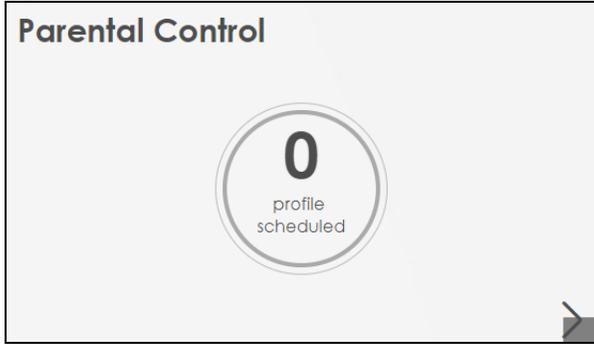
Table 20 Status Screen

| LABEL | DESCRIPTION |
|------------------------|---|
| LAN IP Setup | |
| IP Address | Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default). |
| Subnet Mask | Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so. |
| IP Addressing Values | |
| Beginning IP Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Ending IP Address | This field specifies the last of the contiguous addresses in the IP address pool. |
| DHCP Server State | |
| DHCP Server Lease Time | This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. |
| Days/Hours/Minutes | Enter the lease time of the DHCP server. |
| Save | Click Save to save your changes. |

5.1.6 The Parental Control Screen

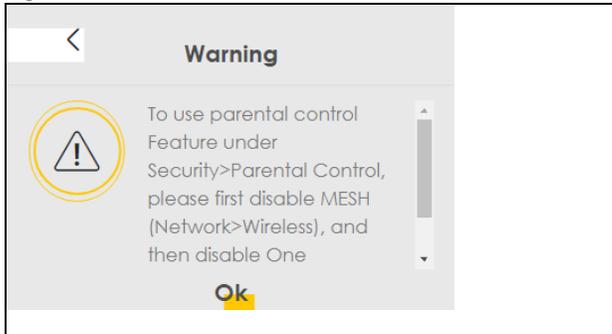
Use this screen to view the number of profiles that were created for parental control.

Figure 38 Parental Control



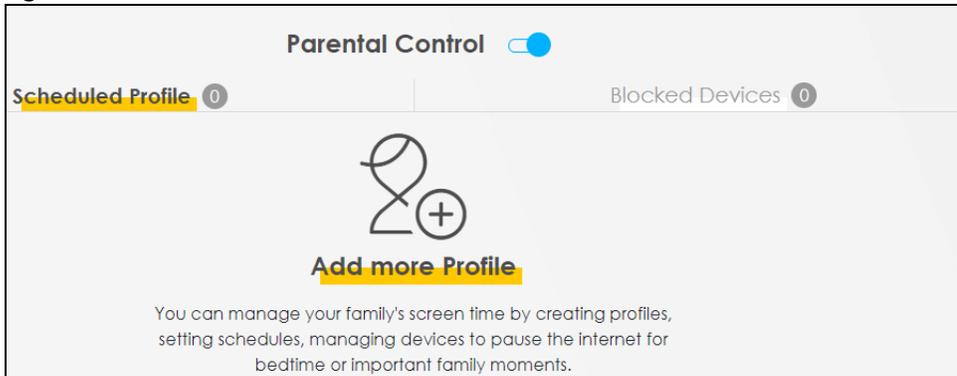
The Arrow icon is grayed out (➤) when the One Connect feature is enabled in the **Network > Home Connectivity** screen. This means you can't configure parental control settings. If you click the grayed-out Arrow icon, the following message will appear.

Figure 39 Cannot Use Parental Control



Disable the One Connect feature in the **Network > Home Connectivity** screen, and the grayed-out Arrow icon should turn yellow (➤). Click the yellow Arrow icon to enable parental control and add more profiles.

Figure 40 Parental Control



Each field is described in the following table.

Table 21 Parental Control: Schedule

| LABEL | DESCRIPTION |
|------------------|--|
| Parental Control | Click this switch to enable or disable parental control. When the switch turns blue (), the function is enabled. Otherwise, it's not. |

Table 21 Parental Control: Schedule (continued)

| LABEL | DESCRIPTION |
|-------------------|---|
| Scheduled Profile | This screen shows all the created profile(s). |
| Blocked Devices | The screen shows the profile devices that are not allowed to access the Internet. |

Click **Add more Profile** to create a profile. Use this screen to add a device(s) in a profile and block Internet access on the profile device(s).

Figure 41 Parental Control: Add More Profile

Each field is described in the following table.

Table 22 Parental Control: Add More Profile

| LABEL | DESCRIPTION |
|---------------------|--|
| Profile Name | Enter a descriptive name for the profile. |
| Internet Blocking | Click this switch to enable or disable Internet access. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Profile Device List | This field shows the devices selected on the right for this profile. |
| Blocking Schedule | This field shows the time during which Internet access is blocked on the profile device(s). |
| | Select a device(s) on your network for this profile. |

Click **Next** to define time periods and days during which Internet access is blocked on the profile device(s).

Figure 42 Parental Control: Schedule

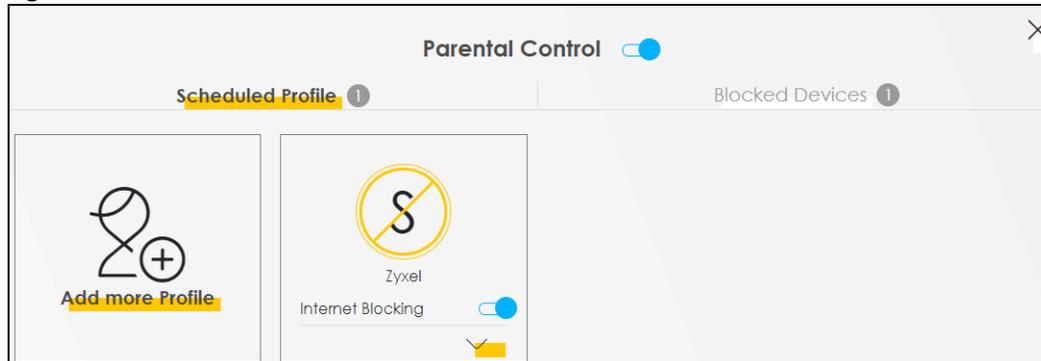
Each field is described in the following table.

Table 23 Parental Control: Schedule

| LABEL | DESCRIPTION |
|---------------------|--|
| Profile Name | Enter a descriptive name for the profile. |
| Internet Blocking | Click this switch to enable or disable Internet access. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Profile Device List | This field shows the devices selected on the right for this profile. |
| Blocking Schedule | This field shows the time during which Internet access is blocked on the profile device(s). |
| Schedule | |
| Add New Schedule | Click this to add a new block for scheduling. |
| Start/End blocking | Select the time period when Internet access is blocked on the profile device(s). Select All Day and the scheduler rule will be activated for 24 hours. |
| Repeat On | Select the days when Internet access is blocked on the profile device(s). |
| Back | Click Back to return to the previous screen. |
| Save | Click Save to save your changes. |

Once a profile is created, it'll show in the following screen. Click this  to **Delete** or **Edit** a profile.

Figure 43 Parental Control: Added Profile



CHAPTER 6

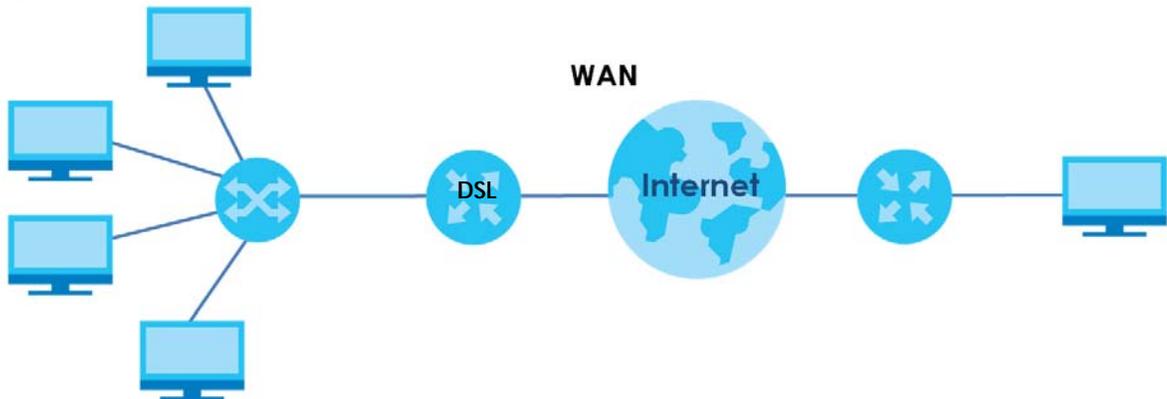
Broadband

6.1 Overview

This chapter discusses the Zyxel Device's **Broadband** screens. Use these screens to configure your Zyxel Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 44 LAN and WAN



6.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the Zyxel Device for Internet access ([Section 6.2 on page 97](#)).
- Use the **Cellular Backup** screen to configure cellular WAN connection ([Section 6.3 on page 107](#)).
- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions ([Section 6.4 on page 113](#)).

Table 24 WAN Setup Overview

| LAYER-2 INTERFACE | | INTERNET CONNECTION | | |
|--------------------|---------------|---------------------|---------------|--|
| CONNECTION | DSL LINK TYPE | MODE | ENCAPSULATION | CONNECTION SETTINGS |
| ADSL/VDSL over PTM | N/A | Routing | PPPoE | PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | | IPoE | IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | Bridge | N/A | VLAN and QoS |

Table 24 WAN Setup Overview

| LAYER-2 INTERFACE | | INTERNET CONNECTION | | |
|-------------------|---------------|---------------------|---------------|---|
| CONNECTION | DSL LINK TYPE | MODE | ENCAPSULATION | CONNECTION SETTINGS |
| ADSL over ATM | EoA | Routing | PPPoE/PPPoA | ATM PVC configuration, PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | | IPoE/IPoA | ATM PVC configuration, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | Bridge | N/A | ATM PVC configuration, and QoS |
| Ethernet | N/A | Routing | PPPoE | PPP user name and password, WAN IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU |
| | | | IPoE | WAN IPv4/IPv6 IP address, NAT, DNS server and routing feature |
| | | Bridge | N/A | VLAN and QoS |

6.1.2 What You Need to Know

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

WAN IP Address

The WAN IP address is an IP address for the Zyxel Device, which makes it accessible from an outside network. It is used by the Zyxel Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the Zyxel Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

ATM

Asynchronous Transfer Mode (ATM) is a WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between Finding Out More

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

IPv6 Introduction

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

IPv6 Subnet Masking

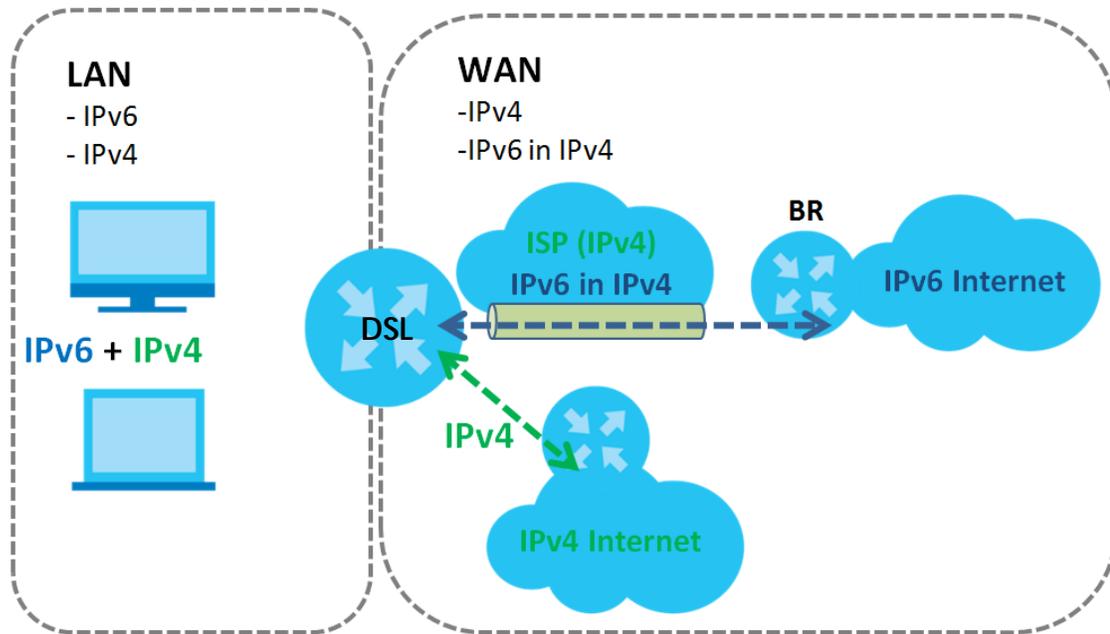
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example,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

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the Zyxel Device has an IPv4 WAN address and you set **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The Zyxel Device generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The Zyxel Device uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 45 IPv6 Rapid Deployment

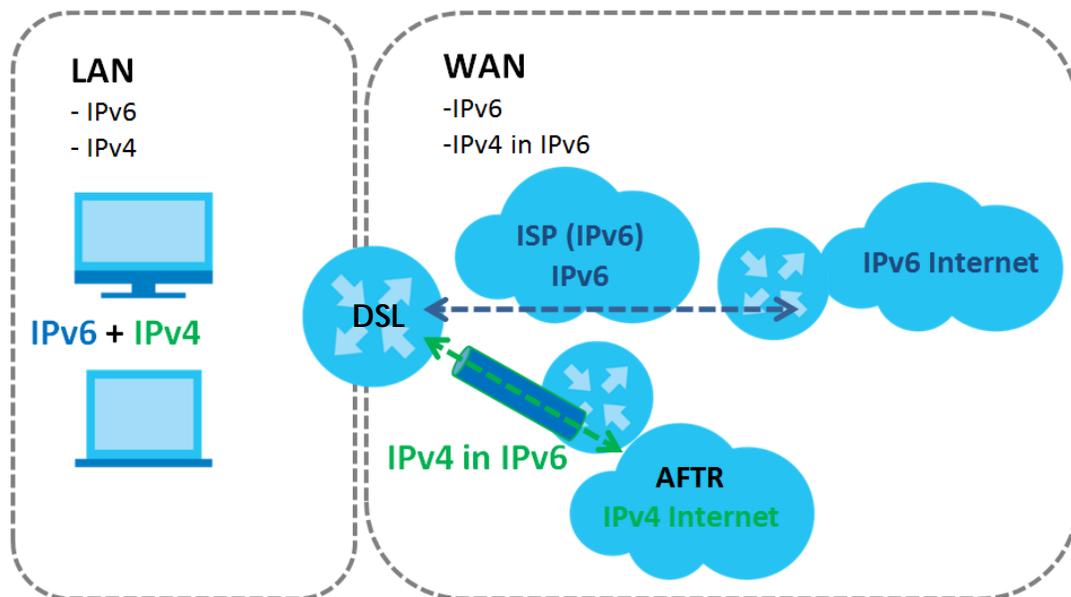


Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the Zyxel Device has an IPv6 WAN address and you set **IPv6/IPv4 Mode** to **IPv6 Only**, you can enable Dual Stack Lite to use IPv4 computers and services.

The Zyxel Device tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP's Address Family Transition Router (AFTR in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The Zyxel Device uses its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 46 Dual Stack Lite



6.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

6.2 The Broadband Screen

Use this screen to change your Zyxel Device's Internet access settings. The summary table shows you the configured WAN services (connections) on the Zyxel Device. Use information provided by your ISP to configure WAN settings.

Click **Network Setting > Broadband** to access this screen.

Figure 47 Network Setting > Broadband

| # | Name | Type | Mode | Encapsulation | 802.1p | 802.1q | IGMP Proxy | NAT | Default Gateway | IPv6 | MLD Proxy | Modify |
|---|--------|------|---------|---------------|--------|--------|------------|-----|-----------------|------|-----------|--------|
| 1 | ADSL | ATM | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |
| 2 | VDSL | PTM | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |
| 3 | ETHWAN | ETH | Routing | IPoE | N/A | N/A | Y | Y | Y | Y | Y | |

The following table describes the labels in this screen.

Table 25 Network Setting > Broadband

| LABEL | DESCRIPTION |
|-----------------------|---|
| Add New WAN Interface | Click this button to create a new connection. |
| # | This is the index number of the entry. |
| Name | This is the service name of the connection. |
| Type | This shows whether it is an ATM, Ethernet or a PTM connection. |
| Mode | This shows whether the connection is in routing or bridge mode. |
| Encapsulation | This is the method of encapsulation used by this connection. |
| 802.1p | This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays N/A when there is no priority level assigned. |
| 802.1q | This indicates the VLAN ID number assigned to traffic sent through this connection. This displays N/A when there is no VLAN ID number assigned. |
| IGMP Proxy | This shows whether the Zyxel Device act as an IGMP proxy on this connection. |
| NAT | This shows whether NAT is activated or not for this connection. |

Table 25 Network Setting > Broadband (continued)

| LABEL | DESCRIPTION |
|-----------------|--|
| Default Gateway | This shows whether the Zyxel Device use the WAN interface of this connection as the system default gateway. |
| IPv6 | This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service. |
| MLD Proxy | This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service. |
| Modify | Click the Edit icon to configure the WAN connection. Click the Delete icon to remove the WAN connection. |

6.2.1 Add/Edit Internet Connection

Click **Add New WAN Interface** in the **Broadband** screen or the **Edit** icon next to an existing WAN interface to configure a WAN connection. The screen varies depending on the interface type, mode, encapsulation, and IPv6/IPv4 mode you select.

6.2.1.1 Routing Mode

Use **Routing** mode if your ISP give you one IP address only and you want multiple computers to share an Internet account.

The following example screen displays when you select the **ADSL over ATM** connection type, **Routing** mode, and **PPPoE** encapsulation. The screen varies when you select other interface type, encapsulation, and IPv6/IPv4 mode.

Figure 48 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)

Add New WAN Interface

General

Name:

Type: ADSL over ATM

Mode: Routing

Encapsulation: PPPoE

IPv4/IPv6 Mode: **IPv4 IPv6 DualStack**

PPP Information

PPP User Name: admin

PPP Password:

PPP Connection: Auto Connect On Demand

PPP Trigger:

PPPoE Passthrough:

ATM PVC Configuration

VPI [0-255]: 0

VCI [32-65535]: 33

Encapsulation: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

VLAN

802.1p: 0

802.1q: [1-4094]

MTU

MTU: 1492

IP Address

Obtain an IP Address Automatically

Static IP Address

DNS Server

Obtain DNS Info Automatically

Use Following Static DNS Address

Routing Feature

NAT: IGMP Proxy:

Apply as Default Gateway: Fullcone NAT:

IPv6 Address

Obtain an IPv6 Address Automatically

Static IPv6 Address

IPv6 DNS Server

Obtain IPv6 DNS Info Automatically

Use Following Static IPv6 DNS Address

IPv6 Routing Feature

MLD Proxy: Apply as Default Gateway:

Cancel Apply

The following table describes the labels in this screen.

Table 26 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)

| LABEL | DESCRIPTION |
|---------|--|
| General | Click this switch to enable or disable the interface. When the switch turns blue <input checked="" type="checkbox"/> , the function is enabled. Otherwise, it's not. |
| Name | Specify a descriptive name for this connection. |
| Type | Select whether it is an ADSL/VDSL over PTM or ADSL over ATM connection. |

Table 26 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Mode | Select Routing if your ISP give you one IP address only and you want multiple computers to share an Internet account. |
| Encapsulation | Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select Routing in the Mode field. The choices depend on the connection type you selected. If your connection type is ADSL/VDSL over PTM , the choices are PPPoE and IPoE . If your connection type is ADSL over ATM , the choices are PPPoE , PPPoA , IPoE and IPoA . If your connection type is Ethernet , the choices are PPPoE and IPoE . |
| IPv4/IPv6 Mode | Select IPv4 Only if you want the Zyxel Device to run IPv4 only. Select IPv4 IPv6 DualStack to allow the Zyxel Device to run IPv4 and IPv6 at the same time. Select IPv6 Only if you want the Zyxel Device to run IPv6 only. |
| PPP Information (This is available only when you select PPPoE or PPPoA in the Mode field.) | |
| PPP User Name | Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given. |
| PPP Password | Enter the password associated with the user name above. Select password unmask to show your entered password in plain text. |
| PPP Connection Trigger | Select when to have the Zyxel Device establish the PPP connection. Auto Connect - select this to not let the connection time out. On Demand - select this to automatically bring up the connection when the Zyxel Device receives packets destined for the Internet. |
| Idle Timeout | This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not available if you select Auto Connect in the PPP Connection Trigger field. |
| PPPoE Passthrough | This field is available when you select PPPoE encapsulation. In addition to the Zyxel Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Zyxel Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP. |
| ATM PVC Configuration (These fields appear when the Type is set to ADSL over ATM .) | |
| VPI [0-255] | The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. |
| VCI [32-65535] | The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you. |
| Encapsulation | Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: <ul style="list-style-type: none"> LLC/SNAP-BRIDGING: In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select IPoE or PPPoE in the Select DSL Link Type field. VC/MUX: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Zyxel Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. |

Table 26 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|--|
| Service Category | Select UBR Without PCR for applications that are non-time sensitive, such as e-mail. Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation. |
| Peak Cell Rate [cells/s] | Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. |
| Sustainable Cell Rate | The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. |
| Maximum Burst Size [cells] | Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. |
| VLAN | (These fields appear when the Type is set to ADSL/VDSL over PTM or ADSL over ATM .) Click this switch to enable or disable VLAN on this WAN interface. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| 802.1p | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| 802.1q | Type the VLAN ID number (from 1 to 4094) for traffic through this connection. |
| MTU | |
| MTU | Enter the MTU (Maximum Transfer Unit) size for this traffic. |
| IP Address (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.) | |
| Obtain an IP Address Automatically | A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address. |
| Static IP Address | Select this option if the ISP assigned a fixed IP address. |
| IP Address | Enter the static IP address provided by your ISP. |
| Subnet Mask | Enter the subnet mask provided by your ISP. |
| Gateway IP Address | Enter the gateway IP address provided by your ISP. |
| DNS Server (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.) | |
| | Select Obtain DNS Info Automatically if you want the Zyxel Device to use the DNS server addresses assigned by your ISP. Select Use Following Static DNS Address if you want the Zyxel Device to use the DNS server addresses you configure manually. |
| Primary DNS Server | Enter the first DNS server address assigned by the ISP. |
| Secondary DNS Server | Enter the second DNS server address assigned by the ISP. |
| Routing Feature (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.) | |
| NAT | Click this switch to activate or deactivate NAT on this connection. When the switch turns blue  , the function is enabled. Otherwise, it's not. |

Table 26 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| IGMP Proxy | <p>Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p> <p>Click this switch to have the Zyxel Device act as an IGMP proxy on this connection. When the switch turns blue , the function is enabled. Otherwise, it's not.</p> <p>This allows the Zyxel Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.</p> |
| Apply as Default Gateway | <p>Click this switch to have the Zyxel Device use the WAN interface of this connection as the system default gateway. When the switch turns blue , the function is enabled. Otherwise, it's not.</p> |
| Fullcone NAT Enable | <p>Click this switch to enable or disable full cone NAT on this connection. When the switch turns blue , the function is enabled. Otherwise, it's not.</p> <p>This field is available only when you activate NAT.</p> <p>In full cone NAT, the Zyxel Device maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The Zyxel Device also maps packets coming to that external IP address and port to the internal IP address and port.</p> |
| DHCP Options (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.) | |
| Request Options | <p>Select Option 43 to have the Zyxel Device automatically add vendor specific information in the DHCP packets to request the vendor specific options from the DHCP server.</p> <p>Select Option 120 to have the Zyxel Device get the IP address or a fully-qualified domain name of SIP server from DHCP.</p> <p>Select Option 121 to have the Zyxel Device push static routes to clients.</p> |
| Sent Options | |
| option 60 | <p>Select this and enter the device identity you want the Zyxel Device to add in the DHCP discovery packets that go to the DHCP server.</p> |
| Vendor ID | <p>Enter the Vendor Class Identifier, such as the type of the hardware or firmware.</p> |
| option 61 | <p>Select this and enter any string that identifies the device.</p> |
| IAID | <p>Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.</p> |
| DUID | <p>Enter the hardware type, a time value and the MAC address of the device.</p> |
| option 125 | <p>Select this to have the Zyxel Device automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.</p> |
| IPv6 Address (This is available only when you select IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field.) | |
| Obtain an IPv6 Address Automatically | <p>Select Obtain an IPv6 Address Automatically if you want to have the Zyxel Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.</p> |
| Static IPv6 Address | <p>Select Static IPv6 Address if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.</p> |
| IPv6 Address | <p>Enter an IPv6 IP address that your ISP gave to you for this WAN interface.</p> |
| PrefixLength | <p>Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.</p> |
| IPv6 Default Gateway | <p>Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.</p> |
| IPv6 DNS Server (This is available only when you select IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field. Configure the IPv6 DNS server in the following section.) | |
| Obtain IPv6 DNS Info Automatically | <p>Select Obtain IPv6 DNS Info Automatically to have the Zyxel Device get the IPv6 DNS server addresses from the ISP automatically.</p> |

Table 26 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Use Following Static IPv6 DNS Address | Select Use Following Static IPv6 DNS Address to have the Zyxel Device use the IPv6 DNS server addresses you configure manually. |
| Primary DNS Server | Enter the first IPv6 DNS server address assigned by the ISP. |
| Secondary DNS Server | Enter the second IPv6 DNS server address assigned by the ISP. |
| IPv6 Routing Feature (This is available only when you select IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field. You can enable IPv6 routing features in the following section.) | |
| MLD Proxy Enable | Select this check box to have the Zyxel Device act as an MLD proxy on this connection. This allows the Zyxel Device to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly. |
| Apply as Default Gateway | Select this option to have the Zyxel Device use the WAN interface of this connection as the system default gateway. |
| DS-Lite | This is available only when you select IPv6 Only in the IPv4/IPv6 Mode field. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 96 for more information. Click this switch to let local computers use IPv4 through an ISP's IPv6 network. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| DS-Lite Relay Server IP | Specify the transition router's IPv6 address. |
| 6RD | The 6RD (IPv6 rapid deployment) fields display when you set the IPv6/IPv4 Mode field to IPv4 Only . See IPv6 Rapid Deployment on page 95 for more information. Click this switch to tunnel IPv6 traffic from the local network through the ISP's IPv4 network. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| | Select Manually Configured if you have the IPv4 address of the relay server. Otherwise, select Automatically configured by DHCP to have the Zyxel Device detect it automatically through DHCP. The Automatically configured by DHCP option is configurable only when you set the method of encapsulation to IPoE . |
| Service Provider IPv6 Prefix | Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet. |
| IPv4 Mask Length | Enter the subnet mask number (1~32) for the IPv4 network. |
| Border Relay IPv4 Address | When you select Manually Configured , specify the relay server's IPv4 address in this field. |
| Bridge and Routing mode in the same WAN | |
| | |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

6.2.1.2 Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Bridge** as the encapsulation mode. The screen varies depending on the interface type you select.

If you select **ADSL/VDSL over PTM** or **Ethernet** as the interface type, the following screen appears.

Figure 49 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM or Ethernet-Bridge Mode)

The following table describes the fields in this screen.

Table 27 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM or Ethernet-Bridge Mode)

| LABEL | DESCRIPTION |
|---------|--|
| General | Click this switch to enable or disable the interface. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Name | Enter a service name of the connection. |
| Type | Select ADSL/VDSL over PTM as the interface that you want to configure. The Zyxel Device uses the VDSL technology for data transmission over the DSL port. |
| Mode | Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select Bridge , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s). |
| VLAN | This section is available when you select ADSL/VDSL over PTM in the Type field. Click this switch to enable or disable VLAN on this WAN interface. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| 802.1p | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| 802.1q | Type the VLAN ID number (from 0 to 4094) for traffic through this connection. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

If you select **ADSL over ATM** as the interface type, the following screen appears.

Figure 50 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

The following table describes the fields in this screen.

Table 28 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

| LABEL | DESCRIPTION |
|---|---|
| General | Click this switch to enable or disable the interface. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Name | Enter a service name of the connection. |
| Type | Select ADSL over ATM as the interface that you want to configure. The Zyxel Device uses the ADSL technology for data transmission over the DSL port. |
| Mode | Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select Bridge , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s). |
| ATM PVC Configuration (These fields appear when the Type is set to ADSL over ATM .) | |
| VPI [0-255] | The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. |
| VCI [32-65535] | The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you. |
| Encapsulation | Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: <ul style="list-style-type: none"> • LLC/SNAP-BRIDGING: In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. • VC/MUX: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the Zyxel Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. |
| Service Category | Select UBR Without PCR for applications that are non-time sensitive, such as e-mail. Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation. |

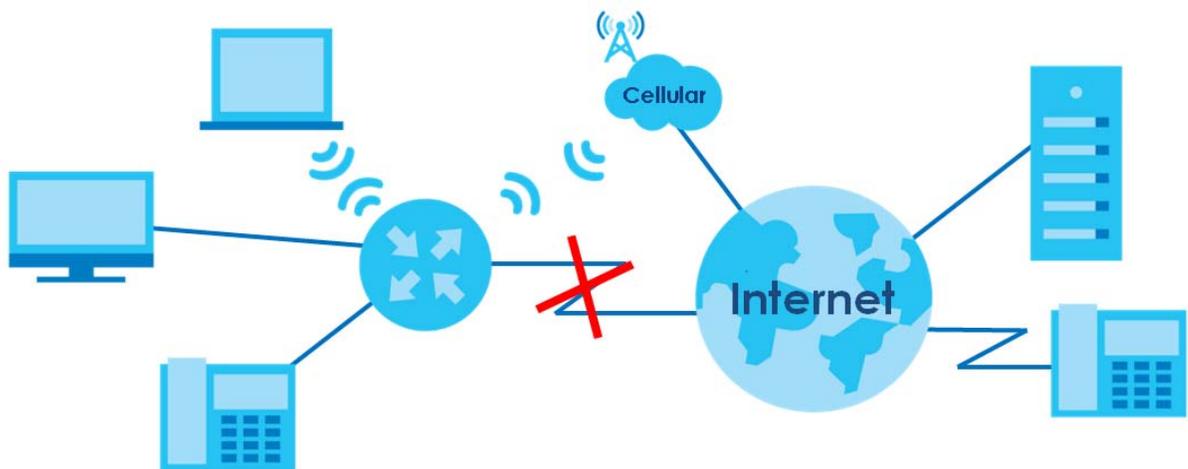
Table 28 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

| LABEL | DESCRIPTION |
|----------------------------|--|
| Peak Cell Rate [cells/s] | Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. |
| Sustainable Cell Rate | The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. |
| Maximum Burst Size [cells] | Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. |
| VLAN | This section is available only when you select ADSL over ATM in the Type field. Click this switch to enable or disable VLAN on this WAN interface. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| 802.1p | IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level. |
| 802.1q | Type the VLAN ID number (from 0 to 4094) for traffic through this connection. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

6.3 The Cellular Backup Screen

The USB port of the Zyxel Device allows you to attach a cellular dongle to wirelessly connect to a cellular network for Internet access. You can have the Zyxel Device use the cellular WAN connection as a backup to keep you online when the primary WAN connection fails. Consult with your cellular service provider to configure the settings in this screen. Disconnect the DSL and Ethernet WAN ports to use the cellular dongle as your primary WAN connection, as the Zyxel Device automatically uses a wired WAN connection when available.

Figure 51 Internet Access Application: Cellular WAN



Use this screen to configure your cellular settings. Click **Network Setting > Broadband > Cellular Backup**.

The actual data rate you obtain varies depending the cellular card you use, the signal strength to the service provider's base station, and so on.

Note: Entering a wrong PIN code three times will lock the SIM card.

Note: Budget control uses approximate values.

Figure 52 Network Setting > Broadband > Cellular Backup (General & Cellular Connection Setting)

Broadband

Broadband **Cellular Backup** Advanced

Whenever the WAN connection is down, Cellular Backup takes over the job and keeps you online. It is valid when a Cellular USB dongle is attached to the device and proper settings are configured. You may consult your Cellular service provider for the following settings.

General

Cellular Backup

Ping Check

Check Cycle Every (20~180 Sec)

Consecutive Fail (2~5 times)

Ping Default Gateway

Ping Host (Host name or IP address)

Note
Primary WAN is not in service when ping failed after consecutive times.

Cellular Connection Settings

Card Description N/A

Username (Optional)

Password (Optional)

Authentication ▼

PIN (Optional) (Only for unlock PIN next time)
(PIN remaining authentication times: N/A)

Dial String

APN

Connection ▼

Obtain an IP Address Automatically

Use the Following Static IP Address

Obtain DNS Info Dynamically

Use the Following Static DNS IP Address

Enable E-mail Notification

Note
Entering the wrong PIN code 3 times will lock SIM card.

Figure 53 Network > Broadband > Cellular Backup (Budget Setup)

Budget Setup

Enable Budget Control

Time Budget hours per month

Data Budget Mbytes per month

Data Budget kPackets per month

Reset all budget counters on day of the month

Reset time and data budget counters

Actions before over budget

Data Budget % of time budget

Data Budget % of data budget (Mbytes)

Data Budget % of data budget (Packets)

Actions when over budget

Current Cellular Connection

Actions

Enable E-mail Notification

Enable Log: Interval minutes

Note
Budget control is an approximate value.

[Cancel](#) [Apply](#)

The following table describes the labels in this screen.

Table 29 Network Setting > Broadband > Cellular Backup

| LABEL | DESCRIPTION |
|------------------------------|--|
| General | |
| Cellular Backup | Click this switch to have the Zyxel Device use the cellular connection as your WAN or a backup when the wired WAN connection fails. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Ping Check | Click this switch to ping check the connection status of your WAN. When the switch turns blue  , the function is enabled. Otherwise, it's not. You can configure the frequency of the ping check and number of consecutive failures before triggering cellular backup. |
| Check Cycle | Enter the frequency of the ping check in this field. |
| Consecutive Fail | Enter how many consecutive failures are required before cellular backup is triggered. |
| Ping Default Gateway | Select this to have the Zyxel Device ping the WAN interface's default gateway IP address. |
| Ping the Host | Select this to have the Zyxel Device ping the particular host name or IP address you typed in this field. |
| Cellular Connection Settings | |
| Card description | This field displays the manufacturer and model name of your cellular card if you inserted one in the Zyxel Device. Otherwise, it displays N/A . |
| Username | Type the user name (of up to 64 ASCII printable characters) given to you by your service provider. |
| Password | Type the password (of up to 64 ASCII printable characters) associated with the user name above. |

Table 29 Network Setting > Broadband > Cellular Backup (continued)

| LABEL | DESCRIPTION |
|---|---|
| PIN | <p>A PIN (Personal Identification Number) code is a key to a cellular card. Without the PIN code, you cannot use the cellular card.</p> <p>If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the cellular card may be blocked by your ISP and you cannot use the account to access the Internet.</p> <p>If your ISP disabled PIN code authentication, leave this field blank.</p> |
| Dial string | <p>Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number.</p> <p>For example, *99# is the dial string to establish a GPRS or cellular connection in Taiwan.</p> |
| APN | <p>Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method.</p> <p>You can enter up to 32 ASCII printable characters. Spaces are allowed.</p> |
| Connection | <p>Select Nailed UP if you do not want the connection to time out.</p> <p>Select on Demand if you do not want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.</p> |
| Max Idle Timeout | <p>This value specifies the time in minutes that elapses before the Zyxel Device automatically disconnects from the ISP.</p> |
| Obtain an IP Address Automatically | <p>Select this option if your ISP did not assign you a fixed IP address.</p> |
| Use the following static IP address | <p>Select this option if the ISP assigned a fixed IP address.</p> |
| IP Address | <p>Enter your WAN IP address in this field if you selected Use the following static IP address.</p> |
| Subnet Mask | <p>Enter the subnet mask of the IP address.</p> |
| Obtain DNS info dynamically | <p>Select this to have the Zyxel Device get the DNS server addresses from the ISP automatically.</p> |
| Use the following static DNS IP address | <p>Select this to have the Zyxel Device use the DNS server addresses you configure manually.</p> |
| Primary DNS server | <p>Enter the first DNS server address assigned by the ISP.</p> |
| Secondary DNS server | <p>Enter the second DNS server address assigned by the ISP.</p> |
| Enable Email Notification | <p>Select this to enable the e-mail notification function. The Zyxel Device will e-mail you a notification when the cellular connection is up.</p> |
| Mail Account | <p>Select an e-mail address you have configured in Maintenance > Email Notification. The Zyxel Device uses the corresponding mail server to send notifications.</p> <p>You must have configured a mail server already in the Maintenance > Email Notification screen.</p> |
| Cellular backup Email Title | <p>Type a title that you want to be in the subject line of the e-mail notifications that the Zyxel Device sends.</p> |
| Send Notification to Email | <p>Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail.</p> |
| | <p>Click this  to show the advanced cellular backup settings.</p> |
| Budget Setup | |

Table 29 Network Setting > Broadband > Cellular Backup (continued)

| LABEL | DESCRIPTION |
|--|---|
| Enable Budget Control | <p>Click this switch to set a monthly limit for the user account of the installed cellular card. When the switch turns blue , the function is enabled. Otherwise, it's not.</p> <p>You can set a limit on the total traffic and/or call time. The Zyxel Device takes the actions you specified when a limit is exceeded during the month.</p> |
| Time Budget | <p>Select this and specify the amount of time (in hours) that the cellular connection can be used within one month. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.</p> |
| Data Budget (Mbytes) | <p>Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the cellular connection within one month.</p> <p>Select Download/Upload to set a limit on the total traffic in both directions.</p> <p>Select Download to set a limit on the downstream traffic (from the ISP to the Zyxel Device).</p> <p>Select Upload to set a limit on the upstream traffic (from the Zyxel Device to the ISP).</p> <p>If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.</p> |
| Data Budget (kPackets) | <p>Select this and specify how much downstream and/or upstream data (in k Packets) can be transmitted via the cellular connection within one month.</p> <p>Select Download/Upload to set a limit on the total traffic in both directions.</p> <p>Select Download to set a limit on the downstream traffic (from the ISP to the Zyxel Device).</p> <p>Select Upload to set a limit on the upstream traffic (from the Zyxel Device to the ISP).</p> <p>If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.</p> |
| Reset all budget counters on | <p>Select the date on which the Zyxel Device resets the budget every month. Select last if you want the Zyxel Device to reset the budget on the last day of the month. Select specific and enter the number of the date you want the Zyxel Device to reset the budget</p> |
| Reset time and data budget counters | <p>Click this button to reset the time and data budgets immediately. The count starts over with the cellular connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.</p> |
| Actions before over budget | <p>Specify the actions the Zyxel Device takes before the time or data limit exceeds.</p> |
| Data Budget % of time budget/data budget (Mbytes)/data budget (kPackets) | <p>Select the check boxes and enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.</p> |
| Actions when over budget | <p>Specify the actions the Zyxel Device takes when the time or data limit is exceeded.</p> |
| Current Cellular connection | <p>Select Keep to maintain an existing cellular connection or Drop to disconnect it.</p> |
| Actions | |
| Enable Email Notification | <p>Click this switch to enable or disable the e-mail notification function. When the switch turns blue , the function is enabled. Otherwise, it's not.</p> <p>The Zyxel Device will e-mail you a notification when there over budget occurs.</p> |

Table 29 Network Setting > Broadband > Cellular Backup (continued)

| LABEL | DESCRIPTION |
|------------------------------|---|
| Mail Account | Select an e-mail address you have configured in Maintenance > Email Notification . The Zyxel Device uses the corresponding mail server to send notifications. You must have configured a mail server already in the Maintenance > Email Notification screen. |
| Cellular Backup E-mail Title | Type a title that you want to be in the subject line of the e-mail notifications that the Zyxel Device sends. |
| Send Notification to Email | Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail. |
| Interval | Enter the interval of how many minutes you want the Zyxel Device to e-mail you. |
| Enable Log | Select this to activate the logging function at the interval you set in this field. |
| Cancel | Click Cancel to return to the previous configuration. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |

6.4 The Broadband Advanced Screen

Use the **Advanced** screen to enable or disable ADSL over PTM, Annex M, DSL PhyR, and SRA (Seamless Rate Adaptation) functions. The Zyxel Device supports the PhyR retransmission scheme. PhyR is a retransmission scheme designed to provide protection against noise on the DSL line. It improves voice, video and data transmission resilience by utilizing a retransmission buffer. It also lists ITU-T G.993.2 standard VDSL profiles you can comply with.

ITU-T G.993.2 standard defines a wide range of settings for various parameters, some of which are encompassed in profiles as shown in the next table.

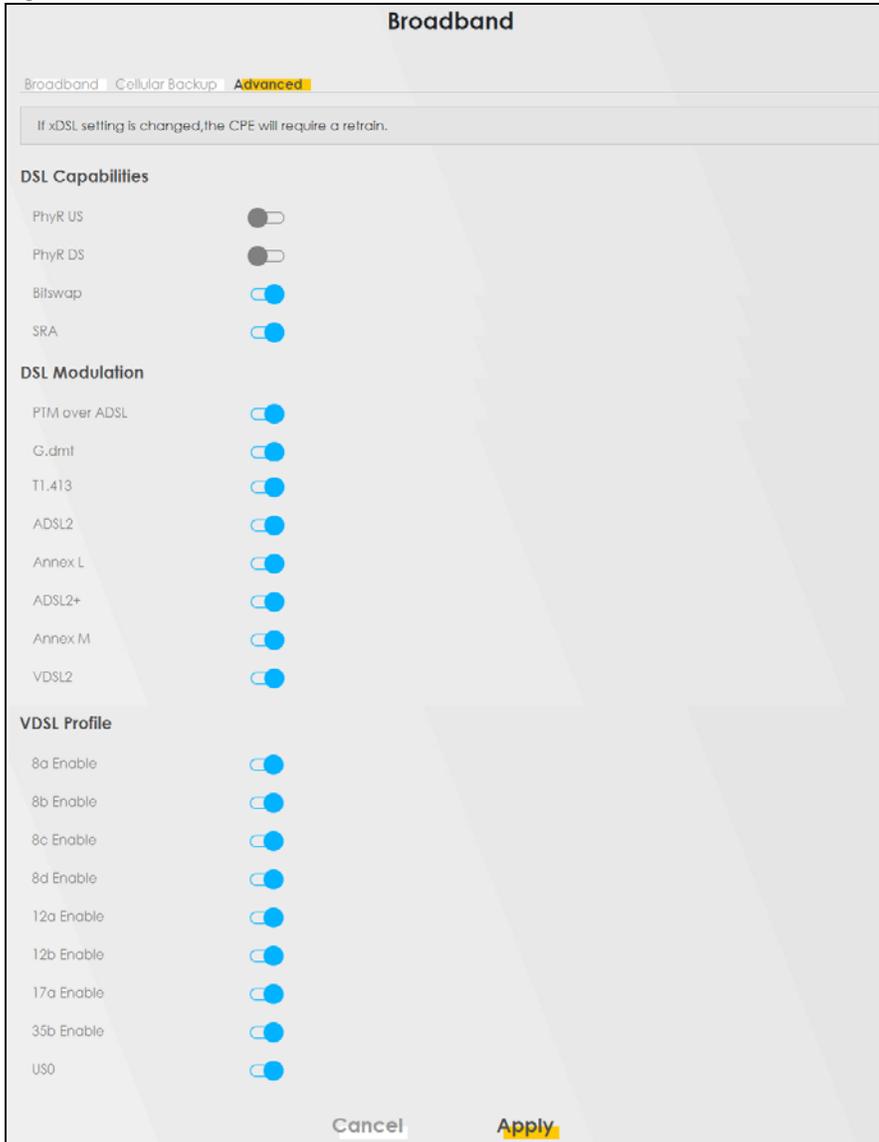
Note: If the settings in the screen are changes, the Zyxel Device will re-establish the DSL connection(s).

Table 30 VDSL Profiles

| PROFILE | BANDWIDTH (MHZ) | NUMBER OF DOWNSTREAM CARRIERS | CARRIER BANDWIDTH (KHZ) | POWER (DBM) | MAX. DOWNSTREAM THROUGHPUT (MBIT/S) |
|---------|-----------------|-------------------------------|-------------------------|-------------|-------------------------------------|
| 8a | 8.832 | 2048 | 4.3125 | 17.5 | 50 |
| 8b | 8.832 | 2048 | 4.3125 | 20.5 | 50 |
| 8c | 8.5 | 1972 | 4.3125 | 11.5 | 50 |
| 8d | 8.832 | 2048 | 4.3125 | 14.5 | 50 |
| 12a | 12 | 2783 | 4.3125 | 14.5 | 68 |
| 12b | 12 | 2783 | 4.3125 | 14.5 | 68 |
| 17a | 17.664 | 4096 | 4.3125 | 14.5 | 100 |
| 35b | 35.328 | 8192 | 4.3125 | 17.0 | 300 |

Click **Network Setting > Broadband > Advanced** to display the following screen.

Figure 54 Network Setting > Broadband > Advanced



The following table describes the labels in this screen.

Table 31 Network Setting > Broadband > Advanced

| LABEL | DESCRIPTION |
|------------------|--|
| DSL Capabilities | |
| PhyR US | Enable or disable PhyR US (upstream) for upstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled. |
| PhyR DS | Enable or disable PhyR DS (downstream) for downstream transmission from the WAN. PhyR DS should be enabled if data being transmitted downstream is sensitive to noise. However, enabling PhyR DS can decrease the DS line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled. |
| Bitswap | Select Enable to allow the Zyxel Device to adapt to line changes when you are using G.dmt. Bit-swapping is a way of keeping the line more stable by constantly monitoring and redistributing bits between channels. |

Table 31 Network Setting > Broadband > Advanced (continued)

| LABEL | DESCRIPTION |
|--|---|
| SRA | Enable or disable Seamless Rate Adaption (SRA). Select Enable to have the Zyxel Device automatically adjust the connection's data rate according to line conditions without interrupting service. |
| DSL Modulation | |
| PTM over ADSL: | Select Enable to use PTM over ADSL. Since PTM has less overhead than ATM, some ISPs use this for better performance. |
| G.Dmt: | ITU G.992.1 (better known as G.dmt) is an ITU standard for ADSL using discrete multitone modulation. G.dmt full-rate ADSL expands the usable bandwidth of existing copper telephone lines, delivering high-speed data communications at rates up to 8 Mbit/s downstream and 1.3 Mbit/s upstream. |
| G.lite : | ITU G.992.2 (better known as G.lite) is an ITU standard for ADSL using discrete multitone modulation. G.lite does not strictly require the use of DSL filters, but like all variants of ADSL generally functions better with splitters. |
| T1.413 : | ANSI T1.413 is a technical standard that defines the requirements for the single asymmetric digital subscriber line (ADSL) for the interface between the telecommunications network and the customer installation in terms of their interaction and electrical characteristics. |
| ADSL2 : | It optionally extends the capability of basic ADSL in data rates to 12 Mbit/s downstream and, depending on Annex version, up to 3.5 Mbit/s upstream (with a mandatory capability of ADSL2 transceivers of 8 Mbit/s downstream and 800 kbit/s upstream). |
| Annex L : | Annex L is an optional specification in the ITU-T ADSL2 recommendation G.992.3 titled Specific requirements for a Reach Extended ADSL2 (READSL2) system operating in the frequency band above POTS, therefore it is often referred to as Reach Extended ADSL2 or READSL2. The main difference between this specification and commonly deployed Annex A is the maximum distance that can be used. The power of the lower frequencies used for transmitting data is boosted up to increase the reach of this signal up to 7 kilometers (23,000 ft). |
| ADSL2+ : | ADSL2+ extends the capability of basic ADSL by doubling the number of downstream channels. The data rates can be as high as 24 Mbit/s downstream and up to 1.4 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises. |
| Annex M : | Annex M is an optional specification in ITU-T recommendations G.992.3 (ADSL2) and G.992.5 (ADSL2+), also referred to as ADSL2 M and ADSL2+ M. This specification extends the capability of commonly deployed Annex A by more than doubling the number of upstream bits. The data rates can be as high as 12 or 24 Mbit/s downstream and 3 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises. |
| VDSL2 | VDSL2 (Very High Speed Digital Subscriber Line 2) is the second generation of the VDSL standard (which is currently denoted VDSL1). VDSL2 allows a frequency band of up to 30MHz and transmission rates of up to 100 Mbps in each direction. VDSL2 is defined in G.993.2. |
| VDSL Profile | VDSL2 profiles differ in the width of the frequency band used to transmit the broadband signal. Profiles that use a wider frequency band can deliver higher maximum speeds. |
| 8a, 8b, 8c, 8d, 12a, 12b, 17a, 35b US0 | The G.993.2 VDSL standard defines a wide range of profiles that can be used in different VDSL deployment settings, such as in a central office, a street cabinet or a building. The Zyxel Device must comply with at least one profile specified in G.993.2. but compliance with more than one profile is allowed. |
| Cancel | Click Cancel to return to the previous configuration. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |

6.5 Technical Reference

The following section contains additional technical information about the Zyxel Device features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The Zyxel Device can work in bridge mode or routing mode. When the Zyxel Device is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over ATM (PPPoA)

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The Zyxel Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

PPP over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Zyxel Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Zyxel Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

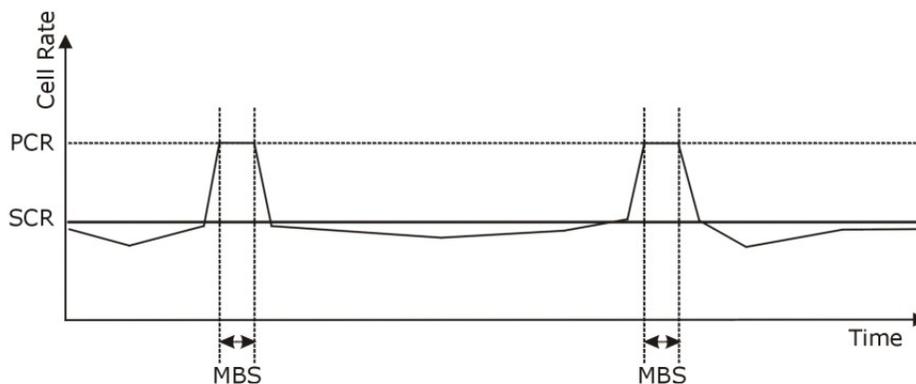
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 55 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

| TPID | User Priority | CFI | VLAN ID |
|---------|---------------|-------|---------|
| 2 Bytes | 3 Bits | 1 Bit | 12 Bits |

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the Zyxel Device queries all directly connected networks to gather group membership. After that, the Zyxel Device periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Zyxel Device can get the DNS server addresses in the following ways.

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the Zyxel Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

`2001:db8:1a2b:15::1a2f:0/32`

means that the first 32 bits (`2001:db8`) is the subnet prefix.

CHAPTER 7

Wireless

7.1 Wireless Overview

This chapter describes the Zyxel Device's **Network Setting > Wireless** screens. Use these screens to set up your Zyxel Device's wireless LAN connection and security settings.

7.1.1 What You Can Do in this Chapter

This section describes the Zyxel Device's **Wireless** screens. Use these screens to set up your Zyxel Device's wireless connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode ([Section 7.2 on page 122](#)).
- Use the **Guest/More AP** screen to set up multiple wireless networks on your Zyxel Device ([Section 7.3 on page 125](#)).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Zyxel Device ([Section 7.4 on page 129](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 7.5 on page 131](#)).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications ([Section 7.6 on page 132](#)).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold ([Section 7.7 on page 133](#)).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results ([Section 7.8 on page 136](#)).
- Use the **MESH** screen to enable or disable Zyxel Mesh (Multy Pro) ([Section 7.9 on page 136](#)).

7.1.2 What You Need to Know

Wireless Basics

“Wireless” is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Finding Out More

See [Section 7.10 on page 138](#) for advanced technical information on wireless networks.

7.2 The Wireless General Settings Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode. These are basic elements for starting a wireless service. It's recommended that you select **More Secure** to enable **WPA2-PSK** data encryption.

Note: If you are configuring the Zyxel Device from a computer connected to the wireless LAN and you change the Zyxel Device's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Zyxel Device's new settings.

Note: If upstream/downstream bandwidth is empty, the CPE sets the value automatically. Using maximum upstream/downstream bandwidth will significantly decrease wireless performance.

Click **Network Setting > Wireless** to open the **General** screen.

Figure 56 Network Setting > Wireless > General

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than no security to protect your data from unauthorized access or damage via wireless network.

Wireless

Wireless Keep 2.4G and 5G wireless network name the same

Wireless Network Setup

Band: 2.4GHz

Wireless:

Channel: 5 (Current: / MHz)

Bandwidth: 40MHz

Control Sideband: Lower

Wireless Network Settings

Wireless Network Name: Home&Life SuperWiFi-F0FD

Max Clients: 32

Hide SSID

Multicast Forwarding

Max. Upstream Bandwidth:

Max. Downstream Bandwidth:

Note

(1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.

(2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.

(3) If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

(4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID: 00:00:00:00:00:00

Security Level

No Security More Secure (Recommended)

Security Mode:

Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits [0-9, 'A-F']:

Password: F77P6CJ2BNK17G

Cancel **Apply**

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

Table 32 Network Setting > Wireless > General

| LABEL | DESCRIPTION |
|---------------------------|---|
| Wireless | |
| Wireless | Select Keep 2.4G and 5G wireless network name the same and the 2.4 GHz and 5 GHz wireless networks will use the same SSID. |
| Wireless Network Setup | |
| Band | This shows the wireless band which this radio profile is using. 2.4GHz is the frequency used by IEEE 802.11b/g/n wireless clients while 5GHz is used by IEEE 802.11a/ac wireless clients. |
| Wireless | Click this switch to enable or disable the wireless LAN in this field. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Channel | Use Auto to have the Zyxel Device automatically determine a channel to use. |
| Bandwidth | <p>Select whether the Zyxel Device uses a wireless channel width of 20MHz, 40MHz or 80MHz.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>An 80MHz channel groups adjacent 40MHz channels into pairs to increase bandwidth even higher.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p> |
| Control Sideband | This is available for some regions when you select a specific channel and set the Bandwidth field to 40MHz . Set whether the control channel (set in the Channel field) should be in the Lower or Upper range of channel bands. |
| Wireless Network Settings | |
| Wireless Network Name | <p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.</p> <p>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.</p> |
| Max Clients | Specify the maximum number of clients that can connect to this network at the same time. |
| Hide SSID | <p>Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.</p> <p>This check box is grayed out if the WPS function is enabled in the Network > Wireless > WPS screen.</p> |
| Multicast Forwarding | Select this check box to allow the Zyxel Device to convert wireless multicast traffic into wireless unicast traffic. |
| Max. Upstream Bandwidth | Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps). |
| Max. Downstream Bandwidth | Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps). |
| BSSID | This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled. |
| Security Level | |

Table 32 Network Setting > Wireless > General (continued)

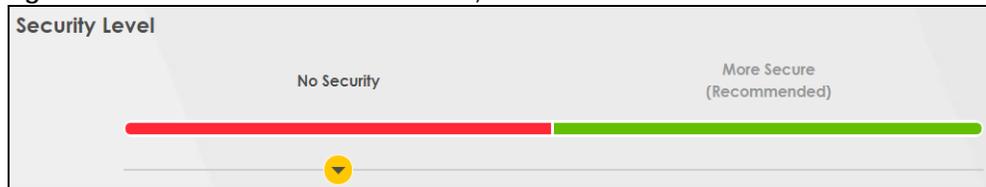
| LABEL | DESCRIPTION |
|---------------|--|
| Security Mode | Select More Secure (WPA(2)-PSK) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

7.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your Zyxel Device, your network is accessible to any wireless networking device that is within range.

Figure 57 Wireless > General: No Security



The following table describes the labels in this screen.

Table 33 Wireless > General: No Security

| LABEL | DESCRIPTION |
|----------------|--|
| Security Level | Choose No Security to allow all wireless connections without data encryption or authentication. |

7.2.2 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the Zyxel Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Setting > Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA/WPA2-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 58 Wireless > General: More Secure: WPA(2)-PSK

The screenshot shows the configuration interface for WPA(2)-PSK security. At the top, a progress bar indicates the security level, with 'More Secure (Recommended)' highlighted in green. The configuration options include:

- Security Mode:** WPA2-PSK
- Generate password automatically:** Checked
- Password:** F7FPPKCFJTNKYL7G
- Encryption:** AES
- Timer:** 3600 sec

The following table describes the labels in this screen.

Table 34 Wireless > General: More Secure: WPA(2)-PSK

| LABEL | DESCRIPTION |
|---------------------------------|--|
| Security Level | Select More Secure to enable WPA(2)-PSK data encryption. |
| Security Mode | Select WPA-PSK/WPA2-PSK or WPA2-PSK from the drop-down list box. |
| Generate password automatically | Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option. |
| Password | WPA(2)-PSK uses a simple common password, instead of user-specific credentials. If you did not select Generate password automatically , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters. Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed  , you'll see the password in plain text. Otherwise, it's hidden. |
| | Click this  to show more fields in this section. Click again to hide them. |
| Encryption | Select the encryption type (AES or TKIP+AES) for data encryption. Select AES if your wireless clients can all use AES. Select TKIP+AES to allow the wireless clients to use either TKIP or AES. |
| Timer | The Timer is the rate at which the RADIUS server sends a new group key out to all clients. |

7.3 The Guest/More AP Screen

This screen allows you to configure a Guest wireless network that allows access to the Internet only through the Zyxel Device. You can also configure additional wireless networks, each with different security settings, in this screen.

Click **Network Setting > Wireless > Guest/More AP**. The following screen displays.

The following table introduces the supported wireless networks..

Table 35 Supported Wireless Networks

| WIRELESS NETWORKS | WHERE TO CONFIGURE |
|-------------------|---|
| Main/1 | Network Setting > Wireless > General screen |
| Guest/3 | Network Setting > Wireless > Guest/More AP screen |

Figure 59 Network Setting > Wireless > Guest/More AP

| # | Status | SSID | Security | Guest WLAN | Modify |
|---|---|-------------------|---------------|----------------|---|
| 1 |  | ZyxeL_9DE5_guest1 | WPA2-Personal | External Guest |  |
| 2 |  | ZyxeL_9DE5_guest2 | WPA2-Personal | External Guest |  |
| 3 |  | ZyxeL_9DE5_guest3 | WPA2-Personal | External Guest |  |

The following table describes the labels in this screen.

Table 36 Network Setting > Wireless > Guest/More AP

| LABEL | DESCRIPTION |
|------------|---|
| # | This is the index number of the entry. |
| Status | This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active, while a gray bulb signifies that this SSID is not active. |
| SSID | An SSID profile is the set of parameters relating to one of the Zyxel Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility. |
| Security | This field indicates the security mode of the SSID profile. |
| Guest WLAN | This displays if the guest WLAN function has been enabled for this WLAN. If Home Guest displays, clients can connect to each other directly. If External Guest displays, clients are blocked from connecting to each other directly. N/A displays if guest WLAN is disabled. |
| Modify | Click the Edit icon to configure the SSID profile. |

7.3.1 The Edit Guest/More AP Screen

Use this screen to edit an SSID profile and select a wireless security mode for additional wireless networks.

Note: If upstream/downstream bandwidth is empty, the CPE sets the value automatically. Using maximum upstream/downstream bandwidth will significantly decrease wireless performance.

Click the **Edit** icon next to an SSID in the **Guest/More AP** screen. The following screen displays.

Figure 60 Network Setting > Wireless > Guest/More AP > Edit

More AP Edit

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

Wireless Network Setup

Wireless

Security Level

Wireless Network Name:

Hide SSID

Guest WLAN

Access Scenario: ⓘ

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Note

- (1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.
- (2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.
- (3) If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.
- (4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID:

SSID Subnet:

DHCP Start Address: . . .

DHCP End Address: . . .

SSID Subnet Mask: . . .

LAN IP Address: . . .

Security Level

No Security More Secure (Recommended)

Security Mode:

Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").

Password: ⓘ

Strength: weak

Encryption:

Timer: sec

Cancel OK

The following table describes the fields in this screen.

Table 37 Network Setting > Wireless > Guest/More AP > Edit

| LABEL | DESCRIPTION |
|---------------------------------|--|
| Wireless Network Setup | |
| Wireless | Click this switch to enable or disable the wireless LAN in this field. When the switch turns blue  , the function is enabled; otherwise, it's not. |
| Security Level | |
| Wireless Network Name | The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN. |
| Hide SSID | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| Guest WLAN | Select this to create Guest WLANs for home and external clients. Select the WLAN type in the Access Scenario field. |
| Access Scenario | If you select Home Guest , clients can connect to each other directly. If you select External Guest , clients are blocked from connecting to each other directly. |
| Max. Upstream Bandwidth | Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps). |
| Max. Downstream Bandwidth | Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps). |
| BSSID | This shows the MAC address of the wireless interface on the Zyxel Device when wireless LAN is enabled. |
| SSID Subnet | Click on this switch to Enable this function if you want the wireless network interface to assign DHCP IP addresses to the associated wireless clients. This option cannot be used if the WPS function is enabled in the Network > Wireless > WPS screen or if the Keep 2.4G and 5G wireless network name the same check box is selected in Network > Wireless > General . |
| DHCP Start Address | Specify the first of the contiguous addresses in the DHCP IP address pool. The Zyxel Device assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID. |
| DHCP End Address | Specify the last of the contiguous addresses in the DHCP IP address pool. |
| SSID Subnet Mask | Specify the subnet mask of the Zyxel Device for the SSID subnet. |
| LAN IP Address | Specify the IP address of the Zyxel Device for the SSID subnet. |
| Security Level | |
| Security Mode | Select More Secure (WPA(2)-PSK) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See Section 7.2.1 on page 124 for more details about this field. |
| Generate password automatically | Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option. |

Table 37 Network Setting > Wireless > Guest/More AP > Edit (continued)

| LABEL | DESCRIPTION |
|------------|---|
| Password | <p>WPA(2)-PSK uses a simple common password, instead of user-specific credentials.</p> <p>If you did not select Generate password automatically, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.</p> <p>Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed , you'll see the password in plain text. Otherwise, it's hidden.</p> |
| | <p>Click this  to show more fields in this section. Click again to hide them.</p> |
| Encryption | <p>Select the encryption type (AES or TKIP+AES) for data encryption.</p> <p>Select AES if your wireless clients can all use AES.</p> <p>Select TKIP+AES to allow the wireless clients to use either TKIP or AES.</p> |
| Timer | <p>The Timer is the rate at which the RADIUS server sends a new group key out to all clients.</p> |
| Cancel | <p>Click Cancel to exit this screen without saving.</p> |
| OK | <p>Click OK to save your changes.</p> |

7.4 The MAC Authentication Screen

This screen allows you to configure the Zyxel Device to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the Zyxel Device (**Deny**) based on the device(s) MAC address. Every Ethernet device has a unique MAC (Media Access Control) address. It is assigned at the factory and consists of six pairs of hexadecimal characters; for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the device(s) you want to allow/deny to configure this screen.

Note: You can have up to 25 MAC authentication rules.

Use this screen to view your Zyxel Device's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wireless > MAC Authentication**. The screen appears as shown.

Figure 61 Network Setting> Wireless > MAC Authentication

MAC Authentication can allow or block the access of the device(s) to your wireless network. Edit the list in the table to decide the rule of the access on device(s).

General

SSID: Home&Life SuperWiFi-F0FD

MAC Restrict Mode: Disable Deny Allow

MAC address List

[+ Add new MAC address](#)

| # | MAC Address | Modify |
|---|-------------|--------|
| | | |

Note
A maximum of 25 MAC Authentication rules can be configured.

[Cancel](#) [Apply](#)

The following table describes the labels in this screen.

Table 38 Network Setting> Wireless > MAC Authentication

| LABEL | DESCRIPTION |
|---------------------|--|
| General | |
| SSID | Select the SSID for which you want to configure MAC filter settings. |
| MAC Restrict Mode | Define the filter action for the list of MAC addresses in the MAC Address table. Select Disable to turn off MAC filtering. Select Deny to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device. Select Allow to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device. |
| MAC address List | |
| Add new MAC address | This field is available when you select Deny or Allow in the MAC Restrict Mode field. Click this if you want to add a new MAC address entry to the MAC filter list below. Enter the MAC addresses of the wireless devices that are allowed or denied access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |
| # | This is the index number of the entry. |
| MAC Address | This is the MAC addresses of the wireless devices that are allowed or denied access to the Zyxel Device. |
| Modify | Click the Edit icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the Delete icon to delete the entry. |

Table 38 Network Setting > Wireless > MAC Authentication (continued)

| LABEL | DESCRIPTION |
|--------|---|
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

7.5 The WPS Screen

WiFi Protected Setup (WPS) allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. To set up a WPS connection between two devices, both devices must support WPS. It is recommended to use the Push Button Configuration (PBC) method if your wireless client supports it. See [Section 7.10.8.3 on page 146](#) for more information about WPS.

Note: The Zyxel Device applies the security settings of the **SSID1** profile (see [Section 7.2 on page 122](#)). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA2-PSK** or **No Security**.

Note: If WPS is enabled, UPnP will automatically be turned on.

Click **Network Setting > Wireless > WPS**. The following screen displays. Click this switch and makes it turn blue. Click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 62 Network Setting > Wireless > WPS

Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS.

General

WPS

Add a new device with WPS Method

Method 1 PBC

Step1. Click WPS button WPS

Step2. Press the WPS button on your new wireless client device within 120 seconds

Method 2 PIN

Step1. Enter the PIN of your new wireless client device and then click Register

Register

Step2. Press the WPS button on your new wireless client device within 120 seconds

Method 3

Enter AP's PIN Number in Wireless Client
Current state Configured

1. Please release configuration if you want to configure the wireless settings
Release Configuration

2. Enter current PIN number on your wireless client
Generate New PIN

Note

(1) If WPS is Enabled, UPnP will automatically be turned on.
(2) This feature is available only when WPA2-PSK or No Security mode is configured.
(3) The WPS button will be grey-out when Wireless or WPS is disabled

Cancel Apply

The following table describes the labels in this screen.

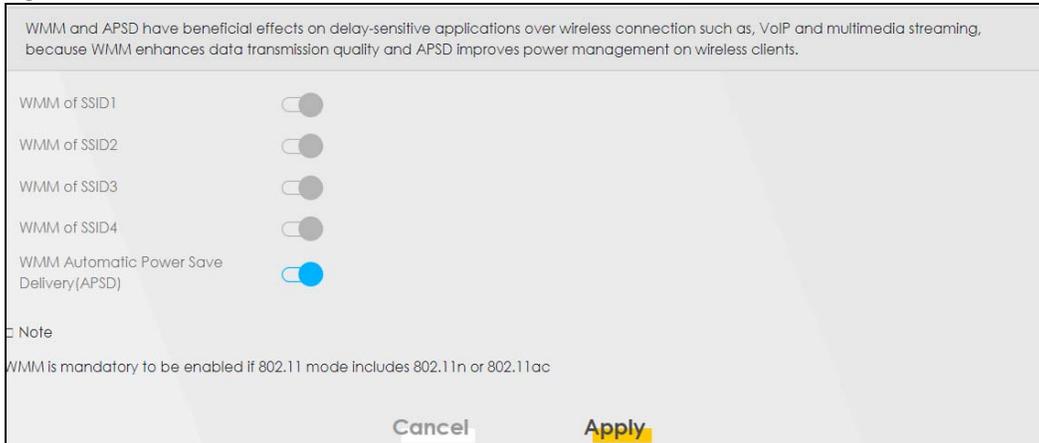
Table 39 Network Setting > Wireless > WPS

| LABEL | DESCRIPTION |
|----------------------------------|--|
| General | |
| WPS | Click this switch to activate or deactivate WPS on this Zyxel Device. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Add a new device with WPS Method | |
| Method 1 | Use this section to set up a WPS wireless network using Push Button Configuration (PBC). Click this switch and makes it turn blue. Click Apply to activate WPS method 1 on the Zyxel Device. |
| WPS | Click this button to add another WPS-enabled wireless device (within wireless range of the Zyxel Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the WPS button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button. |
| Method 2 | Use this section to set up a WPS wireless network by entering the PIN of the client into the Zyxel Device. Click this switch and make it turn blue. Click Apply to activate WPS method 2 on the Zyxel Device. |
| Register | Enter the PIN of the device that you are setting up a WPS connection with and click Register to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the Zyxel Device. |
| Method 3 | Use this section to set up a WPS wireless network by entering the PIN of the Zyxel Device into the client. Click this switch and make it turn blue. Click Apply to activate WPS method 3 on the Zyxel Device. |
| Release Configuration | The default WPS status is configured. Click this button to remove all configured wireless and wireless security settings for WPS connections on the Zyxel Device. |
| Generate New PIN Number | If this method has been enabled, the PIN (Personal Identification Number) of the Zyxel Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the Generate New PIN button to have the Zyxel Device create a new PIN. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

7.6 The WMM Screen

Use this screen to enable Wi-Fi MultiMedia (**WMM**) and **WMM Automatic Power Save (APSD)** in wireless networks for multimedia applications. **WMM** enhances data transmission quality, while **APSD** improves power management of wireless clients. This allows delay-sensitive applications, such as voice and videos, to run more smoothly.

Click **Network Setting > Wireless > WMM** to display the following screen.

Figure 63 Network Setting > Wireless > WMM

The following table describes the labels in this screen.

Table 40 Network Setting > Wireless > WMM

| LABEL | DESCRIPTION |
|--|---|
| WMM of SSID1~4 | Select On to have the Zyxel Device automatically give the wireless network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. If the 802.11 Mode in Network Setting > Wireless > Others is set to include 802.11n or 802.11ac, WMM cannot be disabled. |
| WMM Automatic Power Save Delivery (APSD) | Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Zyxel Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Zyxel Device until the Zyxel Device "wakes up". The Zyxel Device wakes up periodically to check for incoming data. Note: This works only if the wireless device to which the Zyxel Device is connected also supports this feature. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

7.7 The Others Screen

Use this screen to configure advanced wireless settings, such as additional security settings, power saving, and data transmission settings. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See [Section 7.10.2 on page 140](#) for detailed definitions of the terms listed in this screen.

Figure 64 Network Setting > Wireless > Others

The configurations below are the advanced WiFi settings.

| | | |
|-----------------------------|--|----|
| RTS/CTS Threshold | <input type="text" value="2347"/> | |
| Fragmentation Threshold | <input type="text" value="2346"/> | |
| Output Power | <input type="text" value="100%"/> | ▼ |
| Beacon Interval | <input type="text" value="100"/> | ms |
| DTIM Interval | <input type="text" value="1"/> | ms |
| 802.11 Mode | <input type="text" value="802.11b/g/n Mixed"/> | ▼ |
| 802.11 Protection | <input type="text" value="Auto"/> | ▼ |
| Preamble | <input type="text" value="Long"/> | |
| Protected Management Frames | <input type="text" value="Capable"/> | ▼ |

The following table describes the labels in this screen.

Table 41 Network Setting > Wireless > Others

| LABEL | DESCRIPTION |
|-------------------------|---|
| RTS/CTS Threshold | Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347. |
| Fragmentation Threshold | This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346. |
| Output Power | Set the output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: 20%, 40%, 60%, 80% or 100% . |
| Beacon Interval | When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50ms to 1000ms. A high value helps save current consumption of the access point. |
| DTIM Interval | Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255. |

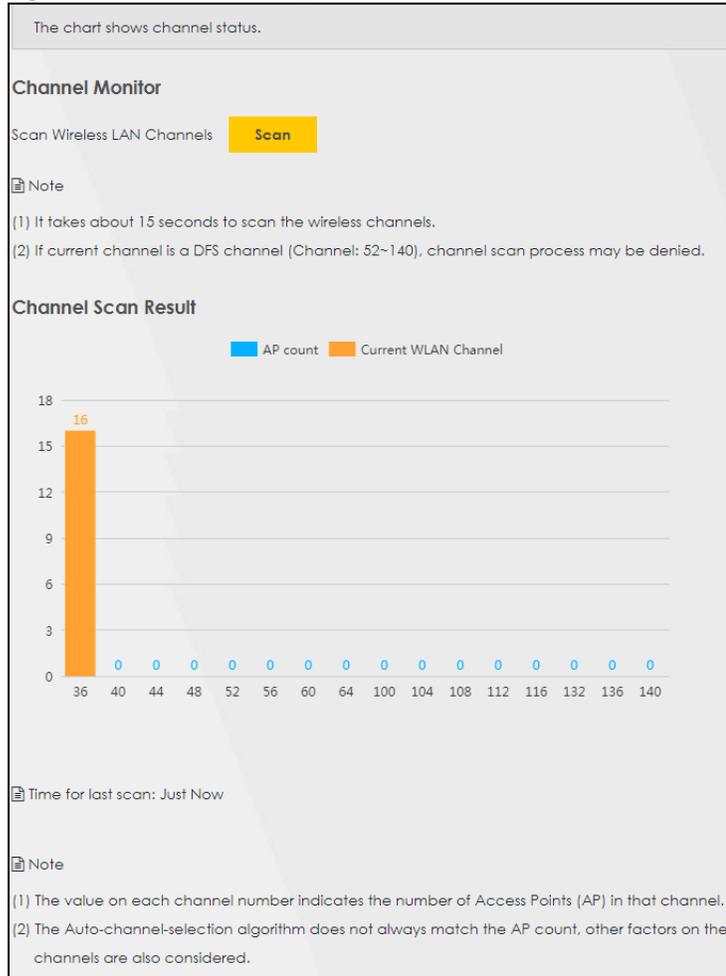
Table 41 Network Setting > Wireless > Others (continued)

| LABEL | DESCRIPTION |
|-----------------------------|---|
| 802.11 Mode | <p>For 2.4GHz frequency WLAN devices:</p> <ul style="list-style-type: none"> • Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the Zyxel Device. • Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. • Select 802.11n Only to allow only IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. • Select 802.11b/g Mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11b/g/n Mixed to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. <p>For 5GHz frequency WLAN devices:</p> <ul style="list-style-type: none"> • Select 802.11a Only to allow only IEEE 802.11a compliant WLAN devices to associate with the Zyxel Device. • Select 802.11n Only to allow only IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. • Select 802.11ac Only to allow only IEEE 802.11ac compliant WLAN devices to associate with the Zyxel Device. • Select 802.11a/n Mixed to allow either IEEE 802.11a or IEEE 802.11n compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11n/ac Mixed to allow either IEEE 802.11n or IEEE 802.11ac compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select 802.11a/n/ac Mixed to allow IEEE 802.11a, IEEE 802.11n or IEEE802.11ac compliant WLAN devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. |
| 802.11 Protection | <p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select Off to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network.</p> <p>This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.</p> |
| Preamble | <p>Select a preamble type from the drop-down list box. Choices are Long or Short. See Section 7.10.7 on page 143 for more information.</p> <p>This field is configurable only when you set 802.11 Mode to 802.11b.</p> |
| Protected Management Frames | <p>This option is only available when using WPA2 as the Security Mode and AES Encryption in Network Setting > Wireless > General. Management frame protection (MFP) helps prevent wireless DoS attacks.</p> <p>Select Disable if you don't want to use MFP.</p> <p>Select Capable to encrypt management frames of wireless clients that support MFP. Clients that do not support MFP will still be allowed to join the wireless network, but remain unprotected.</p> <p>Select Required to allow only clients that support MFP to join the wireless network.</p> |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

7.8 The Channel Status Screen

Use the **Channel Status** screen to scan wireless LAN channel noises and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **Scan** to scan the wireless LAN channels. You can view the results in the **Channel Scan Result** section.

Figure 65 Network Setting > Wireless > Channel Status



7.9 The MESH Screen

Use this screen to enable or disable Zyxel MESH for Multy Pro supported devices. It supports AP steering and Band steering. AP steering allows wireless clients to roam seamlessly between Multy-Pro-supported devices in your MESH network by using the same SSID and WiFi password. Also, AP steering helps monitor wireless clients and drop their connections to optimize the Zyxel Device bandwidth when the clients are idle or have a low signal. When a wireless client is dropped, it has the opportunity to steer to a Multy-Pro-supported device with a strong signal. Band steering allows 2.4G/5G dual-band wireless clients to steer from one band to another.

A MESH network consists of a controller, the Zyxel Device, and Multy-Pro-supported extenders. Multy-Pro-supported extenders use the same wireless settings as the controller.

When Multy Pro is enabled:

- One Connect will be enabled and grayed out automatically. See [Section Chapter 17 on page 233](#) for more information about One Connect. One Connect is used for the communication between the Zyxel Device and Multy-Pro-supported extenders for the setup of a MESH network.
- The SSID and WiFi password of the main 2.4GHz wireless network will be copied to the main 5GHz wireless network.

See the steps below on how to set up a MESH network. The setup could take you 30 minutes.

Configurations on a Multy-Pro-Supported Extender(s)

- 1 Prepare a Multy-Pro-supported extender(s) from Zyxel.
The following table lists the Multy-Pro-supported extenders from Zyxel at the time of writing.

Table 42 Multy-Pro-Supported Extenders from Zyxel

| MODELS |
|---------|
| WAP6804 |
| WAP6906 |
| WAP7205 |

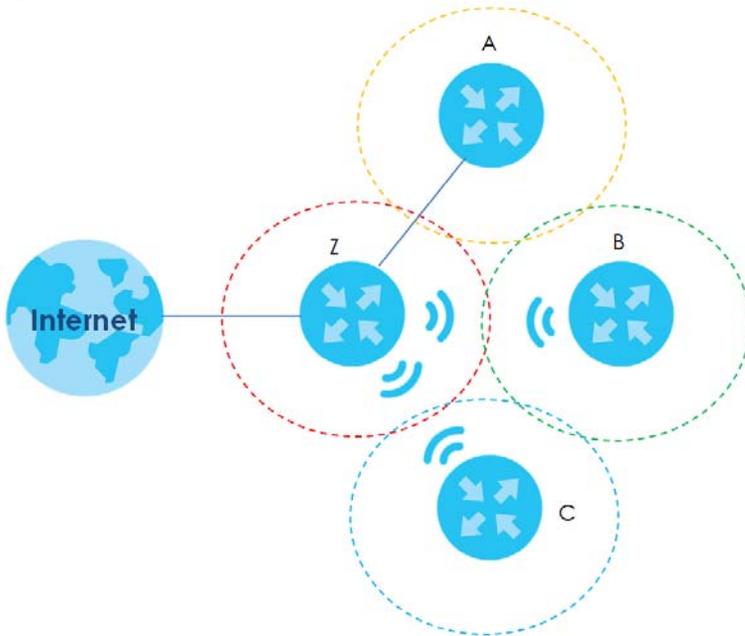
- 2 If the Multy-Pro-supported extender is in repeater mode, enable the wireless LAN. See your Multy-Pro-supported extender's UG for how to enable the wireless LAN.
- 3 If the Multy-Pro-supported extender is in AP mode, connect it to the Zyxel Device using an Ethernet cable.
- 4 Turn on the Multy-Pro-supported extender.
- 5 Enable Zyxel MESH in the Web Configurator. See your Multy-Pro-supported extender's UG for how to enable Zyxel MESH.

Configurations on the Zyxel Device

- 1 If the Multy-Pro-supported extender is in repeater mode, enable the wireless LAN. See [Section 5.1.3 on page 84](#) or [Section 1.5.1 on page 32](#) for more information on enabling the wireless LAN.
- 2 Enable Zyxel MESH in the **Network > Wireless > MESH** screen.
- 3 Press the **WPS** button for more than five seconds on the Zyxel Device.
Or
Click **Add Extender** in the Multy Pro App. Install from Google Play or the Apple App store.

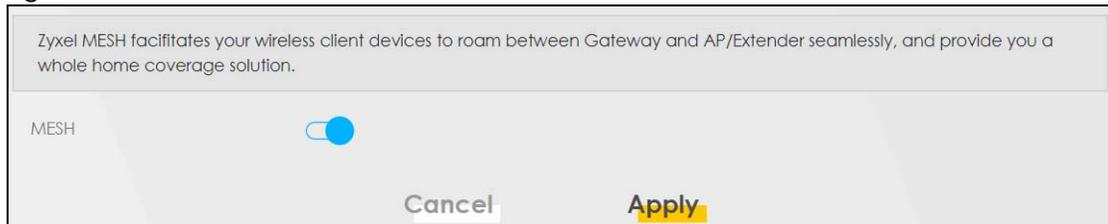
The following figure shows the Multy Pro application. Device **Z** is the controller, the Zyxel Device. Device **A** is a Multy-Pro-supported extender in AP mode. Devices **B** and **C** are Multy-Pro-supported extenders in repeater Mode.

Figure 66 MESH Application



Click **Network > Wireless > MESH**. The following screen displays.

Figure 67 Network > Wireless > MESH



7.10 Technical Reference

This section discusses wireless LANs in depth. For more information, see [Appendix B on page 356](#).

7.10.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

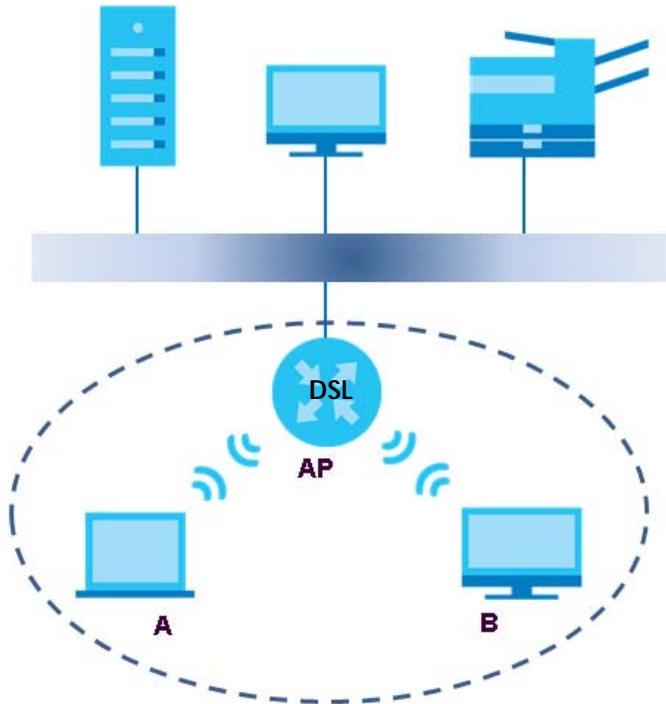
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An “infrastructure” type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An “ad-hoc” type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 68 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your Zyxel Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.
The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of

networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

7.10.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the Zyxel Device's Web Configurator.

Table 43 Additional Wireless Terms

| TERM | DESCRIPTION |
|-------------------------|---|
| RTS/CTS Threshold | In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the Zyxel Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the Zyxel Device. |
| Preamble | A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the Zyxel Device does, it cannot communicate with the Zyxel Device. |
| Authentication | The process of verifying whether a wireless device is allowed to use the wireless network. |
| Fragmentation Threshold | A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy. |

7.10.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

7.10.3.1 SSID

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

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

7.10.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.¹ A MAC address is usually written using twelve hexadecimal characters²; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the Zyxel Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

7.10.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

valid user name and password. Then, they can use that user name and password to use the wireless network.

7.10.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See [Section 7.10.3.3 on page 141](#) for information about this.)

Table 44 Types of Encryption for Each Type of Authentication

| | NO AUTHENTICATION | RADIUS SERVER |
|-----------|-------------------|---------------|
| Weakest | No Security | WPA |
| ↕ | WPA-PSK | |
| Strongest | WPA2-PSK | |

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **WPA-PSK**, or **WPA2-PSK**.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

7.10.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

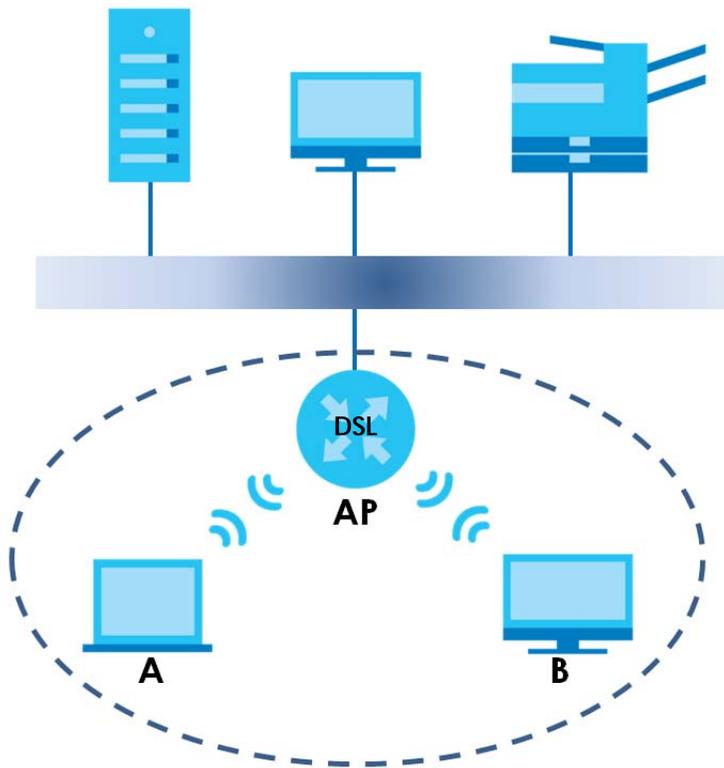
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.10.5 BSS

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

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

Figure 69 Basic Service set



7.10.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The Zyxel Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

7.10.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

7.10.7 Preamble Type

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

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

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

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

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

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

7.10.8 WiFi Protected Setup (WPS)

Your Zyxel Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

7.10.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the Zyxel Device, see [Section 7.6 on page 132](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the Zyxel Device you must press the WPS button for more than five seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.10.8.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

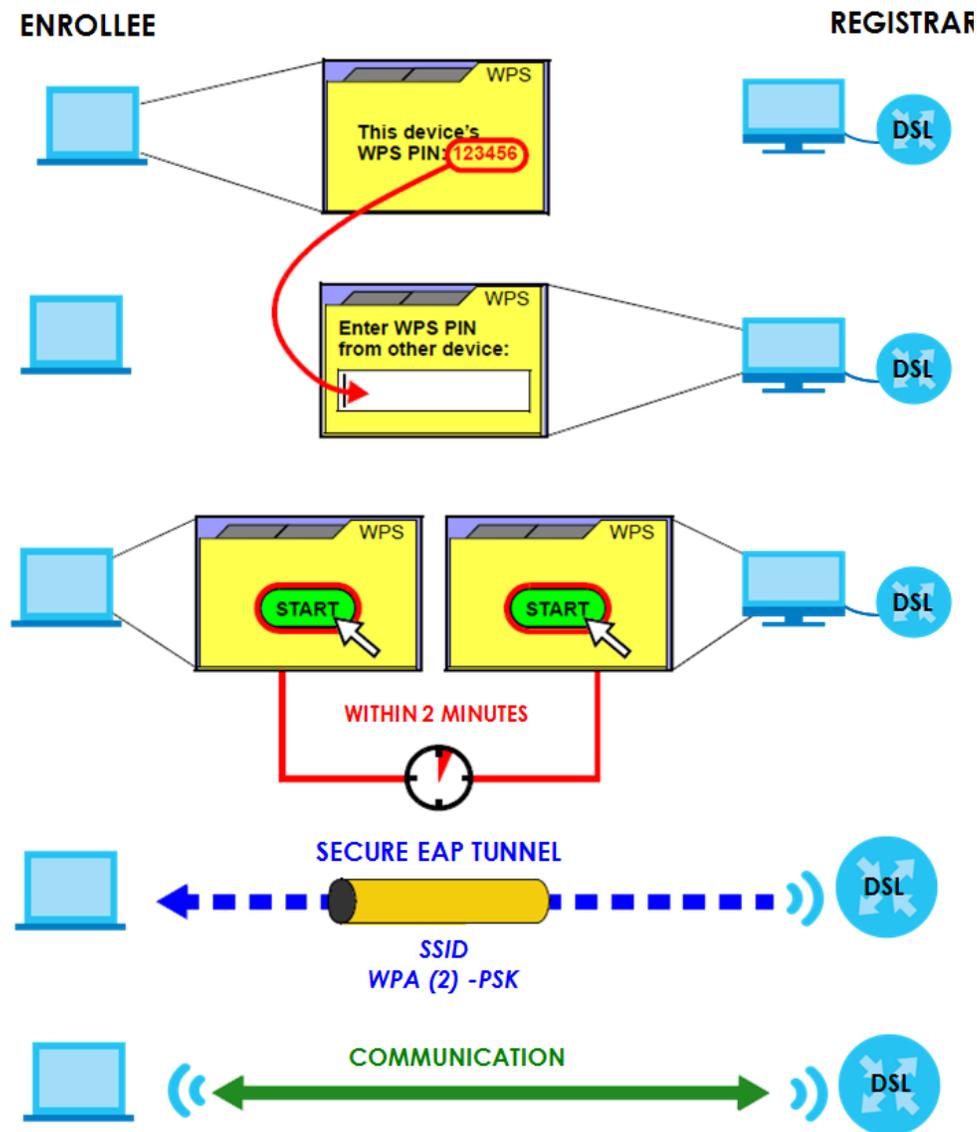
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the Zyxel Device, see [Section 7.5 on page 131](#)).
- 4 Enter the client's PIN in the AP's configuration interface.
- 5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6 Start WPS on both devices within two minutes.
- 7 Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 70 Example WPS Process: PIN Method

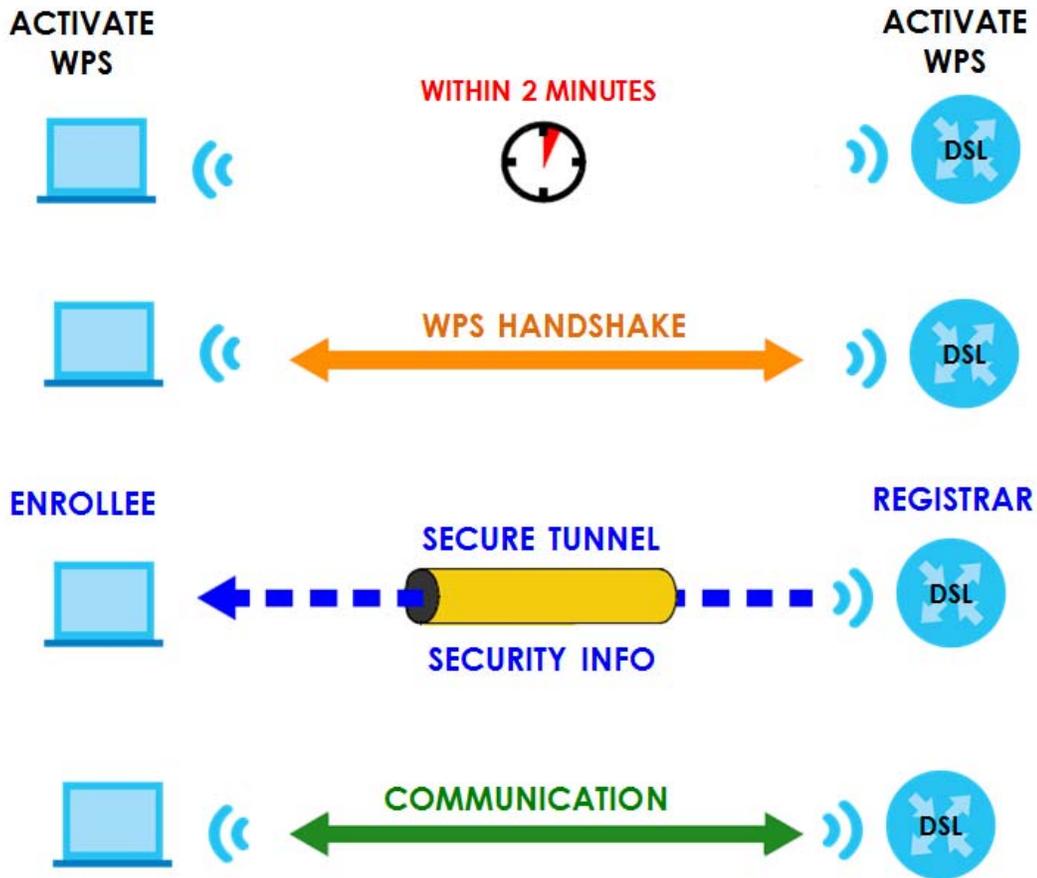


7.10.8.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 71 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

7.10.8.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

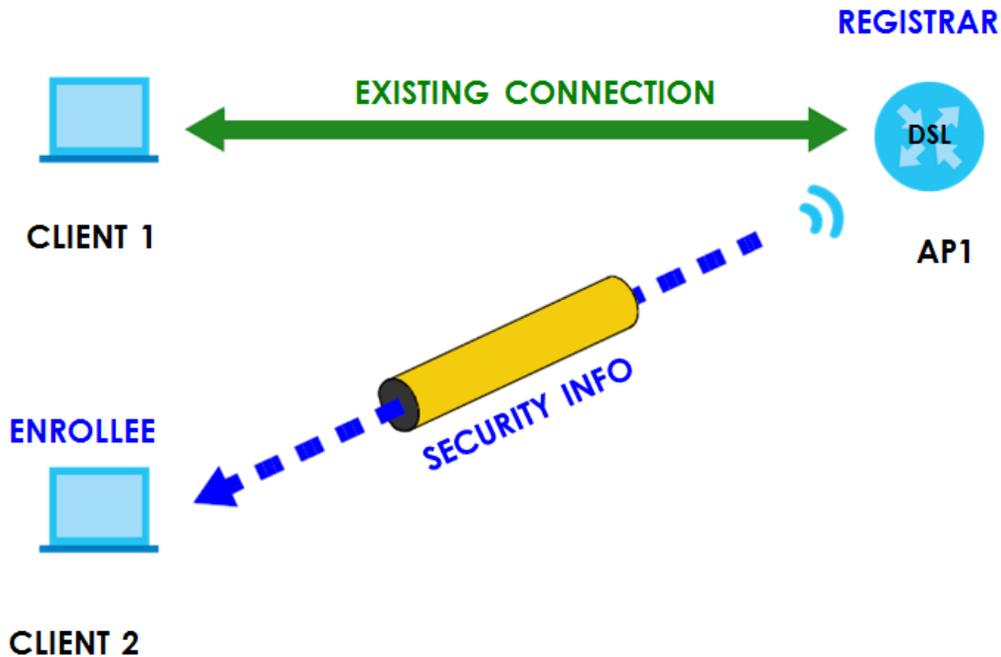
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 72 WPS: Example Network Step 1



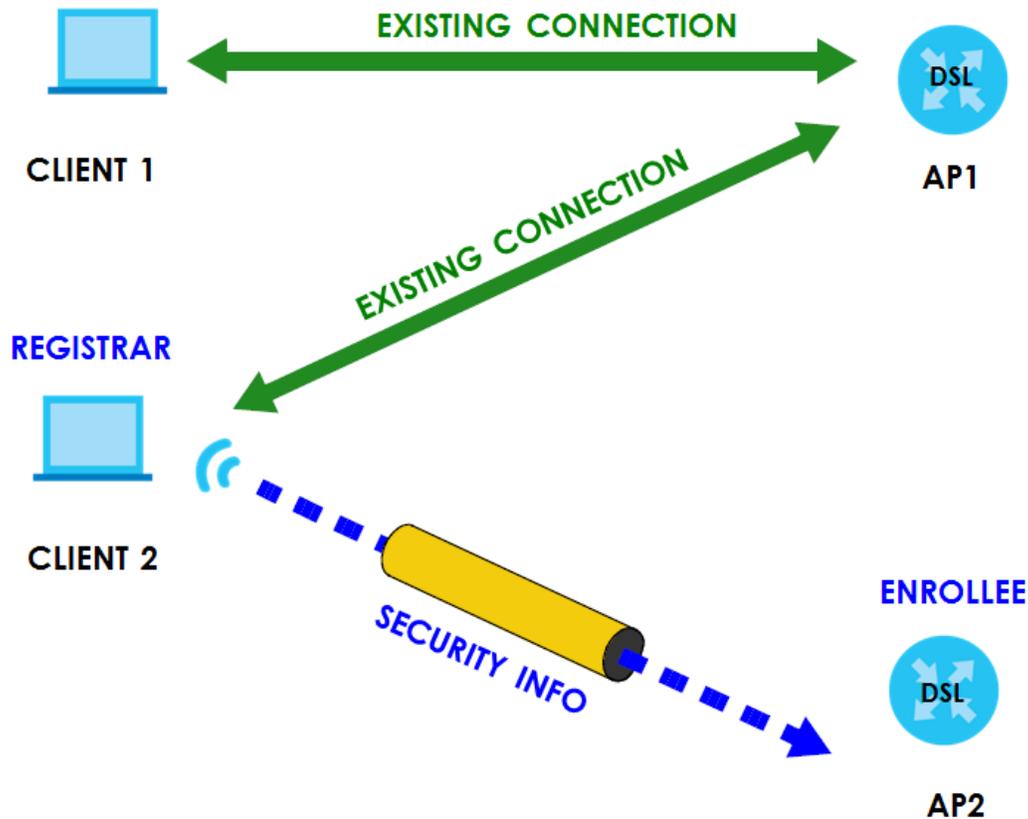
In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 73 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 74 WPS: Example Network Step 3



7.10.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

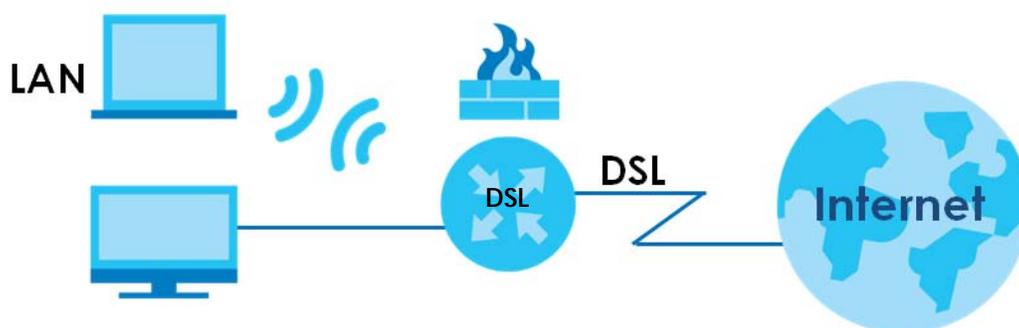
CHAPTER 8

Home Networking

8.1 Home Networking Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.



8.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device ([Section 8.2 on page 153](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 8.3 on page 157](#)).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the Zyxel Device ([Section 8.4 on page 159](#)).
- Use the **Additional Subnet** screen to configure IP alias and public static IP ([Section 8.5 on page 161](#)).
- Use the **STB Vendor ID** screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses ([Section 8.6 on page 163](#)).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. ([Section 8.7 on page 163](#)).
- Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. ([Section 8.8 on page 164](#)).

8.1.2 What You Need To Know

8.1.2.1 About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your Zyxel Device an IP address, subnet mask, DNS and other routing information when it's turned on.

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

RADVD (Router Advertisement Daemon)

When an IPv6 host sends a Router Solicitation (RS) request to discover the available routers, RADVD with Router Advertisement (RA) messages in response to the request. It specifies the minimum and maximum intervals of RA broadcasts. RA messages containing the address prefix. IPv6 hosts can be generated with the IPv6 prefix an IPv6 address.

8.1.2.2 About UPnP

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses

- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the [Chapter 11 on page 195](#) for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the Zyxel Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and Zyxel

Zyxel has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). Zyxel's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See [Section 8.4.1 on page 160](#) for examples of installing and using UPnP.

Finding Out More

See [Section 8.9 on page 165](#) for technical background information on LANs.

8.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

8.2 The LAN Setup Screen

Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to lay down the rules for assigning IP addresses to devices. Click **Network Setting** > **Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

- 1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your Zyxel Device.
- 2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

- 3 Click **Apply** to save your settings.

Figure 75 Network Setting > Home Networking > LAN Setup

Home Networking

[LAN Setup](#) | [Static DHCP](#) | [IPv6](#) | [Additional Subnet](#) | [STB Vendor ID](#) | [Wake on LAN](#) | [TFTP Server Name](#)

The LAN IP address is the IP address you use to log into the web configurator. The DHCP server settings define the rules on how to assign IP addresses to the LAN clients on your network.

Interface Group

Group Name:

LAN IP Setup

IP Address: . . .

Subnet Mask: . . .

IGMP Snooping

Active:

IGMP Mode: Standard Mode Blocking Mode

DHCP Server State

DHCP: Enable Disable DHCP Relay

IP Addressing Values

Beginning IP Address: . . .

Ending IP Address: . . .

Auto reserve IP for the same host:

DHCP Server Lease Time

days hours minutes

DNS Values

DNS: DNS Proxy Static From ISP

LAN IPv6 Mode Setup

IPv6 Active:

Link Local Address Type

EUI64 Manual

LAN Global Identifier Type

EUI64 Manual

LAN IPv6 Prefix Setup

Delegate prefix from WAN:

Static

MLD Snooping

Active:

MLD Mode: Standard Mode Blocking Mode

LAN IPv6 Address Assign Setup

LAN IPv6 DNS Assign Setup

DHCPv6 Configuration

DHCPv6 Active: DHCPv6 Server:

IPv6 Router Advertisement State

RADVD Active: Enable:

IPv6 DNS Values

IPv6 DNS Server 1:

IPv6 DNS Server 2:

IPv6 DNS Server 3:

DNS Query Scenario

The following table describes the fields in this screen.

Table 45 Network Setting > Home Networking > LAN Setup

| LABEL | DESCRIPTION |
|-----------------------------------|---|
| Interface Group | |
| Group Name | Select the interface group name for which you want to configure LAN settings. See Chapter 15 on page 222 for how to create a new interface group. |
| LAN IP Setup | |
| IPAddress | Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default). |
| Subnet Mask | Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so. |
| IGMP Snooping | |
| Active | Select Enable to allow the Zyxel Device to passively learn multicast group. |
| IGMP Mode | Select Standard Mode to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select Blocking Mode to block all unknown multicast packets from the WAN. |
| DHCP Server State | |
| DHCP | Select Enable to have the Zyxel Device act as a DHCP server or DHCP relay agent. Select Disable to stop the DHCP server on the Zyxel Device. Select DHCP Relay to have the Zyxel Device forward DHCP request to the DHCP server. |
| DHCP Relay Server Address | This field is only available when you select DHCP Relay in the DHCP field. |
| IP Address | Enter the IPv4 IP address of the actual remote DHCP server in this field. |
| IP Addressing Values | This field is only available when you select Enable in the DHCP field. |
| Beginning IP Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Ending IP Address | This field specifies the last of the contiguous addresses in the IP address pool. |
| Auto reserve IP for the same host | Click this switch to have the Zyxel Device record DHCP IP addresses with the MAC addresses the IP addresses are assigned to. When the switch turns blue  , the function is enabled. Otherwise, it's not. The Zyxel Device assigns the same IP address to the same MAC address when the host requests an IP address again through DHCP. |
| DHCP Server Lease Time | This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select Enable in the DHCP field. |
| Days/Hours/Minutes | Enter the lease time of the DHCP server. |
| DNS Values | This field is only available when you select Enable in the DHCP field. |
| DNS | Select the type of service that you are registered for from your DNS service provider (From ISP). Select DNS Proxy if you have the DNS proxy service. The Zyxel Device redirects clients' DNS queries to a DNS server for resolving domain names. Select Static if you have the Static DNS service. |

Table 45 Network Setting > Home Networking > LAN Setup (continued)

| LABEL | DESCRIPTION |
|---------------------------------|--|
| DNS Server 1/2 | Enter the first and second DNS (Domain Name System) server IP addresses the Zyxel Device passes to the DHCP clients. |
| LAN IPv6 Mode Setup | |
| IPv6 Active | Click this switch to enable or disable the IPv6 mode and configure IPv6 settings on the Zyxel Device. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Link Local Address Type | |
| EUI64 | Select this to have the Zyxel Device generate an interface ID for the LAN interface's link-local address using the EUI-64 format. |
| Manual | Select this to manually enter an interface ID for the LAN interface's link-local address. |
| LAN Global Identifier Type | |
| EUI64 | Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address . |
| Manual | Select this to manually enter an interface ID for the LAN interface's global IPv6 address. |
| LAN IPv6 Prefix Setup | |
| Delegate prefix from WAN | Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router. |
| Static | Select this option to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address. |
| MLD Snooping | Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. |
| Active | Click this switch to enable or disable MLD Snooping on the Zyxel Device. When the switch turns blue  , the function is enabled. Otherwise, it's not. This allows the Zyxel Device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic. |
| MLD Mode | Select Standard Mode to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select Blocking Mode to block all unknown multicast packets from the WAN. |
| LAN IPv6 Address Assign Setup | Select how you want to obtain an IPv6 address: <ul style="list-style-type: none"> • Stateless: The Zyxel Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • Stateful: The Zyxel Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients. |
| LAN IPv6 DNS Assign Setup | Select how the Zyxel Device provide DNS server and domain name information to the clients: <ul style="list-style-type: none"> • From Router Advertisement: The Zyxel Device provides DNS information through router advertisements. • From DHCPv6 Server: The Zyxel Device provides DNS information through DHCPv6. • From RA & DHCPv6 Server: The Zyxel Device provides DNS information through both router advertisements and DHCPv6. |
| DHCPv6 Configuration | |
| DHCPv6 Active | This shows the status of the DHCPv6. DHCP Server displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients. |
| IPv6 Router Advertisement State | |
| RADVD Active | This shows whether RADVD is enabled or not. |
| IPv6 DNS Values | |

Table 45 Network Setting > Home Networking > LAN Setup (continued)

| LABEL | DESCRIPTION |
|---------------------|---|
| IPv6 DNS Server 1-3 | Select From ISP if your ISP dynamically assigns IPv6 DNS server information. Select User-Defined if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients. Select None if you do not want to configure IPv6 DNS servers. |
| DNS Query Scenario | Select how the Zyxel Device handles clients' DNS information requests. <ul style="list-style-type: none"> IPv4/IPv6 DNS Server: The Zyxel Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. IPv6 DNS Server Only: The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives. IPv4 DNS Server Only: The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. IPv6 DNS Server First: The Zyxel Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives. IPv4 DNS Server First: The Zyxel Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

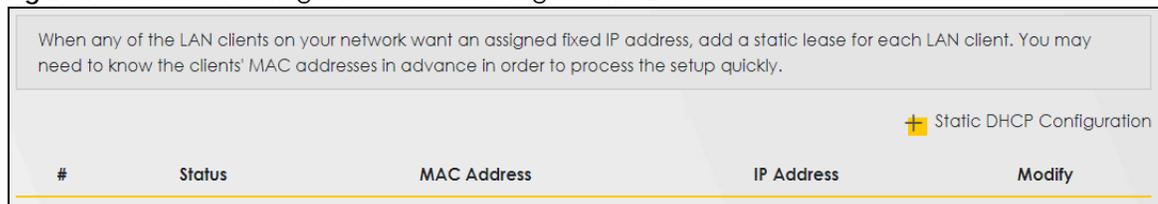
8.3 The LAN Static DHCP Screen

This table allows you to assign IP addresses on the LAN to individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Use this screen to change your Zyxel Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 76 Network Setting > Home Networking > Static DHCP



The following table describes the labels in this screen.

Table 46 Network Setting > Home Networking > Static DHCP

| LABEL | DESCRIPTION |
|---------------------------|--|
| Static DHCP Configuration | Click this to add a new static DHCP entry. |
| # | This is the index number of the entry. |
| Status | This field displays whether the client is connected to the Zyxel Device. |

Table 46 Network Setting > Home Networking > Static DHCP

| LABEL | DESCRIPTION |
|-------------|--|
| MAC Address | The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| Modify | Click the Edit icon to have the IP address field editable and change it. Click the Delete icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry. |

If you click **Static DHCP Configuration** in the **Static DHCP** screen or the Edit icon next to a static DHCP entry, the following screen displays. Using a static DHCP means a client will always have the same IP address assigned to it by the DHCP server. Assign a fixed IP address to a device by selecting the interface group of this device and its IP address type and selecting the device/computer from a list or manually entering its MAC address and assigned IP address.

Figure 77 Static DHCP: Static DHCP Configuration/Edit

The following table describes the labels in this screen.

Table 47 Static DHCP: Static DHCP Configuration/Edit

| LABEL | DESCRIPTION |
|--------------------|---|
| Active | Click this switch to enable or disable the connection between the client and the Zyxel Device. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Group Name | Select the interface group name for which you want to configure static DHCP settings. See Chapter 15 on page 222 for how to create a new interface group. |
| IP Type | This field displays IPv4 for the type of the DHCP IP address. At the time of writing, it is not allowed to select other type. |
| Select Device Info | Select a device or computer from the drop-down list or select Manual Input to manually enter a device's MAC address and IP address in the following fields. |
| MAC Address | If you select Manual Input , enter the MAC address of a computer on your LAN. |
| IP Address | If you select Manual Input , enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify. |

Table 47 Static DHCP: Static DHCP Configuration/Edit (continued)

| LABEL | DESCRIPTION |
|--------|---|
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

8.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. A device can then leave a network smoothly and automatically when it is no longer in use.

See [page 152](#) for more information on UPnP.

Use the following screen to configure the UPnP settings on your Zyxel Device. Click **Network Setting > Home Networking > UPnP** to display the screen shown next.

Note: To use **UPnP NAT-T**, enable **UPnP**.

Figure 78 Network Setting > Home Networking > UPnP

Universal Plug and Play (UPnP) is a networking standard for easy network connectivity among networking devices and software that also have UPnP enabled.

UPnP State

UPnP

UPnP NAT-T State

UPnP NAT-T

Note

UPnP NAT-T only works when NAT is enable

| # | Description | Destination IP Address | External Port | Internal Port | Protocol |
|---|-------------|------------------------|---------------|---------------|----------|
|---|-------------|------------------------|---------------|---------------|----------|

Cancel Apply

The following table describes the labels in this screen.

Table 48 Network Setting > Home Networking > UPnP

| LABEL | DESCRIPTION |
|------------------|--|
| UPnP State | |
| UPnP | Click this switch to enable or disable UPnP. When the switch turns blue <input checked="" type="checkbox"/> , the function is enabled. Otherwise, it's not. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the web configurator). |
| UPnP NAT-T State | |

Table 48 Network Setting > Home Networking > UPnP (continued)

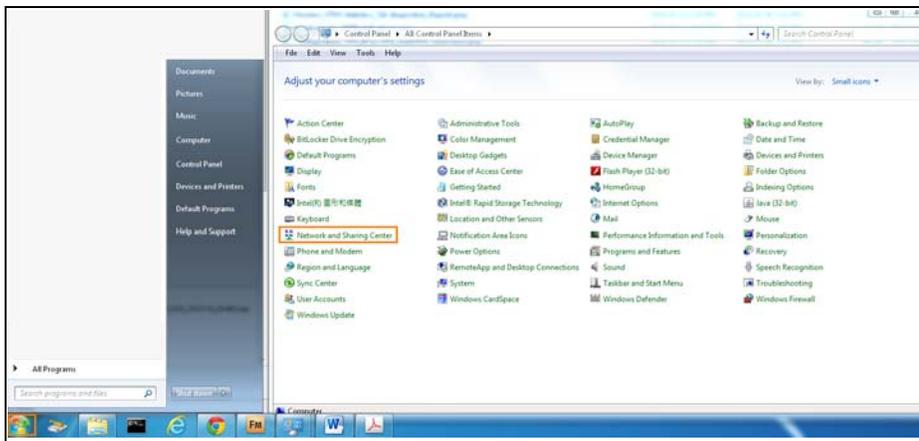
| LABEL | DESCRIPTION |
|------------------------|--|
| UPnP NAT-T | Click this switch to allow UPnP-enabled applications to automatically configure the Zyxel Device so that they can communicate through the Zyxel Device by using NAT traversal. When the switch turns blue  , the function is enabled. Otherwise, it's not. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. The table below displays the NAT port forwarding rules added automatically by UPnP NAT-T. |
| # | This is the index number of the UPnP NAT-T connection. |
| Description | This is the description of the UPnP NAT-T connection. |
| Destination IP Address | This is the IP address of the other connected UPnP-enabled device. |
| External Port | This is the external port number that identifies the service. |
| Internal Port | This is the internal port number that identifies the service. |
| Protocol | This is the transport layer protocol used for the service. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

8.4.1 Turning On UPnP in Windows 7 Example

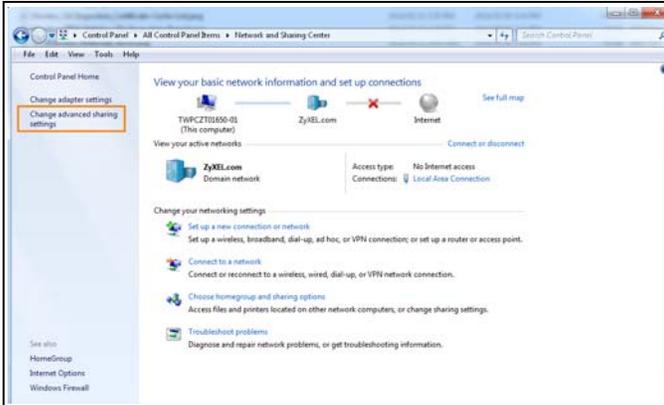
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the Zyxel Device.

Make sure the computer is connected to a LAN port of the Zyxel Device. Turn on your computer and the Zyxel Device.

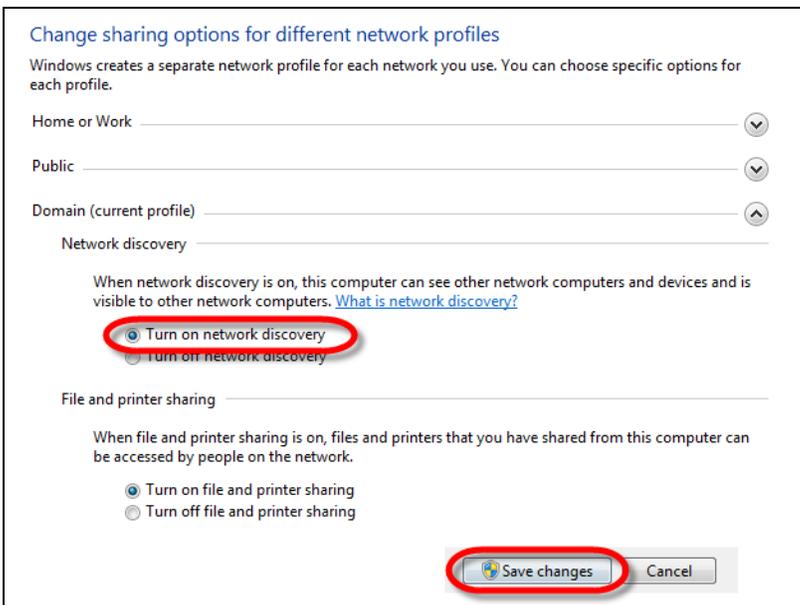
- 1 Click the start icon, **Control Panel** and then the **Network and Sharing Center**.



- 2 Click **Change Advanced Sharing Settings**.



- 3 Select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



8.5 The LAN Additional Subnet Screen

Use this screen to configure IP alias and public static IP.

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Zyxel Device supports multiple logical LAN interfaces via its physical Ethernet interface

with the Zyxel Device itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

If your ISP provides the Public LAN service, the Zyxel Device may use a LAN IP address that can be accessed from the WAN.

Click **Network Setting > Home Networking > Additional Subnet** to display the screen shown next.

Figure 79 Network Setting > Home Networking > Additional Subnet

The following table describes the labels in this screen.

Table 49 Network Setting > Home Networking > Additional Subnet

| LABEL | DESCRIPTION |
|----------------|--|
| IP Alias Setup | |
| Group Name | Select the interface group name for which you want to configure the IP alias settings. See Chapter 15 on page 222 for how to create a new interface group. |
| Active | Click this switch to configure a LAN network for the Zyxel Device. When the switch turns blue  , the following fields will be configurable. Otherwise, they're not. |
| IPv4 Address | Enter the IP address of your Zyxel Device in dotted decimal notation. |
| Subnet Mask | Your Zyxel Device will automatically calculate the subnet mask based on the IPv4 address that you assign. Unless you are implementing subnetting, use this value computed by the Zyxel Device. |
| Public LAN | |
| Active | Click this switch to enable or disable the Public LAN feature. When the switch turns blue  , the function is enabled. Otherwise, it's not. Your ISP must support Public LAN and Static IP. |
| IPv4 Address | Enter the public IP address provided by your ISP. |
| Subnet Mask | Enter the public IPv4 subnet mask provided by your ISP. |

Table 49 Network Setting > Home Networking > Additional Subnet (continued)

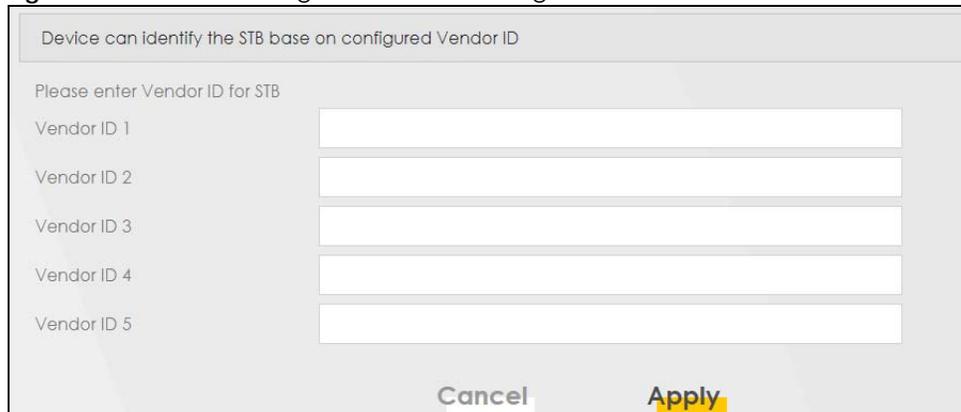
| LABEL | DESCRIPTION |
|-------------------------|---|
| Offer Public IP by DHCP | Click this switch to enable or disable the Zyxel Device to provide public IP addresses by DHCP server. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Enable ARP Proxy | Click this switch to enable or disable the ARP (Address Resolution Protocol) proxy. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

8.6 The STB Vendor ID Screen

Set Top Box (STB) devices with dynamic IP addresses sometimes don't renew their IP addresses before the lease time expires. This could lead to IP address conflicts if the STB continues to use an IP address that gets assigned to another device. Use this screen to configure the Vendor IDs of connected STBs, so the Zyxel Device can automatically create static DHCP entries for them when they request IP addresses.

Click **Network Setting > Home Networking > STB Vendor ID** to open this screen.

Figure 80 Network Setting > Home Networking > STB Vendor ID



The following table describes the labels in this screen.

Table 50 Network Setting > Home Networking > STB Vendor ID

| LABEL | DESCRIPTION |
|---------------|--|
| Vendor ID 1~5 | These are STB's Vendor Class Identifiers (DHCP option 60). A Vendor Class Identifier is usually used to inform the DHCP server a DHCP client's vendor and functionality. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

8.7 The Wake on LAN Screen

Use this screen to remotely turn on a device on the LAN network. To use this feature, the remote device must also support Wake On LAN.

You need to know the MAC address of the LAN device. It may be on a label on the device or in its documentation.

Click **Network Setting > Home Networking > Wake on Lan** to open this screen.

Figure 81 Network Setting > Home Networking > Wake on Lan

The following table describes the labels in this screen.

Table 51 Network Setting > Home Networking > Wake on Lan

| LABEL | DESCRIPTION |
|-----------------|---|
| Wake by Address | Select Manual and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the Zyxel Device's ARP table. Select an IP address and it will then automatically update the IP address and MAC address in the following fields. |
| IP Address | Enter the IPv4 IP address of the device to turn it on. |
| MAC Address | Enter the MAC address of the device to turn it on. A MAC address consists of six hexadecimal character pairs. |
| Wake up | Click this to send a wake up packet to wake up the specified device. |

8.8 The TFTP Server Name Screen

Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. RFC 2132 defines the option 66 open standard. DHCP option 66 supports the IP address or the hostname of a single TFTP server.

Click **Network Setting > Home Networking > TFTP Server Name** to open this screen.

Figure 82 Network Setting > Home Networking > TFTP Server Name

The following table describes the labels in this screen.

Table 52 Network Setting > Home Networking > TFTP Server Name

| LABEL | DESCRIPTION |
|------------------|---|
| TFTP Server Name | Enter the IP address or the hostname of a single TFTP server. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

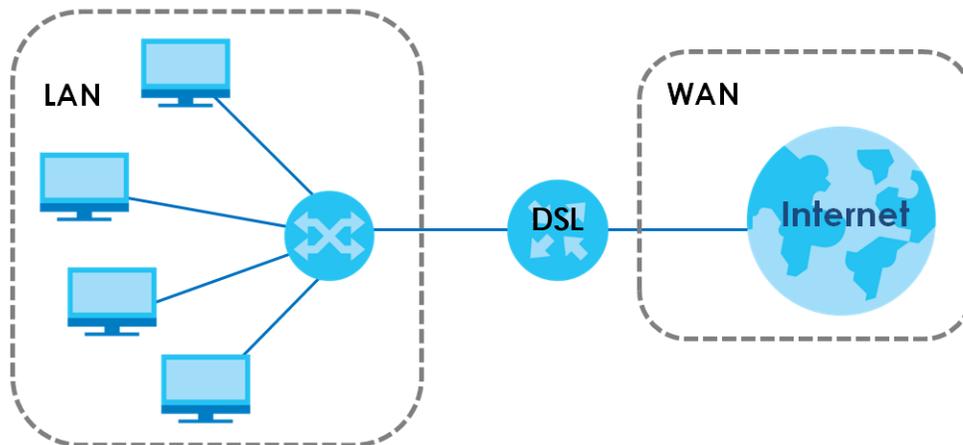
8.9 Technical Reference

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

8.9.1 LANs, WANs and the Zyxel Device

The actual physical connection determines whether the Zyxel Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 83 LAN and WAN IP Addresses



8.9.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Zyxel Device as a DHCP server or disable it. When configured as a server, the Zyxel Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The Zyxel Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

8.9.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Zyxel Device supports the IPCP DNS server extensions through the DNS proxy feature.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

8.9.4 LAN TCP/IP

The Zyxel Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Zyxel Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Zyxel Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Zyxel Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Zyxel Device unless you are instructed to do otherwise.

Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

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

CHAPTER 9

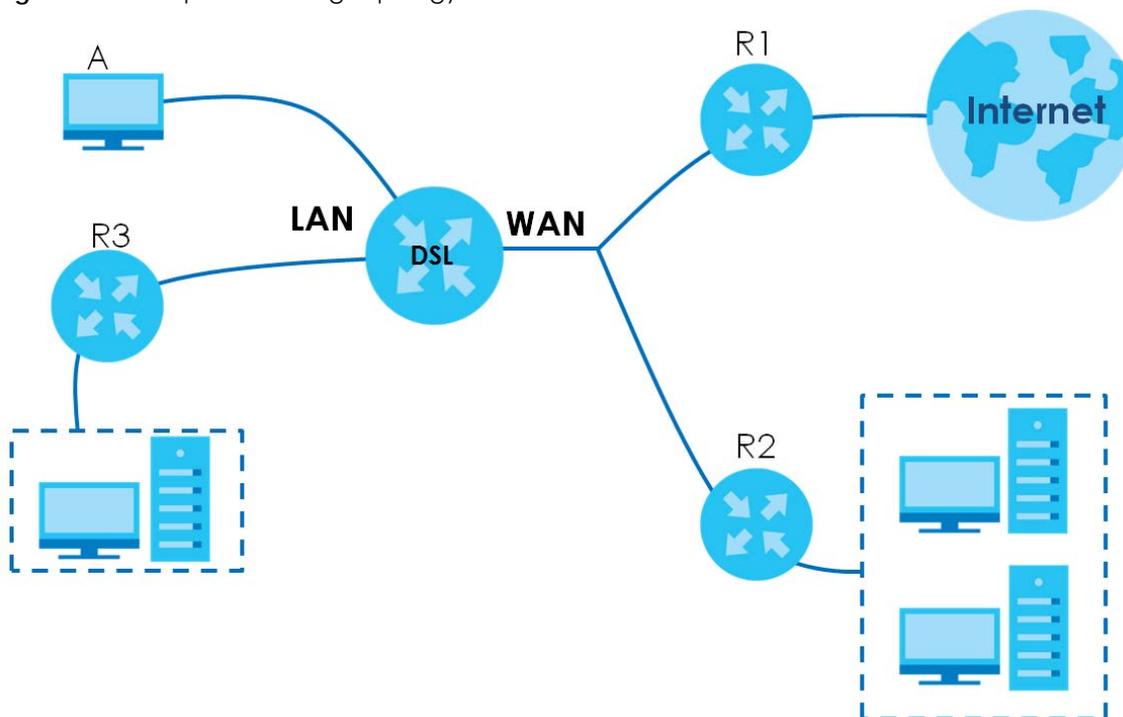
Routing

9.1 Overview

The Zyxel Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Zyxel Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Zyxel Device's LAN interface. The Zyxel Device routes most traffic from **A** to the Internet through the Zyxel Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 84 Example of Routing Topology

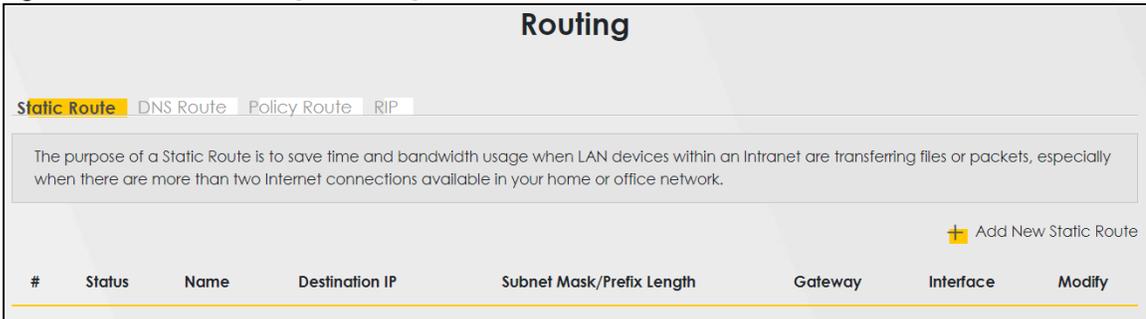


9.2 The Routing Screen

Use this screen to view and configure the static route rules on the Zyxel Device. A static route is used to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets,

especially when there are more than two Internet connections available in your home or office network. Click **Network Setting > Routing > Static Route** to open the following screen.

Figure 85 Network Setting > Routing > Static Route



The following table describes the labels in this screen.

Table 53 Network Setting > Routing > Static Route

| LABEL | DESCRIPTION |
|---------------------------|---|
| Add New Static Route | Click this to configure a new static route. |
| # | This is the index number of the entry. |
| Status | This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active. |
| Name | This is the name that describes or identifies this route. |
| Destination IP | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Subnet Mask/Prefix Length | This parameter specifies the IP network subnet mask of the final destination. |
| Gateway | This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Interface | This is the WAN interface used for this static route. |
| Modify | Click the Edit icon to edit the static route on the Zyxel Device. Click the Delete icon to remove a static route from the Zyxel Device. A window displays asking you to confirm that you want to delete the route. |

9.2.1 Add/Edit Static Route

Use this screen to add or edit a static route. Click **Add new static route** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

Note: The **Gateway IP Address** must be within the range of the selected interface in **Use Interface**.

Figure 86 Routing: Add/Edit

Add New Static Route

Active

Route Name

IP Type

Destination IP Address

Subnet Mask

Use Gateway IP Address

Gateway IP Address

Use Interface

Note
The input range of the Gateway IP Address must be in the same range of the Use Interface.

Cancel OK

The following table describes the labels in this screen.

Table 54 Routing: Add/Edit

| LABEL | DESCRIPTION |
|------------------------|--|
| Active | Click this switch to enable or disable this static route. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Route Name | Enter a descriptive name for the static route. |
| IP Type | Select whether your IP type is IPv4 or IPv6 . |
| Destination IP Address | Enter the IPv4 or IPv6 network address of the final destination. |
| Subnet Mask | If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here. |
| Use Gateway IP Address | The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. Click this switch to enable or disable the gateway IP address. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Gateway IP Address | Enter the IP address of the gateway. |
| Use Interface | Select the WAN interface you want to use for this static route. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

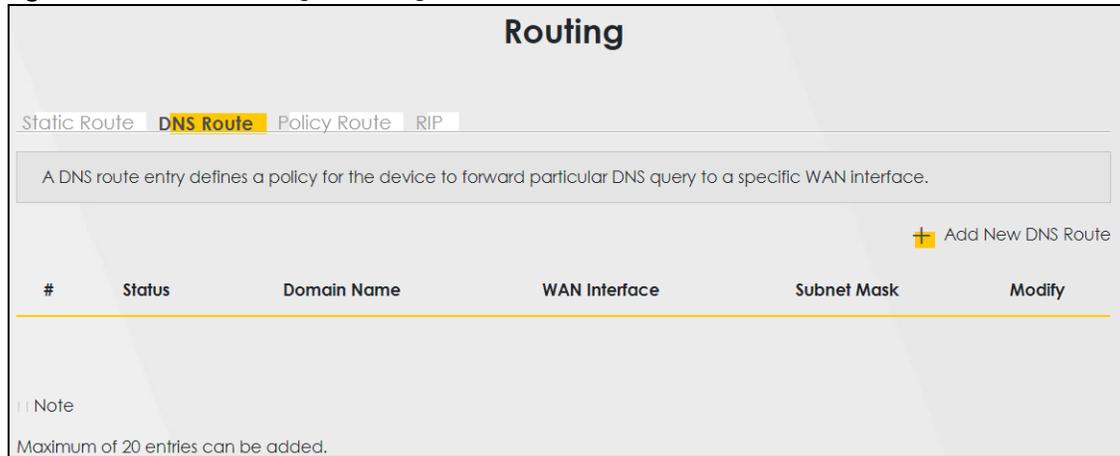
9.3 The DNS Route Screen

Use this screen to view and configure DNS routes on the Zyxel Device. A DNS route entry defines a policy for the Zyxel Device to forward a particular DNS query to a specific WAN interface.

Note: A maximum of 20 DNS routes can be added.

Click **Network Setting > Routing > DNS Route** to open the following screen.

Figure 87 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

Table 55 Network Setting > Routing > DNS Route

| LABEL | DESCRIPTION |
|-------------------|---|
| Add New DNS Route | Click this to add a new DNS route. |
| # | This is the index number of a DNS route. |
| Status | This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active. |
| Domain Name | This is the host name or domain name of the DNS route entry. |
| WAN Interface | This is the WAN connection through which the Zyxel Device forwards DNS requests for this domain name. |
| Subnet Mask | This is the subnet mask of the DNS route entry. |
| Modify | Click the Edit icon to modify the DNS route. Click the Delete icon to delete the DNS route. |

9.3.1 The DNS Route Add Screen

You can manually add the Zyxel Device's DNS route entry. Click **Add New DNS Route** in the **Network Setting > Routing > DNS Route** screen. The screen shown next appears.

Figure 88 DNS Route Add

The following table describes the labels in this screen.

Table 56 DNS Route Add

| LABEL | DESCRIPTION |
|---------------|--|
| Active | Click this switch to enable or disable the DNS route. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Domain Name | Enter the domain name of the DNS route entry. |
| Subnet Mask | Enter the subnet mask of the DNS route entry. |
| WAN Interface | Select the WAN connection through which the Zyxel Device forwards DNS requests for this domain name. WWAN means the wireless cellular interface. |
| Cancel | Click this to exit this screen without saving any changes. |
| OK | Click this to save your changes. |

9.4 The Policy Route Screen

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. Policy routes allow the Zyxel Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

The **Policy Route** screen let you view and configure routing policies on the Zyxel Device. Click **Network Setting > Routing > Policy Route** to open the following screen.

Figure 89 Network Setting > Routing > Policy Route

The purpose of a Policy Route is to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections available in your home or office network.

 Add New Policy Route

| # | Status | Name | Source IP | Source Subnet Mask | Protocol | Source Port | Source MAC | Source Interface | WAN Interface | Modify |
|---|--------|------|-----------|--------------------|----------|-------------|------------|------------------|---------------|--------|
|---|--------|------|-----------|--------------------|----------|-------------|------------|------------------|---------------|--------|

The following table describes the labels in this screen.

Table 57 Network Setting > Routing > Policy Route

| LABEL | DESCRIPTION |
|----------------------|---|
| Add New Policy Route | Click this to create a new policy forwarding rule. |
| # | This is the index number of the entry. |
| Status | This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active. |
| Name | This is the name of the rule. |
| Source IP | This is the source IP address. |
| Source Subnet Mask | This is the source subnet mask address. |
| Protocol | This is the transport layer protocol. |
| Source Port | This is the source port number. |
| Source MAC | This is the source MAC address. |
| Source Interface | This is the interface from which the matched traffic is sent. |
| WAN Interface | This is the WAN interface through which the traffic is routed. |
| Modify | Click the Edit icon to edit this policy. Click the Delete icon to remove a policy from the Zyxel Device. A window displays asking you to confirm that you want to delete the policy. |

9.4.1 Add/Edit Policy Route

Click **Add New Policy Route** in the **Policy Route** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 90 Policy Route: Add/Edit

The screenshot shows a dialog box titled "Add New Policy Route" with a close button in the top right corner. The dialog contains the following fields and controls:

- Active:** A toggle switch that is currently turned on (blue).
- Route Name:** A text input field.
- Source IP Address:** A text input field for IP address.
- Source Subnet Mask:** A text input field for subnet mask.
- Protocol:** A dropdown menu currently set to "None".
- Source Port:** A text input field containing the value "0".
- Source MAC:** A text input field for MAC address, with dashes as placeholders.
- Source Interface(ex: br0 or LAN1-LAN4):** A text input field.
- WAN Interface:** A dropdown menu currently set to "WWAN".

At the bottom of the dialog are two buttons: "Cancel" and "OK".

The following table describes the labels in this screen.

Table 58 Policy Route: Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | Click this switch to enable or disable the policy route. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Route Name | Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces. |
| Source IP Address | Enter the source IP address. |
| Source Subnet Mask | Enter the source subnet mask address. |
| Protocol | Select the transport layer protocol (TCP or UDP). |
| Source Port | Enter the source port number. |
| Source MAC | Enter the source MAC address. |
| Source Interface (ex: br0 or LAN1~LAN4) | Type the name of the interface from which the matched traffic is sent. |
| WAN Interface | Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the Broadband screens. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

9.5 The RIP Screen

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

Click **Network Setting > Routing > RIP** to open the **RIP** screen.

Figure 91 Network Setting > Routing > RIP

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the Enabled checkbox. To stop RIP on the WAN Interface, uncheck the Enabled checkbox. Click the Apply button to start/stop RIP and save the configuration.

| # | Interface | Version | Operation | Enable | Disable Default Gateway |
|---|-----------|---------|-----------|--------------------------|--------------------------|
| 1 | ADSL | RIPv2 ▼ | Active ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | VDSL | RIPv2 ▼ | Active ▼ | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | ETHWAN | RIPv2 ▼ | Active ▼ | <input type="checkbox"/> | <input type="checkbox"/> |

The following table describes the labels in this screen.

Table 59 Network Setting > Routing > RIP

| LABEL | DESCRIPTION |
|-----------|--|
| # | This is the index of the interface in which the RIP setting is used. |
| Interface | This is the name of the interface in which the RIP setting is used. |

Table 59 Network Setting > Routing > RIP

| LABEL | DESCRIPTION |
|-------------------------|---|
| Version | The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). RIP version 1 is universally supported but RIP version 2 carries more information. RIP version 1 is probably adequate for most networks, unless you have an unusual network topology. |
| Operation | Select Passive to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select Active to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers. |
| Enable | Select the check box to activate the settings. |
| Disable Default Gateway | Select the check box to set the Zyxel Device to not send the route information to the default gateway. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |

CHAPTER 10

Quality of Service (QoS)

10.1 QoS Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

Configure QoS on the Zyxel Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

- 1 Configure classifiers to sort traffic into different flows.
- 2 Assign priority and define actions to be performed for a classified traffic flow.

The Zyxel Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

This chapter contains information about configuring QoS and editing classifiers.

10.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth ([Section 10.3 on page 178](#)).
- The **Queue Setup** screen lets you configure QoS queue assignment ([Section 10.4 on page 180](#)).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers ([Section 10.5 on page 182](#)).
- The **Shaper Setup** screen limits outgoing traffic transmission rate on the selected interface ([Section 10.6 on page 187](#)).
- The **Policer Setup** screen to control incoming traffic transmission rate and bursts ([Section 10.7 on page 188](#)).

10.2 What You Need to Know

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

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

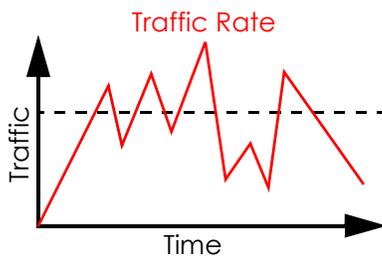
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

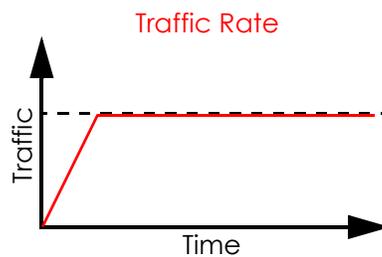
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Zyxel Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



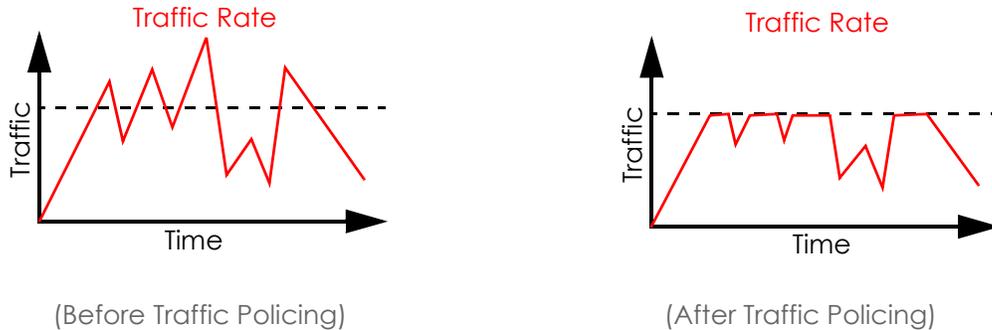
(Before Traffic Shaping)



(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



The Zyxel Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Marker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See [Section 10.8 on page 190](#) for more information on each metering algorithm.

10.3 The Quality of Service General Screen

Click **Network Setting > QoS > General** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority. See [Section 10.1 on page 176](#) for more information.

Note: If upstream bandwidths are set to zero, the CPE sets the value. If the value set here is greater than the current WAN interface linkup rate, the current WAN linkup rate will be used instead. Manually defined QoS is ignored when Upstream Traffic Priority is selected.

Note: Upstream Traffic Priority makes use of a strict eight-level traffic priority QoS.

Figure 92 Network > QoS > General

Quality of Service (QoS) defines the traffic priority of Internet services to the home network.

QoS

WAN Managed Upstream Bandwidth (kbps)

LAN Managed Downstream Bandwidth (kbps)

Upstream Traffic Priority Assigned by

Note

(1) You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.

(2) If Upstream Traffic Priority is selected, 8 level strict priority QoS will be applied automatically according to the selected criteria. In this mode, user manually defined QoS will not be applied until Auto-Priority Mapping is disabled.

(3) If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

The following table describes the labels in this screen.

Table 60 Network Setting > QoS > General

| LABEL | DESCRIPTION |
|----------------------------------|---|
| QoS | Select the Enable check box to turn on QoS to improve your network performance. |
| WAN Managed Upstream Bandwidth | <p>Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.</p> <p>You can set this number higher than the interfaces' actual transmission speed. The Zyxel Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed.</p> <p>You can also set this number lower than the interfaces' actual transmission speed. This will cause the Zyxel Device to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the Zyxel Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.</p> |
| LAN Managed Downstream Bandwidth | <p>Enter the amount of downstream bandwidth for the LAN interfaces (including WLAN) that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection.</p> <p>You can also set this number lower than the WAN interfaces' actual transmission speed. This will cause the Zyxel Device to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the Zyxel Device automatically sets this to the LAN interfaces' maximum supported connection speed.</p> |

Table 60 Network Setting > QoS > General (continued) (continued)

| LABEL | DESCRIPTION |
|---------------------------------------|---|
| Upstream traffic priority Assigned by | <p>Select how the Zyxel Device assigns priorities to various upstream traffic flows.</p> <ul style="list-style-type: none"> None: Disables auto priority mapping and has the Zyxel Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. Ethernet Priority: Automatically assign priority based on the IEEE 802.1p priority level. IP Precedence: Automatically assign priority based on the first three bits of the TOS field in the IP header. Packet Length: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

10.4 The Queue Setup Screen

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment and decide the priority on WAN/LAN interfaces.

Figure 93 Network Setting > QoS > Queue Setup

Queue Setup decides the priority on WAN/LAN interfaces. Use this page to configure QoS queue assignment.

+ Add New Queue

| # | Status | Name | Interface | Priority | Weight | Buffer Management | Rate Limit | Modify |
|---|--------|---------------|-----------|----------|--------|-------------------|------------|--------|
| 1 | | default queue | WAN | 8 | 1 | DT | | |
| 2 | | VOIP | WAN | 1 | 1 | DT | | |

Note

(1) You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.

(2) If Upstream Traffic Priority is selected, 8 level strict priority QoS will be applied automatically according to the selected criteria. In this mode, user manually defined QoS will not be applied until Auto-Priority Mapping is disabled.

(3) If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

The following table describes the labels in this screen.

Table 61 Network Setting > QoS > Queue Setup

| LABEL | DESCRIPTION |
|---------------|---|
| Add New Queue | Click this button to create a new queue entry. |
| # | This is the index number of the entry. |
| Status | This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active. |
| Name | This shows the descriptive name of this queue. |
| Interface | This shows the name of the Zyxel Device's interface through which traffic in this queue passes. |

Table 61 Network Setting > QoS > Queue Setup (continued)

| LABEL | DESCRIPTION |
|-------------------|--|
| Priority | This shows the priority of this queue. |
| Weight | This shows the weight of this queue. |
| Buffer Management | This shows the queue management algorithm used for this queue. Queue management algorithms determine how the Zyxel Device should handle packets when it receives too many (network congestion). |
| Rate Limit | This shows the maximum transmission rate allowed for traffic on this queue. |
| Modify | Click the Edit icon to edit the queue. Click the Delete icon to delete an existing queue. Note that subsequent rules move up by one when you take this action. |

10.4.1 Adding a QoS Queue

Click **Add New Queue** or the **Edit** icon in the **Queue Setup** screen to configure a queue.

Figure 94 Queue Setup: Add

The following table describes the labels in this screen.

Table 62 Queue Setup: Add

| LABEL | DESCRIPTION |
|-----------|--|
| Active | Click this switch to enable or disable the queue. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Name | Enter the descriptive name of this queue. |
| Interface | Select the interface to which this queue is applied. This field is read-only if you are editing the queue. |

Table 62 Queue Setup: Add (continued)

| LABEL | DESCRIPTION |
|-------------------|---|
| Priority | Select the priority level (from 1 to 7) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested. |
| Weight | Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Zyxel Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights. |
| Buffer Management | This field displays Drop Tail (DT) . Drop Tail (DT) is a simple queue management algorithm that allows the Zyxel Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it). |
| Rate Limit | Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

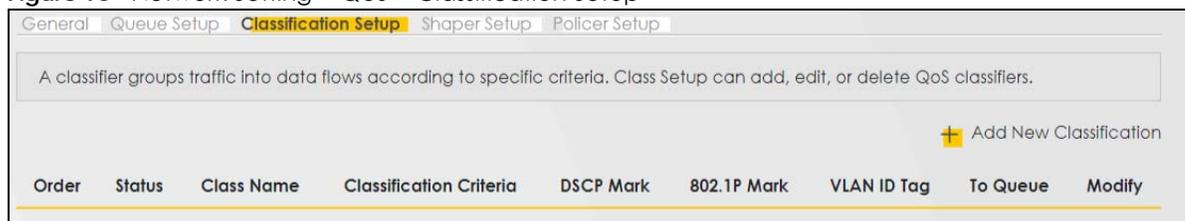
10.5 The QoS Classification Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Zyxel Device forwards through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Classification Setup** to open the following screen.

Figure 95 Network Setting > QoS > Classification Setup



The following table describes the labels in this screen.

Table 63 Network Setting > QoS > Classification Setup

| LABEL | DESCRIPTION |
|------------------------|--|
| Add New Classification | Click this to create a new classifier. |
| Order | This is the index number of the entry. The classifiers are applied in order of their numbering. |
| Status | This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active. |
| Class Name | This is the name of the classifier. |

Table 63 Network Setting > QoS > Classification Setup (continued)

| LABEL | DESCRIPTION |
|-------------------------|---|
| Classification Criteria | This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier. |
| DSCP Mark | This is the DSCP number added to traffic of this classifier. |
| 802.1P Mark | This is the IEEE 802.1p priority level assigned to traffic of this classifier. |
| VLAN ID Tag | This is the VLAN ID number assigned to traffic of this classifier. |
| To Queue | This is the name of the queue in which traffic of this classifier is put. |
| Modify | Click the Edit icon to edit the classifier. Click the Delete icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action. |

10.5.1 Add/Edit QoS Class

Click **Add New Classification** in the **Classification Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 96 Classification Setup: Add/Edit

Add New Classification ✕

Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

Active

Class Name

Classification Order Last

Step2: Criteria Configuration

Use the configurations below to specify the characteristics of a data flow needed to be managed by this QoS rule

Basic

From Interface LAN

Ether Type NA

Source

Address Subnet Mask Exclude

Port Range - Exclude

MAC - - - - - MAC Mask Exclude

Destination

Address Subnet Mask Exclude

Port Range ~ Exclude

MAC - - - - - MAC Mask Exclude

Others

Service RTSP Server Exclude

IP protocol TCP Exclude

DHCP Exclude

IP Packet Length - Exclude

DSCP (0-63) Exclude

802.1P 0 BE Exclude

VLAN ID (1-4094) Exclude

TCP ACK Exclude

Step3: Packet Modification

The content of the packet can be modified by applying the following settings

DSCP Mark Unchange (0-63)

VLAN ID Tag Unchange (1-4094)

802.1P Mark 0 BE

Step4: Class Routing

This module can route a packet to a certain interface according to the class setting

Forward To Interface Unchange

Step5: Outgoing Queue Selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface.

To Queue Index default queue

Cancel OK

The following table describes the labels in this screen.

Table 64 Classification Setup: Add/Edit

| LABEL | DESCRIPTION |
|-------------------------------|--|
| Step1: Class Configuration | |
| Active | Click this switch to enable or disable the classifier. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Class Name | Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces. |
| Classification Order | Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking Apply . Select Last to put this rule in the back of the classifier list. |
| Step2: Criteria Configuration | |
| Basic | |
| From Interface | If you want to classify the traffic by an ingress interface, select an interface from the From Interface drop-down list box. |
| Ether Type | Select a predefined application to configure a class for the matched traffic. If you select IP , you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select 802.1Q , you can configure an 802.1p priority level. |
| Source | |
| Address | Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| Subnet Mask | Enter the source subnet mask. |
| Port Range | If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source. |
| MAC | Select the check box and enter the source MAC address of the packet. |
| MAC Mask | Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| Destination | |
| Address | Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| Subnet Mask | Enter the source subnet mask. |
| Port Range | If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source. |
| MAC | Select the check box and enter the source MAC address of the packet. |
| MAC Mask | Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. |
| Exclude | Select this option to exclude the packets that match the specified criteria from this classifier. |
| Others | |

Table 64 Classification Setup: Add/Edit (continued)

| LABEL | DESCRIPTION |
|----------------------------|--|
| Service | <p>This field is available only when you select IP in the Ether Type field.</p> <p>This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.</p> |
| IP Protocol | <p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select the protocol (service type) from TCP, UDP, ICMP or IGMP. If you select User defined, enter the protocol (service type) number.</p> |
| DHCP | <p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select a DHCP option.</p> <p>If you select Vendor Class ID (DHCP Option 60), enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.</p> <p>If you select Client ID (DHCP Option 61), enter the Identity Association Identifier (IAD Option 61) of the matched traffic, such as the MAC address of the device.</p> <p>If you select User Class ID (DHCP Option 77), enter a string that identifies the user's category or application type in the matched DHCP packets.</p> <p>If you select Vendor Specific Info (DHCP Option 125), enter the vendor specific information of the matched traffic, such as the product class, model name, and serial number of the device.</p> |
| IP Packet Length | <p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.</p> |
| DSCP | <p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.</p> |
| 802.1P | <p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.</p> |
| VLAN ID | <p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and specify a VLAN ID number.</p> |
| TCP ACK | <p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.</p> |
| Exclude | <p>Select this option to exclude the packets that match the specified criteria from this classifier.</p> |
| Step3: Packet Modification | |
| DSCP Mark | <p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select Remark, enter a DSCP value with which the Zyxel Device replaces the DSCP field in the packets.</p> <p>If you select Unchange, the Zyxel Device keep the DSCP field in the packets.</p> |
| VLAN ID | <p>If you select Remark, enter a VLAN ID number with which the Zyxel Device replaces the VLAN ID of the frames.</p> <p>If you select Remove, the Zyxel Device deletes the VLAN ID of the frames before forwarding them out.</p> <p>If you select Add, the Zyxel Device treat all matched traffic untagged and add a second VLAN ID.</p> <p>If you select Unchange, the Zyxel Device keep the VLAN ID in the packets.</p> |

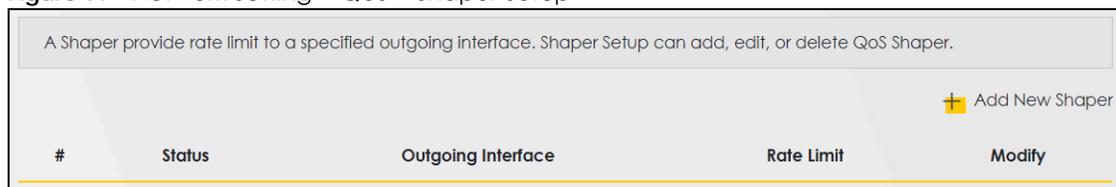
Table 64 Classification Setup: Add/Edit (continued)

| LABEL | DESCRIPTION |
|---------------------------------|--|
| 802.1P Mark | Select a priority level with which the Zyxel Device replaces the IEEE 802.1p priority field in the packets. If you select Unchange , the Zyxel Device keep the 802.1p priority field in the packets. |
| Step4: Class Routing | |
| Forward to Interface | Select a WAN interface through which traffic of this class will be forwarded out. If you select Unchange , the Zyxel Device forward traffic of this class according to the default routing table. |
| Step5: Outgoing Queue Selection | |
| To Queue Index | Select a queue that applies to this class. You should have configured a queue in the Queue Setup screen already. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

10.6 The QoS Shaper Setup Screen

This screen lets you use the token bucket algorithm to allow a certain amount of large bursts while keeping a limit for processing outgoing traffic at the average rate. Click **Network Setting > QoS > Shaper Setup**. The screen appears as shown.

Figure 97 Network Setting > QoS > Shaper Setup



The following table describes the labels in this screen.

Table 65 Network Setting > QoS > Shaper Setup

| LABEL | DESCRIPTION |
|--------------------|---|
| Add New Shaper | Click this to create a new entry. |
| # | This is the index number of the entry. |
| Status | This field displays whether the shaper is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this shaper is not active. |
| Outgoing Interface | This shows the name of the Zyxel Device's interface through which traffic in this shaper applies. |
| Rate Limit | This shows the average rate limit of traffic bursts for this shaper. |
| Modify | Click the Edit icon to edit the shaper. Click the Delete icon to delete an existing shaper. Note that subsequent rules move up by one when you take this action. |

10.6.1 Add/Edit a QoS Shaper

Click **Add New Shaper** in the **Shaper Setup** screen or the **Edit** icon next to a shaper to show the following screen.

Figure 98 Shaper Setup: Add/Edit

The following table describes the labels in this screen.

Table 66 Shaper Setup: Add/Edit

| LABEL | DESCRIPTION |
|------------|---|
| Active | Click this switch to enable or disable the shaper. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Interface | Select the Zyxel Device's interface through which traffic in this shaper applies |
| Rate Limit | Enter the average rate limit of traffic bursts for this shaper. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

10.7 The QoS Policer Setup Screen

Use this screen to view QoS policers that allow you to limit the transmission rate of incoming traffic and apply actions, such as drop, pass, or modify, to the DSCP value of matched traffic. Click **Network Setting > QoS > Policer Setup**. The screen appears as shown.

Figure 99 Network Setting > QoS > Policer Setup

The following table describes the labels in this screen.

Table 67 Network Setting > QoS > Policer Setup

| LABEL | DESCRIPTION |
|-----------------|--|
| Add new Policer | Click this to create a new entry. |
| # | This is the index number of the entry. |

Table 67 Network Setting > QoS > Policer Setup (continued)

| LABEL | DESCRIPTION |
|-------------------|---|
| Status | This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active. |
| Name | This field displays the descriptive name of this policer. |
| Regulated Classes | This field displays the name of a QoS classifier |
| Meter Type | This field displays the type of QoS metering algorithm used in this policer. |
| Rule | These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes. |
| Action | This shows the how the policer has the Zyxel Device treat different types of traffic belonging to the policer's member QoS classes. |
| Modify | Click the Edit icon to edit the policer. Click the Delete icon to delete an existing policer. Note that subsequent rules move up by one when you take this action. |

10.7.1 Add/Edit a QoS Policer

Click **Add New Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 100 Policer Setup: Add/Edit

QoS Policer Configuration

Active

Name

Meter Type Simple Token Bucket

Committed Rate (kbps)

Committed Burst Size (kbytes)

Conforming Action Pass

Non-Conforming Action Drop

Regulated Classes Member Setting

Available Class

VoipCas

VoipEth

VoipCas2

Selected Class

Cancel OK

The following table describes the labels in this screen.

Table 68 Policer Setup: Add/Edit

| LABEL | DESCRIPTION |
|-----------------------|--|
| Active | Click this switch to enable or disable the policer. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Name | Enter the descriptive name of this policer. |
| Meter Type | This shows the traffic metering algorithm used in this policer. The Simple Token Bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size. The Single Rate Three Color Marker (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The Two Rate Three Color Marker (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR). |
| Committed Rate | Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic. |
| Committed Burst Size | Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm. |
| Conforming Action | Specify what the Zyxel Device does for packets within the committed rate and burst size (green-marked packets). <ul style="list-style-type: none"> Pass: Send the packets without modification. DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use. |
| Non-Conforming Action | Specify what the Zyxel Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). <ul style="list-style-type: none"> Drop: Discard the packets. DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network. |
| Available Class | Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. |
| Selected Class | Highlight a QoS classifier in the Available Class box and use the > button to move it to the Selected Class box. To remove a QoS classifier from the Selected Class box, select it and use the < button. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

10.8 Technical Reference

The following section contains additional technical information about the Zyxel Device features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority.

The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 69 IEEE 802.1p Priority Level and Traffic Type

| PRIORITY LEVEL | TRAFFIC TYPE |
|----------------|---|
| Level 7 | Typically used for network control traffic such as router configuration messages. |
| Level 6 | Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay). |
| Level 5 | Typically used for video that consumes high bandwidth and is sensitive to jitter. |
| Level 4 | Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions. |
| Level 3 | Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay. |
| Level 2 | This is for "spare bandwidth". |
| Level 1 | This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users. |
| Level 0 | Typically used for best-effort traffic. |

DiffServ

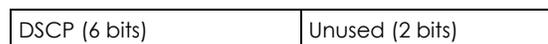
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

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

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



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

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the Zyxel Device, the Zyxel Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the Zyxel Device. On the Zyxel Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 70 Internal Layer2 and Layer3 QoS Mapping

| PRIORITY QUEUE | LAYER 2 | LAYER 3 | | |
|----------------|---|---------------------|--------------------------------------|-------------------------|
| | IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY) | TOS (IP PRECEDENCE) | DSCP | IP PACKET LENGTH (BYTE) |
| 0 | 1 | 0 | 000000 | |
| 1 | 2 | | | |
| 2 | 0 | 0 | 000000 | >1100 |
| 3 | 3 | 1 | 001110 001100 001010 001000 | 250~1100 |
| 4 | 4 | 2 | 010110 010100 010010 010000 | |
| 5 | 5 | 3 | 011110 011100 011010 011000 | <250 |
| 6 | 6 | 4 | 100110 100100 100010 100000 | |
| | | 5 | 101110 101000 | |

Table 70 Internal Layer2 and Layer3 QoS Mapping

| PRIORITY QUEUE | LAYER 2 | LAYER 3 | | |
|----------------|---|---------------------|--------|-------------------------|
| | IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY) | TOS (IP PRECEDENCE) | DSCP | IP PACKET LENGTH (BYTE) |
| 7 | 7 | 6 | 110000 | |
| | | 7 | 111000 | |

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size, so the bucket can hold up to b tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the Zyxel Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Zyxel Device treats the packet in either one of the following ways:

In traffic shaping:

- Holds it in the queue until enough tokens are available in the bucket.

In traffic policing:

- Drops it.
- Transmits it but adds a DSCP mark. The Zyxel Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the Zyxel Device checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the Zyxel Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

CHAPTER 11

Network Address Translation (NAT)

11.1 NAT Overview

This chapter discusses how to configure NAT on the Zyxel Device. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet; for example, the source address of an outgoing packet, used within one network, to a different IP address known within another network.

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network ([Section 11.2 on page 196](#)).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings ([Section 11.3 on page 200](#)).
- Use the **DMZ** screen to configure a default server ([Section 11.4 on page 204](#)).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the Zyxel Device ([Section 11.5 on page 204](#)).
- Use the **Address Mapping** screen to configure the Zyxel Device's address mapping settings ([Section 11.6 on page 205](#)).
- Use the **Sessions** screen to configure the Zyxel Device's maximum number of NAT sessions ([Section 11.6 on page 205](#)).

11.1.2 What You Need To Know

Inside/Outside

Inside/outside denotes where a host is located relative to the Zyxel Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN

side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See [Section 11.8 on page 208](#) for advanced technical information on NAT.

11.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network. Port forwarding is commonly used when you want to use Internet activities such as online gaming, P2P file sharing, or even hosting servers on your network. It creates a bridge that allows another party from the Internet to contact a specific LAN client on your network correctly.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

The most often used port numbers and services are shown in [Appendix D on page 377](#). Please refer to RFC 1700 for further information about port numbers.

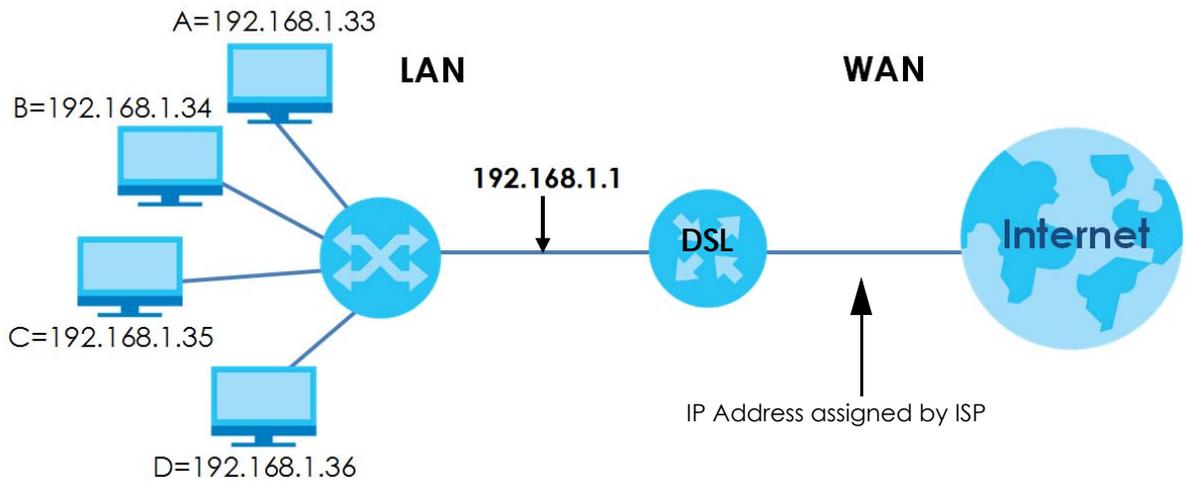
Note: TCP port 7547 is reserved for system use.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 101 Multiple Servers Behind NAT Example



Click **Network Setting > NAT > Port Forwarding** to open the following screen.

Figure 102 Network Setting > NAT > Port Forwarding

Port Forwarding is commonly used when you want to use Internet activities such as, online gaming, P2P file sharing or even hosting servers on your network. It creates a bridge to allow another party from the internet, to contact a specific LAN client on your network correctly.

+ Add New Rule

| # | Status | Service Name | Originating IP | WAN Interface | Server IP Address | Start Port | End Port | Translation Start Port | Translation End Port | Protocol | Modify |
|---|--------|--------------|----------------|---------------|-------------------|------------|----------|------------------------|----------------------|----------|--------|
| Note | | | | | | | | | | | |
| The TCP port 7547 is reserved for system usage. | | | | | | | | | | | |

The following table describes the fields in this screen.

Table 71 Network Setting > NAT > Port Forwarding

| LABEL | DESCRIPTION |
|------------------------|--|
| Add New Rule | Click this to add a new rule. |
| # | This is the index number of the entry. |
| Status | This field displays whether the NAT rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active. |
| Service Name | This shows the service's name. |
| Originating IP | This field displays the source IP address from the WAN interface. |
| WAN Interface | This shows the WAN interface through which the service is forwarded. |
| Server IP Address | This is the server's IP address. |
| Start Port | This is the first external port number that identifies a service. |
| End Port | This is the last external port number that identifies a service. |
| Translation Start Port | This is the first internal port number that identifies a service. |

Table 71 Network Setting > NAT > Port Forwarding (continued)

| LABEL | DESCRIPTION |
|----------------------|--|
| Translation End Port | This is the last internal port number that identifies a service. |
| Protocol | This shows the IP protocol supported by this virtual server, whether it is TCP , UDP , or TCP/UDP . |
| Modify | Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule. |

11.2.1 Add/Edit Port Forwarding

Click **Add New Rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen. Specify either a port or a range of ports, a server IP address, and a protocol to configure a port forwarding rule.

Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

Note: To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

Note: TCP port 7547 is reserved for system use.

Figure 103 Port Forwarding: Add/Edit

Add New Rule

Active

Service Name

WAN Interface Default ▼

Start Port

End Port

Translation Start Port

Translation End Port

Server IP Address . . .

Configure Originating IP Enable

Protocol TCP ▼

Note

1.If Start Port and Translation Start Port, End Port and Translation End Port is configured the same, then Port Forwarding is configured.
 If Start Port and Translation Start Port, End Port and Translation End Port are configured differently, then Port Translation is configured (one to one mapping).
 For example: Start Port: 100 End Port: 120; Translation Start Port: 200 Translation End Port: 220

2.Originating IP is optional. User must enable Configure Originating IP to add a source IP address which from the WAN Interface.

3.The TCP port 7547 is reserved for system usage.

Cancel OK

The following table describes the labels in this screen.

Table 72 Port Forwarding: Add/Edit

| LABEL | DESCRIPTION |
|---------------|---|
| Active | Click this switch to enable or disable the rule. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Service Name | Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on). |
| WAN Interface | Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled. |
| Start Port | Enter the original destination port for the packets. To forward only one port, enter the port number again in the End Port field. To forward a series of ports, enter the start port number here and the end port number in the End Port field. |

Table 72 Port Forwarding: Add/Edit (continued)

| LABEL | DESCRIPTION |
|--------------------------|---|
| End Port | Enter the last port of the original destination port range. To forward only one port, enter the port number in the Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port field above. |
| Translation Start Port | This shows the port number to which you want the Zyxel Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated. |
| Translation End Port | This shows the last port of the translated port range. |
| Server IP Address | Enter the inside IP address of the virtual server here. |
| Configure Originating IP | Select Enable to enter the source IP address of WAN interface. |
| Originating IP | Enter the source IP address of WAN interface. |
| Protocol | Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP . |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

11.3 The Port Triggering Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding addresses this problem. Trigger port forwarding allows computers on the LAN to dynamically take turns using the service. The Zyxel Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Zyxel Device's WAN port receives a response with a specific port number and protocol ("open" port), the Zyxel Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

Note: TCP port 7547 is reserved for system use.

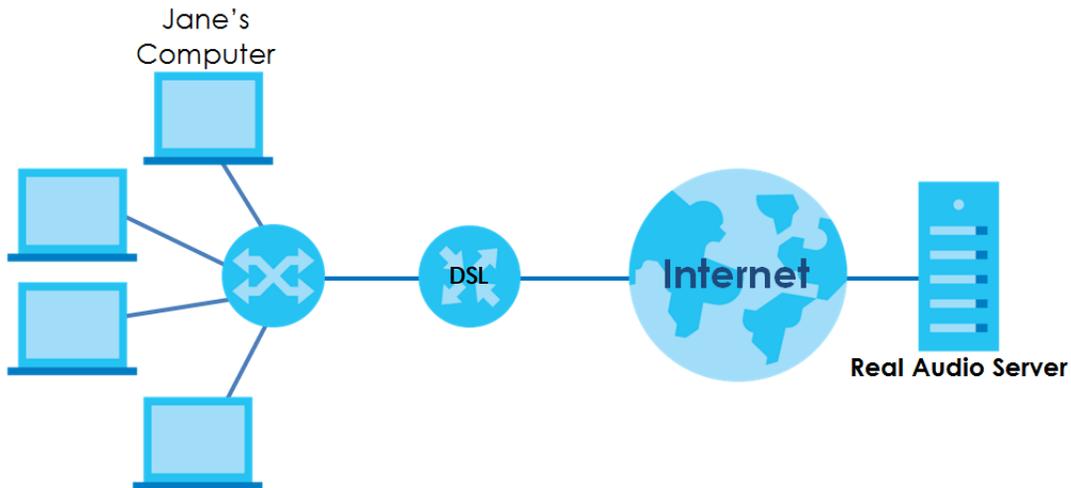
Note: If you select TCP or TCP/UDP for port triggering, the maximum number of trigger ports for a single rule or all rules is 499.

If you select UDP for port triggering, the maximum number of trigger ports for a single rule or all rules is 999.

Note: The maximum number of open ports for a rule is 999.

For example:

Figure 104 Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The Zyxel Device forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Zyxel Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT > Port Triggering** to open the following screen. Use this screen to view your Zyxel Device's trigger port settings.

Figure 105 Network Setting > NAT > Port Triggering

Port Triggering is a way to automate port forwarding with a little better security. It dynamically forwards connection or data to whatever LAN client made a certain outgoing connection. Example: You define port 25 as Trigger Port and port 113 as Open Port. If any of the LAN devices on your network creates an outgoing connection via port 25, all incoming connections via port 113 will temporarily go to that client.

[+ Add New Rule](#)

| # | Status | Service Name | WAN Interface | Trigger Start Port | Trigger End Port | Trigger Proto. | Open Start Port | Open End Port | Open Protocol | Modify |
|--|--------|--------------|---------------|--------------------|------------------|----------------|-----------------|---------------|---------------|--------|
| <p>Note</p> <p>(1) The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000.</p> <p>(2) The TCP port 7547 is reserved for system usage.</p> | | | | | | | | | | |

The following table describes the labels in this screen.

Table 73 Network Setting > NAT > Port Triggering

| LABEL | DESCRIPTION |
|--------------------|--|
| Add New Rule | Click this to create a new rule. |
| # | This is the index number of the entry. |
| Status | This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active. |
| Service Name | This field displays the name of the service used by this rule. |
| WAN Interface | This field shows the WAN interface through which the service is forwarded. |
| Trigger Start Port | The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service. |
| Trigger End Port | This is the last port number that identifies a service. |
| Trigger Proto. | This is the trigger transport layer protocol. |
| Open Start Port | The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service. |
| Open End Port | This is the last port number that identifies a service. |
| Open Proto. | This is the open transport layer protocol. |
| Modify | Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule. |

11.3.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen. Use this screen to configure a port or range of ports and protocols for sending out requests and for receiving responses.

Figure 106 Port Triggering: Add/Edit

The following table describes the labels in this screen.

Table 74 Port Triggering: Configuration Add/Edit

| LABEL | DESCRIPTION |
|--------------------|--|
| Active | Select Enable or Disable to activate or deactivate the rule. |
| Service Name | Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on). |
| WAN Interface | Select a WAN interface for which you want to configure port triggering rules. |
| Trigger Start Port | The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers. |
| Trigger End Port | Type a port number or the ending port number in a range of port numbers. |
| Trigger Protocol | Select the transport layer protocol from TCP , UDP , or TCP/UDP . |
| Open Start Port | The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers. |
| Open End Port | Type a port number or the ending port number in a range of port numbers. |
| Open Protocol | Select the transport layer protocol from TCP , UDP , or TCP/UDP . |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

11.4 The DMZ Screen

A LAN client in the Demilitarized Zone (DMZ) is no longer behind the Zyxel Device and therefore can run any Internet applications such as video conferencing and Internet gaming without restrictions. This, however, poses security threats to the Zyxel Device.

Note: Use an IPv4 address for the DMZ server.

Figure 107 Network Setting > NAT > DMZ

The following table describes the fields in this screen.

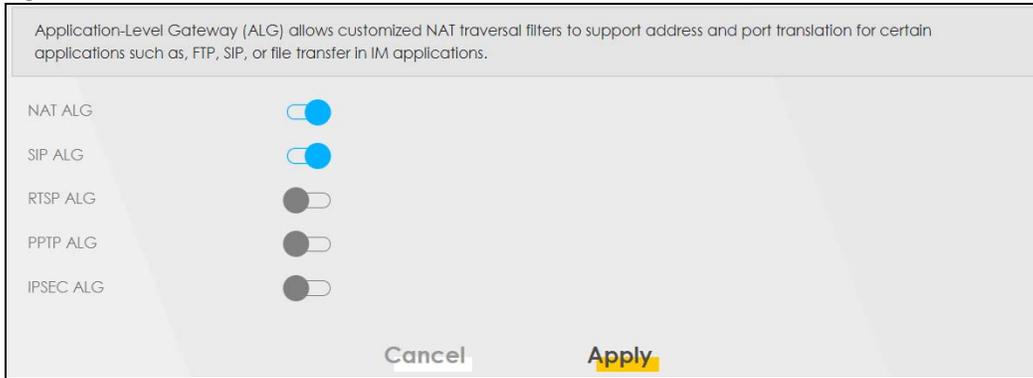
Table 75 Network Setting > NAT > DMZ

| LABEL | DESCRIPTION |
|------------------------|---|
| Default Server Address | Enter the IP address of the default server which receives packets from ports that are not specified in the NAT Port Forwarding screen. Note: If you do not assign a Default Server Address , the Zyxel Device discards all packets received for ports that are not specified in the NAT Port Forwarding screen. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

11.5 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows customized NAT traversal filters to support address and port translation for certain applications such as FTP, SIP, or file transfer in IM applications. It allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the Zyxel Device registers with the SIP register server, the SIP ALG translates the Zyxel Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Zyxel Device is behind a SIP ALG.

Use this screen to enable and disable the NAT and SIP (VoIP) ALG in the Zyxel Device. To access this screen, click **Network Setting > NAT > ALG**.

Figure 108 Network Setting > NAT > ALG

The following table describes the fields in this screen.

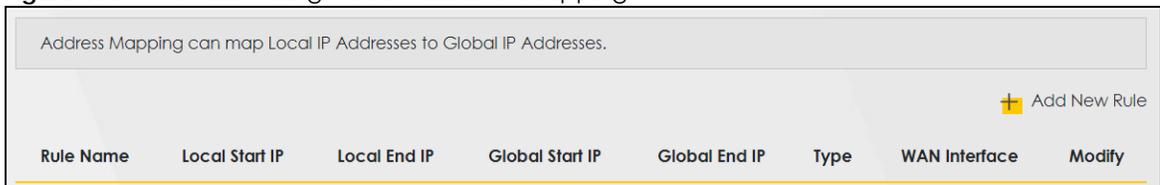
Table 76 Network Setting > NAT > ALG

| LABEL | DESCRIPTION |
|-----------|--|
| NAT ALG | Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules. |
| SIP ALG | Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules. |
| RTSP ALG | Enable this to have the Zyxel Device detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| PPTP ALG | Enable this to turn on the PPTP ALG on the VMG to detect PPTP traffic and help build PPTP sessions through the Zyxel Device's NAT. |
| IPSEC ALG | Enable this to turn on the IPsec ALG on the VMG to detect IPsec traffic and help build IPsec sessions through the Zyxel Device's NAT. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

11.6 The Address Mapping Screen

Address mapping can map local IP Addresses to global IP addresses. Ordering your rules is important because the Zyxel Device applies the rules in the order that you specify. When a rule matches the current packet, the Zyxel Device takes the corresponding action and the remaining rules are ignored.

Click **Network Setting > NAT > Address Mapping** to display the following screen.

Figure 109 Network Setting > NAT > Address Mapping

The following table describes the fields in this screen.

Table 77 Network Setting > NAT > Address Mapping

| LABEL | DESCRIPTION |
|--------------------|--|
| Add New Rule | Click this to create a new rule. |
| Rule Name | This is the name of the rule. |
| Local Start IP | This is the starting Inside Local IP Address (ILA). |
| Local End IP | This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-One mapping types. |
| Global Start IP | This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type. |
| Global End IP | This is the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types. |
| Type | <p>This is the address mapping type.</p> <p>One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p>Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Zyxel Device's Single User Account feature that previous routers supported only.</p> <p>Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses.</p> |
| Wan Interface Name | This is the WAN interface to which the address mapping rule applies. |
| Modify | <p>Click the Edit icon to go to the screen where you can edit the address mapping rule.</p> <p>Click the Delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.</p> |

11.6.1 Add/Edit Address Mapping Rule

To add or edit an address mapping rule, click **Add new rule** or the rule's edit icon in the **Address Mapping** screen to display the screen shown next. Specify the NAT mapping type, the local and global IP address(es), and a WAN interface in this screen.

Figure 110 Address Mapping: Add/Edit

The following table describes the fields in this screen.

Table 78 Address Mapping: Add/Edit

| LABEL | DESCRIPTION |
|-----------------|--|
| Rule Name | Type up to 20 alphanumeric characters for the name of this rule. |
| Type | Choose the IP/port mapping type from one of the following. One-to-One: This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. Many-to-One: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Zyxel Device's Single User Account feature that previous routers supported only. Many-to-Many: This mode maps multiple local IP addresses to shared global IP addresses. |
| Local Start IP | Enter the starting Inside Local IP Address (ILA). |
| Local End IP | Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for One-to-One mapping types. |
| Global Start IP | Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the Many-to-One mapping type. |
| Global End IP | Enter the ending Inside Global IP Address (IGA). This field is blank for One-to-One and Many-to-One mapping types. |
| WAN Interface | Select a WAN interface to which the address mapping rule applies. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

11.7 The NAT Sessions Screen

Use this screen to limit the number of concurrent NAT sessions a client can use, to ensure that no single client uses up too many available NAT sessions. Some applications, such as P2P file sharing, demand a

greater number of NAT sessions in order to get a better uploading and downloading rate. Click **Network Setting > NAT > Sessions** to display the following screen.

Figure 111 Network Setting > NAT > Sessions

The figure below limits the open sessions on a per host (a LAN IP Address) basis. Some applications, especially like P2P file sharing demand a greater number of NAT sessions in order to get a better uploading and downloading rate.

MAX NAT Session Per Host (0 ~ 20480)

Note

(1) Enter IP address and click "Apply" to activate the DMZ host.
 (2) Clear the IP address field and click "Apply" to de-activate the DMZ host.

The following table describes the fields in this screen.

Table 79 Network Setting > NAT > Sessions

| LABEL | DESCRIPTION |
|--------------------------------------|---|
| MAX NAT Session Per Host (0 ~ 20480) | Use this field to set a limit to the number of concurrent NAT sessions each client host can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer-to-peer application use, lower this number to ensure no single client uses too many of the available NAT sessions. |
| Cancel | Click this to exit this screen without saving any changes. |
| Apply | Click this to save your changes on this screen. |

11.8 Technical Reference

This part contains more information regarding NAT.

11.8.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Zyxel Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 80 NAT Definitions

| ITEM | DESCRIPTION |
|---------|-------------------------------------|
| Inside | This refers to the host on the LAN. |
| Outside | This refers to the host on the WAN. |

Table 80 NAT Definitions (continued)

| ITEM | DESCRIPTION |
|--------|---|
| Local | This refers to the packet address (source or destination) as the packet travels on the LAN. |
| Global | This refers to the packet address (source or destination) as the packet travels on the WAN. |

NAT never changes the IP address (either local or global) of an outside host.

11.8.2 What NAT Does

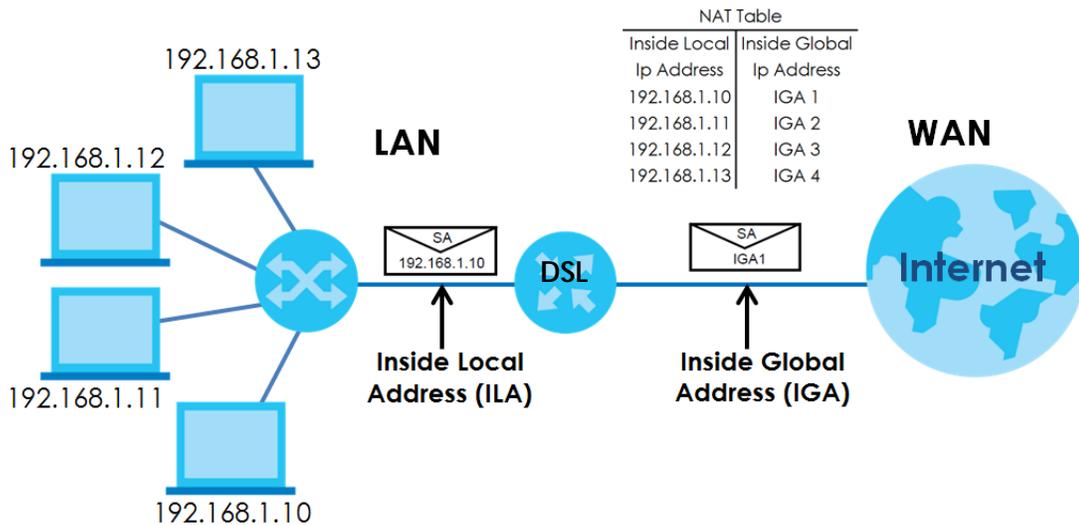
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your Zyxel Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

11.8.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Zyxel Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

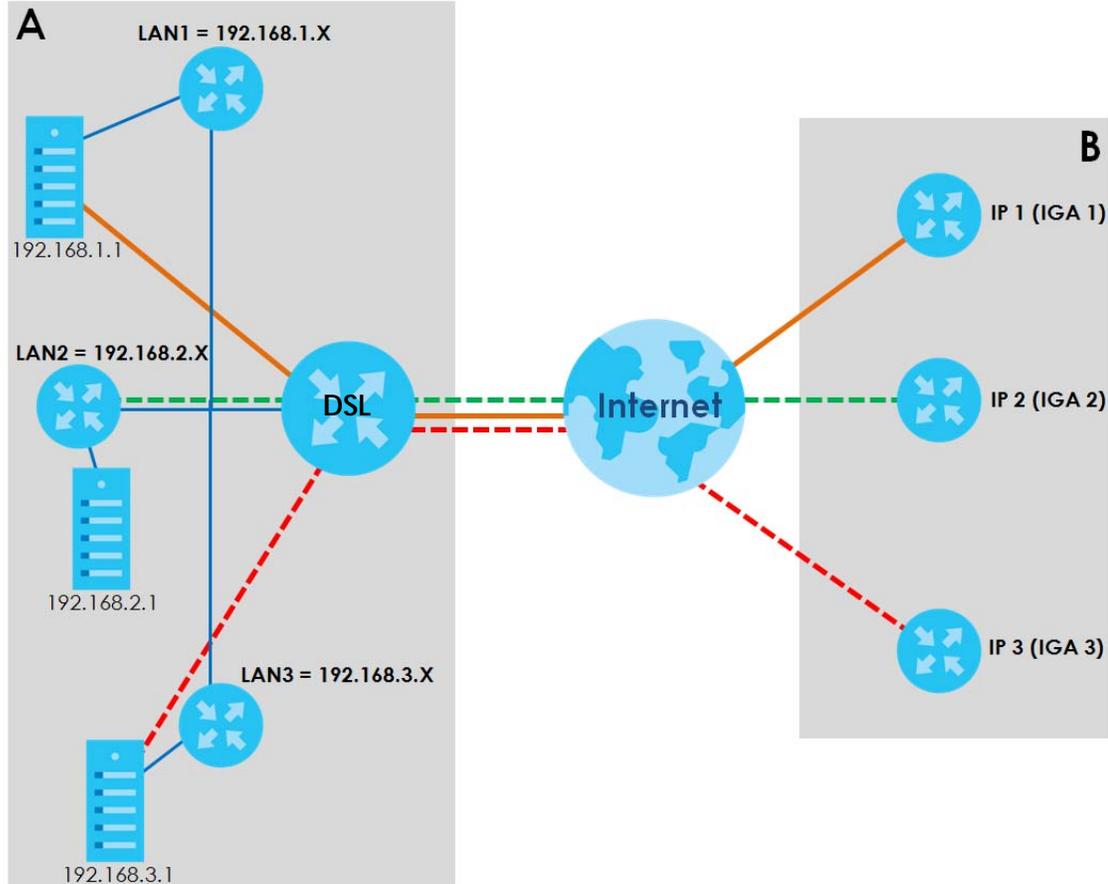
Figure 112 How NAT Works



11.8.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the Zyxel Device can communicate with three distinct WAN networks.

Figure 113 NAT Application With IP Alias



Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

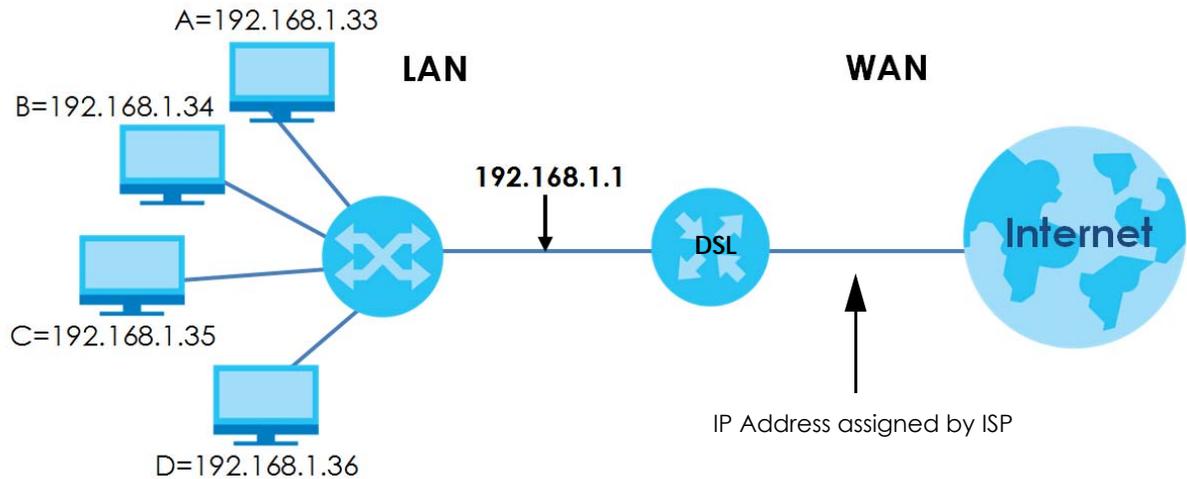
Table 81 Services and Port Numbers

| SERVICES | PORT NUMBER |
|---|-------------|
| ECHO | 7 |
| FTP (File Transfer Protocol) | 21 |
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name System) | 53 |
| Finger | 79 |
| HTTP (Hyper Text Transfer protocol or WWW, Web) | 80 |
| POP3 (Post Office Protocol) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| SNMP (Simple Network Management Protocol) | 161 |
| SNMP trap | 162 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 114 Multiple Servers Behind NAT Example



CHAPTER 12

Dynamic DNS Setup

12.1 DNS Overview

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The Zyxel Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Zyxel Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Dynamic DNS

Dynamic DNS allows you to use a dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

You first need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes ([Section 12.2 on page 214](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device ([Section 12.3 on page 215](#)).

12.1.2 What You Need To Know

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

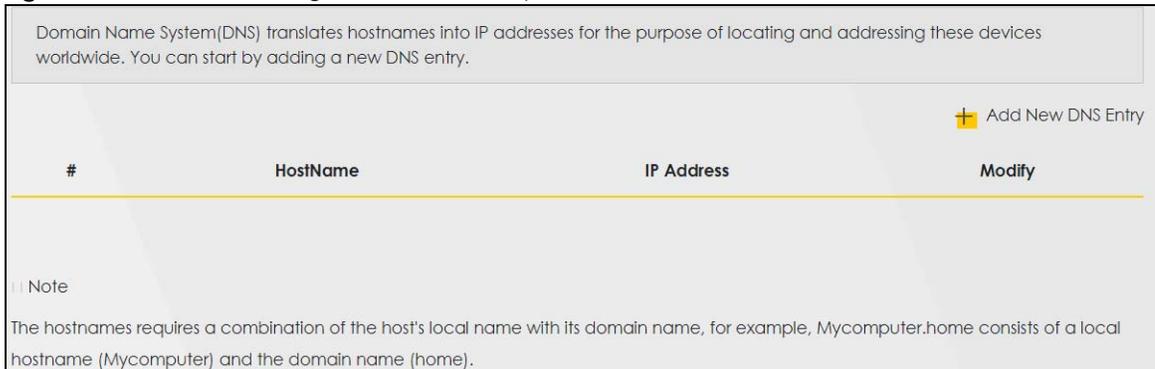
If you have a private WAN IP address, then you cannot use Dynamic DNS.

12.2 The DNS Entry Screen

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP address and vice versa. Use this screen to view and configure DNS routes on the Zyxel Device. Click **Network Setting > DNS** to open the **DNS Entry** screen.

Note: The host name should consist of the host's local name and the domain name. For example, Mycomputer.home is a host name where Mycomputer is the host's local name, and .home is the domain name.

Figure 115 Network Setting > DNS > DNS Entry



The following table describes the fields in this screen.

Table 82 Network Setting > DNS > DNS Entry

| LABEL | DESCRIPTION |
|-------------------|--|
| Add New DNS Entry | Click this to create a new DNS entry. |
| # | This is the index number of the entry. |
| Hostname | This indicates the host name or domain name. |
| IP Address | This indicates the IP address assigned to this computer. |
| Modify | Click the Edit icon to edit the rule. Click the Delete icon to delete an existing rule. |

12.2.1 Add/Edit DNS Entry

You can manually add or edit the Zyxel Device's DNS name and IP address entry. Click **Add New DNS Entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 116 DNS Entry: Add/Edit

The following table describes the labels in this screen.

Table 83 DNS Entry: Add/Edit

| LABEL | DESCRIPTION |
|------------|---|
| Host Name | Enter the host name of the DNS entry. |
| IP Address | Enter the IP address of the DNS entry. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

12.3 The Dynamic DNS Screen

Dynamic DNS can update your current dynamic IP into a hostname. Use this screen to change your Zyxel Device's DDNS setup. Click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 117 Network Setting > DNS > Dynamic DNS

The following table describes the fields in this screen.

Table 84 Network Setting > DNS > > Dynamic DNS

| LABEL | DESCRIPTION |
|---|---|
| Dynamic DNS Setup | |
| Dynamic DNS | Select Enable to use dynamic DNS. |
| Service Provider | Select your Dynamic DNS service provider from the drop-down list box. |
| Host Name | Type the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (","). |
| Username | Type your user name. |
| Password | Type the password assigned to you. |
| Enable Wildcard Option | Select the check box to enable DynDNS Wildcard. |
| Enable Off Line Option (Only applies to custom DNS) | Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line. |
| Dynamic DNS Status | |
| User Authentication Result | This shows Success if the account is correctly set up with the Dynamic DNS provider account. |
| Last Updated Time | This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated. |
| Current Dynamic IP | This shows the IP address your Dynamic DNS provider has currently associated with the hostname. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

CHAPTER 13

IGMP/MLD

13.1 IGMP/MLD Overview

Multicast delivers IP packets to a group of hosts on the network defined by multicast groups. Membership to these multicast groups are established using IGMP/MLD.

Use the **IGMP/MLD** screen to configure IGMP/MLD group settings.

13.1.1 What You Need To Know

Multicast and IGMP

See [Multicast on page 119](#) for more information.

Multicast Listener Discovery (MLD)

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

- MLD allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
- MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.
- MLD filtering controls which multicast groups a port can join.
- An MLD Report message is equivalent to an IGMP Report message, and a MLD Done message is equivalent to an IGMP Leave message.

IGMP Fast Leave

When a host leaves a multicast group (224.1.1.1), it sends an IGMP leave message to inform all routers (224.0.0.2) in the multicast group. When a router receives the leave message, it sends a specific query message to all multicast group (224.1.1.1) members to check if any other hosts are still in the group. Then the router deletes the host's information.

With the IGMP fast leave feature enabled, the router removes the host's information from the group member list once it receives a leave message from a host and the fast leave timer expires.

13.2 The IGMP/MLD Screen

Use this screen to configure multicast groups that the Zyxel Device manages through IGMP/MLD settings. To open this screen, click **Network Setting > IGMP/MLD**.

Figure 118 Network Setting > IGMP/MLD

IGMP/MLD

Enter IGmp/MLD protocol configuration fields if you want modify default values shown below.

IGMP Configuration

| | |
|--|-------------------------------------|
| Default Version | <input type="text" value="3"/> |
| Query Interval | <input type="text" value="125"/> |
| Query Response Interval | <input type="text" value="10"/> |
| Last Member Query Interval | <input type="text" value="10"/> |
| Robustness Value | <input type="text" value="2"/> |
| Maximum Multicast Groups | <input type="text" value="25"/> |
| Maximum Multicast Data Sources(for IGMPv3) | <input type="text" value="10"/> |
| Maximum Multicast Groups Members | <input type="text" value="25"/> |
| Fast Leave Enable | <input checked="" type="checkbox"/> |
| LAN to LAN (Intra LAN) Multicast Enable | <input checked="" type="checkbox"/> |
| Membership Join Immediate (IPTV) | <input checked="" type="checkbox"/> |

MLD Configuration

| | |
|--|-------------------------------------|
| Default Version | <input type="text" value="2"/> |
| Query Interval | <input type="text" value="125"/> |
| Query Response Interval | <input type="text" value="10"/> |
| Last Member Query Interval | <input type="text" value="10"/> |
| Robustness Value | <input type="text" value="2"/> |
| Maximum Multicast Groups | <input type="text" value="10"/> |
| Maximum Multicast Data Sources(for IGMPv3) | <input type="text" value="10"/> |
| Maximum Multicast Groups Members | <input type="text" value="10"/> |
| Fast Leave Enable | <input checked="" type="checkbox"/> |
| LAN to LAN (Intra LAN) Multicast Enable | <input checked="" type="checkbox"/> |

Cancel
Apply

The following table describes the labels in this screen.

Table 85 Network Setting > IGMP/MLD

| LABEL | DESCRIPTION |
|------------------------|--|
| IGMP/MLD Configuration | |
| Default Version | Enter the version of IGMP (1~3) and MLD (1~2) that you want the Zyxel Device to use on the WAN. |
| Query Interval | Enter the number of seconds the Zyxel Device sends a query message to hosts to get the group membership information. |

Table 85 Network Setting > IGMP/MLD (continued)

| LABEL | DESCRIPTION |
|--|--|
| Query Response Interval | Enter the maximum number of seconds the Zyxel Device can wait for receiving a General Query message. Multicast routers use general queries to learn which multicast groups have members. |
| Last Member Query Interval | Enter the maximum number of seconds the Zyxel Device can wait for receiving a response to a Group-Specific Query message. Multicast routers use group-specific queries to learn whether any member remains in a specific multicast group. |
| Robustness Value | Enter the number of times (1~7) the Zyxel Device can resend a packet if packet loss occurs due to network congestion. |
| Maximum Multicast Groups | Enter a number to limit the number of multicast groups an interface on the Zyxel Device is allowed to join. Once a multicast member is registered in the specified number of multicast groups, any new IGMP or MLD join report frames are dropped by the interface. |
| Maximum Multicast Data Sources(for IGMPv3) | Enter a number to limit the number of multicast data sources (1-24) a multicast group is allowed to have. Note: The setting only works for IGMPv3 and MLDv2. |
| Maximum Multicast Group Members | Enter a number to limit the number of multicast members a multicast group can have. |
| Fast Leave Enable | Select this option to set the Zyxel Device to remove a port from the multicast tree immediately (without sending an IGMP or MLD membership query message) once it receives an IGMP or MLD leave message. This is helpful if a user wants to quickly change a TV channel (multicast group change) especially for IPTV applications. |
| LAN to LAN (Intra LAN) Multicast Enable | Select this to enable LAN to LAN IGMP snooping capability. |
| Membership Join Immediate (IPTV) | Select this to have the Zyxel Device add a host to a multicast group immediately once the Zyxel Device receives an IGMP or MLD join message. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |

CHAPTER 14

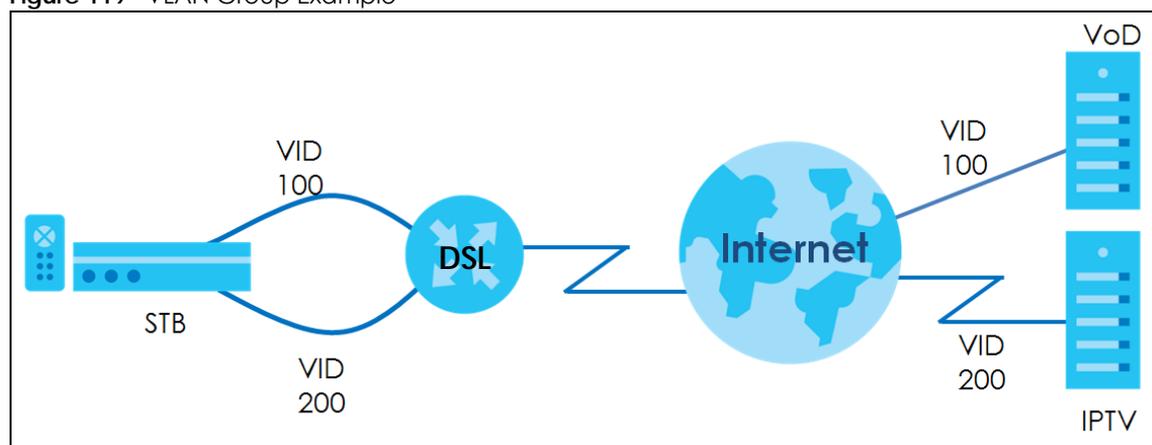
Vlan Group

14.1 Overview

Traffic within a Local Area Network can be clustered into different VLAN groups despite being on one physical network. Virtual LAN IDs are used to identify traffic from these different groups.

In the following example, the Zyxel Device (DSL) can use VLAN IDs (VID) 100 and 200 to identify Video-on-Demand and IPTV traffic respectively coming from the two VoD and IPTV multicast servers. The Zyxel Device (DSL) can also tag outgoing requests to these servers with these VLAN IDs.

Figure 119 VLAN Group Example



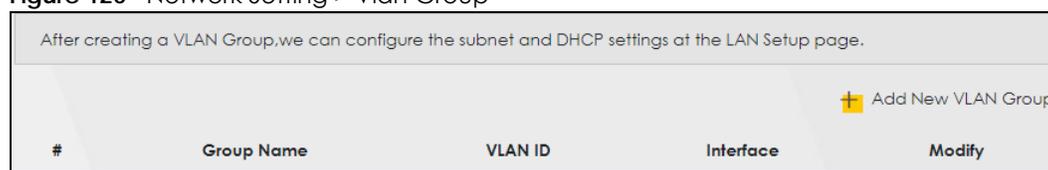
14.1.1 What You Can Do in this Chapter

Use these screens to group separate VLAN groups together to be treated as one VLAN group.

14.2 The Vlan Group Screen

Add a VLAN group and/or change their basic settings in the Vlan Group screen. The subnet and DHCP settings of each group can be configured at the **LAN Setup page**. Click **Network Setting > Vlan Group** to open the following screen.

Figure 120 Network Setting > Vlan Group



The following table describes the fields in this screen.

Table 86 Network Setting > Vlan Group

| LABEL | DESCRIPTION |
|--------------------|---|
| Add New VLAN Group | Click this button to create a new VLAN group. |
| # | This is the index number of the VLAN group. |
| Group Name | This shows the descriptive name of the VLAN group. |
| VLAN ID | This shows the unique ID number that identifies the VLAN group. |
| Interface | This shows the LAN ports included in the VLAN group and if traffic leaving the port will be tagged with the VLAN ID. |
| Modify | Click the Edit icon to change an existing VLAN group setting or click the Delete icon to remove the VLAN group. |

14.2.1 Add/Edit a VLAN Group

Click the **Add New VLAN Group** button in the **Vlan Group** screen to open the following screen. Use this screen to create a new VLAN group.

Figure 121 Add/Edit VLAN Group

The following table describes the fields in this screen.

Table 87 Add/Edit VLAN Group

| LABEL | DESCRIPTION |
|-----------------|--|
| VLAN Group Name | Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed. |
| VLAN ID | Enter a unique ID number, from 1 to 4,094, to identify this VLAN group. Outgoing traffic is tagged with this ID if TX Tagging is selected below. |
| LAN | Select Include to add the associated LAN interface to this VLAN group. Note: Select TX Tagging to tag outgoing traffic from the associated LAN port with the VLAN ID number entered above. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving. |

CHAPTER 15

Interface Grouping

15.1 Interface Grouping Overview

By default, all LAN and WAN interfaces on the Zyxel Device are in the same group and can communicate with each other. Create interface groups to have the Zyxel Device assign IP addresses in different domains to different groups. Each group acts as an independent network on the Zyxel Device. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

15.1.1 What You Can Do in this Chapter

The **Interface Grouping** screens let you create multiple networks on the Zyxel Device ([Section 15.2 on page 222](#)).

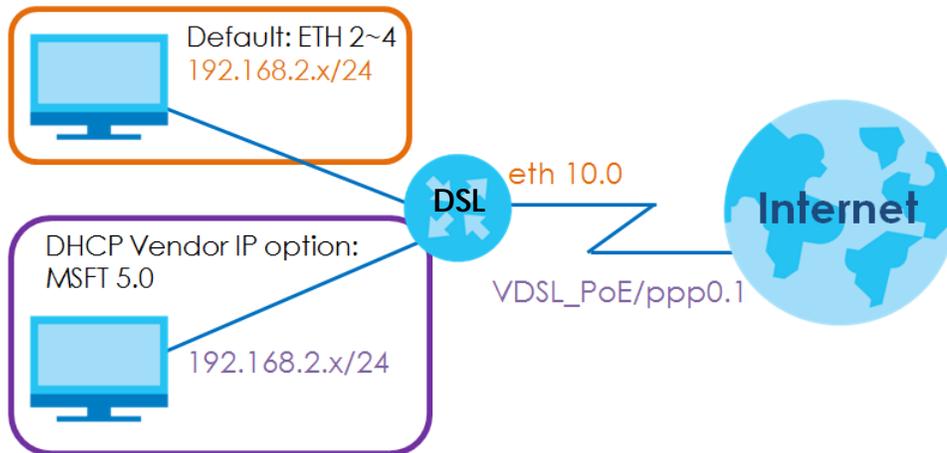
15.2 The Interface Grouping Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the Zyxel Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the Zyxel Device assigns to the clients in the default and/or user-defined groups. If you set the Zyxel Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See [Chapter 8 on page 151](#) for more information.

In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

Figure 122 Interface Grouping Application



You can use this screen to create new user-defined interface groups or modify existing ones. Interfaces that do not belong to any user-defined group always belong to the default group.

Click **Network Setting > Interface Grouping** to open the following screen.

Figure 123 Network Setting > Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

| Group Name | WAN Interface | LAN Interface | Criteria | Modify |
|------------|---------------|--|----------|--------|
| Default | Any WAN | LAN1,LAN2,LAN3,LAN4 .,Zyxel_9DE5,Zyxel_9DE5 _guest1,Zyxel_9DE5_gu est2,Zyxel_9DE5_guest 3,Zyxel_9DE5,Zyxel_9DE 5_guest1,Zyxel_9DE5_g uest2_5G,Zyxel_9DE5_ guest3_5G,Zyx31@198 9816.7dd02bef35ce02 6db42a26095282ec38_ | | |

The following table describes the fields in this screen.

Table 88 Network Setting > Interface Grouping

| LABEL | DESCRIPTION |
|-------------------------|---|
| Add New Interface Group | Click this button to create a new interface group. |
| Group Name | This shows the descriptive name of the group. |
| WAN Interface | This shows the WAN interfaces in the group. |
| LAN Interfaces | This shows the LAN interfaces in the group. |
| Criteria | This shows the filtering criteria for the group. |
| Modify | Click the Edit icon to modify an existing Interface group setting or click the Delete icon to remove the Interface group. |
| Add | Click this button to create a new group. |

15.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group. If you want to automatically add LAN clients to a WAN interface in the new group, add a DHCP vendor ID string. By configuring this, any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

Note: An interface can belong to only one group at a time.

Note: After configuring a vendor ID, reboot the client device attached to the router to obtain an appropriate IP address.

Note: You can have up to 15 filter criteria.

Figure 124 Interface Group Configuration

Add New Interface Group

1. Enter a unique Group name.
2. If you like to automatically add LAN clients to a WAN Interface in the new group, add the DHCP vendor ID string. By configuring a DHCP vendor ID string, any DHCP client request with the specified Vendor ID (DHCP option 60), will be denied an IP address from the local DHCP server.

Group Name

WAN Interfaces used in the grouping

PTM type-

ATM type-

ETH type-

WWAN type-

Available LAN Interfaces

LAN1

LAN2

LAN3

LAN4

ZyxeI_9DE5

Selected LAN Interfaces

Automatically Add Clients With the following DHCP Vendor IDs

| # | Filter Criteria | WildCard Support | Modify |
|---|-----------------|------------------|--------|
| | | | |

Note

(1) If a Vendor ID is configured for a specific client device, please REBOOT the client device attached to the router, to allow the client device to obtain an appropriate IP address.

(2) Total criteria rules can not add over than 15.

The following table describes the fields in this screen.

Table 89 Interface Group Configuration

| LABEL | DESCRIPTION |
|--|---|
| Group Name | Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed. |
| WAN Interfaces used in the grouping | Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface, up to one ETH interface, and up to one WWAN interface. Select None to not add a WAN interface to this group. |
| Selected LAN Interfaces Available LAN Interfaces | Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the Available LAN Interfaces list and use the left arrow to move them to the Selected LAN Interfaces list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the Selected LAN Interfaces , use the right-facing arrow. |
| Automatically Add Clients With the following DHCP Vendor IDs | Click Add to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 15.2.2 on page 225 for more information. |
| # | This shows the index number of the rule. |
| Filter Criteria | This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically. |
| Wildcard Support | This shows if wildcard on DHCP option 60 is enabled. |
| Modify | Click the Edit icon to change the group setting Click the Delete icon to delete this group from the Zyxel Device. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving. |

15.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen. Use this screen to automatically add clients to an interface group based on specified criteria. You can choose to define a group based on a MAC address, a vendor ID (DHCP option 60), an Identity Association Identifier (DHCP option 61), vendor specific information (DHCP option 125), or a VLAN group.

Figure 125 Interface Grouping Criteria

The screenshot shows a mobile-style interface titled "Add new criteria". On the left, under the heading "Criteria", there are five radio button options: "Source MAC address", "DHCP option 60", "DHCP option 61", "DHCP option 125" (which is selected), and "VLAN Group". To the right of the "DHCP option 125" option, there are four text input fields labeled "Enterprise Number", "Manufacturer OUI", "Serial Number", and "Product Class". At the bottom of the screen, there are two buttons: "Cancel" and "OK".

The following table describes the fields in this screen.

Table 90 Interface Grouping Criteria

| LABEL | DESCRIPTION |
|--------------------|---|
| Source MAC Address | Enter the source MAC address of the packet. |
| DHCP Option 60 | Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. |
| Enable wildcard | Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60. |
| DHCP Option 61 | Select this and enter the device identity of the matched traffic. |
| | Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number. |
| DHCP Option 125 | Select this and enter vendor specific information of the matched traffic. |
| Enterprise Number | Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority). |
| Manufacturer OUI | Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address. |
| Serial Number | Enter the serial number of the device. |
| Product Class | Enter the product class of the device. |
| VLAN Group | Select this and the VLAN group of the matched traffic from the drop-down list box. A VLAN group can be configured in Network Setting > Vlan Group . |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to exit this screen without saving. |

CHAPTER 16

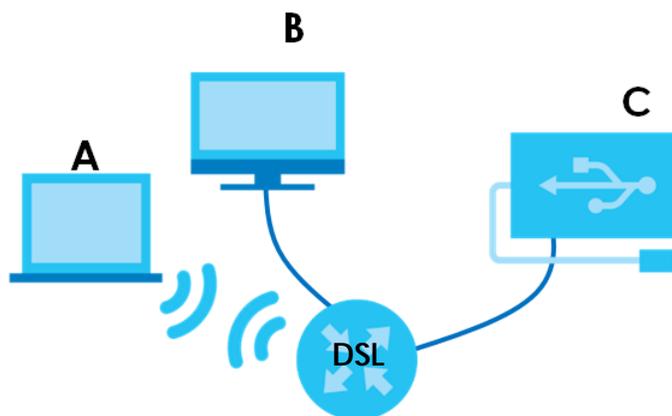
USB Service

16.1 USB Service Overview

You can share files on a USB memory stick or hard drive connected to your Zyxel Device with users on your network.

The following figure is an overview of the Zyxel Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Zyxel Device.

Figure 126 File Sharing Overview



The Zyxel Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

16.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to enable file-sharing server ([Section 16.1.3 on page 228](#)).
- Use the **Media Server** screen to enable or disable the sharing of media files ([Section 16.3 on page 231](#)).

16.1.2 What You Need To Know

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

16.1.2.1 About File Sharing

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Zyxel Device is given a folder, called a "share". If a USB hard drive connected to the Zyxel Device has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Zyxel Device supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The Zyxel Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Zyxel Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

16.1.3 Before You Begin

Make sure the Zyxel Device is connected to your network and turned on.

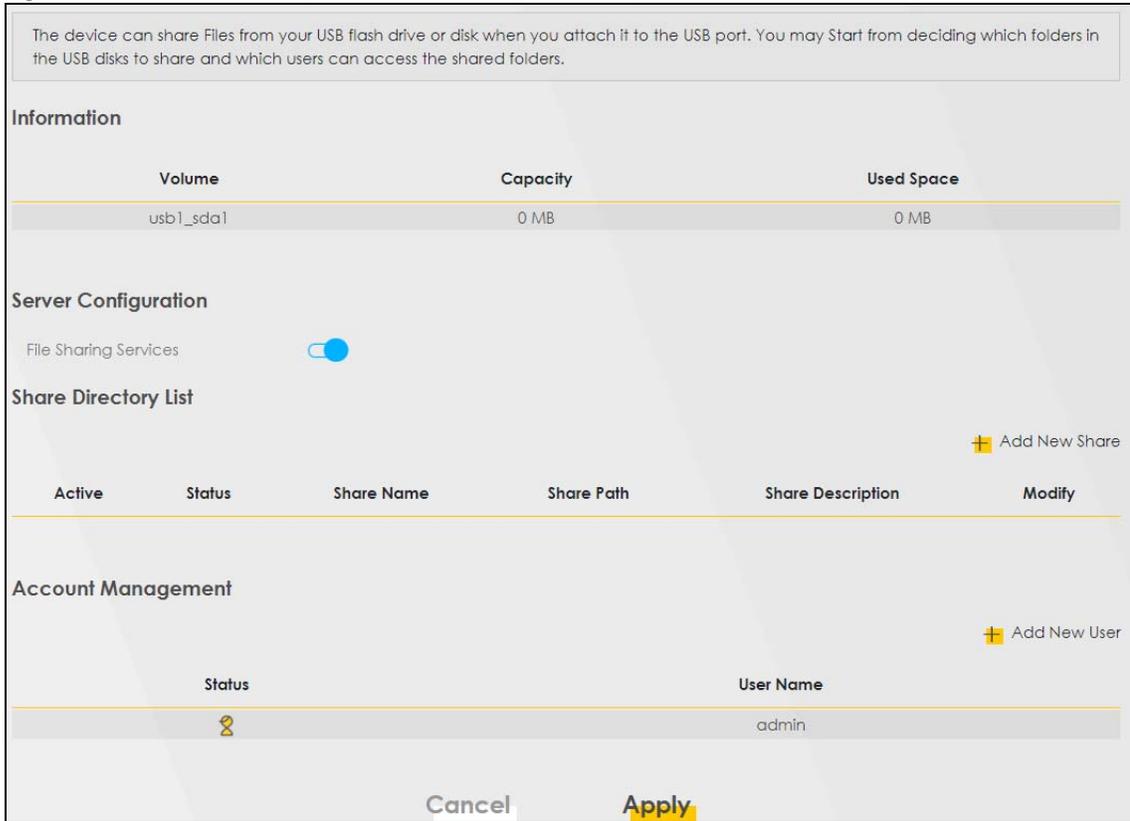
- 1 Connect the USB device to one of the Zyxel Device's USB port. Make sure the Zyxel Device is connected to your network.
- 2 The Zyxel Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the Zyxel Device, see the troubleshooting for suggestions.

16.2 The File Sharing Screen

Use this screen to set up file sharing through the Zyxel Device. The Zyxel Device's LAN users can access the shared folder (or share) from the USB device inserted in the Zyxel Device. To access this screen, click **Network Setting > USB Service > File Sharing**.

Figure 127 Network Setting > USB Service > File Sharing



Note: Share Directory List field appears when you connect a USB device to the USB port. Otherwise, it doesn't.

Each field is described in the following table.

Table 91 Network Setting > USB Service > File Sharing

| LABEL | DESCRIPTION |
|-----------------------|--|
| Information | |
| Volume | This is the volume name the Zyxel Device gives to an inserted USB device. |
| Capacity | This is the total available memory size (in megabytes) on the USB device. |
| Used Space | This is the memory size (in megabytes) already used on the USB device. |
| Server Configuration | |
| File Sharing Services | Click this switch to enable or disable file sharing through the Zyxel Device. When the switch turns blue , the function is enabled. Otherwise, it's not. |
| Share Directory List | |
| Add New Share | Click this to set up a new share on the Zyxel Device. |
| Active | Select this to allow the share to be accessed. |
| Status | This field shows the status of the share : The share is not activated. : The share is activated. |
| Share Name | This field displays the share name on the GPON Device. |

Table 91 Network Setting > USB Service > File Sharing

| LABEL | DESCRIPTION |
|--------------------|--|
| Share Path | This field displays the path for the share directories (folders) on the GPON Device. These are the directories (folders) on your USB storage device. |
| Share Description | This field displays information about the share. |
| Modify | Click the Edit icon to change the settings of an existing share. Click the Delete icon to delete this share in the list. |
| Account Management | |
| Add New User | Click this button to create a user account to access the secured shares. This button redirects you to Maintenance > User Account . |
| Status | This field shows the status of the user. ⌚: The user account is not activated for the share. ⌚: The user account is activated for the share. |
| User Name | This is the name of a user who is allowed to access the secured shares on the USB device. |
| Cancel | Click this to restore your previously saved settings. |
| Apply | Click this to save your changes to the Zyxel Device. |

16.2.1 The Add New Share Screen

Use this screen to set up a new share or edit an existing share on the Zyxel Device. Click **Add new share** in the **File Sharing** screen or click the **Edit** icon next to an existing share.

Please note that you need to set up your shares in the USB before enabling file sharing in the Zyxel Device. Also, spaces and the following special characters listed in the brackets [" < > ^ \$ | & ; \ / : * ?] are not allowed for the USB share name.

Figure 128 Network Setting > USB Service > File Sharing > Add New Sharer

The screenshot shows the 'Add New Share' configuration screen. It includes the following elements:

- Volume:** A dropdown menu showing 'usb1_sda1'.
- Share Path:** A text input field with a yellow 'Browse' button to its right.
- Description:** A text input field.
- Access Level:** A dropdown menu showing 'Security'.
- Allowed:** A checkbox that is currently unchecked.
- User Name:** A text input field containing 'admin'.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom of the screen.

The following table describes the labels in this menu.

Table 92 Network Setting > USB Service > Media Server

| LABEL | DESCRIPTION |
|--------------|---|
| Volume | Select the volume in the USB storage device that you want to add as a share in the Zyxel Device. This field is read-only when you are editing the share. |
| Share Path | Manually enter the file path for the share, or click the Browse button and select the folder that you want to add as a share. This field is read-only when you are editing the share. |
| Description | You can either enter a short description of the share, or leave this field blank. |
| Access Level | Select Public if you want the share to be accessed by users connecting to the Zyxel Device. Otherwise, select Security . |
| Allowed | If Security is selected in the Access Level field, select this check box to allow/prohibit access to the share. |
| User Name | This field specifies the user for which the Allowed setting applies. Users can be added or modified in Maintenance > User Account . |
| Cancel | Click Cancel to return to the previous screen. |
| OK | Click OK to save your changes. |

16.2.2 The Add New User Screen

Once you click the **Add New User** button, you'll be directed to the **User Account** screen. To create a user account that can access the secured shares on the USB device, click the **Add New Account** button in the **Network Setting > Maintenance > User Account** screen.

Please see [Chapter 34 on page 314](#), for detailed information about **User Account** screen.

16.3 The Media Server Screen

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your Zyxel Device without having to copy them to another computer. The Zyxel Device can function as a DLNA-compliant media server, where the Zyxel Device streams files to DLNA-compliant media clients like Windows Media Player. The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

The Zyxel Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the Zyxel Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

To change your Zyxel Device's media server settings, click **Network Setting > USB Service > Media Server**. The screen appears as shown.

Figure 129 Network Setting > USB Service > Media Server

If you would like to play any media contents stored in a USB flash drive or disk through a media client, like PS3, attach the USB flash drive or disk onto this device and enable the Media Server function.

Media Server

Interface

Media Library Path

The following table describes the labels in this menu.

Table 93 Network Setting > USB Service > Media Server

| LABEL | DESCRIPTION |
|--------------------|---|
| Media Server | Click this switch to have the Zyxel Device function as a DLNA-compliant media server. When the switch turns blue  , the function is enabled. Otherwise, it's not. Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares. |
| Interface | Select an interface on which you want to enable the media server function. An interface can be added or modified in Network Setting > Interface Grouping . |
| Media Library Path | Enter the path clients use to access the media files on a USB storage device connected to the Zyxel Device. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

CHAPTER 17

Home Connectivity

17.1 Home Connectivity Overview

ONE Connect complies with the IEEE 1905.1 standard to allow auto-detection and auto-configuration of compatible Zyxel Devices in a wireless network using the Multy Pro App without Zyxel MESH. You can check what Zyxel Devices are in the wireless network, do speed tests, turn on or turn off Zyxel Devices, block or allow access to the wireless network, and set up a guest WiFi network.

If your wireless router supports Zyxel One Connect, the Zyxel Device for example, you can download and install the Multy Pro App in your mobile device.

To let the Multy Pro App detect the Zyxel Device, the following conditions must be met:

- The mobile device with the App installed must be connected to the Zyxel Device wirelessly.
- One Connect is enabled in this screen.

Figure 130 Multy Pro App



17.2 The Home Connectivity Screen

Use this screen to enable or disable One Connect on the Zyxel Device, so you can manage the Zyxel Device using the Multy Pro App. Zyxel One Connect eliminates the hassle of configuring and managing home networks. When the switch turns blue , the function is enabled.

Note that when Zyxel MESH (Multy Pro) is enabled in the **Network Setting > Wireless > MESH** screen, **One Connect** will be enabled and grayed out automatically. To disable One Connect, please deactivate Multy pro in the **Network Setting > Wireless > MESH** screen.

Click **Network Setting > Home Connectivity** to open the following screen.

Figure 131 Network Setting > Home Connectivity



CHAPTER 18

Firewall

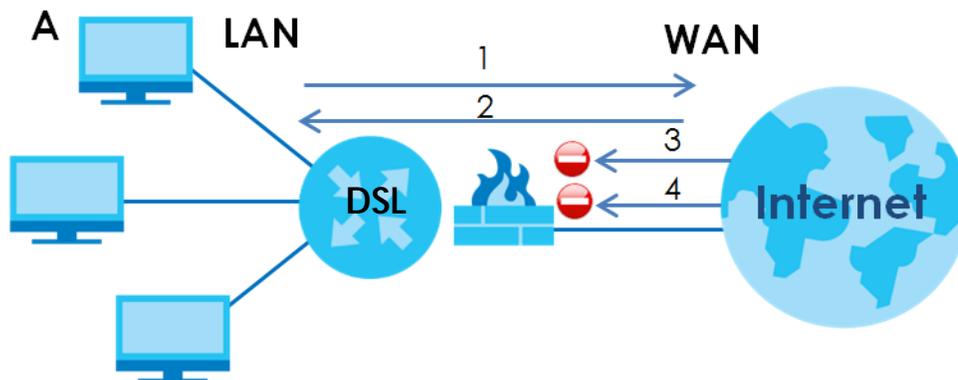
18.1 Firewall Overview

This chapter shows you how to enable and configure the Zyxel Device's security settings. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 132 Default Firewall Action



18.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device ([Section 18.2 on page 236](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 18.3 on page 237](#)).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules ([Section 18.4 on page 239](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 18.5 on page 242](#)).

18.1.2 What You Need to Know

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Zyxel Device is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

18.2 The Firewall Screen

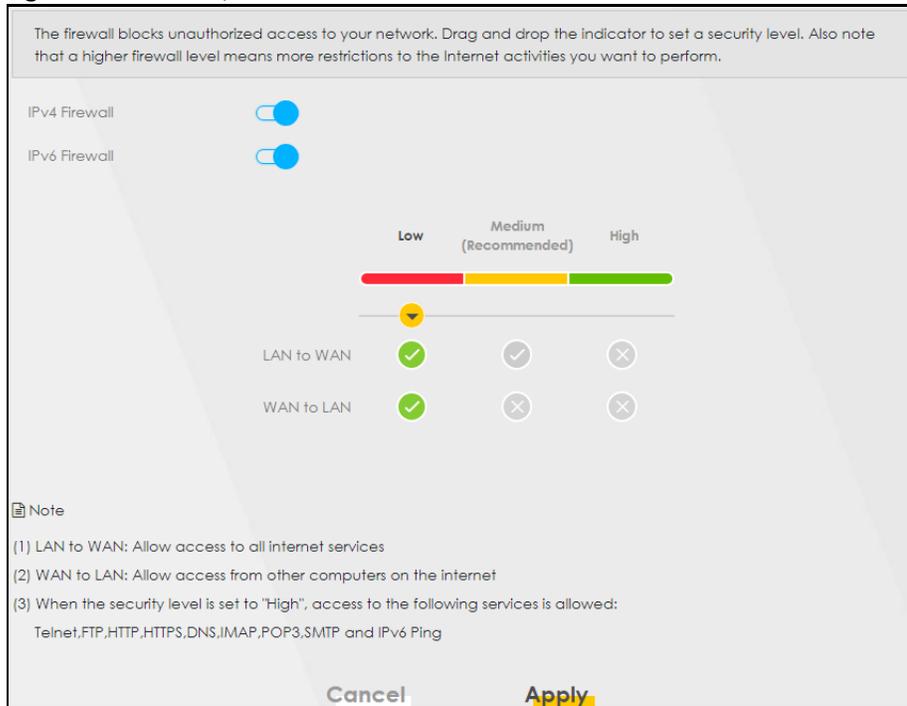
Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets to which they apply. A higher firewall level means more restrictions on the Internet activities you can perform.

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to your device.

Note: When the security level is set to "High", access to Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and IPv6 Ping are still allowed.

Click **Security > Firewall** to display the **General** screen.

Figure 133 Security > Firewall > General



The following table describes the labels in this screen.

Table 94 Security > Firewall > General

| LABEL | DESCRIPTION |
|----------|---|
| Firewall | Select Enable to activate the firewall feature on the Zyxel Device. |
| Low | Select Low to allow LAN to WAN and WAN to LAN packet directions. |
| Medium | Select Medium to allow LAN to WAN but deny WAN to LAN packet directions. |
| High | Select High to deny LAN to WAN and WAN to LAN packet directions. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

18.3 The Protocol Screen

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix D on page 377](#) for some examples.

Note: Removing a protocol rule will also remove associated ACL rules.

Click **Security > Firewall > Protocol** to display the following screen.

Figure 134 Security > Firewall > Protocol

Each entry in the following table represents a protocol rule or a set of custom protocol rules. It is a re-usable object and should be used in conjunction with ACL Rules in Access Control.

+ Add New Protocol Entry

| Name | Description | Ports/Protocol Number | Modify |
|---|-------------|-----------------------|--------|
| <p>Note</p> <p>If a protocol rule is removed, related ACL rules will also be removed.</p> | | | |

The following table describes the labels in this screen.

Table 95 Security > Firewall > Protocol

| LABEL | DESCRIPTION |
|------------------------|---|
| Add New Protocol Entry | Click this to add a new service. |
| Name | This is the name of your customized service. |
| Description | This is the description of your customized service. |
| Ports/Protocol Number | This shows the IP protocol (TCP , UDP , ICMP , or TCP/UDP) and the port number or range of ports that defines your customized service. Other and the protocol number displays if the service uses another IP protocol. |
| Modify | Click the Edit icon to edit the entry. Click the Delete icon to remove this entry. |

18.3.1 Add New/Edit Protocol Entry

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add New Protocol Entry** or the **Edit** icon next to an existing service in the **Protocol** screen to display the following screen.

Figure 135 Protocol Entry: Add New/Edit

Add New Protocol Entry ✕

Service Name

Description

Protocol ▼

Protocol Number (0-255)

Cancel
OK

The following table describes the labels in this screen.

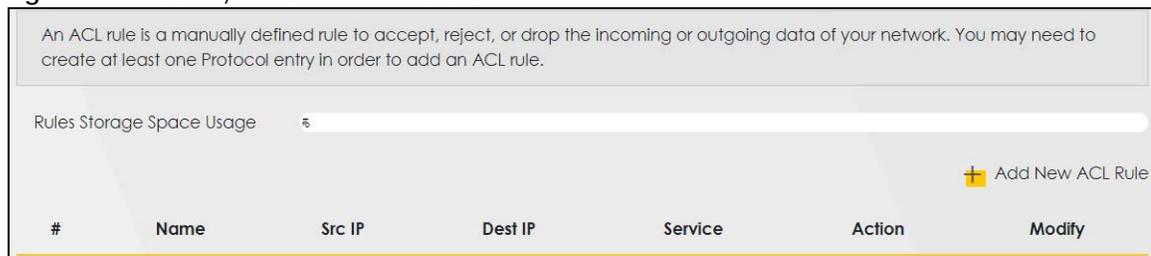
Table 96 Security > Firewall > Protocol: Add/Edit

| LABEL | DESCRIPTION |
|------------------|---|
| Service Name | Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port. |
| Description | Enter a description for your customized port. |
| Protocol | Choose the IP protocol (TCP , UDP , ICMP , or Other) that defines your customized port from the drop-down list box. Select Other to be able to enter a protocol number. |
| Protocol Number | This field is displayed if you select Other as the protocol. Enter the protocol number of your customized port. |
| Source Port | This field is displayed if you select either the TCP or UDP protocol. You may set it to Any , Single , or Range and enter the Port Number or range of Port Numbers for your source port. |
| Destination Port | This field is displayed if you select either the TCP or UDP protocol. You may set it to Any , Single , or Range and enter the Port Number or range of Port Numbers for your destination port.. |
| ICMPv6type | This field is displayed if you select the ICMPv6 protocol. From the drop-down menu, select which type value you would like to use. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

18.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 136 Security > Firewall > Access Control



The following table describes the labels in this screen.

Table 97 Security > Firewall > Access Control

| LABEL | DESCRIPTION |
|------------------|---|
| Add New ACL Rule | Click this to add a filter rule for incoming or outgoing IP traffic. |
| # | This is the index number of the entry. |
| Name | This displays the name of the rule. |
| Src IP | This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to Any . |
| Dst IP | This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to Any . |

Table 97 Security > Firewall > Access Control (continued)

| LABEL | DESCRIPTION |
|---------|---|
| Service | This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies. |
| Action | This field displays whether the rule silently discards packets (DROP), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (REJECT) or allows the passage of packets (ACCEPT). |
| Modify | <p>Click the Edit icon to edit the rule.</p> <p>Click the Delete icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.</p> <p>Click the Move To icon to change the order of the rule. Enter the number in the # field.</p> |

18.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays. Use this screen to accept, reject, or drop packets based on specified parameters, such as source and destination IP address, IP Type, service, and direction. You can also specify a limit as to how many packets this rule applies to at a certain period of time or specify a schedule for this rule.

Figure 137 Access Control: Add/Edit

The following table describes the labels in this screen.

Table 98 Access Control: Add/Edit

| LABEL | DESCRIPTION |
|---------------------------|---|
| Filter Name | Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule. |
| Order | Select the order of the ACL rule. |
| Select Source IP Address | Select the source device to which the ACL rule applies. If you select Specific IP Address , enter the source IP address in the field below. |
| Source IP Address | Enter the source IP address. |
| Select Destination Device | Select the destination device to which the ACL rule applies. If you select Specific IP Address , enter the destination IP address in the field below. |
| Destination IP Address | Enter the destination IP address. |
| IP Type | Select whether your IP type is IPv4 or IPv6 . |

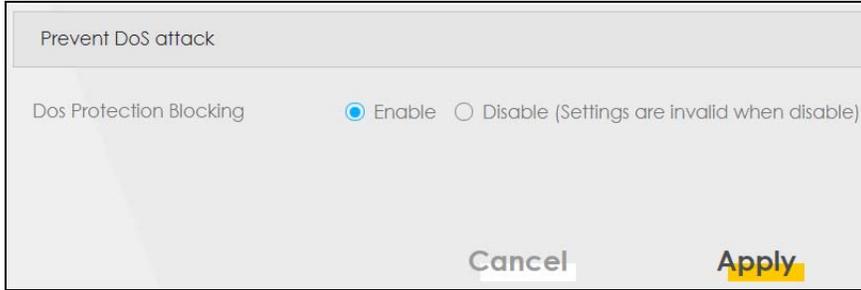
Table 98 Access Control: Add/Edit (continued)

| LABEL | DESCRIPTION |
|-------------------------|--|
| Select Service | Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the Security > Firewall > Protocol > Add screen display in this list. If you want to configure a customized protocol, select Specific Service . |
| Protocol | This field is displayed only when you select Specific Protocol in Select Service . Choose the IP port (TCP/UDP , TCP , UDP , ICMP , or ICMPv6) that defines your customized port from the drop-down list box. |
| Custom Source Port | This field is displayed only when you select Specific Protocol in Select Service and have either TCP or UDP in the Protocol field. Enter a single port number or the range of port numbers of the source. |
| Custom Destination Port | This field is displayed only when you select Specific Protocol in Select Service and have either TCP or UDP in the Protocol field. Enter a single port number or the range of port numbers of the destination. |
| TCP flag | This field is displayed only when you select Specific Protocol in Select Service and have TCP in the Protocol field. Select one of the following TCP flags: SYN (Synchronize), ACK (Acknowledge), URG (Urgent), PSH (Push), RST (Reset), or FIN (Finished). |
| Type | This field is displayed only when you select Specific Protocol in Select Service and ICMPv6 in the protocol field. From the drop-down list box, select which ICMPv6 type you would like to use. |
| Policy | Use the drop-down list box to select whether to discard (DROP), deny and send an ICMP destination-unreachable message to the sender of (REJECT) or allow the passage of (ACCEPT) packets that match this rule. |
| Direction | Use the drop-down list box to select the direction of traffic to which this rule applies. |
| Enable Rate Limit | Select this check box to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packets per minute or second the transmission rate is. |
| Scheduler Rules | Select a schedule rule for this ACL rule from the drop-down list box. You can configure a new schedule rule by click Add New Rule . This will bring you to the Security > Scheduler Rules screen. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

18.5 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 138 Security > Firewall > DoS

Prevent DoS attack

Dos Protection Blocking Enable Disable (Settings are invalid when disable)

Cancel Apply

The following table describes the labels in this screen.

Table 99 Security > Firewall > DoS

| LABEL | DESCRIPTION |
|-------------------------|--|
| DoS Protection Blocking | Select Enable to enable protection against DoS attacks. |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

CHAPTER 19

MAC Filter

19.1 MAC Filter Overview

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the LAN client to configure this screen.

19.2 The MAC Filter Screen

Enable **MAC Address Filter** and add the host name and MAC address of a LAN client to the table if you wish to allow or deny them access to your network. Click **Security > MAC Filter**. The screen appears as shown.

Figure 139 Security > MAC Filter

Enable MAC filters and add the MAC addresses of LAN client in your home or office network to the following table, if you wish to allow or deny them to access your network. Sometimes, MAC Filter is considered a method to increase the security of your network.

MAC Address Filter Enable Disable (Settings are invalid when disable)

MAC Restrict Mode Allow Deny

[+ Add New Rule](#)

| Set | Active | Host Name | MAC Address | Delete |
|-----|--------|-----------|-------------|--------|
|-----|--------|-----------|-------------|--------|

Note
Only devices listed here are granted access to the network

[Cancel](#) [Apply](#)

You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter, as shown in the example below.

Figure 140 Enabling individual MAC filters

| Set | Active | Host Name | MAC Address | Delete |
|-----|-------------------------------------|-----------|-----------------------------|--------|
| 1 | <input type="checkbox"/> | test | BC - 22 - 33 - 44 - 55 - AA | |
| 2 | <input checked="" type="checkbox"/> | Test | BC - 88 - 99 - 00 - 11 - 22 | |

The following table describes the labels in this screen.

Table 100 Security > MAC Filter

| LABEL | DESCRIPTION |
|--------------------|--|
| MAC Address Filter | Select Enable to activate the MAC filter function. |
| MAC Restrict Mode | Select Allow to only permit the listed MAC addresses access to the Zyxel Device. Select Deny to permit anyone access to the Zyxel Device except the listed MAC addresses. |
| Add New Rule | Click this button to create a new entry. |
| Set | This is the index number of the MAC address. |
| Active | Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected. |
| Host Name | Enter the host name of the wireless or LAN clients that are allowed access to the Zyxel Device. |
| MAC Address | Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |
| Delete | Click the Delete icon to delete an existing rule. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

CHAPTER 20

Parental Control

20.1 Parental Control Overview

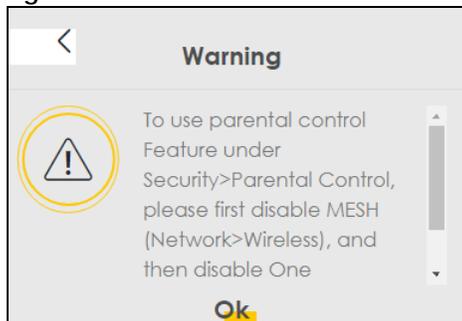
Parental control allows you to limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities.

20.2 The Parental Control Screen

Use this screen to enable parental control and view parental control rules and schedules. You can limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities. These rules are defined in a Parental Control Profile (PCP).

Note that You can't configure parental control settings when **One Connect** is enabled in the **Network Setting > Home Connectivity** screen. If you try to access the **Security > Parental Control** screen with **One Connect** enabled, the following message will appear.

Figure 141 Cannot Use Parental Control



Disable **One Connect** in the **Network Setting > Home Connectivity** screen, then click **Security > Parental Control** to open the following screen.

Figure 142 Security > Parental Control

To limit the time of using Internet or to prevent family members from inappropriate contents and online activities, the administrator can define Parental Control Profile (PCP) to a specific home network user. A maximum of 20 profiles can be created.

General

Parental Control Enable Disable (Settings are invalid when disable)

Parental Control Profile (PCP)

 Add New PCP

| # | Status | PCP Name | Home Network User MAC | Internet Access Schedule | Network Service | Website Blocked | Modify |
|--|--------|----------|-----------------------|--------------------------|-----------------|-----------------|--------|
| <input type="button" value="Cancel"/> <input type="button" value="Apply"/> | | | | | | | |

The following table describes the fields in this screen.

Table 101 Security > Parental Control

| LABEL | DESCRIPTION |
|--------------------------------|--|
| General | |
| Parental Control | Select Enable to activate parental control. |
| Parental Control Profile (PCP) | |
| Add new PCP | Click this if you want to configure a new Parental Control Profile (PCP). |
| # | This shows the index number of the rule. |
| Status | This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active. |
| PCP Name | This shows the name of the rule. |
| Home Network User MAC | This shows the MAC address of the LAN user's computer to which this rule applies. |
| Internet Access Schedule | This shows the day(s) and time on which parental control is enabled. |
| Network Service | This shows whether the network service is configured. If not, None will be shown. |
| Website Block | This shows whether the website block is configured. If not, None will be shown. |
| Modify | Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

20.2.1 Add/Edit a Parental Control Profile

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 143 Security > Parental Control > Add/Edit PCP (General, Rule List & Internet Access Schedule)

✕

Add New PCP

General

Active Enable Disable (Settings are invalid when disable)

Parental Control Profile Name

Home Network User Add

Rule List

| User MAC Address | Delete |
|------------------|--------|
| | |

Internet Access Schedule

Day
 Sun
 Mon
 Tue
 Wed
 Thu
 Fri
 Sat

+ Add New Service

Time (Start-End)

○
○

Figure 144 Security > Parental Control > Add/Edit PCP (Network Service & Site/URL Keyword)

Network Service

Network Service Setting Selected Service(s)

+ Add New Service

| # | Service Name | Protocol:Port | Modify |
|---|--------------|---------------|--------|
| | | | |

Site/URL Keyword

Block or Allow the Web Site + Add

| # | Website | Modify |
|---|---------|--------|
| | | |

Redirect blocked site to Zyxel Family Safety page i

Cancel
OK

The following table describes the fields in this screen.

Table 102 Security > Parental Control >Add/Edit PCP

| LABEL | DESCRIPTION |
|-------------------------------|---|
| General | |
| Active | Select Enable or Disable to activate or deactivate the parental control rule. |
| Parental Control Profile Name | Enter a descriptive name for the rule. |
| Home Network User | Select the LAN user that you want to apply this rule to from the drop-down list box. If you select Custom , enter the LAN user's MAC address. If you select All , the rule applies to all LAN users. |
| Rule List | In Home Network User , select Custom , enter the LAN user's MAC address, then click the Add icon to enter a computer MAC address for this PCP. Up to five are allowed. Click the Delete icon to remove one. |
| Internet Access Schedule | |
| Day | Select check boxes for the days that you want the Zyxel Device to perform parental control. |
| Time | Drag the time bar to define the time that the LAN user is allowed access (Authorized access) or denied access (No access). |
| Add New Service | Click this to add a new time bar. Up to three are allowed. |
| Network Service | |
| Network Service Setting | If you select Block , the Zyxel Device prohibits the users from viewing the Web sites with the URLs listed below. If you select Allow , the Zyxel Device blocks access to all URLs except ones listed below. |
| Add New Service | Click this to show a screen in which you can add a new service rule. You can configure the Service Name , Protocol , and Port of the new rule, as shown in Figure 146 . |
| # | This shows the index number of the rule. |
| Service Name | This shows the name of the rule. |
| Protocol:Port | This shows the protocol and the port of the rule. |
| Modify | Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule. |
| Site/URL Keyword | |
| Block or Allow the Web Site | If you select Block the Web URLs , the Zyxel Device prohibits the users from viewing the Web sites with the URLs listed below. If you select Allow the Web URLs , the Zyxel Device blocks access to all URLs except ones listed below. |
| Add | Click Add to show a screen to enter the URL of web site or URL keyword to which the Zyxel Device blocks or allows access. |
| # | This shows the index number of the rule. |
| WebSite | This shows the URL of web site or URL keyword to which the Zyxel Device blocks or allows access. |
| Modify | Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule. |

Table 102 Security > Parental Control > Add/Edit PCP (continued)

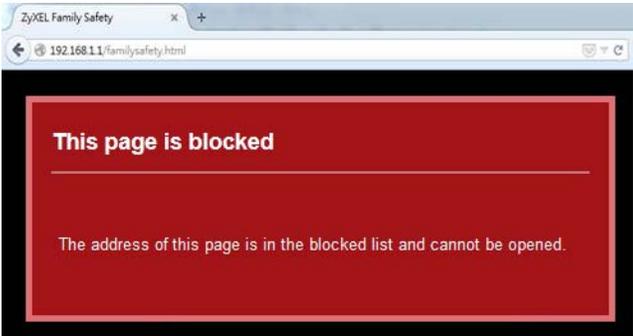
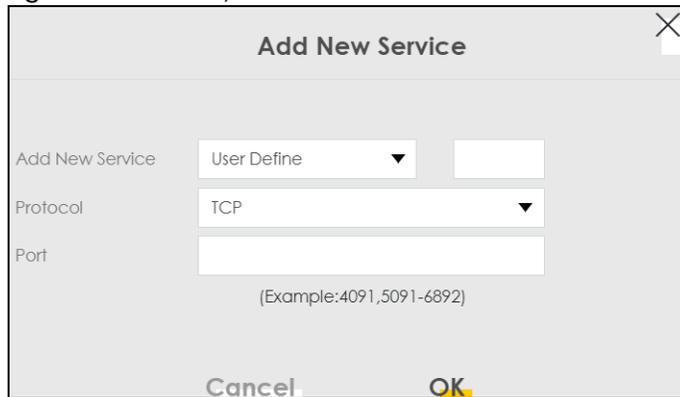
| LABEL | DESCRIPTION |
|---|---|
| Redirect blocked site to Zyxel Family Safety page | <p>Select this to redirect users who access any blocked websites listed above to the Zyxel Family Safety page as shown next.</p> <p>Figure 145 Zyxel Family Safety Page Example</p>  |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

Figure 146 Security > Parental Control > Add/Edit PCP > Add New Service



The following table describes the fields in this screen.

Table 103 Security > Parental Control > Add/Edit PCP > Add New Service

| LABEL | DESCRIPTION |
|-----------------|---|
| Add New Service | <p>Select the name of the service from the drop-down list. Otherwise, select User Define and specify the name, protocol, and port of the service.</p> <p>If you have chosen a pre-defined service in the Service Name field, this field will not be configurable.</p> |
| Protocol | Select the transport layer protocol used for the service. Choices are TCP , UDP , or TCP & UDP . |
| Port | <p>Enter the port of the service.</p> <p>If you have chosen a pre-defined service in the Service Name field, this field will not be configurable.</p> |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

Click **Security > Parental Control > Add New PCP > Add** to open the following screen.

Note: Do not include "HTTP" or "HTTPS" in the keyword. HTTPS connections cannot be blocked by Parental Control.

Figure 147 Security > Parental Control > Add/Edit PCP > Add

Add Blocked Site/URL Keyword [X]

Site/URL Keyword

NOTE: Please enter URL keywords and not include HTTP or HTTPS.
Please Note that for the HTTPS connection, the Parental Control will not be able to block it.

Cancel OK

The following table describes the fields in this screen.

Table 104 Parental Control Rule: Add/Edit > Add Keyword

| LABEL | DESCRIPTION |
|------------------|---|
| Site/URL Keyword | Enter a keyword and click OK to have the Zyxel Device block access to the website URLs that contain the keyword. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

CHAPTER 21

Scheduler Rule

21.1 Scheduler Rule Overview

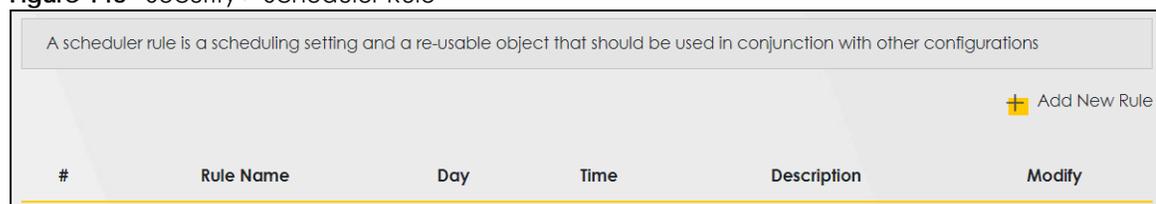
A Scheduler Rule allows you to define time periods and days during which the Zyxel Device performs scheduled rules of certain features (such as Firewall Access Control).

21.2 The Scheduler Rule Screen

Use this screen to view, add, or edit time schedule rules. A scheduler rule is a reusable object that is used in conjunction with other configurations.

Click **Security > Scheduler Rule** to open the following screen.

Figure 148 Security > Scheduler Rule



The following table describes the fields in this screen.

Table 105 Security > Scheduler Rule

| LABEL | DESCRIPTION |
|--------------|---|
| Add New Rule | Click this to create a new rule. |
| # | This is the index number of the entry. |
| Rule Name | This shows the name of the rule. |
| Day | This shows the day(s) on which this rule is enabled. |
| Time | This shows the period of time on which this rule is enabled. |
| Description | This shows the description of this rule. |
| Modify | Click the Edit icon to edit the schedule. Click the Delete icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature. |

21.2.1 Add/Edit a Schedule Rule

Click the **Add New Rule** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

Figure 149 Scheduler Rule: Add/Edit

The following table describes the fields in this screen.

Table 106 Scheduler Rule: Add/Edit

| LABEL | DESCRIPTION |
|-------------------|--|
| Rule Name | Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule. |
| Day | Select check boxes for the days that you want the Zyxel Device to perform this scheduler rule. |
| Time of Day Range | Enter the time period of each day, in 24-hour format, during which the rule will be enforced. |
| Description | Enter a description for this scheduler rule. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

CHAPTER 22

Certificates

22.1 Certificates Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

22.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the Zyxel Device's CA-signed certificates ([Section 22.4 on page 257](#)).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the Zyxel Device ([Section 22.4 on page 257](#)).

22.2 What You Need to Know

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

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the Zyxel Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

22.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import the signed certificates. A maximum of 4 certificates can be stored.

Figure 150 Security > Certificates > Local Certificates

The following table describes the labels in this screen.

Table 107 Security > Certificates > Local Certificates

| LABEL | DESCRIPTION |
|--|---|
| Private Key is protected by a password | Select the checkbox and enter the private key into the text box to store it on the Zyxel Device. The private key should not exceed 63 ASCII characters (not including spaces). |
| Choose File | Click Browse to find the certificate file you want to upload. |
| Import Certificate | Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Zyxel Device. |
| Create Certificate Request | Click this button to go to the screen where you can have the Zyxel Device generate a certification request. |
| Current File | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Modify | Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). For a certification request, click Load Signed to import the signed certificate. Click the Remove icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use. |

22.3.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state/province name, and the two-letter country code for the certificate.

Figure 151 Create Certificate Request

The following table describes the labels in this screen.

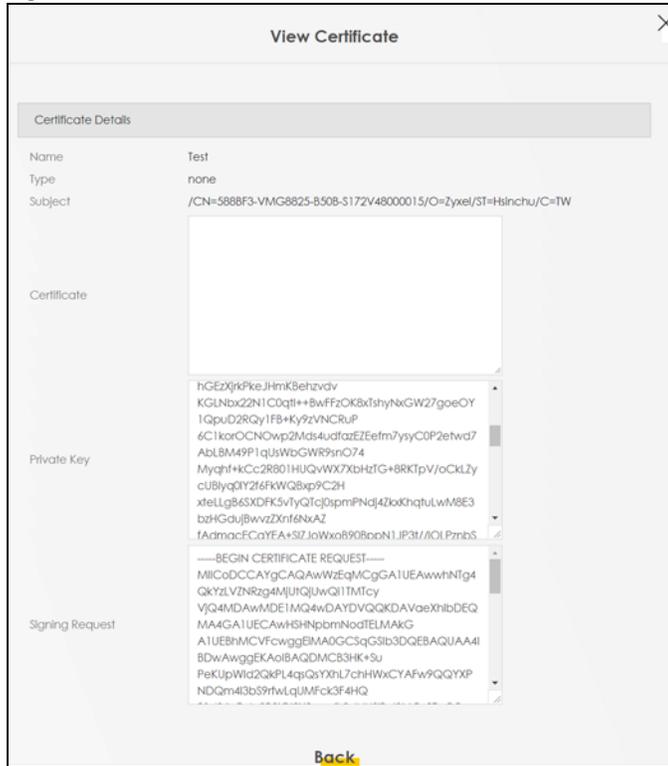
Table 108 Create Certificate Request

| LABEL | DESCRIPTION |
|---------------------|---|
| Certificate Name | Type up to 63 ASCII characters (not including spaces) to identify this certificate. |
| Common Name | Select Auto to have the Zyxel Device configure this field automatically. Or select Customize to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string. |
| Organization Name | Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Zyxel Device drops trailing spaces. |
| State/Province Name | Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Zyxel Device drops trailing spaces. |
| Country/Region Name | Select a country to identify the nation where the certificate owner is located. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

22.3.2 View Certificate Request

Click the **View** icon in the **Local Certificates** screen to open the following screen. Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored.

Figure 152 Certificate Request: View



The following table describes the fields in this screen.

Table 109 Certificate Request: View

| LABEL | DESCRIPTION |
|-----------------|---|
| Name | This field displays the identifying name of this certificate. |
| Type | This field displays general information about the certificate. ca means that a Certification Authority signed the certificate. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Certificate | This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution. |
| Private Key | This field displays the private key of this certificate. |
| Signing Request | This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate. |
| Back | Click Back to return to the previous screen. |

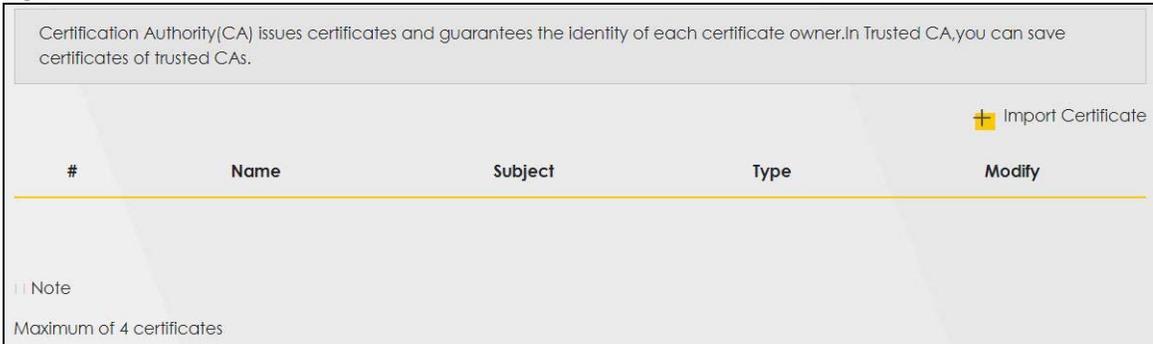
22.4 The Trusted CA Screen

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the Zyxel Device to accept as trusted. The

Zyxel Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Note: You can have a maximum of 4 trusted certificates.

Figure 153 Security > Certificates > Trusted CA



The following table describes the fields in this screen.

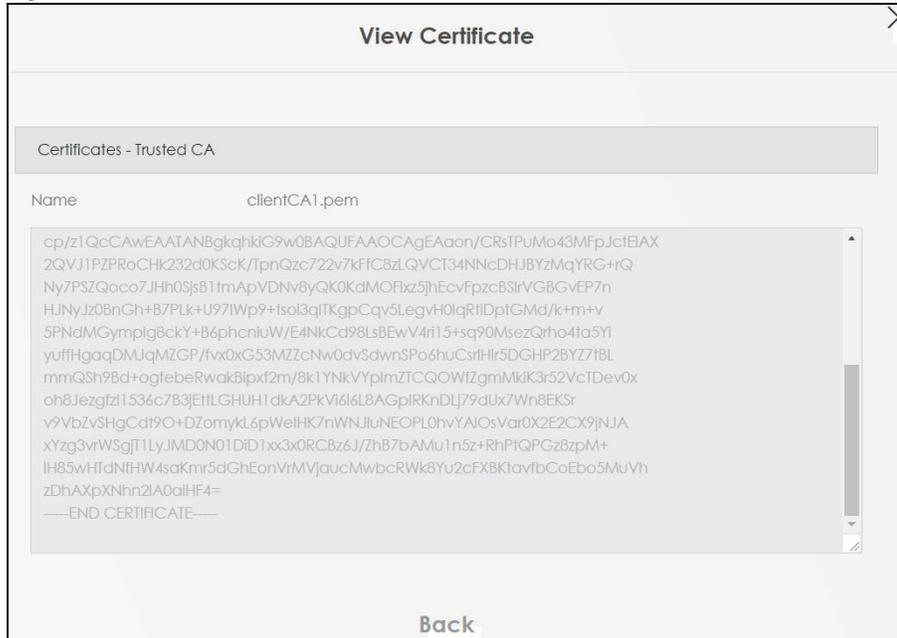
Table 110 Security > Certificates > Trusted CA

| LABEL | DESCRIPTION |
|--------------------|--|
| Import Certificate | Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Zyxel Device. |
| # | This is the index number of the entry. |
| Name | This field displays the name used to identify this certificate. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information. |
| Type | This field displays general information about the certificate. ca means that a Certification Authority signed the certificate. |
| Modify | Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the Remove button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use. |

22.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Figure 154 Trusted CA: View



The following table describes the fields in this screen.

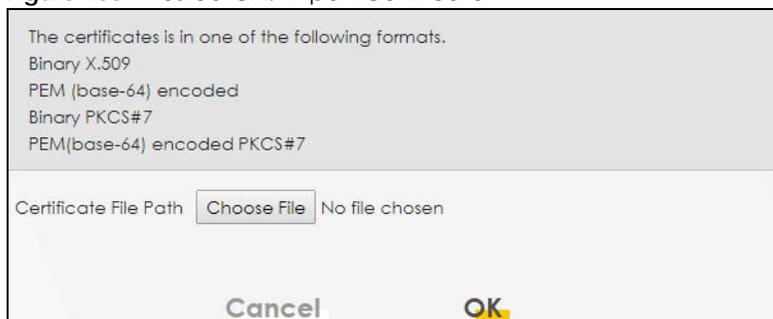
Table 111 Trusted CA: View

| LABEL | DESCRIPTION |
|-------|---|
| Name | This field displays the identifying name of this certificate. |
| | This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Back | Click Back to return to the previous screen. |

22.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The Zyxel Device trusts any valid certificate signed by any of the imported trusted CA certificates. Certificates should be in one of the following formats: Binary X.509, PEM (base-64) encoded, Binary PKCS#7, or PEM (base-64) encoded PKCS#7.

Figure 155 Trusted CA: Import Certificate



The following table describes the fields in this screen.

Table 112 Trusted CA: Import Certificate

| LABEL | DESCRIPTION |
|-----------------------|---|
| Certificate File Path | Click Choose File and select the certificate you want to upload. |
| Cancel | Click Cancel to exit this screen without saving. |
| OK | Click OK to save your changes. |

CHAPTER 23

Voice

23.1 Voice Overview

You can make calls over the Internet using VoIP technology. For this, you first need to set up a SIP account with a SIP service provider.

Use this chapter to:

- Connect an analog phone to the Zyxel Device.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

23.1.1 What You Can Do in this Chapter

These screens allow you to configure your Zyxel Device to make phone calls over the Internet and your regular phone line, and to set up the phones you connect to the Zyxel Device.

- Use the **SIP Account** screen ([Section 23.3 on page 262](#)) to set up information about your SIP account, control which SIP accounts the phones connected to the Zyxel Device use and configure audio settings such as volume levels for the phones connected to the Zyxel Device.
- Use the **SIP Service Provider** screen ([Section 23.4 on page 267](#)) to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions, and dialing plan.
- Use the **Region** screen ([Section 23.6 on page 274](#)) to change settings that depend on the country you are in.
- Use the **Call Rule** screen ([Section 23.7 on page 275](#)) to set up shortcuts for dialing frequently-used (VoIP) phone numbers.
- Use the **Call History** screen ([Section 23.8 on page 276](#)) to view detailed information for each outgoing call you made or each incoming call from someone calling you.
- Use the **Call Summary** screen ([Section 23.9 on page 277](#)) to view the summary list of received, dialed and missed calls.

You don't necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

23.1.2 What You Need to Know About VoIP

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signaling standard that lets one network device (like a computer or the Zyxel Device) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your Zyxel Device, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the Zyxel Device to use your SIP account to make calls, the Zyxel Device is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you don't need a SIP account. It is possible for one SIP device (like the Zyxel Device) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup - figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

How to Find Out More

See [Chapter 4 on page 48](#) for a tutorial showing how to set up these screens in an example scenario.

See [Section 23.10 on page 278](#) for advanced technical information on SIP.

23.2 Before You Begin

- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the Zyxel Device.

23.3 The SIP Account Screen

The Zyxel Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account and map it to a phone port. The SIP account contains information that allows your Zyxel Device to connect to your VoIP service provider.

See [Section 23.3.1 on page 263](#) for how to map a SIP account to a phone port.

Use this screen to view SIP account information. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP > SIP Account**.

Figure 156 VoIP > SIP > SIP Account

In order to make Internet phone calls, a valid SIP account is essential. You may need to consult your SIP service provider for the following settings. This configuration should be used in conjunction with SIP Service Provider.

+ Add New Account

| # | Enable | SIP Account | Service Provider | Account Number | Modify |
|---|----------|-------------|-------------------|----------------|--------|
| 1 | Disabled | SIP1 | sip.infostrada.it | LINEA 1 | |
| 2 | Disabled | SIP2 | sip.infostrada.it | LINEA 2 | |

Each field is described in the following table.

Table 113 VoIP > SIP > SIP Account

| LABEL | DESCRIPTION |
|------------------|--|
| Add new account | Click this to configure a SIP account. |
| # | This is the index number of the entry. |
| Enable | This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is not activated. |
| SIP Account | This shows the name of the SIP account. |
| Service Provider | This shows the name of the SIP service provider. |
| Account Number. | This shows the SIP number. |
| Modify | Click the Edit icon to configure the SIP account. Click the Delete icon to delete this SIP account from the Zyxel Device. |

23.3.1 The SIP Account Add/Edit Screen

Use this screen to configure a SIP account and map it to a phone port. To access this screen, click the **Add new account** button or click the **Edit** icon of an entry in the **VoIP > SIP > SIP Account** screen.

Note: Click **more** to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click **less** to see and configure only the fields needed for this feature.

Figure 157 VoIP > SIP > SIP Account > Add new account/Edit

SIP Account Selection
 SIP Account Selection ChangeMe

SIP Service Provider Association
 SIP Account Associated with:

General
 Enable SIP Account
 SIP Account Number:

Authentication
 Username:
 Password:

URL Type
 URL Type:

Voice Features
 Primary Compression Type:
 Secondary Compression Type:
 Third Compression Type:
 Speaking Volume Control:
 Listening Volume Control:
 Enable G.168 (Echo Cancellation)
 Enable VAD (Voice Active Deflector)

Call Features
 Send Caller ID
 Enable Call Transfer
 Enable Call Waiting
 Call Waiting Reject Timer: (10-60) Second
 Enable Unconditional Forward To Number:
 Enable Busy Forward To Number:
 Enable No Answer Forward To Number:
 No Answer Time: (10-119) Second

Caution:
 If you enable [Unconditional Forward], [Busy Forward] and [No Answer] will be ignored.

Enable Do Not Disturb (DND)

Warning:
 If you enable this item, you will not get indication when somebody call you.

Active Incoming Anonymous Call Block
 Enable MWI
 MWI Subscribe Expiration Time: (120-8400)Second
 Hot Line / Warm Line Number
 Warm Line Hot Line
 Hot Line / Warm Line Number:
 Warm Line Timer: (5-300) Second
 Enable Missed Call Email Notification
 Mail Account:
 Send Notification to E-mail:
 Missed Call E-mail Title:

Notice:
 Please configure mail server in 'Maintenance > E-mail Notification' page and select the mail server for this feature.

Early Media
 IVR Play Index:
 Music On Hold (MOH)
 IVR Play Index:

Cancel

Each field is described in the following table.

Table 114 VoIP > SIP > SIP Account > Add new account/Edit

| LABEL | DESCRIPTION |
|----------------------------------|--|
| SIP Account Selection | |
| SIP Account Selection | This field displays ADD_NEW if you are creating a new SIP account or the SIP account you are modifying. |
| SIP Service Provider Association | |
| SIP Account Associated with | Select the SIP service provider profile to use for the SIP account you are configuring in this screen. This field is read-only when you are modifying a SIP account. |
| General | |
| Enable SIP Account | Select this if you want the Zyxel Device to use this account. Clear it if you do not want the Zyxel Device to use this account. |
| SIP Account Number | Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters. |
| Authentication | |
| Username | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters. |
| Password | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters. |
| | |
| URL Type | |
| URL Type | Select whether or not to include the SIP service domain name when the Zyxel Device sends the SIP number. SIP - include the SIP service domain name. TEL - do not include the SIP service domain name. |
| Voice Features | |
| Primary Compression Type | Select the type of voice coder/decoder (codec) that you want the Zyxel Device to use. |
| Secondary Compression Type | G.711 provides high voice quality but requires more bandwidth (64 kbps). G.711 is the default codec used by phone companies and digital handsets. |
| Third Compression Type | <ul style="list-style-type: none"> • G.711a is typically used in Europe. • G.711u is typically used in North America and Japan. <p>G.726-24 operates at 24 kbps.</p> <p>G.726-32 operates at 32 kbps.</p> <p>G.722 is a 7 KHz wideband voice codec that operates at 48, 56 and 64 kbps. By using a sample rate of 16 kHz, G.722 can provide higher fidelity and better audio quality than narrowband codecs like G.711, in which the voice signal is sampled at 8 KHz.</p> <p>The Zyxel Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.</p> <p>Select the Zyxel Device's first choice for voice coder/decoder.</p> <p>Select the Zyxel Device's second choice for voice coder/decoder. Select None if you only want the Zyxel Device to accept the first choice.</p> <p>Select the Zyxel Device's third choice for voice coder/decoder. Select None if you only want the Zyxel Device to accept the first or second choice.</p> |
| Speaking Volume Control | Select the loudness that the Zyxel Device uses for speech that it sends to the peer device. |

Table 114 VoIP > SIP > SIP Account > Add new account/Edit (continued)

| LABEL | DESCRIPTION |
|--------------------------------------|---|
| Listening Volume Control | Select the loudness that the Zyxel Device uses for speech that it receives from the peer device. |
| Enable G.168 (Echo Cancellation) | Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk. |
| Enable VAD (Voice Active Detector) | Select this if the Zyxel Device should stop transmitting when you are not speaking. This reduces the bandwidth the Zyxel Device uses. |
| Call Features | |
| Enable Call Transfer | Select this to enable call transfer on the Zyxel Device. This allows you to transfer an incoming call (that you have answered) to another phone. |
| Send Caller ID | Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification. |
| Enable Call Waiting | Select this to enable call waiting on the Zyxel Device. This allows you to place a call on hold while you answer another incoming call on the same telephone number. |
| Call Waiting Reject Timer | Specify the time in seconds that the Zyxel Device waits before rejecting the second call if you do not answer it. |
| Enable Unconditional Forward | Select this if you want the Zyxel Device to forward all incoming calls to the specified phone number. Specify the phone number in the To Number field on the right. |
| Enable Busy Forward | Select this if you want the Zyxel Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the To Number field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call. |
| Enable No Answer Forward | Select this if you want the Zyxel Device to forward incoming calls to the specified phone number if the call is unanswered. (See No Answer Time .) Specify the phone number in the To Number field on the right. |
| No Answer Time | This field is used by the Active No Answer Forward feature. Enter the number of seconds the Zyxel Device should wait for you to answer an incoming call before it considers the call unanswered. |
| Enable Do Not Disturb | Select this to set your phone to not ring when someone calls you. |
| Active Incoming Anonymous Call Block | Select this if you do not want the phone to ring when someone tries to call you with caller ID deactivated. |
| Enable MWI | Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature. |
| MWI Subscribe Expiration Time | Keep the default value of this field unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the Zyxel Device subscribes to the service. Before this time passes, the Zyxel Device automatically subscribes again. |
| Hot Line/ Warm Line Number | Select this to enable the hot line or warm line feature on the Zyxel Device. |
| Hot Line | Select this to have the Zyxel Device dial the specified hot line number immediately when you pick up the telephone. |
| Warm Line | Select this to have the Zyxel Device dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time. |

Table 114 VoIP > SIP > SIP Account > Add new account/Edit (continued)

| LABEL | DESCRIPTION |
|---------------------------------------|---|
| Hot Line / Warm Line Number | Enter the number of the hot line or warm line that you want the Zyxel Device to dial. |
| Warm Line Timer | Enter a number of seconds that the Zyxel Device waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad. |
| Enable Missed Call Email Notification | Select this option to have the Zyxel Device e-mail you a notification when there is a missed call. |
| Mail Account | Select a mail account for the e-mail address specified below. If you select None here, e-mail notifications will not be sent via e-mail. You must have configured a mail account already in the Email Notification screen. |
| Send Notification to Email | Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications will not be sent via e-mail. |
| Missed Call Email Title | Type a title that you want to be in the subject line of the e-mail notifications that the Zyxel Device sends. |
| Early Media | Select this if you want people to hear a customized recording when they call you. |
| IVR Play Index | Select the tone you want people to hear when they call you. This field is configurable only when you select Early Media . See Section 23.10 on page 278 for information on how to record these tones. |
| Music On Hold (MOH) | Select this to play a customized recording when you put people on hold. |
| IVR Play Index | Select the tone to play when you put someone on hold. This field is configurable only when you select Music on Hold , See Section 23.10 on page 278 for information on how to record these tones. |
| Cancel | Click this to set every field in this screen to its last-saved value. |
| OK | Click this to save your changes and to apply them to the Zyxel Device. |

23.4 The SIP Service Provider Screen

Use this screen to view the SIP service provider information on the Zyxel Device. An SIP provider offers Internet call services using VoIP technology. You may need to consult your SIP service provider for the following settings. Click **VoIP > SIP > SIP Service Provider** to open the following screen.

Figure 158 VoIP > SIP > SIP Service Provider

| # | SIP Service Provider Name | SIP Proxy Server Address | REGISTER Server Address | SIP Service Domain | Modify |
|---|---------------------------|--------------------------|-------------------------|--------------------|--------|
| 1 | sip.infostrada.it | sip.infostrada.it | sip.infostrada.it | sip.infostrada.it | |

Each field is described in the following table.

Table 115 VoIP > SIP > SIP Service Provider

| LABEL | DESCRIPTION |
|---------------------------|--|
| Add New Provider | Click this button to add a new SIP service provider. |
| # | This is the index number of the entry. |
| SIP Service Provider Name | This shows the name of the SIP service provider. |
| SIP Proxy Server Address | This shows the IP address or domain name of the SIP server. |
| REGISTER Server Address | This shows the IP address or domain name of the SIP register server. |
| SIP Service Domain | This shows the SIP service domain name. |
| Modify | Click the Edit icon to configure the SIP service provider. Click the Delete icon to delete this SIP service provider from the Zyxel Device. |

23.4.1 The SIP Service Provider Add/Edit Screen

Use this screen to configure a SIP service provider on the Zyxel Device. Click the **Add New Provider** button or an **Edit** icon in the **VoIP > SIP > SIP Service Provider** to open the following screen.

Note: Click this  to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click again to see and configure only the fields needed for this feature.

Figure 159 VoIP > SIP > SIP Service Provider > Add new provider/Edit

< **Add New Provider**

SIP Service Provider Selection
Service Provider Selection: ADD_NEW

General

SIP Service Provider: Enable SIP Service Provider

SIP Service Provider Name:

SIP Local Port: (1025~65535)

SIP Proxy Server Address:

SIP Proxy Server Port: (1025~65535)

SIP REGISTRAR Server Address:

SIP REGISTRAR Server Port: (1025~65535)

SIP Service Domain:

RFC Support

PRACK (RFC 3262, Require: 100rel)

VoIP IOP Flags

Replace dial digit '#' to '823' in SIP messages

Remove the 'Route' header in SIP messages

Bound Interface Name

Bound Interface Name: AnyWAN MultiWAN

Outbound Proxy

Outbound Proxy Address:

Outbound Proxy Port: (1025~65535)

Use DHCP Option 120 First

RTP Port Range

Start Port: (1026~65482)

End Port: (1044~65500)

SRTP Support

SRTP Support

Crypto Suite: (Encryption and Authentication Type)

DTMF Mode

DTMF Mode:

Transport Type

Transport Type:

Ignore Direct IP

Enable Disable

FAX Option

G.711 Fax Passthrough T.38 Fax Relay

QoS Tag

SIP DSCP Mark Setting: (0~63)

RTP DSCP Mark Setting: (0~63)

Timer Setting

SIP Register Expiration Duration: (20~65535) second

SIP Register Fail Re-try Timer: (30~65535) second

Session Expires (SE): (100~3600) second

Min-SE: (90~1800) second

Dialing Interval Selection

Dialing Interval Selection: second

DNS SRV

Enable DNS SRV

Cancel OK

Each field is described in the following table.

Table 116 VoIP > SIP > SIP Service Provider > Add new provider/Edit

| LABEL | DESCRIPTION |
|---|---|
| SIP Service Provider Selection | |
| Service Provider Selection | Select the SIP service provider profile you want to use for the SIP account you configure in this screen. If you change this field, the screen automatically refreshes. |
| General | |
| SIP Service Provider | Select Enable SIP Service Provider to enable the SIP service provider. |
| SIP Service Provider Name | Enter the name of your SIP service provider. |
| SIP Local Port | Enter the Zyxel Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| SIP Proxy Server Address | Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server. |
| SIP Proxy Server Port | Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value. |
| SIP REGISTRAR Server Address | Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 95 printable ASCII characters. |
| SIP REGISTRAR Server Port | Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field. |
| SIP Service Domain | Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters. |
| RFC Support | |
| PRACK (RFC 3262, Require: 100rel) | PRACK (RFC 3262) defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select this to have the the peer device require the option tag 100rel to send provisional responses reliably. |
| VoIP IOP Flags | Select the VoIP inter-operability settings you want to activate. |
| Replace dial digit '#' to '%23' in SIP messages | Replace a dial digit "#" with "%23" in the INVITE messages. |
| Remove the 'Route' header in SIP messages | Remove the 'Route' header in SIP packets. |
| Bound Interface Name | |
| Bound Interface Name | If you select Any_WAN , the Zyxel Device automatically activates the VoIP service when any LAN or WAN connection is up. If you select Multi_WAN , you also need to select two or more pre-configured WAN interfaces. The VoIP service is activated only when one of the selected WAN connections is up. |
| Outbound Proxy | |
| Outbound Proxy Address | Enter the IP address or domain name of the SIP outbound proxy server if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Zyxel Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Zyxel Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server). |
| Outbound Proxy Port | Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value. |

Table 116 VoIP > SIP > SIP Service Provider > Add new provider/Edit (continued)

| LABEL | DESCRIPTION |
|---------------------------|--|
| Use DHCP Option 120 First | Select this to enable the SIP server via DHCP option 120. |
| RTP Port Range | |
| Start Port End Port | <p>Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.</p> <p>To enter one port number, enter the port number in the Start Port and End Port fields.</p> <p>To enter a range of ports,</p> <ul style="list-style-type: none"> • enter the port number at the beginning of the range in the Start Port field. • enter the port number at the end of the range in the End Port field. |
| SRTP Support | |
| SRTP Support | <p>When you make a VoIP call using SIP, the Real-time Transport Protocol (RTP) is used to handle voice data transfer. The Secure Real-time Transport Protocol (SRTP) is a security profile of RTP. It is designed to provide encryption and authentication for the RTP data in both unicast and multicast applications.</p> <p>The Zyxel Device supports encryption using AES with a 128-bit key. To protect data integrity, SRTP uses a Hash-based Message Authentication Code (HMAC) calculation with Secure Hash Algorithm (SHA)-1 to authenticate data. HMAC SHA-1 produces a 80 or 32-bit authentication tag that is appended to the packet.</p> <p>Both the caller and callee should use the same algorithms to establish an SRTP session.</p> |
| Crypto Suite | <p>Select the encryption and authentication algorithm set used by the Zyxel Device to set up an SRTP media session with the peer device.</p> <p>Select AES_CM_128_HMAC_SHA1_80 or AES_CM_128_HMAC_SHA1_32 to enable both data encryption and authentication for voice data.</p> <p>Select AES_CM_128_NULL to use 128-bit data encryption but disable data authentication.</p> <p>Select NULL_CIPHER_HMAC_SHA1_80 to disable encryption but require authentication using the default 80-bit tag.</p> |
| DTMF Mode | |
| DTMF Mode | <p>Control how the Zyxel Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.</p> <p>RFC2833 - send the DTMF tones in RTP packets.</p> <p>PCM - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones.</p> <p>SIP INFO - send the DTMF tones in SIP messages.</p> |
| Transport Type | |
| Transport Type | Select the transport layer protocol UDP or TCP (usually UDP) used for SIP. |
| Ignore Direct IP | Select Enable to have the connected CPE devices accept SIP requests only from the SIP proxy/register server specified above. SIP requests sent from other IP addresses will be ignored. |
| FAX Option | This field controls how the Zyxel Device handles fax messages. |
| G711 Fax Passthrough | Select this if the Zyxel Device should use G.711 to send fax messages. You have to also select which operating codec (G.711Mulaw or G.711Alaw) to use for encoding/decoding FAX data. The peer devices must use the same settings. |
| T38 Fax Relay | Select this if the Zyxel Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38. |
| QoS Tag | |

Table 116 VoIP > SIP > SIP Service Provider > Add new provider/Edit (continued)

| LABEL | DESCRIPTION |
|----------------------------------|--|
| SIP DSCP Mark Setting | Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The Zyxel Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits. |
| RTP DSCP Mark Setting | Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Zyxel Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits. |
| Timer Setting | |
| SIP Register Expiration Duration | Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Zyxel Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.) |
| SIP Register Fail Re-try timer | Enter the number of seconds the Zyxel Device waits before it tries again to register the SIP account, if the first try failed or if there is no response. |
| Session Expires (SE) | Enter the number of seconds the Zyxel Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. |
| Min-SE | Enter the minimum number of seconds the Zyxel Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Zyxel Device accepts. |
| Dialing Interval Selection | |
| Dialing Interval Selection | Enter the number of seconds the Zyxel Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. |
| DNS SRV | |
| Enable DNS SRV | Select this to have the Zyxel Device use DNS procedures to resolve the SIP domain and find the SIP server's IP address, port number and supported transport protocol(s). The Zyxel Device first uses DNS Name Authority Pointer (NAPTR) records to determine the transport protocols supported by the SIP server. It then performs DNS Service (SRV) query to determine the port number for the protocol. The Zyxel Device resolves the SIP server's IP address by a standard DNS address record lookup. The SIP Server Port and REGISTER Server Port fields in the General section above are grayed out and not applicable and the Transport Type can also be set to AUTO if you enable this option. |
| Cancel | Click Cancel to restore your previously saved settings. |
| OK | Click OK to save your changes. |

23.5 The Phone Device Screen

Use this screen to view detailed information on phones used for Internet phone calls (SIP). You can define which phone(s) will ring when a specific SIP account number receives an incoming call, and which SIP account number will be used when an outgoing call is made with a specific phone. To access this screen, click **VoIP > Phone > Phone Device**.

Figure 160 VoIP > Phone > Phone Device

Phone Device configuration defines the relations between your SIP account(s) and phone(s). That is, which phone(s) will ring when a specific SIP account number receive an incoming call; and which SIP account number will be used when a specific phone is used to make an outgoing call.

Analog Phone

| # | Phone ID | Internal Number | Incoming SIP Number | Outgoing SIP Number | Modify |
|---|----------|-----------------|---------------------|---------------------|---|
| 1 | PHONE1 | **11 | ChangeMe | ChangeMe |  |
| 2 | PHONE2 | **12 | ChangeMe | ChangeMe |  |

Each field is described in the following table.

Table 117 VoIP > Phone > Phone Device

| LABEL | DESCRIPTION |
|---------------------|--|
| # | This displays the index number of the phone device. |
| Phone ID | This field displays the name of a phone port on the Zyxel Device. |
| Internal Number | This field displays the internal call prefix of a phone port on the Zyxel Device. |
| Incoming SIP Number | This field displays the SIP number that you use to receive calls on this phone port. |
| Outgoing SIP Number | This field displays the SIP number that you use to make calls on this phone port. |
| Modify | Click the Edit icon to configure the SIP account. |

23.5.1 The Phone Device Edit Screen

Use this screen to control which SIP account and PSTN line each phone uses. Click an **Edit** icon in **VoIP > Phone > Phone Device** to open the following screen.

Figure 161 VoIP > Phone > Phone Device > Edit

Each field is described in the following table.

Table 118 VoIP > Phone > Phone Device > Edit

| LABEL | DESCRIPTION |
|---|--|
| SIP Account to Make Outgoing Call | Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port. |
| SIP Account(s) to Receive Incoming Call | Select a SIP account if you want to receive phone calls for the selected SIP account on this phone port. If you select more than one SIP account for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port. |
| Immediate Dial Enable | Select this if you want to use the pound key (#) to tell the Zyxel Device to make the phone call immediately, instead of waiting for the number of second you selected in the Dialog Interval Selection field of the VoIP > SIP > SIP Service Provider > Add New Provider/Edit screen. If you select this, dial the phone number, and then press the pound key. The Zyxel Device makes the call immediately instead of waiting. You can still wait, if you want. |
| Cancel | Click Cancel to exit this screen without saving |
| OK | Click OK to save your changes. |

23.6 The Phone Region Screen

Use this screen to maintain settings that depend on which region of the world the Zyxel Device is in. Selecting the region where the device is physically located improves the quality of phone calls. To access this screen, click **VoIP > Phone > Region**.

Note: You need to reboot the device after changing the region settings for it to take effect.

Figure 162 VoIP > Phone > Region

Selecting current region where this device physically is located provides better quality of phone calls.

Region Setting: ITA - Italy

Call Service Mode: Europe Type

Note
Caution: When Region Setting is changed, you need to reboot device to take settings effect.

Cancel Apply

Each field is described in the following table.

Table 119 VoIP > Phone > Region

| LABEL | DESCRIPTION |
|-------------------|--|
| Region Setting | Select the place in which the Zyxel Device is located. |
| Call Service Mode | Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. Europe Type - use supplementary phone services in European mode USA Type - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider. |
| Cancel | Click this to set every field in this screen to its last-saved value. |
| Apply | Click this to save your changes and to apply them to the Zyxel Device. |

23.7 The Call Rule Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

Figure 163 VoIP > Call Rule

When certain phone numbers are dialed on a regular basis, Speed Dial accelerates dialing process. The following rules apply to all the phone devices connected to this device.

Clear All Speed Dials

| Keys | Number | Description |
|------|--------|-------------|
| #01 | | |
| #02 | | |
| #03 | | |
| #04 | | |
| #05 | | |
| #06 | | |
| #07 | | |
| #08 | | |
| #09 | | |
| #10 | | |

Cancel **Apply**

Each field is described in the following table.

Table 120 VoIP > Call Rule

| LABEL | DESCRIPTION |
|-----------------------|--|
| Clear All Speed Dials | Click this to erase all the speed-dial entries on this screen. |
| Keys | This field displays the speed-dial number you should dial to use this entry. |
| Number | Enter the SIP number you want the Zyxel Device to call when you dial the speed-dial number. |
| Description | Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters. |
| Cancel | Click this to set every field in this screen to its last-saved value. |
| Apply | Click this to save your changes and to apply them to the Zyxel Device. |

23.8 The Call History Screen

This screen allows you to view a call history list. You can also see detailed information for each outgoing call you made or each incoming call from someone calling you. The Zyxel Device stores up to 300 incoming call logs and 300 outgoing call logs. If the number of entries exceed the maximum value, the earliest log of that type will be deleted.

Click **VoIP > Call History > Call History**. The following screen displays.

Figure 164 VoIP > Call History > Call History

Each field is described in the following table.

Table 121 VoIP > Call History > Call History

| LABEL | DESCRIPTION |
|---------------------|---|
| Classify | Select the type of the calls. The call types are: Incoming , Outgoing and Missed . |
| Clear List | Click this button to remove all entries from the call history list. |
| Refresh | Click this button to renew the call history list. |
| Export | Click Export to download a call history list. |
| Type | This displays the type of the calls. |
| Date | This displays the date when the calls were made. |
| Name | This displays the SIP account you called. |
| Number | This displays the SIP number you called. |
| Phone Device | This field displays the name of a phone port on the Zyxel Device. |
| Outgoing Number | This displays how many calls originated from you that day. |
| Duration (hh:mm:ss) | This displays how long the current call has lasted. |
| Modify | Click the Delete icon to remove the call history. |

23.9 The Call Summary Screen

The Zyxel Device logs calls from or to your SIP numbers. This screen allows you to view the summary of received, dialed and missed calls.

Click **VoIP > Call History > Call Summary**. The following screen displays.

Figure 165 VoIP > Call History > Call Summary

Each field is described in the following table.

Table 122 VoIP > Call History > Call Summary

| LABEL | DESCRIPTION |
|-----------|---|
| Refresh | Click this button to renew the call history list. |
| Clear All | Click this button to remove all entries from the call history list. |
| Date | This is the date when the calls were made. |

Table 122 VoIP > Call History > Call Summary

| LABEL | DESCRIPTION |
|------------------------------|---|
| Total Calls | This displays the total number of calls from or to your SIP numbers that day. |
| Outgoing Calls | This displays how many calls originated from you that day. |
| Incoming Calls | This displays how many calls you received that day. |
| Missing Calls | This displays how many incoming calls were not answered that day. |
| Total Duration (hh:mm:ss) | This displays how long all calls lasted that day. |

23.10 Technical Reference

This section contains background material relevant to the **VoIP** screens.

VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain.

SIP Registration

Each Zyxel Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the Zyxel Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The Zyxel Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the Zyxel Device attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC 3261, "SIP: Session Initiation Protocol").

SIP Servers

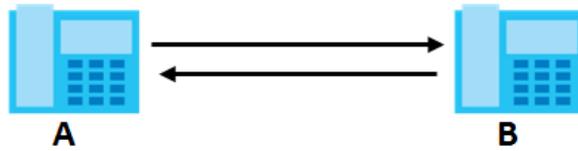
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP SIP user agent to receive the call.

Figure 166 SIP User Agent



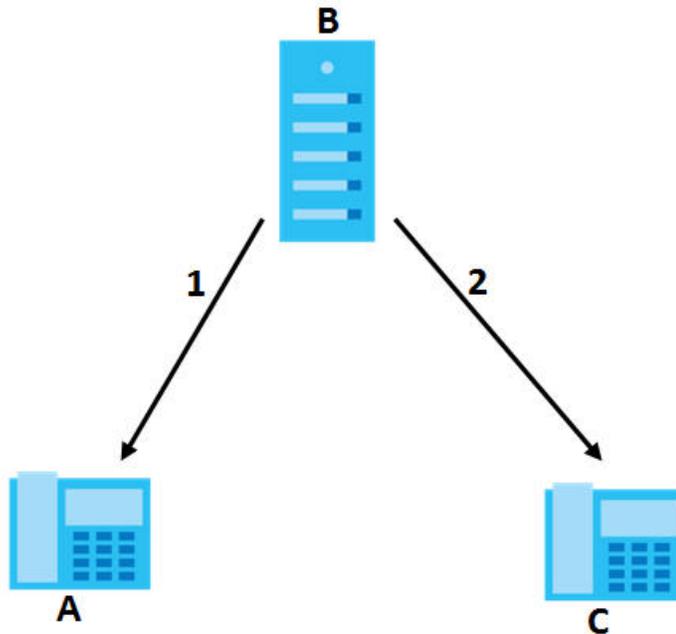
SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device **C**.

- 1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).
- 2 The SIP proxy server forwards the call invitation to **C**.

Figure 167 SIP Proxy Server



SIP Redirect Server

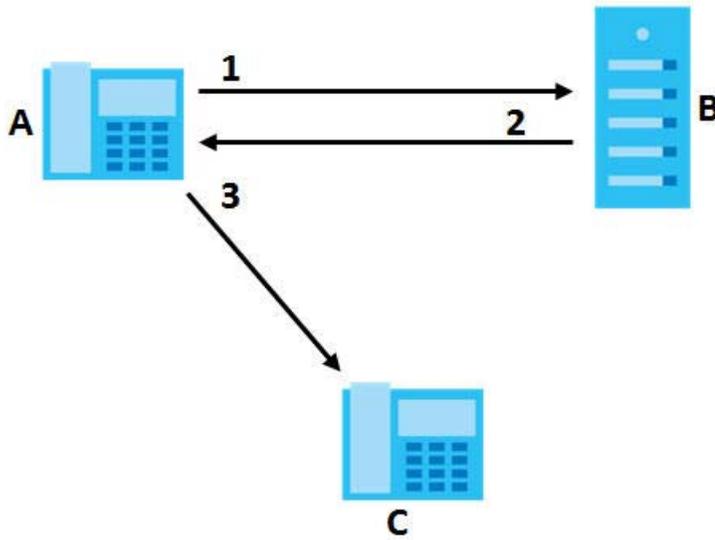
A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device **A** to call someone who is using client device **C**.

- 1 Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).
- 2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).

- 3 Client device **A** then sends the call invitation to client device **C**.

Figure 168 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 123 SIP Call Progression

| A | | B |
|-----------|---|-----------------------------|
| 1. INVITE | → | |
| | ← | 2. Ringing |
| | ← | 3. OK |
| 4. ACK | → | |
| | → | 5. Dialogue (voice traffic) |

Table 123 SIP Call Progression (continued)

| A | | B |
|--------|---|-------|
| 6. BYE | → | |
| | ← | 7. OK |

- 1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.
- 2 **B** sends a response indicating that the telephone is ringing.
- 3 **B** sends an OK response after the call is answered.
- 4 **A** then sends an ACK message to acknowledge that **B** has answered the call.
- 5 Now **A** and **B** exchange voice media (talk).
- 6 After talking, **A** hangs up and sends a BYE request.
- 7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

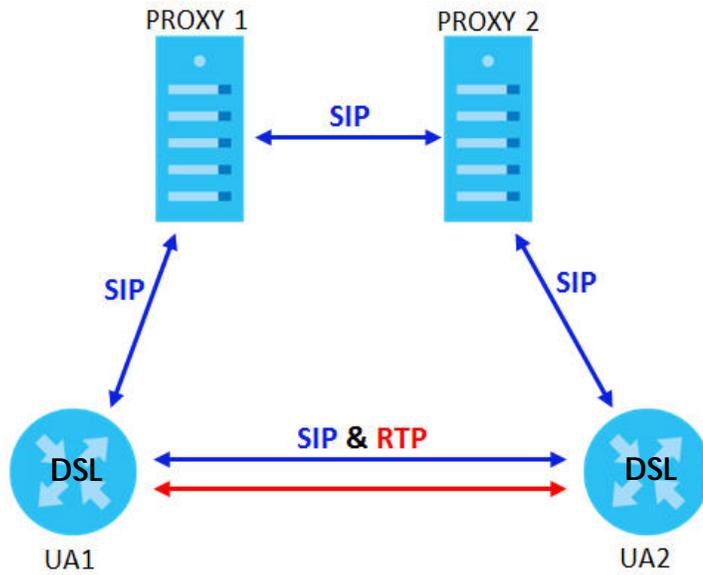
SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

Figure 169 SIP Call Through Proxy Servers



The following table shows the SIP call progression.

Table 124 SIP Call Progression

| UA 1 | | PROXY 1 | | PROXY 2 | | UA 2 |
|--------|---|-------------|---|-------------|---|-------------|
| Invite | → | | | | | |
| | | Invite | → | | | |
| | ← | 100 Trying | | Invite | → | |
| | | | | 100 Trying | | |
| | | | | 180 Ringing | ← | 180 Ringing |
| | ← | 180 Ringing | | 180 Ringing | | |
| | | | | 200 OK | ← | 200 OK |
| | ← | 200 OK | | 200 OK | | |
| ACK | → | | | | | |
| RTP | → | | | | | RTP |
| | ← | | | | | BYE |
| 200 OK | → | | | | | |

- 1 **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.
- 2 **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.
- 3 **Proxy 2** sends a SIP INVITE request to **User Agent 2**.

- 4 **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** via **Proxy 1**.
- 5 **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** via **Proxy 1**.
- 6 **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.
- 7 When **User Agent 2** hangs up, he sends a BYE request.
- 8 **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The Zyxel Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the Zyxel Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

Comfort Noise Generation

When using VAD, the Zyxel Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message-waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the Zyxel Device. The Zyxel Device allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 125 Custom Tones Details

| LABEL | DESCRIPTION |
|----------------------------------|--|
| Total Time for All Tones | 900 seconds for all custom tones combined |
| Maximum Time per Individual Tone | 180 seconds |
| Total Number of Tones Recordable | 5 You can record up to 5 different custom tones but the total time must be 900 seconds or less. |

Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

- 1 Pick up the phone and press “****” on your phone's keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1101~1105 on your phone followed by the “#” key.
- 3 Play your desired music or voice recording into the receiver's mouthpiece. Press the “#” key.
- 4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Listening to Custom Tones

Do the following to listen to a custom tone:

- 1 Pick up the phone and press “****” on your phone's keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1201~1208 followed by the “#” key to listen to the tone.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Deleting Custom Tones

Do the following to delete a custom tone:

- 1 Pick up the phone and press “****” on your phone's keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1301~1308 followed by the “#” key to delete the tone of your choice. Press 14 followed by the “#” key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

23.10.1 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

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

DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.³

DSCP and Per-Hop Behavior

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

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

Figure 170 DiffServ: Differentiated Service Field

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

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

23.10.2 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer, are generally available from your VoIP service provider. The Zyxel Device supports the following services:

3. The Zyxel Device does not support DiffServ at the time of writing.

- Call Return
- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb
- IVR
- Call Completion
- CCBS
- Outgoing SIP

Note: To take full advantage of the supplementary phone services available through the Zyxel Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

23.10.2.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the Zyxel Device.

You can invoke all the supplementary services by using the flash key.

23.10.2.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 126 European Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION |
|---------|-------------|---|
| Flash | | Put a current call on hold to place a second call. Switch back to the call (if there is no second call). |
| Flash | 0 | Drop the call presently on hold or reject an incoming call which is waiting for answer. |
| Flash | 1 | Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold. |

Table 126 European Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION |
|---------|-------------|---|
| Flash | 2 | 1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold). |
| Flash | 3 | Create three-way conference connection. |
| Flash | *98# | Transfer the call to another phone. |

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then "2" to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then "1" to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.
Press the flash key and then press "0".
- Disconnect the first call and answer the second call.
Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.
Press the flash key and then "2".

European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call.
- 3 When the second call is answered, press the flash key and press "3" to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".

23.10.2.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 127 USA Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION |
|---------|-------------|--|
| Flash | | Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call. |
| Flash | *98# | Transfer the call to another phone. |

USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial "**98#" followed by the number to which you want to transfer the call.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

USA Three-Way Conference

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call (to party B).
- 3 When party B answers the second call, press the flash key to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.
- 6 If you want to go back to the three-way conversation, press the flash key again.
- 7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

23.10.2.4 Phone Functions Summary

The following table shows the key combinations you can enter on your phone's keypad to use certain features.

Table 128 Phone Functions Summary

| ACTION | FUNCTION | DESCRIPTION |
|--------|------------------------------|---|
| *98# | Call transfer | Transfer a call to another phone. See Section 23.10.2.2 on page 287 (Europe type) and Section 23.10.2.3 on page 289 (USA type). |
| *66# | Call return | Place a call to the last person who called you. |
| *95# | Enable Do Not Disturb | Use these to set your phone not to ring when someone calls you, or to turn this function off. |
| #95# | Disable Do Not Disturb | |
| *41# | Enable Call Waiting | Use these to allow you to put a call on hold when you are answering another, or to turn this function off. |
| #41# | Disable Call Waiting | |
| **** | IVR | Use these to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold). |
| #### | Internal Call | Call the phone(s) connected to the Zyxel Device. |
| *82 | One Shot Caller Display Call | Activate or deactivate caller ID for the next call only. |
| *67 | One Shot Caller Hidden Call | |

CHAPTER 24

Log

24.1 Log Overview

These screens allow you to determine the categories of events and/or alerts that the Zyxel Device logs and then display these logs or have the Zyxel Device send them to an administrator (through e-mail) or to a syslog server.

24.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 24.2 on page 292](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 24.3 on page 292](#)).

24.1.2 What You Need To Know

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

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 129 Syslog Severity Levels

| CODE | SEVERITY |
|------|--|
| 0 | Emergency: The system is unusable. |
| 1 | Alert: Action must be taken immediately. |
| 2 | Critical: The system condition is critical. |
| 3 | Error: There is an error condition on the system. |
| 4 | Warning: There is a warning condition on the system. |

Table 129 Syslog Severity Levels

| CODE | SEVERITY |
|------|--|
| 5 | Notice: There is a normal but significant condition on the system. |
| 6 | Informational: The syslog contains an informational message. |
| 7 | Debug: The message is intended for debug-level purposes. |

24.2 The System Log Screen

Use the **System Log** screen to see the system logs. You can filter the entries by clicking on the **Level** and/or **Category** drop-down list boxes. Click **System Monitor > Log** to open the **System Log** screen.

Figure 171 System Monitor > Log > System Log

All system events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

Level: Category: [Clear Log](#) [Refresh](#) [Export Log](#) [E-mail Log Now](#)

| # | Time | Facility | Level | Category | Messages |
|---|------|----------|-------|----------|----------|
|---|------|----------|-------|----------|----------|

The following table describes the fields in this screen.

Table 130 System Monitor > Log > System Log

| LABEL | DESCRIPTION |
|---------------|--|
| Level | Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher. |
| Category | Select the type of logs to display. |
| Clear Log | Click this to delete all the logs. |
| Refresh | Click this to renew the log screen. |
| Export Log | Click this to export the selected log(s). |
| Email Log Now | Click this to send the log file(s) to the E-mail address you specify in the Maintenance > Logs Setting screen. |
| # | This field is a sequential value and is not associated with a specific entry. |
| Time | This field displays the time the log was recorded. |
| Facility | The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Level | This field displays the severity level of the log that the device is to send to this syslog server. |
| Category | This field displays the type of the log. |
| Messages | This field states the reason for the log. |

24.3 The Security Log Screen

Use the **Security Log** screen to see the security-related logs for the categories that you select. You can filter the entries by clicking on the **Level** and/or **Category** drop-down list boxes. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 172 System Monitor > Log > Security Log

All security events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

Level Category [Clear Log](#) [Refresh](#) [Export Log](#) [E-mail Log Now](#)

| # | Time | Facility | Level | Category | Messages |
|---|------|----------|-------|----------|----------|
|---|------|----------|-------|----------|----------|

The following table describes the fields in this screen.

Table 131 System Monitor > Log > Security Log

| LABEL | DESCRIPTION |
|---------------|--|
| Level | Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher. |
| Category | Select the type of logs to display. |
| Clear Log | Click this to delete all the logs. |
| Refresh | Click this to renew the log screen. |
| Export Log | Click this to export the selected log(s). |
| Email Log Now | Click this to send the log file(s) to the E-mail address you specify in the Maintenance > Logs Setting screen. |
| # | This field is a sequential value and is not associated with a specific entry. |
| Time | This field displays the time the log was recorded. |
| Facility | The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Level | This field displays the severity level of the log that the device is to send to this syslog server. |
| Category | This field displays the type of the log. |
| Messages | This field states the reason for the log. |

CHAPTER 25

Traffic Status

25.1 Traffic Status Overview

Use the **Traffic Status** screens to look at the network traffic status and statistics of the WAN/LAN interfaces and NAT.

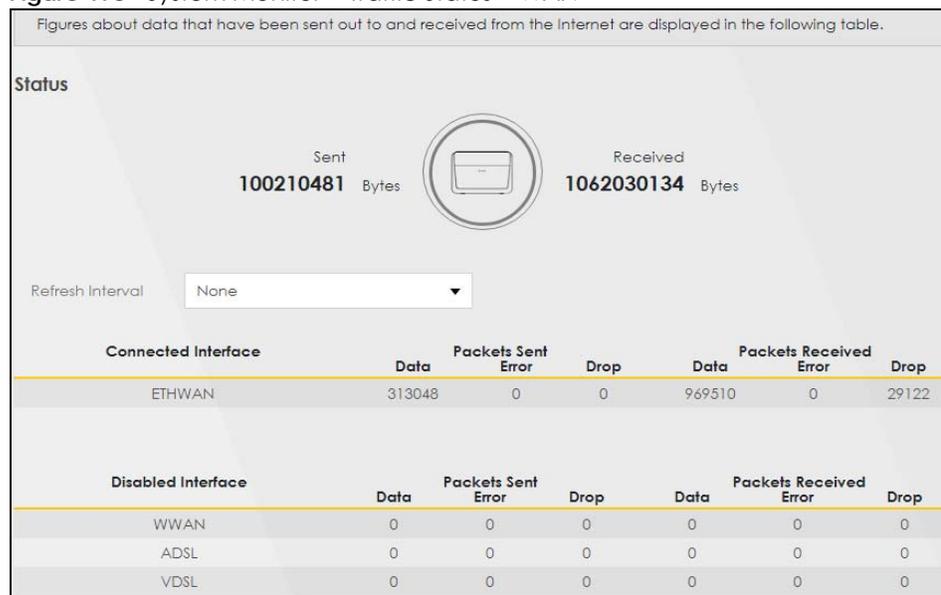
25.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 25.2 on page 294](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 25.3 on page 295](#)).
- Use the **NAT** screen to view the NAT status of the Zyxel Device's client(s) ([Section 25.4 on page 296](#))

25.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figures in this screen show the number of bytes received and sent through the Zyxel Device. Detailed information about each interface are listed in the tables below.

Figure 173 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 132 System Monitor > Traffic Status > WAN

| LABEL | DESCRIPTION |
|---------------------|--|
| Refresh Interval | Select how often you want the Zyxel Device to update this screen. |
| Connected Interface | This shows the name of the WAN interface that is currently connected. |
| Packets Sent | |
| Data | This indicates the number of transmitted packets on this interface. |
| Error | This indicates the number of frames with errors transmitted on this interface. |
| Drop | This indicates the number of outgoing packets dropped on this interface. |
| Packets Received | |
| Data | This indicates the number of received packets on this interface. |
| Error | This indicates the number of frames with errors received on this interface. |
| Drop | This indicates the number of received packets dropped on this interface. |
| Disabled Interface | This shows the name of the WAN interface that is currently disabled. |
| Packets Sent | |
| Data | This indicates the number of transmitted packets on this interface. |
| Error | This indicates the number of frames with errors transmitted on this interface. |
| Drop | This indicates the number of outgoing packets dropped on this interface. |
| Packets Received | |
| Data | This indicates the number of received packets on this interface. |
| Error | This indicates the number of frames with errors received on this interface. |
| Drop | This indicates the number of received packets dropped on this interface. |

25.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figures in this screen show the number of bytes received and sent from each LAN port and wireless network.

Figure 174 System Monitor > Traffic Status > LAN

Figures about data that have been sent to and received from each LAN port (including wireless) are displayed in the following table.

Refresh Interval:

| Interface | LAN1 | LAN2 | LAN3 | LAN4 | 2.4G WLAN | 5G WLAN |
|----------------|---------|------|------|------|-----------|---------|
| Bytes Sent | 2753665 | 0 | 0 | 0 | 0 | 0 |
| Bytes Received | 1415275 | 0 | 0 | 0 | 0 | 0 |

| Interface | LAN1 | LAN2 | LAN3 | LAN4 | 2.4G WLAN | 5G WLAN |
|-------------------|-------|-------|------|------|-----------|---------|
| Sent (Packet) | Data | 18163 | 0 | 0 | 0 | 0 |
| | Error | 0 | 0 | 0 | 0 | 3 |
| | Drop | 0 | 0 | 0 | 0 | 3 |
| Received (Packet) | Data | 13494 | 0 | 0 | 0 | 0 |
| | Error | 0 | 0 | 0 | 0 | 2 |
| | Drop | 7 | 0 | 0 | 0 | 0 |

The following table describes the fields in this screen.

Table 133 System Monitor > Traffic Status > LAN

| LABEL | DESCRIPTION |
|--------------------|--|
| Refresh Interval | Select how often you want the Zyxel Device to update this screen. |
| Interface | This shows the LAN or WLAN interface. |
| Bytes Sent | This indicates the number of bytes transmitted on this interface. |
| Bytes Received | This indicates the number of bytes received on this interface. |
| Interface | This shows the LAN or WLAN interfaces. |
| Sent (Packets) | |
| Data | This indicates the number of transmitted packets on this interface. |
| Error | This indicates the number of frames with errors transmitted on this interface. |
| Drop | This indicates the number of outgoing packets dropped on this interface. |
| Received (Packets) | |
| Data | This indicates the number of received packets on this interface. |
| Error | This indicates the number of frames with errors received on this interface. |
| Drop | This indicates the number of received packets dropped on this interface. |

25.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. The figures in this screen show the NAT session statistics for hosts currently connected to the Zyxel Device. A higher number of open sessions means there's more traffic going through a LAN client.

Figure 175 System Monitor > Traffic Status > NAT

The current connection numbers built by each LAN client are displayed in the following table. A higher number of open sessions that a LAN client creates means busier Internet activities he or she is engaging in.

Refresh Interval

| Device Name | IPv4 Address | MAC Address | NO. of Open Sessions |
|----------------|---------------|-------------------|----------------------|
| TWPCZT02523-01 | 192.168.1.100 | dc:4a:3e:40:ec:67 | 2 |

Total:

The following table describes the fields in this screen.

Table 134 System Monitor > Traffic Status > NAT

| LABEL | DESCRIPTION |
|---------------------|--|
| Refresh Interval | Select how often you want the Zyxel Device to update this screen. |
| Device Name | This displays the name of the connected host. |
| IPv4 Address | This displays the IP address of the connected host. |
| MAC Address | This displays the MAC address of the connected host. |
| No. of Open Session | This displays the number of NAT sessions currently opened for the connected host. |
| Total | This displays what percentage of NAT sessions the Zyxel Device can support is currently being used by all connected hosts. You can also see the number of active NAT sessions and the maximum number of NAT sessions the Zyxel Device can support. |

CHAPTER 26

VoIP Status

26.1 VoIP Status Overview

Click **System Monitor > VoIP Status** to open the following screen. You can view the VoIP registration, current call status, phone numbers, and other related information in this screen.

Figure 176 System Monitor > VoIP Status

Information, such as whether a SIP account is registered and the total call volume made by a SIP account, can be viewed in the page.

Poll Interval(s): sec [Set Interval](#) [Stop](#)

| Account | Register Action | Registration | Registration Time | URI | Message Waiting | Last Incoming Number | Last Outgoing Number |
|---------|--------------------------|--------------|-------------------|-------------------|-----------------|----------------------|----------------------|
| 1 | <input type="checkbox"/> | Disabled | | ChangeMe@ChangeMe | No | | |
| 2 | <input type="checkbox"/> | Disabled | | ChangeMe@ChangeMe | No | | |

| Account | Duration | Status | Call Type | Codec | From Phone Port Type | To Phone Port Type | Peer Number |
|---------|----------|--------|-----------|-------|----------------------|--------------------|-------------|
| | | | | | | | |

| Phone | Outgoing Number | Incoming Number |
|---------|-----------------|-----------------|
| Phone 1 | ChangeMe | ChangeMe |
| Phone 2 | ChangeMe | ChangeMe |

The following table describes the fields in this screen.

Table 135 System Monitor > VoIP Status

| LABEL | DESCRIPTION |
|------------------|--|
| Poll Interval(s) | Enter the number of seconds the Zyxel Device needs to wait before updating this screen and then click Set Interval . Click Stop to have the Zyxel Device stop updating this screen. |
| SIP Status | |
| Account | This column displays each SIP account in the Zyxel Device. |
| Register Action | Click on this switch to register/unregister the SIP account. This switch will turn blue if a registration attempt is successful; otherwise, it will revert to its unregistered setting. Unregistering an account does not delete the SIP account itself, but removes the mapping between your SIP identity and your IP address or domain name, |

Table 135 System Monitor > VoIP Status (continued)

| LABEL | DESCRIPTION |
|----------------------|---|
| Registration | <p>This field displays the current registration status of the SIP account.</p> <p>Disabled - The SIP account is not enabled. You can enable it in VoIP > SIP > SIP Account by pressing the Edit icon in the Modify field, and then selecting the Enable SIP Account check box.</p> <p>Registered - The SIP account is registered with a SIP server and can be used to make a VoIP call. The account must first be enabled in VoIP > SIP > SIP Account and registered by enabling Register Action.</p> <p>Unregistered - This status will show if the last attempt to register the SIP account with the SIP server failed or if Register Action is set to unregistered.</p> |
| Registration Time | <p>This field displays the last time the Zyxel Device successfully registered the SIP account. The field is blank if the Zyxel Device has never successfully registered this account.</p> |
| URI | <p>This field displays the account number and service domain of the SIP account. You can change these in the VoIP > SIP screens.</p> |
| Message Waiting | <p>This field indicates whether or not there are any messages waiting for the SIP account.</p> |
| Last Incoming Number | <p>This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.</p> |
| Last Outgoing Number | <p>This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.</p> |
| Call Status | |
| Account | <p>This column displays each SIP account in the Zyxel Device.</p> |
| Duration | <p>This field displays how long the current call has lasted.</p> |
| Status | <p>This field displays the current state of the phone call.</p> <p>Idle - There are no current VoIP calls, incoming calls or outgoing calls being made.</p> <p>Dial - The callee's phone is ringing.</p> <p>Ring - The phone is ringing for an incoming VoIP call.</p> <p>Process - There is a VoIP call in progress.</p> <p>DISC - The callee's line is busy, the callee hung up or your phone was left off the hook.</p> |
| Call Type | <p>This field displays the call direction type of the current VoIP call.</p> <p>Outgoing Call - It's a SIP VoIP call made by local phone ports, and this SIP account is able to issue a (SIP-based) call setup to the SIP account of remote peers for a VoIP call establishment. This (SIP-based) call setup signal is sent to the SIP server first, and then the SIP server would relay it to the target peer after correctly resolving and locating the target peer. During the call setup (signaling) phase, Calling state is displayed in the Status field, and it turns to InCall state once the call is successfully established.</p> <p>Incoming Call - It's a SIP VoIP call made or originated by remote SIP accounts to connect to this local SIP account. One or more local phone ports can be configured to receive this type of call, see the Incoming Number below, and all of them should begin to ring during the call setup (signaling phase), see the Status above. Once some remote SIP accounts start to ring one local phone, answer by off-hook to the call, and the call is successfully established. The other ringing local phone ports will stop ringing and turning to InCall state in the Status field.</p> <p>Internal Call - It's a local VoIP call between two different local phone ports. No SIP signaling is needed and thus no SIP server is involved to establish this type of call. This type of call is established via the Internal and Non-SIP local setup signaling procedure between the call-originating and call-terminating local phone ports. In general, one or more local phone ports can be designed to receive this type of call, and once any of the ringing phones answer the call, the other ringing ones will stop ringing. During the call setup phase (signaling phase), Calling state is displayed in Status field, and turns to InCall state once the call is successfully established.</p> |

Table 135 System Monitor > VoIP Status (continued)

| LABEL | DESCRIPTION |
|----------------------|---|
| Codec | This field displays what voice codec is being used for a current VoIP call through a phone port. |
| From Phone Port Type | <p>This field displays the phone ports type used to originate, start, or create the current VoIP call. Two possible type values will be displayed here:</p> <p>SIP - For the current call which is categorized as Incoming Call in the Call Type field, this field will show the type SIP.</p> <p>FXS - As for the other cases: Outgoing Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device.</p> |
| To Phone Port Type | <p>This field displays the phone ports type used to receive the current VoIP call. Three possible type values will be displayed here:</p> <p>SIP - For the current call which is categorized as Outgoing Call in the Call Type field, this field will show the type SIP.</p> <p>FXS and Unknown - As for the other cases: Incoming Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device. While the call is established, this field shows Unknown during the call setup phase (signaling phase). This is because one or more local phone ports can be configured or designed to receive these two types of calls, see the Call Type above, and the local phone port will answer the call that hasn't been determined yet at that time.</p> |
| Peer Number | This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port. |
| Phone Status | |
| Phone | This field displays the name of a phone port on the Zyxel Device. |
| Outgoing Number | This field displays the SIP number that you use to make calls on this phone port. |
| Incoming Number | This field displays the SIP number that you use to receive calls on this phone port. |

CHAPTER 27

ARP Table

27.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

27.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

27.2 ARP Table Screen

Use the ARP table to view the IPv4-to-MAC address mapping(s) for the LAN. The neighbor table shows the IPv6-to-MAC address mapping(s) of each neighbor. To open this screen, click **System Monitor > ARP Table**.

Figure 177 System Monitor > ARP Table

| ARP Table displays the IPv4 address and MAC address of each DHCP connection. Neighbour Table displays the IPv6 address and MAC address of each Neighbour. | | | |
|--|---------------|-------------------|--------|
| IPv4 ARP Table | | | |
| # | IPv4 Address | MAC Address | Device |
| 1 | 192.168.1.100 | dc:4a:3e:40:ec:67 | br0 |
| IPv6 Neighbour Table | | | |
| # | IPv6 Address | MAC Address | Device |

The following table describes the labels in this screen.

Table 136 System Monitor > ARP Table

| LABEL | DESCRIPTION |
|-------------------|---|
| # | This is the ARP table entry number. |
| IPv4/IPv6 Address | This is the learned IPv4 or IPv6 IP address of a device connected to a port. |
| MAC Address | This is the MAC address of the device with the listed IP address. |
| Device | This is the type of interface used by the device. You can click on the device type to go to its configuration screen. |

CHAPTER 28

Routing Table

28.1 Routing Table Overview

Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

28.2 The Routing Table Screen

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0' for the default route. The gateway address is written as '*'(IPv4)/':'(IPv6) if none is set.

Click **System Monitor > Routing Table** to open the following screen.

Figure 178 System Monitor > Routing Table

| Destination: The destination network or destination host. | | | | | |
|--|---------|---------------|--------|-----------|-----------|
| Gateway : The gateway address or '*'(IPv4)/':'(IPv6) if none set. | | | | | |
| Subnet Mask (IPv4): The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route. | | | | | |
| Flags: U - up, I - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect). | | | | | |
| Metric: The distance to the target (usually counted in hops). | | | | | |
| Interface: Interface to which packets for this route will be sent. | | | | | |
| IPv4 Routing Table | | | | | |
| Destination | Gateway | Subnet Mask | Flag | Metric | Interface |
| 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | br0 |
| IPv6 Routing Table | | | | | |
| Destination | Gateway | Flag | Metric | Interface | |
| fe80::/64 | :: | U | 256 | eth1.0 | |
| fe80::/64 | :: | U | 256 | eth2.0 | |
| fe80::/64 | :: | U | 256 | eth3.0 | |
| fe80::/64 | :: | U | 256 | eth4.0 | |
| fe80::/64 | :: | U | 256 | br0 | |
| fe80::/64 | :: | U | 256 | wl0.5 | |
| ::1/128 | :: | U | 0 | lo | |

The following table describes the labels in this screen.

Table 137 System Monitor > Routing Table

| LABEL | DESCRIPTION |
|-------------------------|--|
| IPv4/IPv6 Routing Table | |
| Destination | This indicates the destination IPv4 address or IPv6 address and prefix of this route. |
| Gateway | This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic. |
| Subnet Mask | This indicates the destination subnet mask of the IPv4 route. |
| Flag | <p>This indicates the route status.</p> <p>U-Up: The route is up.</p> <p>!-Reject: The route is blocked and will force a route lookup to fail.</p> <p>G-Gateway: The route uses a gateway to forward traffic.</p> <p>H-Host: The target of the route is a host.</p> <p>R-Reinstate: The route is reinstated for dynamic routing.</p> <p>D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.</p> <p>M-Modified (redirect): The route is modified from a routing daemon or redirect.</p> |
| Metric | The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost". |
| Interface | <p>This indicates the name of the interface through which the route is forwarded.</p> <p>brx indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively.</p> <p>ptm0 indicates a VDSL WAN interface using IPoE or in bridge mode.</p> <p>ethx indicates an Ethernet WAN interface using IPoE or in bridge mode.</p> <p>ppp0 indicates a WAN interface using PPPoE.</p> <p>wlx indicates a wireless interface where x can be 0~1. For VMG4927-B10A, wl1 indicates 5 GHz wireless interface, and wl0 indicates 2.4 GHz wireless interface. For the other models, wl1 indicates 5 GHz wireless interface, and wl0 indicates 2.4 GHz wireless interface.</p> |

CHAPTER 29

Multicast Status

29.1 Multicast Status Overview

Use the **Multicast Status** screens to look at IGMP/MLD group status and traffic statistics.

29.2 The IGMP Status Screen

Use this screen to look at the current list of multicast groups the Zyxel Device manages through IGMP. Configure IGMP in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > IGMP Status**.

Figure 179 System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

Table 138 System Monitor > Multicast Status > IGMP Status

| LABEL | DESCRIPTION |
|-----------------|--|
| Refresh | Click this button to update the information on this screen. |
| Interface | This field displays the name of an interface on the Zyxel Device that belongs to an IGMP multicast group. |
| Multicast Group | This field displays the name of the IGMP multicast group to which the interface belongs. |
| Filter Mode | INCLUDE means that only the IP addresses in the Source List get to receive the multicast group's traffic. EXCLUDE means that the IP addresses in the Source List are not allowed to receive the multicast group's traffic but other IP addresses can. |
| Source List | This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode. |
| Member | This is the list of the members of the multicast group. |

29.3 The MLD Status Screen

Use this screen to look at the current list of multicast groups the Zyxel Device manages through MLD. Configure MLD in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > MLD Status**.

Figure 180 System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 139 System Monitor > Multicast Status > MLD Status

| LABEL | DESCRIPTION |
|-----------------|--|
| Refresh | Click this button to update the status on this screen. |
| Interface | This field displays the name of an interface on the Zyxel Device that belongs to an MLD multicast group. |
| Multicast Group | This field displays the name of the MLD multicast group to which the interface belongs. |
| Filter Mode | INCLUDE means that only the IP addresses in the Source List get to receive the multicast group's traffic. EXCLUDE means that the IP addresses in the Source List are not allowed to receive the multicast group's traffic but other IP addresses can. |
| Source List | This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode. |
| Member | This is the list of members in the multicast group. |

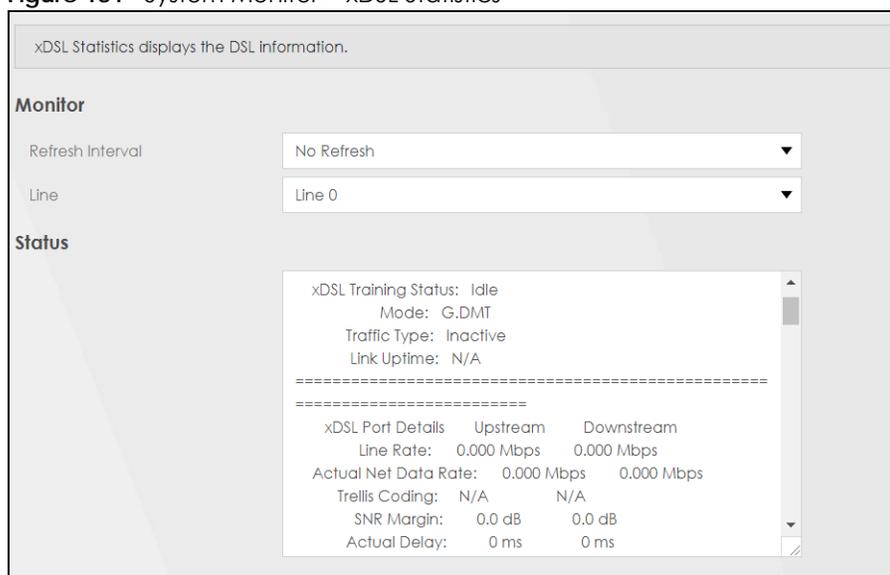
CHAPTER 30

xDSL Statistics

30.1 xDSL Statistics Overview

Use this screen to view detailed DSL information. It allows you to see the DSL status, check port details, and see DSL counters. Click **System Monitor > xDSL Statistics** to open the following screen.

Figure 181 System Monitor > xDSL Statistics



The following table describes the labels in this screen.

Table 140 System > xDSL Statistics

| LABEL | DESCRIPTION |
|----------------------|--|
| Monitor | |
| Refresh Interval | Select the time interval for refreshing statistics. |
| Line | Select which DSL line's statistics you want to display. |
| Status | |
| xDSL Training Status | This displays the current state of setting up the DSL connection. |
| Mode | This displays the ITU standard used for this connection. |
| Traffic Type | This displays the type of traffic the DSL port is sending and receiving. Inactive displays if the DSL port is not currently sending or receiving traffic. |
| Link Uptime | This displays how long the port has been running (or connected) since the last time it was started. |
| xDSL Port Details | |
| Upstream | These are the statistics for the traffic direction going out from the port to the service provider. |

Table 140 System > xDSL Statistics (continued)

| LABEL | DESCRIPTION |
|--------------------------|--|
| Downstream | These are the statistics for the traffic direction coming into the port from the service provider. |
| Line Rate | These are the data transfer rates at which the port is sending and receiving data. |
| Actual Net Data Rate | These are the rates at which the port is sending and receiving the payload data without transport layer protocol headers and traffic. |
| Trellis Coding | This displays whether or not the port is using Trellis coding for traffic it is sending and receiving. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable. |
| SNR Margin | This is the upstream and downstream Signal-to-Noise Ratio margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the system still being able to meet its transmission targets. |
| Actual Delay | This is the upstream and downstream interleave delay. It is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed. |
| Transmit Power | This is the upstream and downstream far end actual aggregate transmit power (in dBm). Upstream is how much power the port is using to transmit to the service provider. Downstream is how much power the service provider is using to transmit to the port. |
| Receive Power | Upstream is how much power the service provider is receiving from the port. Downstream is how much power the port is receiving from the service provider. |
| Actual INP | Sudden spikes in the line's level of external noise (impulse noise) can cause errors and result in lost packets. This could especially impact the quality of multimedia traffic such as voice or video. Impulse noise protection (INP) provides a buffer to allow for correction of errors caused by error correction to deal with this. The number of DMT (Discrete Multi-Tone) symbols shows the level of impulse noise protection for the upstream and downstream traffic. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may increase error rates in received multimedia data. |
| Attainable Net Data Rate | These are the highest theoretically possible transfer rates at which the port could send and receive payload data without transport layer protocol headers and traffic. |
| xDSL Counters | |
| Downstream | These are the statistics for the traffic direction coming into the port from the service provider. |
| Upstream | These are the statistics for the traffic direction going out from the port to the service provider. |
| FEC | This is the number of Far End Corrected blocks. |
| CRC | This is the number of Cyclic Redundancy Checks. |
| ES | This is the number of Errored Seconds meaning the number of seconds containing at least one errored block or at least one defect. |
| SES | This is the number of Severely Errored Seconds meaning the number of seconds containing 30% or more errored blocks or at least one defect. This is a subset of ES. |
| UAS | This is the number of UnAvailable Seconds. |
| LOS | This is the number of Loss Of Signal seconds. |
| LOF | This is the number of Loss Of Frame seconds. |
| LOM | This is the number of Loss of Margin seconds. |
| Retr. | This is the number of DSL retraining count in the BRCM DSL driver. |
| HostInitRetr | This is the number of the retraining counts the host initiated. |
| FastRetr | This is the number of DSL fast retraining counts. |
| FailedRetr | This is the number of failed retraining attempts. |
| FailedFastRetr | This is the number of failed fast retraining attempts. |

CHAPTER 31

WLAN Station Status

31.1 WLAN Station Status Overview

Click **System Monitor > WLAN Station Status** to open the following screen. View the wireless stations that are currently associated to the Zyxel Device. Being associated means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel, and security settings.

Figure 182 System Monitor > WLAN Station Status

The screenshot shows the 'WLAN Station Status' interface. At the top, it says 'WLAN Station Status lists associated WiFi clients.' Below this, there are two sections: 'WLAN 2.4G Station Status' and 'WLAN 5G Station Status'. Each section contains a table with the following columns: '#', 'MAC Address', 'Rate (Mbps)', 'RSSI (dBm)', 'SNR', and 'Level'. The tables are currently empty.

The following table describes the labels in this screen.

Table 141 System Monitor > WLAN Station Status

| LABEL | DESCRIPTION |
|-------------|--|
| # | This is the index number of an associated wireless station. |
| MAC Address | This field displays the MAC address of an associated wireless station. |
| Rate (Mbps) | This field displays the transmission rate of the wireless LAN traffic between an associated wireless station and an AP. |
| RSSI (dBm) | This field displays the strength of the wireless LAN signal between an associated wireless station and an AP. The normal range is -30dBm to -79dBm. If the value drops below -80dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength. |

Table 141 System Monitor > WLAN Station Status

| LABEL | DESCRIPTION |
|-------|--|
| SNR | <p>SNR (Signal-to-Noise Ratio) measures the strength of the wireless LAN signal and the background noise on the line. The greater the number, the better the quality of the wireless LAN.</p> <p>The normal range is 15 to 40. If the value drops below 15, try moving the associated wireless station closer to the Zyxel Device to get better quality of wireless LAN.</p> |
| Level | <p>This field displays a number which represents the strength of the wireless LAN signal between an associated wireless station and an AP. The Zyxel Device uses the RSSI and SNR values to determine the strength of the wireless LAN signal.</p> <p>5 means the Zyxel Device is receiving an excellent wireless LAN signal.</p> <p>4 means the Zyxel Device is receiving a very good wireless LAN signal.</p> <p>3 means the Zyxel Device is receiving a weak wireless LAN signal,</p> <p>2 means the Zyxel Device is receiving a very weak wireless LAN signal.</p> <p>1 means the Zyxel Device is not receiving a wireless LAN signal.</p> |

CHAPTER 32

Cellular Statistics

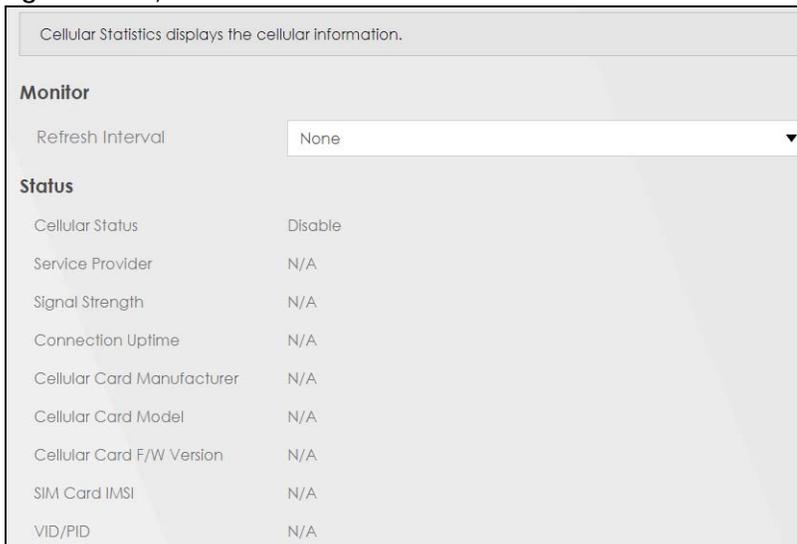
32.1 Cellular Statistics Overview

Use the **Cellular Statistics** screens to look at cellular Internet connection status. By default, a cellular WAN connection is used as a backup for the wired DSL/Ethernet WAN connections.

32.2 The Cellular Statistics Screen

To open this screen, click **System Monitor > Cellular Statistics**. Cellular information is available on this screen only when you insert a compatible cellular dongle in the USB port on the Zyxel Device.

Figure 183 System Monitor > Cellular Statistics



The following table describes the labels in this screen.

Table 142 System Monitor > Cellular Statistics

| LABEL | DESCRIPTION |
|----------------------------|---|
| Refresh Interval | Select how often you want the Zyxel Device to update this screen. Select No Refresh to stop refreshing. |
| Cellular Status | This field displays the status of the cellular Internet connection. This field can display: GSM - Global System for Mobile Communications, 2G GPRS - General Packet Radio Service, 2.5G EDGE - Enhanced Data rates for GSM Evolution, 2.75G WCDMA - Wideband Code Division Multiple Access, 3G HSDPA - High-Speed Downlink Packet Access, 3.5G HSUPA - High-Speed Uplink Packet Access, 3.75G HSPA - HSDPA+HSUPA, 3.75G |
| Service Provider | This field displays the name of the service provider. |
| Signal Strength | This field displays the strength of the signal in dBm. |
| Connection Uptime | This field displays the time the connection has been up. |
| Cellular Card Manufacturer | This field displays the manufacturer of the cellular card. |
| Cellular Card Model | This field displays the model name of the cellular card. |
| Cellular Card F/W Version | This field displays the firmware version of the cellular card. |
| SIM Card IMSI | The International Mobile Subscriber Identity or IMSI is a unique identification number associated with all cellular networks. This number is provisioned in the SIM card. |
| VID/PID | This field displays the USB Vendor ID and Product ID of the cellular card. |

CHAPTER 33

System

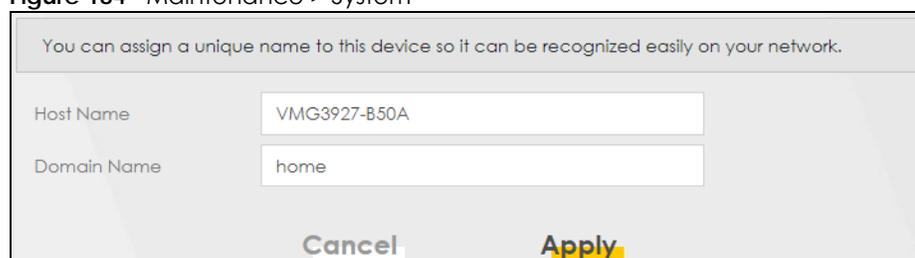
33.1 System Overview

In the **System** screen, you can name your Zyxel Device (Host) and give it an associated domain name for identification purposes.

33.2 The System Screen

Click **Maintenance > System** to open the following screen. Assign a unique name to this device so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Figure 184 Maintenance > System



You can assign a unique name to this device so it can be recognized easily on your network.

Host Name: VMG3927-B50A

Domain Name: home

Buttons: Cancel, Apply

The following table describes the labels in this screen.

Table 143 Maintenance > System

| LABEL | DESCRIPTION |
|-------------|---|
| Host Name | Type a hostname for your Zyxel Device. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. |
| Domain Name | Type a Domain name for your host Zyxel Device. |
| Cancel | Click Cancel to abandon this screen without saving. |
| Apply | Click Apply to save your changes. |

CHAPTER 34

User Account

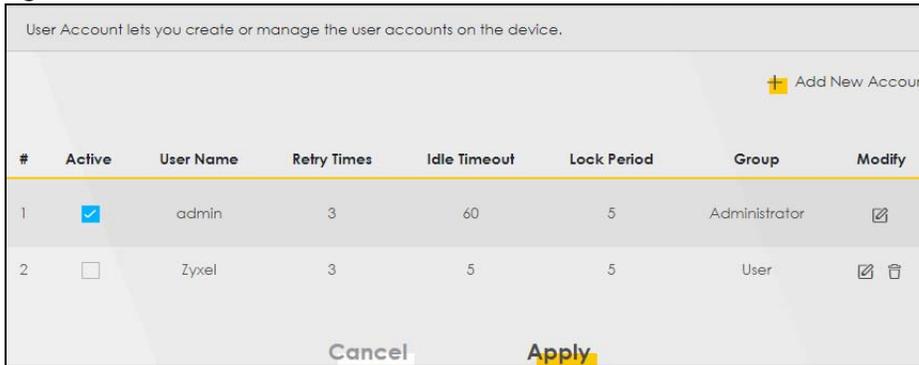
34.1 User Account Overview

In the **User Account** screen, you can view the settings of the "admin" and other user accounts that you use to log into the Zyxel Device.

34.2 The User Account Screen

Click **Maintenance > User Account** to open the following screen. Use this screen to create or manage user accounts and their privileges on the Zyxel Device.

Figure 185 Maintenance > User Account



The following table describes the labels in this screen.

Table 144 Maintenance > User Account

| LABEL | DESCRIPTION |
|-----------------|--|
| Add New Account | Click this button to add a new user account. |
| # | This is the index number |
| Active | This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it. |
| User Name | This field displays the name of the account used to log into the Zyxel Device web configurator. |
| Retry Times | This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit. |
| Idle Timeout | This field displays the length of inactive time before the Zyxel Device will automatically log the user out of the web configurator. |

Table 144 Maintenance > User Account (continued) (continued)

| LABEL | DESCRIPTION |
|-------------|--|
| Lock Period | This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in Retry Times . |
| Group | This field displays whether this user has Administrator or User privileges. |
| Modify | Click the Edit icon to configure the entry. Click the Delete icon to remove the entry. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

34.2.1 The User Account Add/Edit Screen

Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance > User Account** to open the following screen.

Figure 186 Maintenance > User Account > Add/Edit

The following table describes the labels in this screen.

Table 145 Maintenance > User Account > Add/Edit

| LABEL | DESCRIPTION |
|---------------------|--|
| Active | Select Enable or Disable to activate or deactivate the user account. |
| User Name | Enter a new name for the account. This field displays the name of an existing account. |
| Password | Type your new system password (up to 256 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Zyxel Device. |
| Verify New Password | Type the new password again for confirmation. |
| Retry Times | Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit. |

Table 145 Maintenance > User Account > Add/Edit (continued) (continued)

| LABEL | DESCRIPTION |
|--------------|--|
| Idle Timeout | Enter the length of inactive time before the Zyxel Device will automatically log the user out of the web configurator. |
| Lock Period | Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in Retry Times . |
| Group | Specify whether this user will have Administrator or User privileges. |
| Cancel | Click Cancel to restore your previously saved settings. |
| OK | Click OK to save your changes. |

CHAPTER 35

Remote Management

35.1 Remote Management Overview

Use remote management to control through which interface(s), each service can access the Zyxel Device.

Note: The Zyxel Device is managed using the Web Configurator.

35.2 The MGMT Services Screen

Use this screen to configure through which interface(s), each service can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance > Remote Management > MGMT Services** to open the following screen.

Figure 187 Maintenance > Remote Management > MGMT Services

Remote MGMT enables various approaches to access this device remotely from a WAN and/or LAN connection.

Service Control

WAN Interface used for services: Any_WAN Multi_WAN

WWAN ADSL VDSL ETHWAN

| Service | LAN/WLAN | WAN | Trust Domain | Port |
|---------|--|---------------------------------|---------------------------------|------|
| HTTP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | 80 |
| HTTPS | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | 443 |
| FTP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | 21 |
| TELNET | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | 23 |
| SSH | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | 22 |
| SNMP | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | 161 |
| PING | <input checked="" type="checkbox"/> Enable | <input type="checkbox"/> Enable | <input type="checkbox"/> Enable | |

Cancel **Apply**

The following table describes the fields in this screen.

Table 146 Maintenance > Remote Management > MGMT Services

| LABEL | DESCRIPTION |
|---------------------------------|--|
| WAN Interface used for services | Select Any_WAN to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select Multi_WAN and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up. |
| Service | This is the service you may use to access the Zyxel Device. |
| LAN/WLAN | Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN/WLAN. |
| WAN | Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections. |
| Trust Domain | Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted hosts configured in the Maintenance > Remote MGMT > Trust Domain screen. If you only want certain WAN connections to have access to the Zyxel Device using the corresponding services, then clear WAN , select Trust Domain and configure the allowed IP address(es) in the Trust Domain screen. |
| Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |

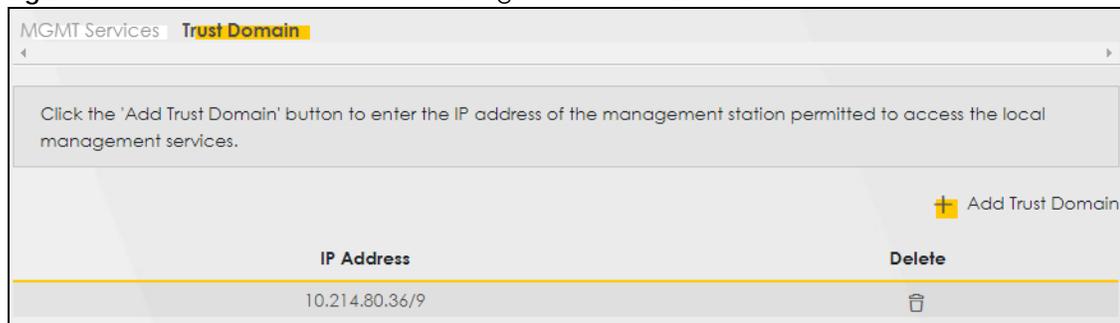
35.3 The Trust Domain Screen

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance > Remote Management > MGMT Services** screen.

Click **Maintenance > Remote Management > Trust Domain** to open the following screen.

Note: If this list is empty, all public IP addresses can access the Zyxel Device from the WAN through the specified services.

Figure 188 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

Table 147 Maintenance > Remote Management > Trust Domain

| LABEL | DESCRIPTION |
|------------------|--|
| Add Trust Domain | Click this to add a trusted host IP address. |
| IP Address | This field shows a trusted host IP address. |
| Delete | Click the Delete icon to remove the trust IP address. |

35.4 The Add Trust Domain Screen

Use this screen to configure a public IP address which is allowed to access the Zyxel Device. Click the **Add Trust Domain** button in the **Maintenance > Remote Management > Trust Domain** screen to open the following screen.

Figure 189 Maintenance > Remote Management > Trust Domain > Add Trust Domain

Enter the IP address of the management station permitted to access the local management services, and click 'Apply'.

IP Address [prefix length]

Cancel OK

The following table describes the fields in this screen.

Table 148 Maintenance > Remote Management > Trust Domain > Add Trust Domain

| LABEL | DESCRIPTION |
|------------|---|
| IP Address | Enter a public IPv4 IP address which is allowed to access the service on the Zyxel Device from the WAN. |
| OK | Click OK to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to restore your previously saved settings. |

CHAPTER 36

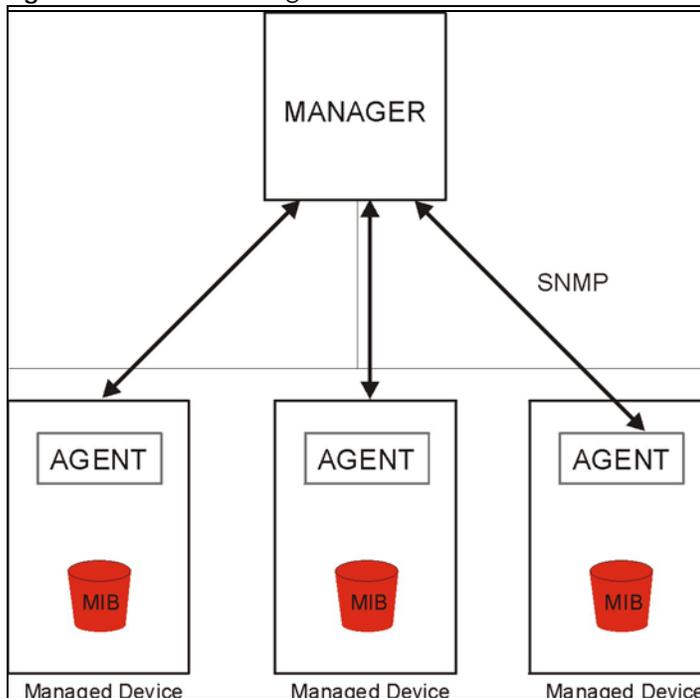
SNMP

36.1 SNMP Overview

This screen allows you to configure the SNMP settings on the Zyxel Device.

The Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The next figure illustrates an SNMP management operation.

Figure 190 SNMP Management Model



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

An agent is a management software module that resides in a managed device (the Zyxel Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include the number of packets received, node port status, etc. A Management Information Base (MIB) is a collection of managed

objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- **Get** - Allows the manager to retrieve an object variable from the agent.
- **GetNext** - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- **Set** - Allows the manager to set values for object variables within an agent.

Trap - Used by the agent to inform the manager of some events.

36.2 The SNMP Screen

Click **Maintenance > SNMP** to open the following screen. Use this screen to configure the Zyxel Device SNMP settings.

Configure how this device reports to the Network Management System (NMS) via SNMP using the screen below.

Figure 191 Maintenance > SNMP

The following table describes the fields in this screen.

Table 149 Maintenance > SNMP

| LABEL | DESCRIPTION |
|---------------|--|
| SNMP Agent | Enable this switch to let the Zyxel Device act as an SNMP agent, which allows a manager station to manage and monitor the Zyxel Device through the network. Click on this switch to enable/disable it. When the switch turns blue  , the function is enabled. |
| Get Community | Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. |
| Set Community | Enter the Set Community , which is the password for the incoming Set requests from the management station |

Table 149 Maintenance > SNMP

| LABEL | DESCRIPTION |
|------------------|---|
| Trap Community | Enter the Trap Community , which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. |
| System Name | Enter the SNMP system name. |
| System Location | Enter the SNMP system location. |
| System Contact | Enter the SNMP system contact. |
| Trap Destination | Type the IP address of the station to send your SNMP traps to. |
| Apply | Click Apply to save your changes back to the Zyxel Device. |
| Cancel | Click Cancel to restore your previously saved settings. |

CHAPTER 37

Time Settings

37.1 Time Settings Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

37.2 The Time Screen

To change your Zyxel Device's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the Zyxel Device's time based on your local time zone. You can add a time server address, select your time zone, and configure Daylight Savings if your location uses it.

Figure 192 Maintenance > Time

In order to get a correct time for the device, fill in a time server address, select the time zone where this device is physically located, and complete the daylight saving settings if needed.

Current Date/Time

Current Time 09:21:28
Current Date 2018-04-16

Time and Date Setup

Time Protocol SNTP [RFC-1769]

First Time Server Address poolntp.org
Second Time Server Address clocknyc.he.net
Third Time Server Address clocksjc.he.net
Fourth Time Server Address None
Fifth Time Server Address None

Time Zone

Time Zone [GMT-12:00] International Date Line West

Daylight Savings

Active

Start Rule

Day 1 in
 Last Sunday in
Month April
Hour 2 : 0

End Rule

Day 1 in
 Last Sunday in
Month November
Hour 3 : 0

Cancel Apply

The following table describes the fields in this screen.

Table 150 Maintenance > Time

| LABEL | DESCRIPTION |
|-----------------------------------|---|
| Current Date/Time | |
| Current Time | This field displays the time of your Zyxel Device. Each time you reload this page, the Zyxel Device synchronizes the time with the time server. |
| Current Date | This field displays the date of your Zyxel Device. Each time you reload this page, the Zyxel Device synchronizes the date with the time server. |
| Time and Date Setup | |
| First ~ Fifth Time Server Address | Select an NTP time server from the drop-down list box. Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select None if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information. |
| Time Zone | |
| Time zone | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Savings | Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. |
| Active | Click this switch to enable or disable Daylight Saving Time. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Start Rule | Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to Second, Sunday , the month to March and the time to 2 in the Hour field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to Last, Sunday and the month to March . The time you select in the o'clock field depends on your time zone. In Germany for instance, you would select 2 in the Hour field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Rule | Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The Time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to First, Sunday , the month to November and the time to 2 in the Hour field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to Last, Sunday , and the month to October . The time you select in the o'clock field depends on your time zone. In Germany for instance, you would select 2 in the Hour field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Cancel | Click Cancel to exit this screen without saving. |
| Apply | Click Apply to save your changes. |

CHAPTER 38

E-mail Notification

38.1 E-mail Notification Overview

A mail server is an application or a computer that can receive, forward and deliver e-mail messages.

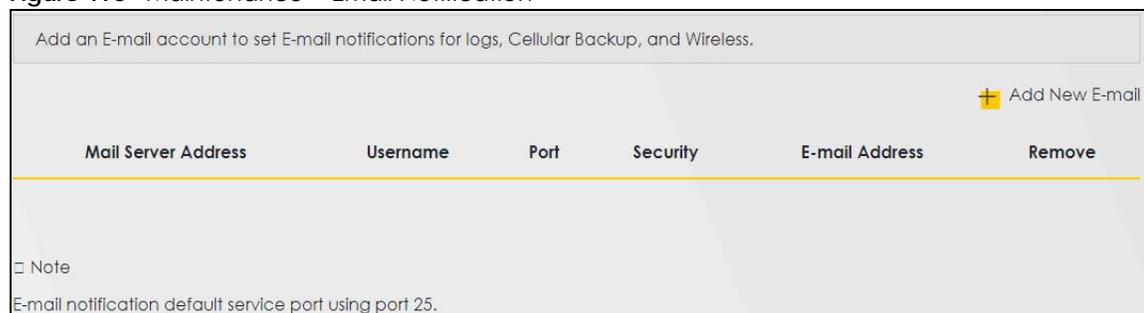
To have the Zyxel Device send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

38.2 The Email Notification Screen

Click **Maintenance > Email Notification** to open the **Email Notification** screen. Use this screen to view, remove and add E-mail account information on the Zyxel Device. This account can be set to receive e-mail notifications for logs.

Note: The default port number of the mail server is 25.

Figure 193 Maintenance > Email Notification



The following table describes the labels in this screen.

Table 151 Maintenance > Email Notification

| LABEL | DESCRIPTION |
|---------------------|---|
| Add New E-mail | Click this button to create a new entry. |
| Mail Server Address | This field displays the server name or the IP address of the mail server. |
| Username | This field displays the user name of the sender's mail account. |
| Port | This field displays the port number of the mail server. |
| Security | This field displays the protocol used for encryption. |
| E-mail Address | This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the Zyxel Device sends. |
| Remove | Click this button to delete the selected entry(ies). |

38.2.1 Email Notification Edit

Click the **Add** button in the **Email Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 194 Email Notification > Add

The following table describes the labels in this screen.

Table 152 Email Notification > Add

| LABEL | DESCRIPTION |
|-------------------------|---|
| Mail Server Address | Enter the server name or the IP address of the mail server for the e-mail address specified in the Account Email Address field. If this field is left blank, reports, logs or notifications will not be sent via e-mail. |
| Port | Enter the same port number here as is on the mail server for mail traffic. |
| Authentication Username | Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the Account Email Address field. |
| Authentication Password | Enter the password associated with the user name above. |
| Account E-mail Address | Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the Zyxel Device sends. If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well. |
| Connection Security | Select SSL to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select STARTTLS to upgrade a plain text connection to a secure connection using SSL/TLS. |
| Cancel | Click this button to begin configuring this screen afresh. |
| OK | Click this button to save your changes and return to the previous screen. |

CHAPTER 39

Log Setting

39.1 Logs Setting Overview

You can configure where the Zyxel Device sends logs and which logs and/or immediate alerts the Zyxel Device records in the **Logs Setting** screen.

39.2 The Log Settings Screen

To change your Zyxel Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

If you have a LAN client on your network or a remote server that is running a syslog utility, you can also save its log files by enabling **Syslog Logging**, selecting **Remote** or **Local File and Remote** in the **Mode** field, and entering the IP address of the LAN client in the **Syslog Server** field. **Remote** allows you to store logs in a server, while **Local File** allows you to store them locally. **Local File and Remote** means your logs are stored both locally and in a server.

Figure 195 Maintenance > Log Setting

Log Setting defines which types of logs and which log levels you want to record. If you have a LAN client on your network that is running a syslog utility, you can also save the log files there by enabling Syslog Logging and enter the IP address of that LAN client.

Syslog Setting

Syslog Logging

Mode

Syslog Server (Server NAME or IPv4/IPv6 Address)

UDP Port (Server Port)

E-mail Log Settings

E-mail Log Settings

Active Log

| | |
|---|--|
| System Log | Security Log |
| <input checked="" type="checkbox"/> WAN-DHCP | <input type="checkbox"/> Account |
| <input checked="" type="checkbox"/> DHCP Server | <input checked="" type="checkbox"/> Attack |
| <input checked="" type="checkbox"/> PPPoE | <input checked="" type="checkbox"/> Firewall |
| <input type="checkbox"/> TR-069 | <input type="checkbox"/> MAC Filter |
| <input type="checkbox"/> HTTP | |
| <input type="checkbox"/> UPNP | |
| <input checked="" type="checkbox"/> System | |
| <input checked="" type="checkbox"/> xDSL | |
| <input type="checkbox"/> ACL | |
| <input type="checkbox"/> Wireless | |
| <input type="checkbox"/> MESH | |

The following table describes the fields in this screen.

Table 153 Maintenance > Log Setting

| LABEL | DESCRIPTION |
|---------------------|--|
| Syslog Setting | |
| Syslog Logging | The Zyxel Device sends a log to an external syslog server. Click this switch to enable or disable to enable syslog logging. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Mode | Select the syslog destination from the drop-down list box. If you select Remote , the log(s) will be sent to a remote syslog server. If you select Local File , the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select Local File and Remote . |
| Syslog Server | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| UDP Port | Enter the port number used by the syslog server. |
| E-mail Log Settings | |
| E-mail Log Settings | Click this switch to have the Zyxel Device send logs and alarm messages to the configured e-mail addresses. When the switch turns blue  , the function is enabled. Otherwise, it's not. |

Table 153 Maintenance > Log Setting (continued)

| LABEL | DESCRIPTION |
|---------------------------|---|
| Mail Account | Select a mail account from which you want to send logs. You can configure mail accounts in the Maintenance > Email Notification screen. |
| System Log Mail Subject | Type a title that you want to be in the subject line of the system log e-mail message that the Zyxel Device sends. |
| Security Log Mail Subject | Type a title that you want to be in the subject line of the security log e-mail message that the Zyxel Device sends. |
| Send Log to | The Zyxel Device sends logs to the e-mail address specified in this field. If this field is left blank, the Zyxel Device does not send logs via E-mail. |
| Send Alarm to | Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail. |
| Alarm Interval | Specify how often the alarm should be updated. |
| Active Log | |
| System Log | Select the categories of system logs that you want to record. |
| Security Log | Select the categories of security logs that you want to record. |
| Cancel | Click Cancel to restore your previously saved settings. |
| Apply | Click Apply to save your changes. |

39.2.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "End of Log" message shows that a complete log has been sent.

Figure 196 E-mail Log Example

```

Subject:
    Firewall Alert From
Date:
    Fri, 07 Apr 2000 10:05:42
From:
    user@zyxel.com
To:
    user@zyxel.com
1|Apr 7 00 |From:192.168.1.1      To:192.168.1.255  |default policy |forward
  |09:54:03 |UDP      src port:00520 dest port:00520  |<1,00>        |
2|Apr 7 00 |From:192.168.1.131   To:192.168.1.255  |default policy |forward
  |09:54:17 |UDP      src port:00520 dest port:00520  |<1,00>        |
3|Apr 7 00 |From:192.168.1.6     To:10.10.10.10   |match          |forward
  |09:54:19 |UDP      src port:03516 dest port:00053  |<1,01>        |
.....{snip}.....
.....{snip}.....
126|Apr 7 00 |From:192.168.1.1     To:192.168.1.255  |match          |forward
   |10:05:00 |UDP      src port:00520 dest port:00520  |<1,02>        |
127|Apr 7 00 |From:192.168.1.131   To:192.168.1.255  |match          |forward
   |10:05:17 |UDP      src port:00520 dest port:00520  |<1,02>        |
128|Apr 7 00 |From:192.168.1.1     To:192.168.1.255  |match          |forward
   |10:05:30 |UDP      src port:00520 dest port:00520  |<1,02>        |

End of Firewall Log

```

CHAPTER 40

Firmware Upgrade

40.1 Firmware Upgrade Overview

This screen lets you upload new firmware to your Zyxel Device. You can download new firmware releases from your nearest Zyxel FTP site (or www.zyxel.com) to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your Zyxel Device.

40.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. Download the latest firmware file from the Zyxel website and upload it to your Zyxel Device using this screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the Zyxel Device will reboot.

Do NOT turn off the Zyxel Device while firmware upload is in progress!

Figure 197 Maintenance > Firmware Upgrade

Firmware Upgrade is where you can update the device with newly released features by upgrading the latest firmware. You can download the latest firmware file from the manufacturer website of this device.

Upgrade Firmware

Restore Default Settings After Firmware Upgrade

Current Firmware Version: V5.13(ABLZ.1)b4

File Path No file chosen

Upgrade WWAN Package

Current WWAN Package Version: 1.16

File Path No file chosen

The following table describes the labels in this screen. After you see the firmware updating screen, wait two minutes before logging into the Zyxel Device again.

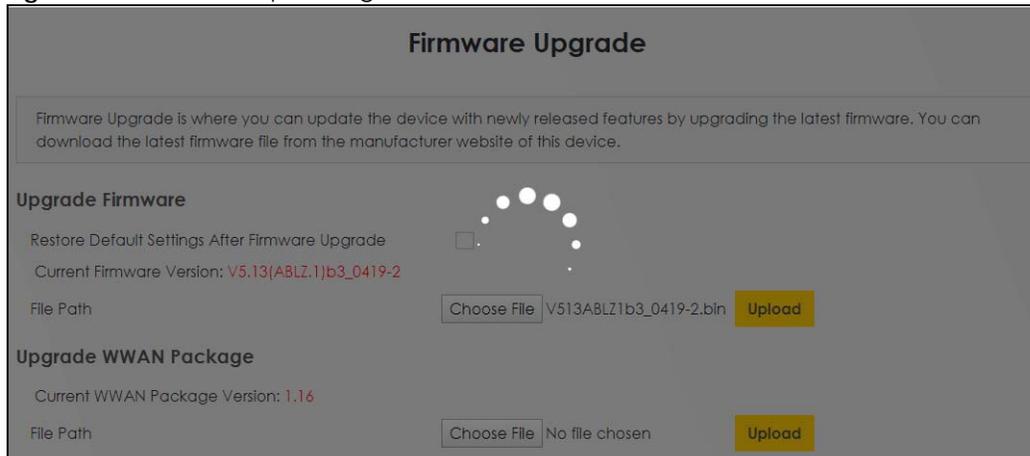
Table 154 Maintenance > Firmware Upgrade

| LABEL | DESCRIPTION |
|---|--|
| Upgrade Firmware | |
| Restore Default Settings After Firmware Upgrade | Select the check box to have the Zyxel Device automatically reset itself after the new firmware is uploaded. |

Table 154 Maintenance > Firmware Upgrade

| LABEL | DESCRIPTION |
|------------------------------|--|
| Current Firmware Version | This is the present Firmware version and the date created. |
| File Path | Type in the location of the file you wasn't to upload in this field or click Choose File to find it. |
| Choose File | Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload | Click this to begin the upload process. This process may take up to two minutes. |
| Upgrade WWAN Package | |
| Current WWAN Package Version | This is the present WWAN Package version and the date created. |
| File Path | Type in the location of the file you want to upload in this field or click Choose File to find it. |
| Choose File | Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload | Click this to begin the upload process. This process may take up to two minutes. |

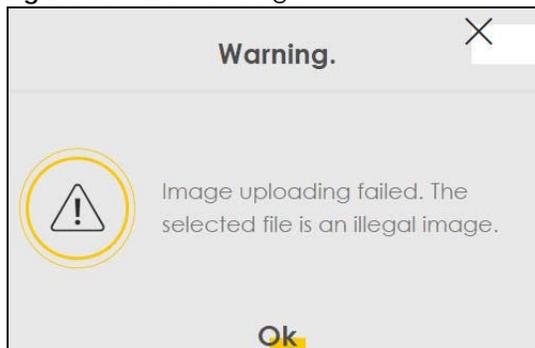
Figure 198 Firmware Uploading



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

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 199 Error Message



Note that the Zyxel Device automatically restarts during the upload, causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Network Temporarily Disconnected



CHAPTER 41

Backup Restore

41.1 Backup Restore Overview

The **Backup Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

41.2 The Backup Restore Screen

Click **Maintenance > Backup Restore**. Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore previous device configurations.

Figure 200 Maintenance > Backup Restore

You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.

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

Backup

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

File Path No file chosen **Upload**

Back to Factory Default Settings
Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- Password is printed on a label on the bottom of the device, written after the text "Password".
- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

Reset

Backup Configuration

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once your Zyxel Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Zyxel Device's current configuration to your computer.

Restore Configuration

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

Table 155 Restore Configuration

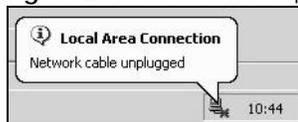
| LABEL | DESCRIPTION |
|-------------|---|
| File Path | Type in the location of the file you want to upload in this field or click Choose File to find it. |
| Choose File | Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload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

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

After the Zyxel Device configuration has been restored successfully, the login screen appears. Login again to restart the Zyxel Device.

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

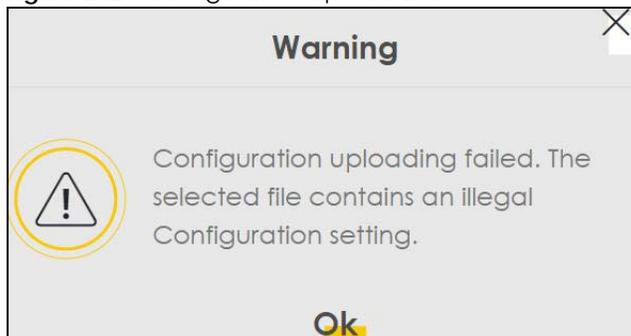
Figure 201 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

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

Figure 202 Configuration Upload Error



Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Zyxel Device to its factory defaults. The following warning screen appears.

Figure 203 Reset Warning Message

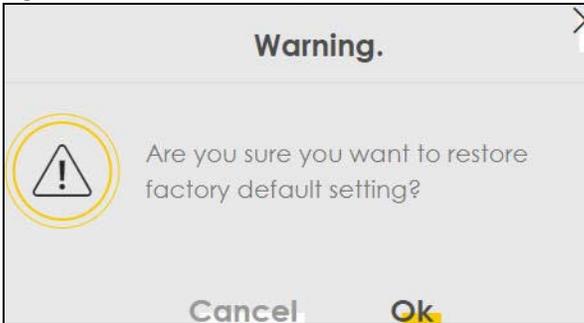
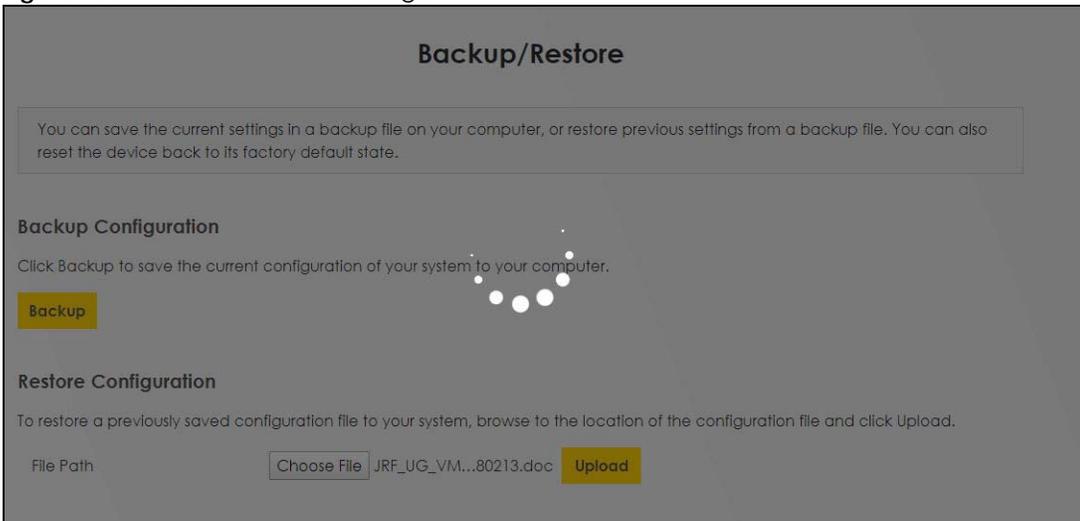


Figure 204 Reset In Process Message



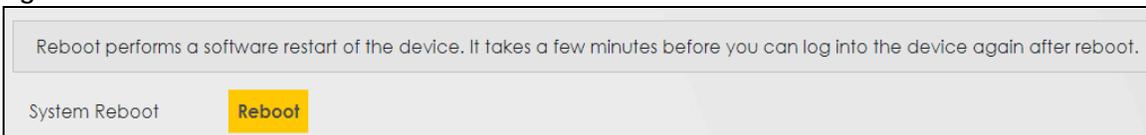
You can also press the **RESET** button on the rear panel to reset the factory defaults of your Zyxel Device. Refer to [Section 1.5.2 on page 33](#) for more information on the **RESET** button.

41.3 The Reboot Screen

System Reboot allows you to reboot the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the Zyxel Device reboot. This does not affect the Zyxel Device's configuration.

Figure 205 Maintenance > Reboot



CHAPTER 42

Diagnostic

42.1 Diagnostic Overview

The **Diagnostic** screens display information to help you identify problems with the Zyxel Device.

The route between a Central Office Very-high-bit-rate Digital Subscriber Line (CO VDSL) switch and one of its Customer-Premises Equipment (CPE) may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

42.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you ping an IP address or trace the route packets take to a host ([Section 42.3 on page 338](#)).
- The **802.1ag** screen lets you perform CFM actions ([Section 42.6 on page 341](#)).
- The **802.3ah** screen lets you configure link OAM port parameters([Section 42.5 on page 340](#)).
- The **OAM Ping** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. ([Section 42.6 on page 341](#)).

42.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.

- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

42.3 Ping & TraceRoute & NsLookup

Use this screen to ping, traceroute, or nslookup an IP address. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking on one of the buttons to start a test, the results will be shown in the Ping/Traceroute Test area. Click **Maintenance > Diagnostic > Ping&TraceRoute&NsLookup** to open the screen shown next.

Figure 206 Maintenance > Diagnostic > Ping&TraceRoute&NsLookup

Ping and TraceRoute are network utilities used to test whether a particular host is reachable. Enter either an IP address or a host name and click one of the buttons to start a Ping or TraceRoute test. The test result will be shown in the Info area.

Ping/TraceRoute Test

TCP/IP

Address

Ping Ping 6 Trace Route Trace Route 6 Nslookup

The following table describes the fields in this screen.

Table 156 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

| LABEL | DESCRIPTION |
|-------------------|---|
| URL or IP Address | Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection. |
| Ping | Click this to ping the IPv4 address that you entered. |
| Ping 6 | Click this to ping the IPv6 address that you entered. |
| Trace Route | Click this to display the route path and transmission delays between the Zyxel Device to the IPv4 address that you entered. |
| Trace Route 6 | Click this to display the route path and transmission delays between the Zyxel Device to the IPv6 address that you entered. |
| Nslookup | Click this button to perform a DNS lookup on the IP address of a computer you enter. |

42.4 The 802.1ag (CFM) Screen

Click **Maintenance > Diagnostic > 802.1ag** to open the following screen. Use this screen to configure and perform Connectivity Fault Management (CFM) actions as defined by the IEEE802.1ag standard. CFM protocols include Continuity Check Protocol (CCP), Link Trace (LT), and Loopback (LB).

Figure 207 Maintenance > Diagnostic > 802.1ag

The following table describes the fields in this screen.

Table 157 Maintenance > Diagnostic > 802.1ag

| LABEL | DESCRIPTION |
|---------------------------------------|--|
| 802.1ag Connectivity Fault Management | |
| IEEE 802.1ag CFM | Click this switch to enable or disable the IEEE802.1ag CFM specification, which allows network administrators to identify and manage connection faults. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Y.1731 | Click this switch to enable or disable Y.1731, which monitors Ethernet performance. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Interface | Select the interface on which you want to enable the IEE 802.1ag CFM. |

Table 157 Maintenance > Diagnostic > 802.1ag (continued)

| LABEL | DESCRIPTION |
|--|--|
| Maintenance Domain (MD) Level | Select a level (0-7) under which you want to create an MA. |
| MD Name | Enter a descriptive name for the MD (Maintenance Domain). |
| MA ID | Enter a descriptive name to identify the Maintenance Association. |
| 802.1Q VLAN ID | Type a VLAN ID (1-4094) for this MA. |
| Local MEP ID | Enter the local Maintenance Endpoint Identifier (1~8191). |
| CCM | Select Enable to continue sending MEP information by CCM (Connectivity Check Messages). When CCMs are received the VMG will always process it, whether CCM is enabled or not. |
| Remote MEP ID | Enter the remote Maintenance Endpoint Identifier (1~8191). |
| Test the connection to another Maintenance End Point (MEP) | |
| Destination MAC Address | Enter the target device's MAC address to which the Zyxel Device performs a CFM loopback and linktrace test. |
| Test Result | |
| Loopback Message (LBM) | This shows Pass if a Loop Back Messages (LBMs) responses are received. If LBMs do not get a response it shows Fail . |
| Linktrace Message (LTM) | This shows the MAC address of MEPs that respond to the LTMs. |
| Apply | Click this button to save your changes. |
| Send Loopback | Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point. |
| Send Linktrace | Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point. |

42.5 The 802.3ah (OAM) Screen

Click **Maintenance > Diagnostic > 803.ah** to open the following screen. Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units (OAM PDU's) to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah.

Figure 208 Maintenance > Diagnostic > 802.3ah

The following table describes the labels in this screen.

Table 158 Maintenance > Diagnostics > 802.3ah

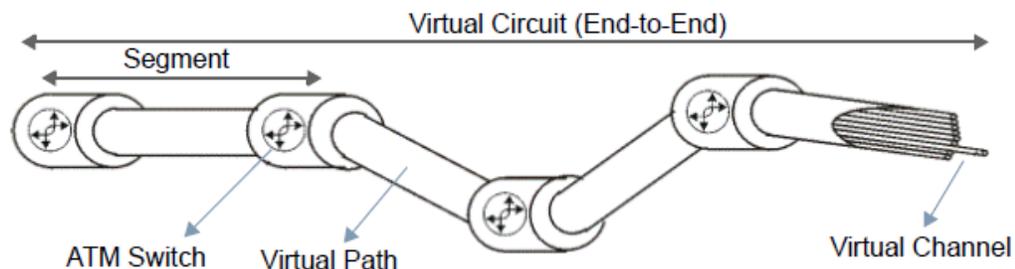
| LABEL | DESCRIPTION |
|---------------------------|--|
| IEEE 802.3ah Ethernet OAM | Click this switch to enable or disable the Ethernet OAM on the specified interface. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Interface | Select the interface on which you want to enable the IEEE802.3ah. |
| OAM ID | Enter a positive integer to identify this node. |
| Auto Event | Click this switch to detect link status and send a notification when an error (such as errors in symbol, frames, or seconds) is detected. Otherwise, disable this and you will not be notified. When the switch turns blue  , the function is enabled. Otherwise, it's not. |
| Features | <p>Select Variable Retrieval so the Zyxel Device can respond to requests for information, such as requests for Ethernet counters and statistics, about link events.</p> <p>Select Link Events so the Zyxel Device can interpret link events, such as link fault and dying asp. Link events are set in event notification PDUs (Protocol Data Units), and indicate when the number of errors in a certain given interval (time, number of frames, number of symbols, or number of errored frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well.</p> <p>Select Remote Loopback so the Zyxel Device can accept loopback control PDUs to convert VMG into loopback mode.</p> <p>Select Active Mode so the Zyxel Device initiates OAM discovery, send information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs.</p> |
| Apply | Click this button to save your changes. |

42.6 The OAM Ping Screen

Click **Maintenance > Diagnostic > OAM Ping** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The Zyxel Device sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the Zyxel Device. The test result then displays in the text box. ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel (VC) Logical connections between ATM devices
- Virtual Path (VP) A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end points

Figure 209 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefined Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the Zyxel Device is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 210 Maintenance > Diagnostic > OAM Ping

The following table describes the fields in this screen.

Table 159 Maintenance > Diagnostic > OAM Ping

| LABEL | DESCRIPTION |
|------------|--|
| | Select a PVC on which you want to perform the loopback test. |
| F4 segment | Press this to perform an OAM F4 segment loopback test. |
| F4 end-end | Press this to perform an OAM F4 end-to-end loopback test. |
| F5 segment | Press this to perform an OAM F5 segment loopback test. |
| F5 end-end | Press this to perform an OAM F5 end-to-end loopback test. |

CHAPTER 43

Troubleshooting

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

- [Power, Hardware Connections, and LEDs](#)
- [Zyxel Device Access and Login](#)
- [Internet Access](#)
- [Wireless Internet Access](#)
- [USB Device Connection](#)
- [UPnP](#)

43.1 Power, Hardware Connections, and LEDs

[The Zyxel Device does not turn on. None of the LEDs turn on.](#)

- 1 Make sure the Zyxel Device is turned on.
- 2 Make sure you are using the power adaptor or cord included with the Zyxel Device.
- 3 Make sure the power adaptor or cord is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the Zyxel Device off and on.
- 5 If the problem continues, contact the vendor.

[One of the LEDs does not behave as expected.](#)

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5 on page 24](#).
- 2 Check the hardware connections.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the Zyxel Device off and on.

- 5 If the problem continues, contact the vendor.

43.2 Zyxel Device Access and Login

I forgot the IP address for the Zyxel Device.

- 1 The default LAN IP address is 192.168.1.1.
 - 2 If you changed the IP address and have forgotten it, you might get the IP address of the Zyxel Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device (it depends on the network), so enter this IP address in your Internet browser.
 - 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.5.2 on page 33](#).
-

I forgot the password.

- 1 See the cover page for the default login names and associated passwords.
 - 2 If those do not work, you have to reset the device to its factory defaults. See [Section 1.5.2 on page 33](#).
-

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

- 1 Make sure you are using the correct IP address.
 - The default IP address is [192.168.1.1](#).
 - If you changed the IP address ([Section 8.2 on page 153](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Zyxel Device](#).
 - 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 1.5 on page 24](#).
 - 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
 - 4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).
 - 5 Reset the device to its factory defaults, and try to access the Zyxel Device with the default IP address. See [Section 1.5.2 on page 33](#).
-

- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

I can see the [Login](#) screen, but I cannot log in to the Zyxel Device.

- 1 Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.
- 3 Turn the Zyxel Device off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 43.1 on page 343](#).

I cannot Telnet to the Zyxel Device.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

43.3 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.5 on page 24](#).

- 2 Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure that you enabled the wireless LAN in the Zyxel Device and your wireless client and that the wireless settings in the wireless client are the same as the settings in the Zyxel Device.
- 4 Disconnect all the cables from your device and reconnect them.
- 5 If the problem continues, contact your ISP.

I cannot access the Internet through a DSL connection.

- 1 Make sure you have the **DSL WAN** port connected to a telephone jack (or the DSL or modem jack on a splitter if you have one).
- 2 Make sure you configured a proper DSL WAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.
- 3 Check that the LAN interface you are connected to is in the same interface group as the DSL connection (**Network Setting > Interface Grouping**).
- 4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a second DSL connection.

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

I cannot connect to the Internet using an Ethernet connection.

- 1 The DSL connection has priority. If the DSL connection is up, then the Ethernet connection will be down.
- 2 Make sure you have the Ethernet WAN port connected to a MODEM or Router.
- 3 Make sure you configured a proper EthernetWAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.
- 4 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting > Interface Group**).
- 5 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a cellular connection.

- 1 The DSL and Ethernet connections have priority in that order. If the DSL or Ethernet connection is up, then the cellular connection will be down.
- 2 Make sure you have connected a compatible cellular dongle to the USB port.
- 3 Make sure you have configured **Network Setting > Broadband > Cellular Backup** correctly.
- 4 Check that the Zyxel Device is within range of a cellular base station.

I cannot access the Zyxel Device anymore. I had access to the Zyxel Device, but my connection is not available anymore.

- 1 Your session with the Zyxel Device may have expired. Try logging into the Zyxel Device again.
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.5 on page 24](#).
- 3 Turn the Zyxel Device off and on.
- 4 If the problem continues, contact your vendor.

43.4 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.

- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

43.5 USB Device Connection

The Zyxel Device fails to detect my USB device.

- 1 Disconnect the USB device.
- 2 Reboot the Zyxel Device.
- 3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
- 4 Re-connect your USB device to the Zyxel Device.

43.6 UPnP

When using UPnP and the Zyxel Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

- 1 Disconnect the Ethernet cable from the Zyxel Device's LAN port or from your computer.
- 2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

PART III

Appendices

Appendices contain general information. Some information may not apply to your device.

APPENDIX A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <http://www.zyxel.com/homepage.shtml> and also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com>

Asia

China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- Zyxel Kazakhstan
- <http://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- Zyxel BY
- <http://www.zyxel.by>

Belgium

- Zyxel Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

Bulgaria

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- Zyxel Communications A/S
- <http://www.zyxel.dk>

Estonia

- Zyxel Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- Zyxel Communications
- <http://www.zyxel.fi>

France

- Zyxel France
- <http://www.zyxel.fr>

Germany

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- Zyxel Hungary & SEE
- <http://www.zyxel.hu>

Italy

- Zyxel Communications Italy
- <http://www.zyxel.it/>

Latvia

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- Zyxel Benelux
- <http://www.zyxel.nl>

Norway

- Zyxel Communications
- <http://www.zyxel.no>

Poland

- Zyxel Communications Poland
- <http://www.zyxel.pl>

Romania

- Zyxel Romania
- <http://www.zyxel.com/ro/ro>

Russia

- Zyxel Russia
- <http://www.zyxel.ru>

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- Zyxel Communications ES Ltd
- <http://www.zyxel.es>

Sweden

- Zyxel Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG

- <http://www.zyxel.ch/>

Turkey

- Zyxel Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Brazil

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Ecuador

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Israel

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

Middle East

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

Oceania

Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

APPENDIX B

Wireless LANs

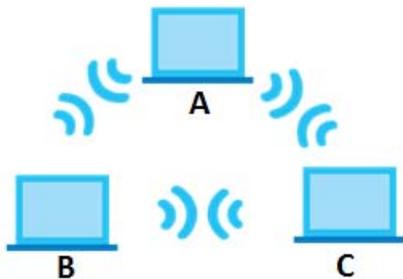
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 211 Peer-to-Peer Communication in an Ad-hoc Network

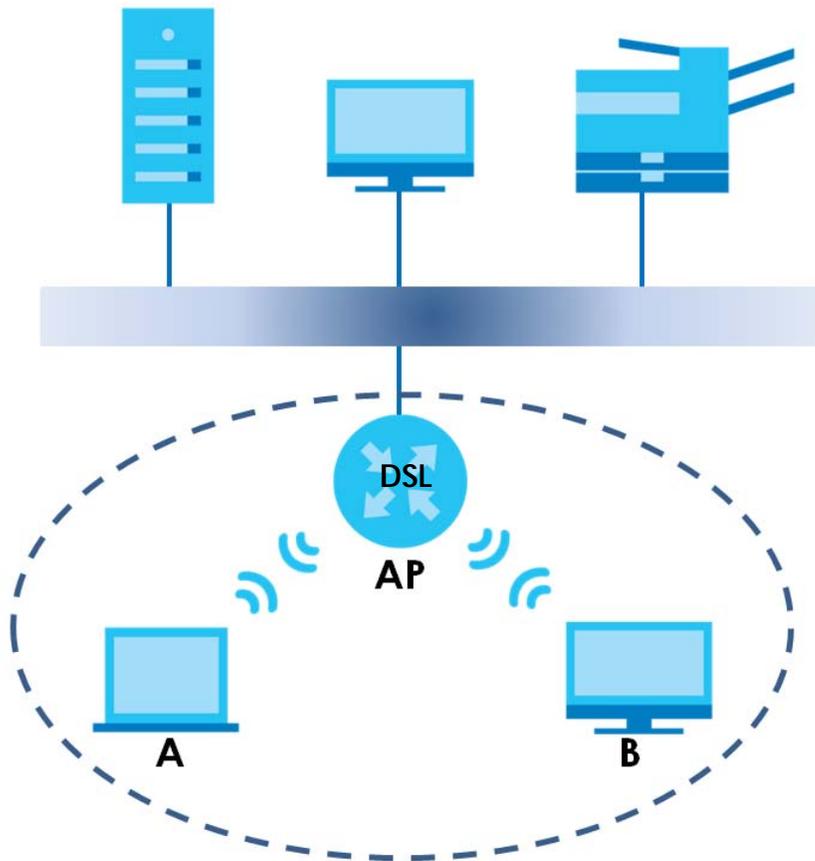


BSS

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

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

Figure 212 Basic Service Set



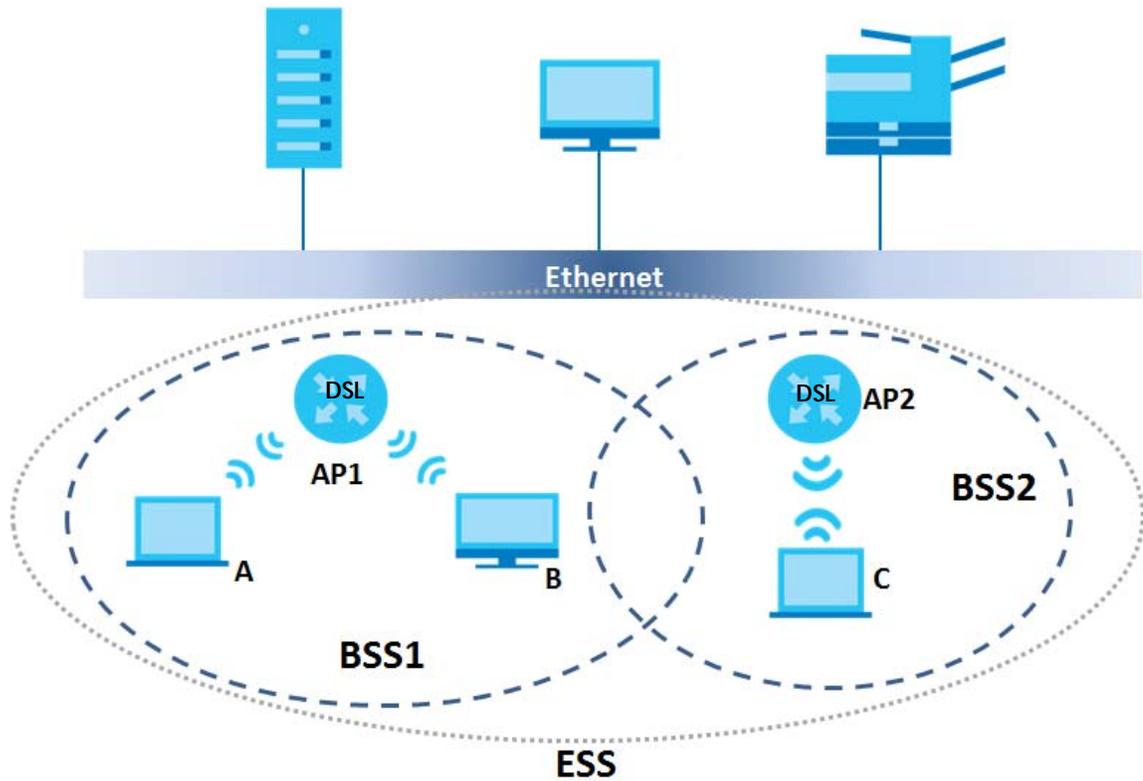
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 213 Infrastructure WLAN



Channel

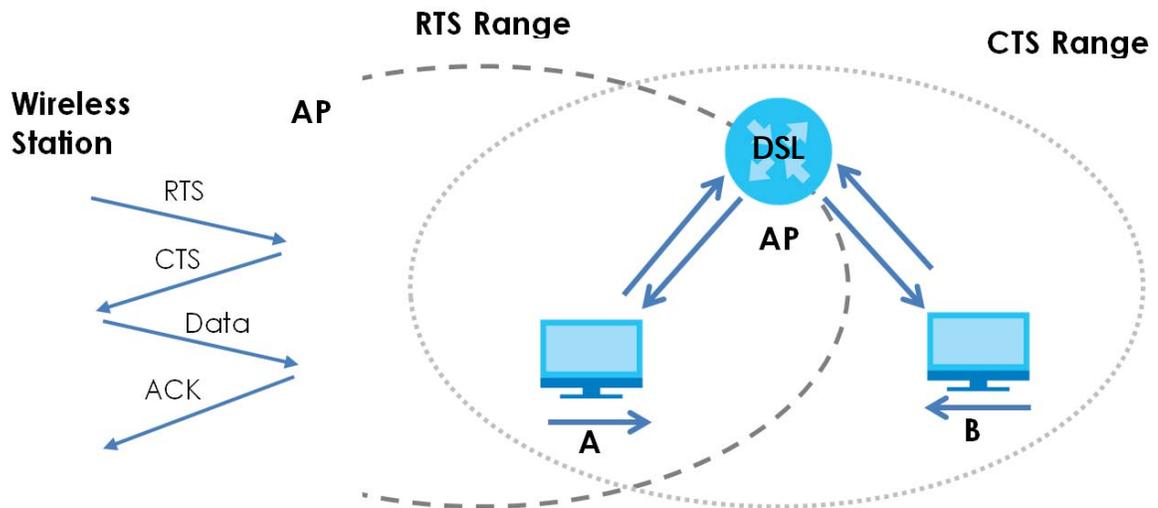
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference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

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 214 RTS/CTS



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

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

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

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

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

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

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

Fragmentation Threshold

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

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

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

IEEE 802.11g Wireless LAN

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

Table 160 IEEE 802.11g

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

Wireless Security Overview

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

Wireless security methods available on the Zyxel Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Zyxel Device identity.

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

Table 161 Wireless Security Levels

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

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

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
Determines the identity of the users.
- Authorization
Determines the network services available to authenticated users once they are connected to the network.
- Accounting
Keeps track of the client's network activity.

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

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
Sent by an access point requesting authentication.
- Access-Reject
Sent by a RADIUS server rejecting access.
- Access-Accept
Sent by a RADIUS server allowing access.
- Access-Challenge
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
Sent by the access point requesting accounting.
- Accounting-Response
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 162 Comparison of EAP Authentication Types

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

WPA and WPA2

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

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

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point,

wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

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

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

Encryption

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

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

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

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

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

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

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

User Authentication

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

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

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

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

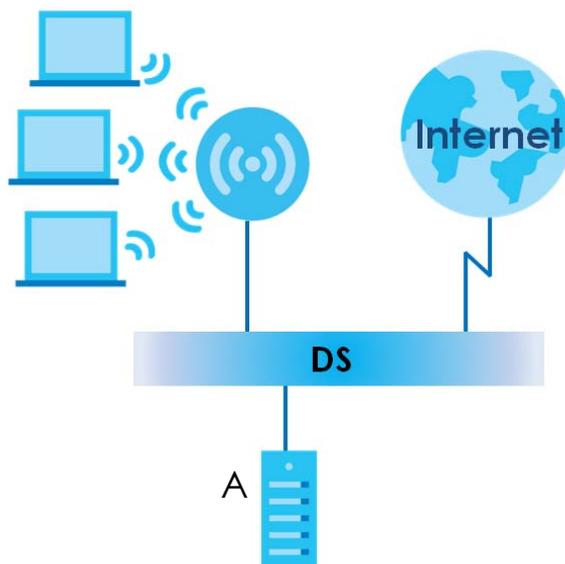
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

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

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

Figure 215 WPA(2) with RADIUS Application Example

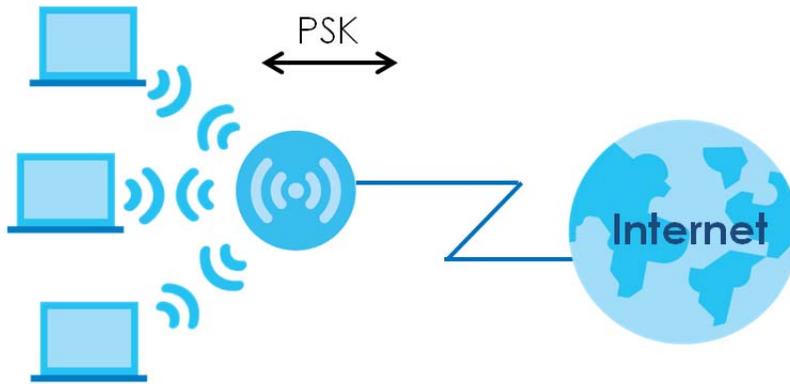


WPA(2)-PSK Application Example

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

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 216 WPA(2)-PSK Authentication



Security Parameters Summary

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

Table 163 Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X |
|--|----------------------|---------------------|--------------------------------|
| Open | None | No | Disable |
| | | | Enable without Dynamic WEP Key |
| Open | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| Shared | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |

Table 163 Wireless Security Relational Matrix (continued)

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X |
|--|----------------------|---------------------|-------------|
| WPA | TKIP/AES | No | Enable |
| WPA-PSK | TKIP/AES | Yes | Disable |
| WPA2 | TKIP/AES | No | Enable |
| WPA2-PSK | TKIP/AES | Yes | Disable |

Antenna Overview

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

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

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

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

Antenna Gain

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

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

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

Types of Antennas for WLAN

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

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.

- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

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

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

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

APPENDIX C

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as “/x” where x is a number. For example,

`2001:db8:1a2b:15::1a2f:0/32`

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of `fe80::/10`. The link-local unicast address format is as follows.

Table 164 Link-local Unicast Address Format

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

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

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

Loopback Address

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

Multicast Address

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

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

Table 165 Predefined Multicast Address

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

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

Table 166 Reserved Multicast Address

| MULTICAST ADDRESS |
|--------------------|
| FF00:0:0:0:0:0:0:0 |
| FF01:0:0:0:0:0:0:0 |
| FF02:0:0:0:0:0:0:0 |
| FF03:0:0:0:0:0:0:0 |
| FF04:0:0:0:0:0:0:0 |
| FF05:0:0:0:0:0:0:0 |
| FF06:0:0:0:0:0:0:0 |
| FF07:0:0:0:0:0:0:0 |
| FF08:0:0:0:0:0:0:0 |
| FF09:0:0:0:0:0:0:0 |
| FF0A:0:0:0:0:0:0:0 |
| FF0B:0:0:0:0:0:0:0 |
| FF0C:0:0:0:0:0:0:0 |
| FF0D:0:0:0:0:0:0:0 |

Table 166 Reserved Multicast Address (continued)

| MULTICAST ADDRESS |
|--------------------|
| FF0E:0:0:0:0:0:0:0 |
| FF0F:0:0:0:0:0:0:0 |

Subnet Masking

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

Interface ID

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

EUI-64

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

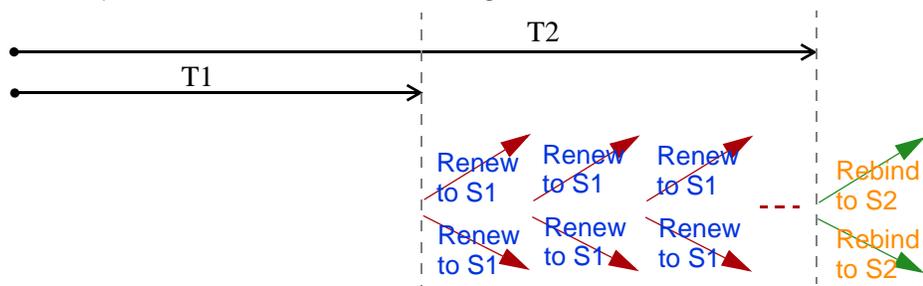
| | |
|--------|---------------------------------------|
| MAC | 00 : 13 : 49 : 12 : 34 : 56 |
| EUI-64 | 02 : 13 : 49 : FF : FE : 12 : 34 : 56 |

Identity Association

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

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

does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

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

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

Prefix Delegation

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

ICMPv6

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

Neighbor Discovery Protocol (NDP)

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

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.

- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

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

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

Multicast Listener Discovery

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

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

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

MLD filtering controls which multicast groups a port can join.

MLD Messages

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

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

Example - Enabling IPv6 on Windows XP/2003/Vista

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

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

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

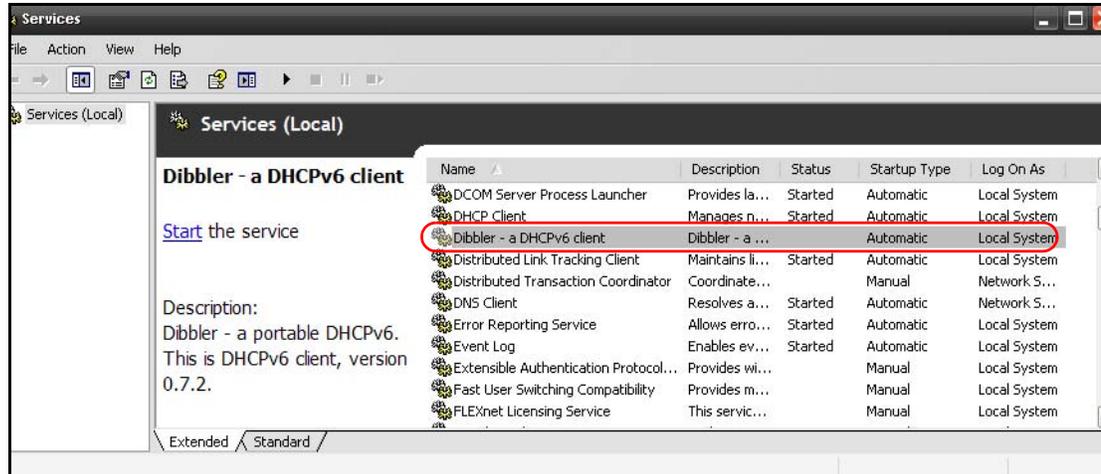
IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

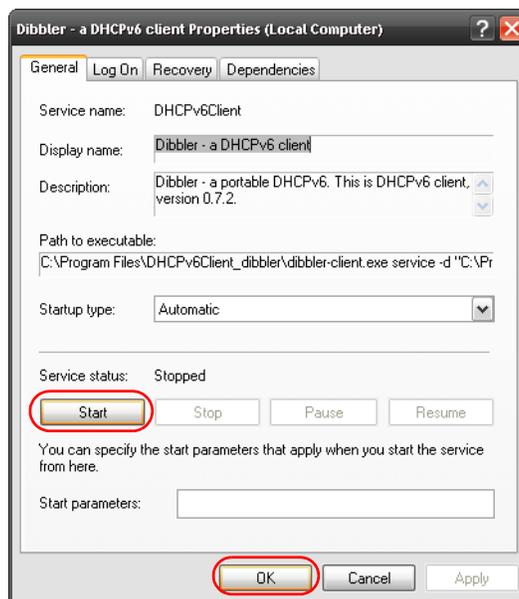
Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

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

- 1 Install Dibbler and select the DHCPv6 client option on your computer.
- 2 After the installation is complete, select **Start > All Programs > Dibbler-DHCPv6 > Client Install as service**.
- 3 Select **Start > Control Panel > Administrative Tools > Services**.
- 4 Double click **Dibbler - a DHCPv6 client**.



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



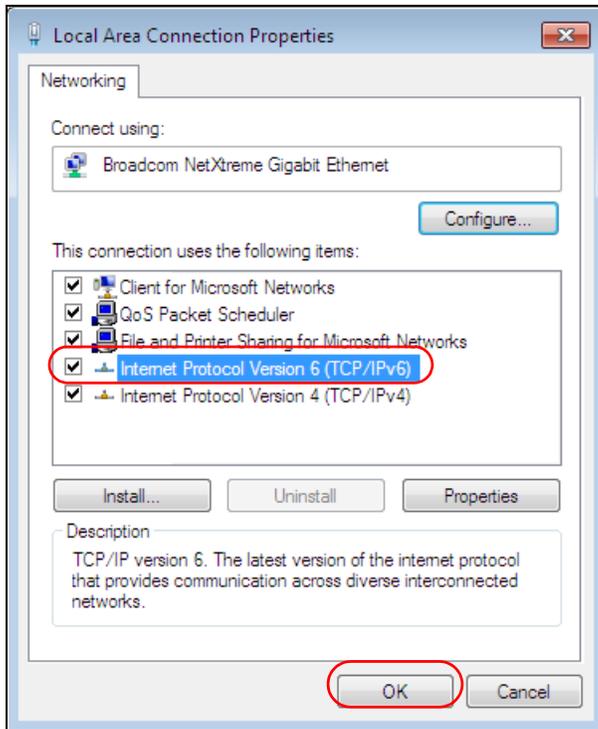
- 6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

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

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

APPENDIX D

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
 - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 167 Examples of Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|--------------------|--|--------------------------|--|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM | TCP | 5190 | AOL's Internet Messenger service. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP/UDP TCP/UDP | 7648 24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers. |
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP | TCP TCP | 20 21 | File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IMAP4 | TCP | 143 | The Internet Message Access Protocol is used for e-mail. |
| IMAP4S | TCP | 993 | This is a more secure version of IMAP4 that runs over SSL. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NetBIOS | TCP/UDP TCP/UDP TCP/UDP TCP/UDP | 137 138 139 445 | The Network Basic Input/Output System is used for communication between computers in a LAN. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |

Table 167 Examples of Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|-------------------|--------------|---------|---|
| NFS | UDP | 2049 | Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| POP3S | TCP | 995 | This is a more secure version of POP3 that runs over SSL. |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| ROADRUNNER | TCP/UDP | 1026 | This is an ISP that provides services mainly for cable modems. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | The Simple File Transfer Protocol is an old way of transferring files between computers. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SMTPS | TCP | 465 | This is a more secure version of SMTP that runs over SSL. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSDP | UDP | 1900 | The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP). |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |

Table 167 Examples of Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|-------------|-----------------|--------------------------|--|
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| VDOLIVE | TCP UDP | 7000 user- defined | A videoconferencing solution. The UDP port number is specified in the application. |

APPENDIX E

Legal Information

Copyright

Copyright © 2018 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

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

Regulatory Notice and Statement

UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
 - Reorient or relocate the receiving antenna
 - Increase the separation between the devices
 - Connect the equipment to an outlet other than the receiver's
 - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

FCC Part 68 Statement

- This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA.
- List all applicable certification jack Universal Service Order Codes ("USOC") for the equipment. USOC JACK: RJ11C (Depend on EUT interface)
- A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

- The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.
- If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
- The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.
- If trouble is experienced with this equipment, for repair or warranty information, please contact Zyxel Communication Inc.; 1130 N Miller street Anaheim, CA 92806-2001, USA ;TEL: 002 +1 714-6320882. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.
- Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.
- If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

CANADA

The following information applies if you use the product within Canada area.

Industry Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

Industry Canada CS-03 Statement

- This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.
- The Ringer Equivalence Number (REN) indicates the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five.

Déclaration de conformité

- Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.
- L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de dispositifs qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme des IES de tous les dispositifs n'exécède pas cinq.

Industry Canada RSS-GEN & RSS-247 statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limits.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio de modèle s'il fait partie du matériel de catégorie I) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION



The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:

VMG3625-T20A

- the band 2,400 to 2,483.5 MHz is 86.3 mW,
- the bands 5,150 MHz to 5,350 MHz is 173 mW,
- the 5,470 MHz to 5,725 MHz is 412 mW.

VMG3925-B10C

- the band 2,400 to 2,483.5 MHz is 97.72 mW,
- the bands 5,150 MHz to 5,350 MHz is 193.29 mW,
- the 5,470 MHz to 5,725 MHz is 939.72 mW.

VMG8823-BX0B

- the band 2,400 to 2,483.5 MHz is 198.609 mW,
- the bands 5,150 MHz to 5,350 MHz is 199,067 mW,
- the 5,470 MHz to 5,725 MHz is 981.748 mW.

VMG8924-B10D

- the band 2,400 to 2,483.5 MHz is 81.85 mW,
- the bands 5,150 MHz to 5,350 MHz is 166,34 mW,
- the 5,470 MHz to 5,725 MHz is 548.28 mW.

VMG1312-B10D

- the band 2,400 to 2,483.5 MHz is 98.4 mW,

VMG3312-T20A

- the band 2,400 to 2,483.5 MHz is 99.08 mW,

VMG3925-B10B

- the band 2,400 to 2,483.5 MHz is 82.6 mW,
- the bands 5,150 MHz to 5,350 MHz is 165.2 mW,
- the 5,470 MHz to 5,725 MHz is 233.88 mW.

VMG3927-B50A, XMG3927-B50A, VMG8825-B50A

- the band 2,400 to 2,483.5 MHz is 92.27 mW,
- the bands 5,150 MHz to 5,350 MHz is 175.79 mW,
- the 5,470 MHz to 5,725 MHz is 845.28 mW.

| | |
|----------------------------------|--|
| <p>Български (Bulgarian)</p> | <p>С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.</p> <p>National Restrictions</p> <ul style="list-style-type: none"> • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails. |
| <p>Español (Spanish)</p> | <p>Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE..</p> |
| <p>Čeština (Czech)</p> | <p>Zyxel tímto prohlašuje, že tento zařízenj je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.</p> |

| | |
|-----------------------------|--|
| Dansk (Danish) | Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. National Restrictions <ul style="list-style-type: none">In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs. |
| Deutsch (German) | Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet. |
| Eesti keel (Estonian) | Käesolevaga kinnitab Zyxel seadme vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. |
| Ελληνικά (Greek) | ΜΕ ΤΗΝ ΠΑΡΟΥΣΙΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ. |
| English | Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. |
| Français (French) | Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE. |
| Hrvatski (Croatian) | Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE. |
| Íslenska (Icelandic) | Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE. |
| Italiano (Italian) | Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. National Restrictions <ul style="list-style-type: none">This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli. |
| Latviešu valoda (Latvian) | Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. National Restrictions <ul style="list-style-type: none">The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv. |
| Lietuvių kalba (Lithuanian) | Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas. |
| Magyar (Hungarian) | Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak. |
| Malti (Maltese) | Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ftigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 2014/53/UE. |
| Nederlands (Dutch) | Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. |
| Polski (Polish) | Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE. |
| Português (Portuguese) | Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE. |
| Română (Romanian) | Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE. |
| Slovenčina (Slovak) | Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ. |
| Slovenščina (Slovene) | Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. |
| Suomi (Finnish) | Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
| Svenska (Swedish) | Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. |
| Norsk (Norwegian) | Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53/EU. |

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.

- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

| COUNTRY | ISO 3166 2 LETTER CODE | COUNTRY | ISO 3166 2 LETTER CODE |
|----------------|------------------------|----------------|------------------------|
| Austria | AT | Liechtenstein | LI |
| Belgium | BE | Lithuania | LT |
| Bulgaria | BG | Luxembourg | LU |
| Croatia | HR | Malta | MT |
| Cyprus | CY | Netherlands | NL |
| Czech Republic | CZ | Norway | NO |
| Denmark | DK | Poland | PL |
| Estonia | EE | Portugal | PT |
| Finland | FI | Romania | RO |
| France | FR | Serbia | RS |
| Germany | DE | Slovakia | SK |
| Greece | GR | Slovenia | SI |
| Hungary | HU | Spain | ES |
| Iceland | IS | Switzerland | CH |
| Ireland | IE | Sweden | SE |
| Italy | IT | Turkey | TR |
| Latvia | LV | United Kingdom | GB |

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adaptor or cord is prohibited. 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.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device.
 - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
 - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Pour réduire les risques d'incendie n'utiliser que des câbles de type 26 AWG ou des câbles de connexion plus épais
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive)" as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to "Wireless" chapter for more detail.)

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 若使用高增益指向性天線，該產品僅應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

| SYMBOL | EXPLANATION |
|---|--|
|  | Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction. |
|  | Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers. |
|  | Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor. |
|  | Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation. |

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

Zyxel Limited Warranty

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

Note

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

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

Registration

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

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

A

ACK message [282](#)
ACL rule [240](#)
activation
 firewalls [236](#)
 media server [232](#)
 SIP ALG [205](#)
 SSID [126](#)
Address Resolution Protocol [301](#)
antenna
 directional [368](#)
 gain [367](#)
 omni-directional [367](#)
AP (access point) [358](#)
applications
 Internet access [18](#)
 media server [231](#)
 activation [232](#)
 iTunes server [231](#)
applications, NAT [210](#)
ARP Table [301](#), [303](#)
authentication [140](#), [141](#)
 RADIUS server [141](#)

B

backup
 configuration [334](#)
Basic Service Set, See BSS [356](#)
Basic Service Set, see BSS
blinking LEDs [24](#)
Broadband [93](#)
broadcast [119](#)
BSS [142](#), [356](#)
 example [143](#)
BYE request [282](#)

C

CA [254](#), [362](#)
call history [277](#)
call hold [288](#), [289](#)
call service mode [287](#), [289](#)
call transfer [288](#), [289](#)
call waiting [288](#), [289](#)
Canonical Format Indicator See CFI
CCMs [337](#)
certificate
 factory default [255](#)
Certificate Authority
 See CA.
certificates [254](#)
 authentication [254](#)
 CA
 creating [255](#)
 public key [254](#)
 replacing [255](#)
 storage space [255](#)
Certification Authority [254](#)
Certification Authority, see CA
certifications [385](#)
 viewing [387](#)
CFI [119](#)
CFM [337](#)
 CCMs [337](#)
 link trace test [338](#)
 loopback test [337](#)
 MA [337](#)
 MD [337](#)
 MEP [337](#)
 MIP [337](#)
channel [358](#)
 interference [358](#)
channel, wireless LAN [139](#)
Class of Service [286](#)
Class of Service, see CoS
client list [157](#)
client-server protocol [279](#)

comfort noise generation [284](#)
 configuration
 backup [334](#)
 firewalls [236](#)
 reset [335](#)
 restoring [335](#)
 static route [169, 171, 214](#)

Connectivity Check Messages, see CCMs

contact information [350](#)

copyright [381](#)

CoS [191, 286](#)

CoS technologies [177](#)

creating certificates [255](#)

CTS (Clear to Send) [359](#)

CTS threshold [134, 140](#)

customer support [350](#)

D

data fragment threshold [134, 140](#)

DDoS [236](#)

default server address [204](#)

Denials of Service, see DoS

DHCP [152, 165](#)

differentiated services [286](#)

Differentiated Services, see DiffServ [191](#)

DiffServ [191](#)

 marking rule [191](#)

DiffServ (Differentiated Services) [286](#)

 code points [286](#)

 marking rule [286](#)

digital IDs [254](#)

disclaimer [381](#)

DLNA [231](#)

DMZ [204](#)

DNS [152, 166](#)

DNS server address assignment [119](#)

Domain Name [211](#)

Domain Name System, see DNS

Domain Name System. See DNS.

DoS [236](#)

DS field [191, 286](#)

DS, dee differentiated services

DSCP [191, 286](#)

dynamic DNS [213](#)

 wildcard [213](#)

Dynamic Host Configuration Protocol, see DHCP

dynamic WEP key exchange [363](#)

DYNDNS wildcard [213](#)

E

EAP Authentication [362](#)

ECHO [211](#)

echo cancellation [284](#)

e-mail

 log example [329](#)

Encapsulation [116](#)

 MER [116](#)

 PPP over Ethernet [116](#)

encapsulation

 RFC 1483 [116](#)

encryption [142, 364](#)

ESS [357](#)

Europe type call service mode [287](#)

Extended Service Set IDentification [123, 128](#)

Extended Service Set, See ESS [357](#)

F

Fast Leave [219](#)

file sharing [21](#)

filters

 MAC address [129, 141](#)

Finger [211](#)

firewalls [235](#)

 add protocols [237](#)

 configuration [236](#)

 DDoS [236](#)

 DoS [236](#)

 LAND attack [236](#)

 Ping of Death [236](#)

 SYN attack [236](#)

firmware [331](#)

 version [83](#)

flash key [287](#)

flashing [287](#)
forwarding ports [196](#)
fragmentation threshold [134](#), [140](#), [359](#)
FTP [196](#), [211](#)

G

G.168 [284](#)

H

hidden node [358](#)
HTTP [211](#)

I

IBSS [356](#)
ICMPv6 [217](#)
IEEE 802.11g [360](#)
IEEE 802.1Q [119](#)
IGA [208](#)
IGMP [119](#)
 multicast group list [217](#), [305](#), [306](#)
 version [119](#)
IGMP Fast Leave [217](#)
IGMPv2 [217](#)
IGMPv3 [217](#)
ILA [208](#)
Independent Basic Service Set
 See IBSS [356](#)
initialization vector (IV) [364](#)
Inside Global Address, see IGA
Inside Local Address, see ILA
interface group [222](#)
Internet
 wizard setup [42](#)
Internet access [18](#)
 wizard setup [42](#)
Internet Protocol version 6 [94](#)
Internet Protocol version 6, see IPv6
Intra LAN Multicast [219](#)

IP address [152](#), [166](#)
 ping [338](#)
 private [167](#)
 WAN [94](#)
IP Address Assignment [118](#)
IP alias
 NAT applications [211](#)
IPv6 [94](#), [369](#)
 addressing [95](#), [120](#), [369](#)
 EUI-64 [371](#)
 global address [369](#)
 interface ID [371](#)
 link-local address [369](#)
 Neighbor Discovery Protocol [369](#)
 ping [369](#)
 prefix [95](#), [120](#), [369](#)
 prefix delegation [97](#)
 prefix length [95](#), [120](#), [369](#)
 unspecified address [370](#)
iTunes server [231](#)
ITU-T [284](#)

K

key combinations [290](#)
keypad [290](#)

L

LAN [151](#)
 client list [157](#)
 DHCP [152](#), [165](#)
 DNS [152](#), [166](#)
 IP address [152](#), [153](#), [166](#)
 MAC address [158](#)
 status [84](#), [89](#)
 subnet mask [152](#), [153](#), [166](#)
LAN to LAN multicast [219](#)
LAND attack [236](#)
LBR [337](#)
limitations
 wireless LAN [142](#)
 WPS [149](#)
link trace [338](#)

Link Trace Message, see LTM
 Link Trace Response, see LTR
 listening port [270](#)
 login [34](#)
 passwords [34](#)
 logs [291](#), [294](#), [305](#), [311](#), [327](#)
 Loop Back Response, see LBR
 loopback [337](#)
 LTM [338](#)
 LTR [338](#)

M

MA [337](#)
 MAC address [130](#), [158](#)
 filter [129](#), [141](#)
 MAC authentication [129](#)
 Mac filter [244](#)
 Maintenance Association, see MA
 Maintenance Domain, see MD
 Maintenance End Point, see MEP
 managing the device
 good habits [23](#)
 Maximum Burst Size (MBS) [117](#)
 MBSSID [143](#)
 MD [337](#)
 media server [231](#)
 activation [232](#)
 iTunes server [231](#)
 MEP [337](#)
 MLD [217](#)
 MLDv1 [217](#)
 MLDv2 [217](#)
 MTU (Multi-Tenant Unit) [118](#)
 multicast [119](#)
 Multicast Listener Discovery, see MLD
 multimedia [278](#)
 Multiple BSS, see MBSSID
 multiplexing [116](#)
 LLC-based [117](#)
 VC-based [117](#)
 multiprotocol encapsulation [116](#)

N

NAT [195](#), [197](#), [208](#), [209](#)
 applications [210](#)
 IP alias [211](#)
 example [210](#)
 global [209](#)
 IGA [208](#)
 ILA [208](#)
 inside [208](#)
 local [209](#)
 outside [208](#)
 port forwarding [196](#)
 port number [211](#)
 services [211](#)
 SIP ALG [204](#)
 activation [205](#)
 NAT example [212](#)
 Network Address Translation, see NAT
 Network Map [81](#)
 network map [37](#)
 NNTP [211](#)
 non-proxy calls [275](#)

O

OK response [282](#), [284](#)

P

Pairwise Master Key (PMK) [364](#), [366](#)
 passwords [34](#)
 PBC [144](#)
 Peak Cell Rate (PCR) [117](#)
 peer-to-peer calls [275](#)
 Per-Hop Behavior, see PHB [191](#)
 PHB [191](#), [286](#)
 phone book
 speed dial [275](#)
 phone functions [290](#)
 PIN, WPS [145](#)
 example [146](#)
 Ping of Death [236](#)

Point-to-Point Tunneling Protocol, see PPTP

POP3 [211](#)

port forwarding [196](#)

ports [24](#)

PPPoE [116](#)

 Benefits [116](#)

PPTP [211](#)

preamble [135, 140](#)

preamble mode [143](#)

prefix delegation [97](#)

private IP address [167](#)

PSK [364](#)

push button [32](#)

Push Button Configuration, see PBC

push button, WPS [144](#)

Q

QoS [176, 191, 286](#)

 marking [177](#)

 setup [176](#)

 tagging [177](#)

 versus CoS [177](#)

Quality of Service, see QoS

R

RADIUS [361](#)

 message types [361](#)

 messages [361](#)

 shared secret key [362](#)

RADIUS server [141](#)

Real time Transport Protocol, see RTP

reset [33, 335](#)

restart [336](#)

restoring configuration [335](#)

RFC 1058. See RIP.

RFC 1389. See RIP.

RFC 1483 [116](#)

RFC 1889 [281](#)

RFC 3164 [291](#)

RIP [174](#)

router features [18](#)

Routing Information Protocol. See RIP

RTP [281](#)

RTS (Request To Send) [359](#)

 threshold [358, 359](#)

RTS threshold [134, 140](#)

S

security

 wireless LAN [140](#)

Security Log [292](#)

Security Parameter Index, see SPI

service access control [317](#)

Service Set [123, 128](#)

Services [211](#)

Session Initiation Protocol, see SIP

setup

 firewalls [236](#)

 static route [169, 171, 214](#)

silence suppression [284](#)

Single Rate Three Color Marker, see srTCM

SIP [278](#)

 account [278](#)

 call progression [281](#)

 client [279](#)

 identities [278](#)

 INVITE request [282, 283](#)

 number [278](#)

 OK response [284](#)

 proxy server [280](#)

 redirect server [280](#)

 register server [281](#)

 servers [279](#)

 service domain [279](#)

 URI [278](#)

 user agent [279](#)

SIP ALG [204](#)

 activation [205](#)

SMTP [211](#)

SNMP [211](#)

SNMP trap [211](#)

speed dial [275](#)

SPI [236](#)

srTCM [193](#)

SSID **141**
 activation **126**
 MBSSID **143**

static route **168, 174**
 configuration **169, 171, 214**
 example **168**

static VLAN

status **81**
 firmware version **83**
 LAN **84, 89**
 WAN **83**
 wireless LAN **84**

status indicators **24**

subnet mask **152, 166**

supplementary services **286**

Sustained Cell Rate (SCR) **117**

SYN attack **236**

syslog
 protocol **291**
 severity levels **291**

system
 firmware **331**
 version **83**
 passwords **34**
 reset **33**
 status **81**
 LAN **84, 89**
 WAN **83**
 wireless LAN **84**
 time **323**

T

Tag Control Information See TCI

Tag Protocol Identifier See TPID

TCI

The **94**

three-way conference **289, 290**

thresholds
 data fragment **134, 140**
 RTS/CTS **134, 140**

time **323**

ToS **286**

TPID **119**

traffic shaping **117**

trTCM **194**

Two Rate Three Color Marker, see trTCM

Type of Service, see ToS

U

unicast **119**

Uniform Resource Identifier **278**

Universal Plug and Play, see UPnP

upgrading firmware **331**

UPnP **159**
 cautions **153**
 NAT traversal **152**

USA type call service mode **289**

USB features **21**

V

VAD **284**

Vendor ID **163**

VID

Virtual Circuit (VC) **116**

Virtual Local Area Network See VLAN

VLAN **118**
 Introduction **118**
 number of possible VIDs
 priority frame
 static

VLAN ID **119**

VLAN Identifier See VID

VLAN tag **119**

voice activity detection **284**

voice coding **284**

VoIP **278**
 peer-to-peer calls **275**

VoIP features **22**

VoIP status **298**

W

Wake on LAN **163**

- WAN
 - status [83](#)
 - Wide Area Network, see WAN [93](#)
 - warranty [387](#)
 - note [387](#)
 - web configurator
 - login [34](#)
 - passwords [34](#)
 - WEP Encryption [125](#)
 - Wi-Fi Protected Access [363](#)
 - wireless client WPA supplicants [365](#)
 - wireless LAN [121, 138](#)
 - authentication [140, 141](#)
 - BSS [142](#)
 - example [143](#)
 - channel [139](#)
 - encryption [142](#)
 - example [139](#)
 - fragmentation threshold [134, 140](#)
 - limitations [142](#)
 - MAC address filter [129, 141](#)
 - MBSSID [143](#)
 - preamble [135, 140](#)
 - RADIUS server [141](#)
 - RTS/CTS threshold [134, 140](#)
 - security [140](#)
 - SSID [141](#)
 - activation [126](#)
 - status [84](#)
 - WPS [144, 146](#)
 - example [147](#)
 - limitations [149](#)
 - PIN [145](#)
 - push button [32, 144](#)
 - wireless security [360](#)
 - Wireless tutorial [54](#)
 - wizard setup
 - Internet [42](#)
 - WLAN
 - interference [358](#)
 - security parameters [366](#)
 - WPA [363](#)
 - key caching [365](#)
 - pre-authentication [365](#)
 - user authentication [364](#)
 - vs WPA-PSK [364](#)
 - wireless client supplicant [365](#)
 - with RADIUS application example [365](#)
 - WPA2 [363](#)
 - user authentication [364](#)
 - vs WPA2-PSK [364](#)
 - wireless client supplicant [365](#)
 - with RADIUS application example [365](#)
 - WPA2-Pre-Shared Key [363](#)
 - WPA2-PSK [363, 364](#)
 - application example [366](#)
 - WPA-PSK [364](#)
 - application example [366](#)
 - WPS [144, 146](#)
 - example [147](#)
 - limitations [149](#)
 - PIN [145](#)
 - example [146](#)
 - push button [32, 144](#)
- ## Z
- ZyXEL Family Safety page [250](#)