



VMG4381-B10A

Wireless N VDSL2 4-port Bonding Combo WAN Gigabit Gateway
with MoCA

Version 1.0
Edition 2, 05/2014



User's Guide

Default Login Details

LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Note: This guide is a reference for a series of products. Therefore some features or options in this guide may not be available in your product.

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

Related Documentation

- Quick Start Guide

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

- Support Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

Please refer to www.zyxel.com for additional support documentation and product certifications.

Contents Overview

User's Guide	15
Introducing the Device	17
The Web Configurator	25
Quick Start	33
Tutorials	35
Technical Reference	69
Network Map and Status Screens	71
Broadband	75
Wireless	101
Home Networking	133
Routing	157
Quality of Service (QoS)	163
Network Address Translation (NAT)	181
Dynamic DNS Setup	197
Interface Group	201
USB Service	207
Firewall	213
MAC Filter	223
Parental Control	227
Scheduler Rules	231
Certificates	233
Log	241
Traffic Status	245
ARP Table	249
Routing Table	251
IGMP Status	253
xDSL Statistics	255
User Account	259
Remote Management	261
TR-069 Client	263
TR-064	265
Time Settings	267
E-mail Notification	271
Logs Setting	273
Firmware Upgrade	277
Configuration	279
Diagnostic	282

Troubleshooting287

Table of Contents

Contents Overview	3
Table of Contents	5
Part I: User's Guide	15
Chapter 1	
Introducing the Device	17
1.1 Overview	17
1.2 Ways to Manage the Device	17
1.3 Good Habits for Managing the Device	17
1.4 Applications for the Device	18
1.4.1 Internet Access	18
1.4.2 HomePNA	19
1.4.3 Device's USB Support	20
1.5 LEDs (Lights)	21
1.6 The RESET Button	22
1.7 Wireless Access	23
1.7.1 Using the WLAN/WPS Button	23
Chapter 2	
The Web Configurator	25
2.1 Overview	25
2.1.1 Accessing the Web Configurator	25
2.2 Web Configurator Layout	28
2.2.1 Title Bar	28
2.2.2 Main Window	29
2.2.3 Navigation Panel	29
Chapter 3	
Quick Start	33
3.1 Overview	33
3.2 Quick Start Setup	33
Chapter 4	
Tutorials	35
4.1 Overview	35
4.2 Setting Up an ADSL PPPoE Connection	35

4.3 Setting Up a Secure Wireless Network	38
4.3.1 Configuring the Wireless Network Settings	38
4.3.2 Using WPS	40
4.3.3 Without WPS	43
4.4 Setting Up Multiple Wireless Groups	44
4.5 Configuring Static Route for Routing to Another Network	47
4.6 Configuring QoS Queue and Class Setup	50
4.7 Access the Device Using DDNS	53
4.7.1 Registering a DDNS Account on www.dyndns.org	53
4.7.2 Configuring DDNS on Your Device	54
4.7.3 Testing the DDNS Setting	54
4.8 Configuring the MAC Address Filter	54
4.9 Access Your Shared Files From a Computer	56
4.10 Using the Media Server Feature	57
4.10.1 Configuring the Device	57
4.10.2 Using Windows Media Player	57
4.10.3 Using a Digital Media Adapter	60
4.11 Using the Print Server Feature	62

Part II: Technical Reference..... 69

**Chapter 5
Network Map and Status Screens 71**

5.1 Overview	71
5.2 The Network Map Screen	71
5.3 The Status Screen	72

**Chapter 6
Broadband..... 75**

6.1 Overview	75
6.1.1 What You Can Do in this Chapter	75
6.1.2 What You Need to Know	76
6.1.3 Before You Begin	79
6.2 The Broadband Screen	79
6.2.1 Add/Edit Internet Connection	81
6.3 The 3G Backup Screen	89
6.4 The Advanced Screen	93
6.4.1 DSL Bonding	93
6.5 The 8021x Screen	95
6.5.1 Edit 802.1x Settings	96
6.6 Technical Reference	96

Chapter 7	
Wireless	101
7.1 Overview	101
7.1.1 What You Can Do in this Chapter	101
7.1.2 What You Need to Know	102
7.2 The General Screen	102
7.2.1 No Security	105
7.2.2 Basic (WEP Encryption)	105
7.2.3 More Secure (WPA(2)-PSK)	107
7.2.4 WPA(2) Authentication	108
7.3 The More AP Screen	109
7.3.1 Edit More AP	110
7.4 MAC Authentication	111
7.5 The WPS Screen	112
7.6 The WMM Screen	114
7.7 The WDS Screen	114
7.7.1 WDS Scan	115
7.8 The Others Screen	116
7.9 The Channel Status Screen	118
7.10 Technical Reference	118
7.10.1 Wireless Network Overview	118
7.10.2 Additional Wireless Terms	120
7.10.3 Wireless Security Overview	120
7.10.4 Signal Problems	122
7.10.5 BSS	123
7.10.6 MBSSID	123
7.10.7 Preamble Type	124
7.10.8 Wireless Distribution System (WDS)	124
7.10.9 WiFi Protected Setup (WPS)	124
Chapter 8	
Home Networking	133
8.1 Overview	133
8.1.1 What You Can Do in this Chapter	133
8.1.2 What You Need To Know	134
8.1.3 Before You Begin	135
8.2 The LAN Setup Screen	135
8.3 The Static DHCP Screen	138
8.4 The UPnP Screen	140
8.5 Installing UPnP in Windows Example	141
8.6 Using UPnP in Windows XP Example	143
8.7 The Additional Subnet Screen	149
8.8 The STB Vendor ID Screen	150

8.9 The 5th Ethernet Port Screen	150
8.10 The MoCA Screen	151
8.11 The LAN VLAN Screen	152
8.12 TFTP Server Name Screen	152
8.13 Technical Reference	153
8.13.1 LANs, WANs and the Device	153
8.13.2 DHCP Setup	153
8.13.3 DNS Server Addresses	154
8.13.4 LAN TCP/IP	154
Chapter 9	
Routing	157
9.1 Overview	157
9.1.1 What You Can Do in this Chapter	157
9.2 The Routing Screen	158
9.2.1 Add/Edit Static Route	158
9.3 The Policy Forwarding Screen	159
9.3.1 Add/Edit Policy Forwarding	160
9.4 The RIP Screen	161
Chapter 10	
Quality of Service (QoS).....	163
10.1 Overview	163
10.1.1 What You Can Do in this Chapter	163
10.2 What You Need to Know	164
10.3 The Quality of Service General Screen	165
10.4 The Queue Setup Screen	166
10.4.1 Adding a QoS Queue	168
10.5 The Class Setup Screen	168
10.5.1 Add/Edit QoS Class	169
10.6 The QoS Policer Setup Screen	173
10.6.1 Add/Edit a QoS Policer	174
10.7 The QoS Monitor Screen	175
10.8 Technical Reference	176
Chapter 11	
Network Address Translation (NAT).....	181
11.1 Overview	181
11.1.1 What You Can Do in this Chapter	181
11.1.2 What You Need To Know	181
11.2 The Port Forwarding Screen	182
11.2.1 Add/Edit Port Forwarding	184
11.3 The Applications Screen	185

11.3.1 Add New Application	185
11.4 The Port Triggering Screen	186
11.4.1 Add/Edit Port Triggering Rule	188
11.5 The DMZ Screen	189
11.6 The ALG Screen	190
11.7 The Address Mapping Screen	190
11.7.1 Add/Edit Address Mapping Rule	191
11.8 Technical Reference	192
11.8.1 NAT Definitions	192
11.8.2 What NAT Does	193
11.8.3 How NAT Works	194
11.8.4 NAT Application	194
Chapter 12	
Dynamic DNS Setup	197
12.1 Overview	197
12.1.1 What You Can Do in this Chapter	197
12.1.2 What You Need To Know	198
12.2 The DNS Entry Screen	198
12.2.1 Add/Edit DNS Entry	198
12.3 The Dynamic DNS Screen	199
Chapter 13	
Interface Group	201
13.1 Overview	201
13.1.1 What You Can Do in this Chapter	201
13.2 The Interface Group Screen	201
13.2.1 Interface Group Configuration	202
13.2.2 Interface Grouping Criteria	204
Chapter 14	
USB Service	207
14.1 Overview	207
14.1.1 What You Can Do in this Chapter	207
14.1.2 What You Need To Know	207
14.2 The File Sharing Screen	208
14.2.1 Before You Begin	209
14.3 The Media Server Screen	210
14.4 The Printer Server Screen	211
14.4.1 Before You Begin	211
Chapter 15	
Firewall	213

15.1 Overview	213
15.1.1 What You Can Do in this Chapter	213
15.1.2 What You Need to Know	214
15.2 The Firewall Screen	215
15.3 The Service Screen	215
15.3.1 Add/Edit a Service	216
15.4 The Access Control Screen	217
15.4.1 Add/Edit an ACL Rule	218
15.5 The DoS Screen	220
Chapter 16	
MAC Filter	223
16.1 Overview	223
16.2 The MAC Filter Screen	224
Chapter 17	
Parental Control	227
17.1 Overview	227
17.2 The Parental Control Screen	227
17.2.1 Add/Edit a Parental Control Rule	228
Chapter 18	
Scheduler Rules.....	231
18.1 Overview	231
18.2 The Scheduler Rules Screen	231
18.2.1 Add/Edit a Schedule	231
Chapter 19	
Certificates	233
19.1 Overview	233
19.1.1 What You Can Do in this Chapter	233
19.2 What You Need to Know	233
19.3 The Local Certificates Screen	233
19.3.1 Create Certificate Request	234
19.3.2 Load Signed Certificate	236
19.4 The Trusted CA Screen	237
19.4.1 View Trusted CA Certificate	237
19.4.2 Import Trusted CA Certificate	238
Chapter 20	
Log	241
20.1 Overview	241
20.1.1 What You Can Do in this Chapter	241

20.1.2 What You Need To Know	241
20.2 The System Log Screen	242
20.3 The Security Log Screen	243
Chapter 21	
Traffic Status	245
21.1 Overview	245
21.1.1 What You Can Do in this Chapter	245
21.2 The WAN Status Screen	245
21.3 The LAN Status Screen	246
Chapter 22	
ARP Table	249
22.1 Overview	249
22.1.1 How ARP Works	249
22.2 ARP Table Screen	249
Chapter 23	
Routing Table	251
23.1 Overview	251
23.2 The Routing Table Screen	251
Chapter 24	
IGMP Status	253
24.1 Overview	253
24.2 The IGMP Group Status Screen	253
Chapter 25	
xDSL Statistics	255
25.1 The xDSL Statistics Screen	255
Chapter 26	
User Account	259
26.1 Overview	259
26.2 The User Account Screen	259
Chapter 27	
Remote Management	261
27.1 Overview	261
27.2 The Remote MGMT Screen	261
Chapter 28	
TR-069 Client	263

28.1 Overview	263
28.2 The TR-069 Client Screen	263
Chapter 29	
TR-064.....	265
29.1 Overview	265
29.2 The TR-064 Screen	265
Chapter 30	
Time Settings	267
30.1 Overview	267
30.2 The Time Screen	267
Chapter 31	
E-mail Notification	271
31.1 Overview	271
31.2 The Email Notification Screen	271
31.2.1 Email Notification Edit	271
Chapter 32	
Logs Setting	273
32.1 Overview	273
32.2 The Log Settings Screen	273
32.2.1 Example E-mail Log	274
Chapter 33	
Firmware Upgrade	277
33.1 Overview	277
33.2 The Firmware Screen	277
Chapter 34	
Configuration	279
34.1 Overview	279
34.2 The Configuration Screen	279
34.3 The Reboot Screen	281
Chapter 35	
Diagnostic	282
35.1 Overview	282
35.1.1 What You Can Do in this Chapter	282
35.2 What You Need to Know	282
35.3 Ping & TraceRoute & Nslookup	283
35.4 802.1ag	283

35.5 OAM Ping Test	285
Chapter 36	
Troubleshooting.....	287
36.1 Power, Hardware Connections, and LEDs	287
36.2 Device Access and Login	288
36.3 Internet Access	290
36.4 Wireless Internet Access	291
36.5 USB Device Connection	292
36.6 UPnP	292
Appendix A Setting up Your Computer's IP Address.....	295
Appendix B IP Addresses and Subnetting.....	315
Appendix C Pop-up Windows, JavaScripts and Java Permissions	323
Appendix D Wireless LANs.....	331
Appendix E IPv6	345
Appendix F Services.....	353
Appendix G Legal Information	357
Index	361

PART I

User's Guide

Introducing the Device

1.1 Overview

The Device is a wireless VDSL router and Gigabit Ethernet gateway. It has two DSL ports and Gigabit Ethernet for super-fast Internet access over analog (POTS) telephone lines. If the DSLAM of the ISP supports bonding function, the two DSL ports on the Device can be connected to two separate telephone jacks to provide increased throughput at longer distances. The Device supports both Packet Transfer Mode (PTM) and Asynchronous Transfer Mode (ATM). It is backward compatible with ADSL, ADSL2 and ADSL2+ in case VDSL is not available. The Device also provides IEEE 802.11b/g/n wireless networking to extend the range of your existing wired network without additional wiring. The VMG4381θ-B10A models also include Home Phoneline

- VMG4381θ-B10A has Home Phoneline Networking Alliance (HPNA) [and Multimedia over Coax Alliance \(moCA\) capabilities](#).

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

The Device has a USB port used to share files via a USB memory stick or a USB hard drive.

1.2 Ways to Manage the Device

Use any of the following methods to manage the Device.

- Web Configurator. This is recommended for everyday management of the Device using a (supported) web browser.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the Device

Do the following things regularly to make the Device more secure and to manage the 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 Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Device. You could simply restore your last configuration.

1.4 Applications for the Device

Here are some example uses for which the Device is well suited.

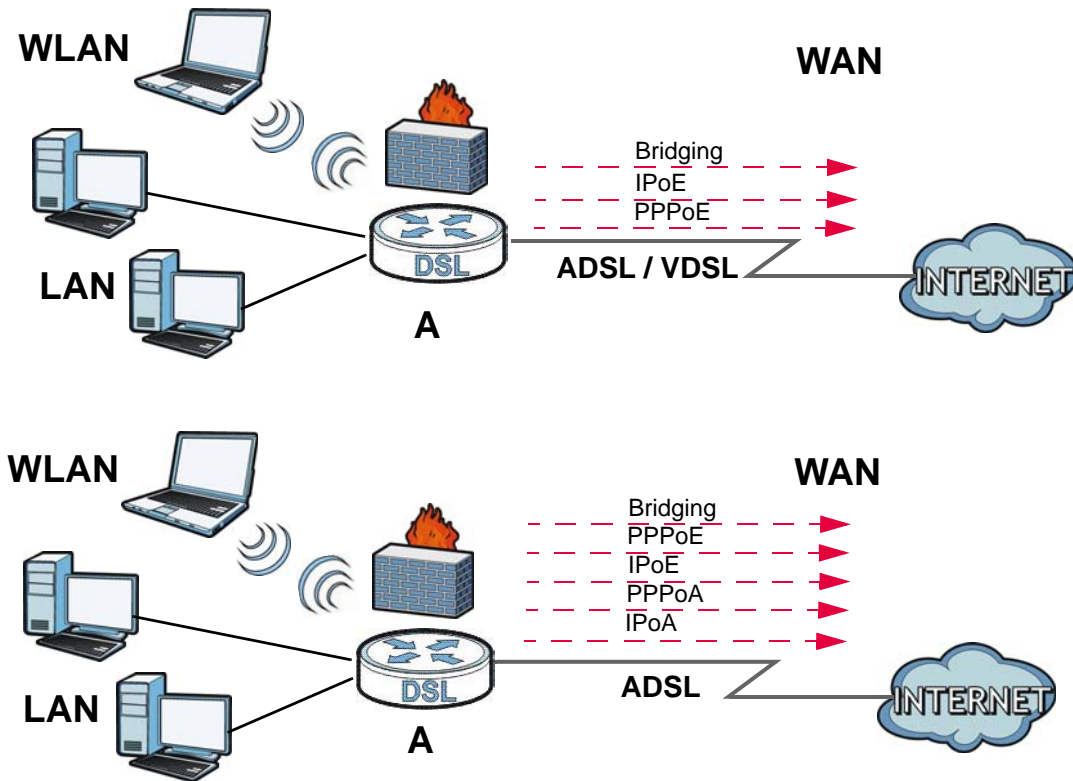
1.4.1 Internet Access

Your 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 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 Device. Refer to [Section 6.2 on page 79](#) for the **Network Setting > Broadband** screen.

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

Figure 1 Device's Internet Access Application



You can also configure IP filtering on the 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

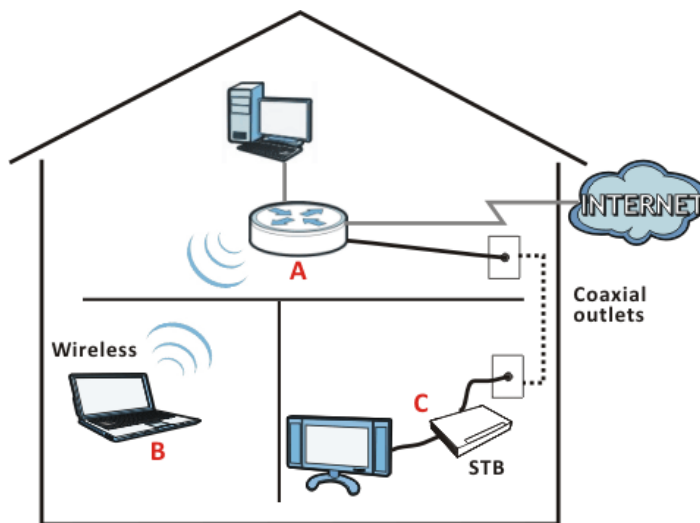
your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

1.4.2 HomePNA

Models with HPNA comply with HomePNA (Home Phoneline Networking Alliance, also known as HPNA) 3.1, a home networking technology for carrying data over existing coaxial cables and telephone wiring.

The figure below shows your Device (**A**) connecting to a phone line outlet for DSL Internet access and a coaxial outlet to relay Internet connectivity to other coaxial outlets in the building. The laptop (**B**) connects wirelessly to the Device. The set-up box (**C**) connects into a coaxial outlet in another part of the house for access to online videos.

Figure 2 HomePNA Application



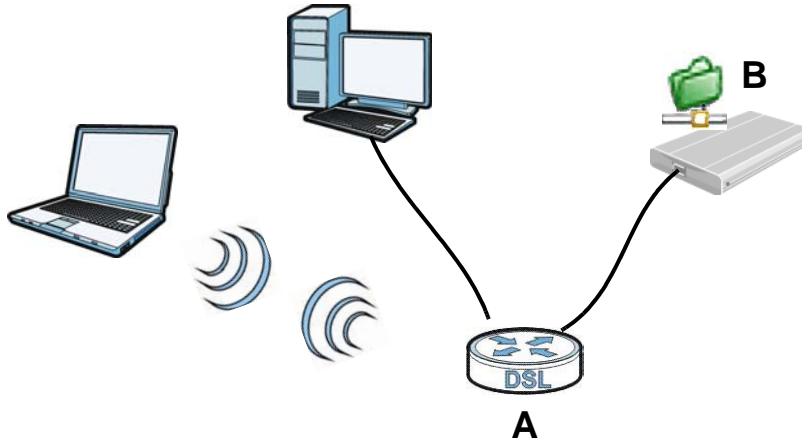
1.4.3 Device's USB Support

The USB port of the Device is used for file-sharing.

File Sharing

Use the built-in USB 2.0 port to share files on a USB memory stick or a USB hard drive (**B**). You can connect one USB hard drive to the Device at a time. Use FTP to access the files on the USB device.

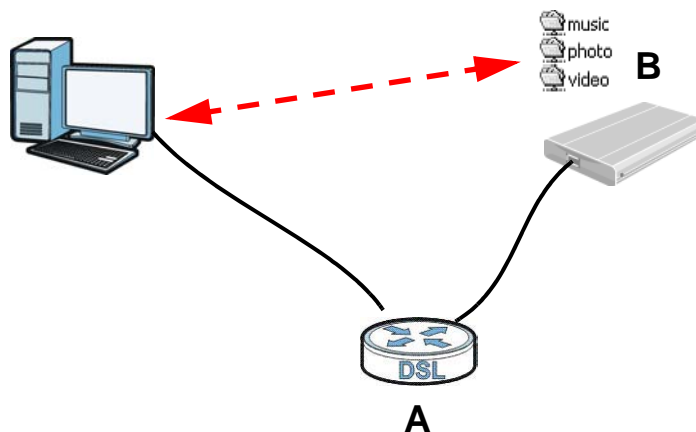
Figure 3 USB File Sharing Application



Media Server

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

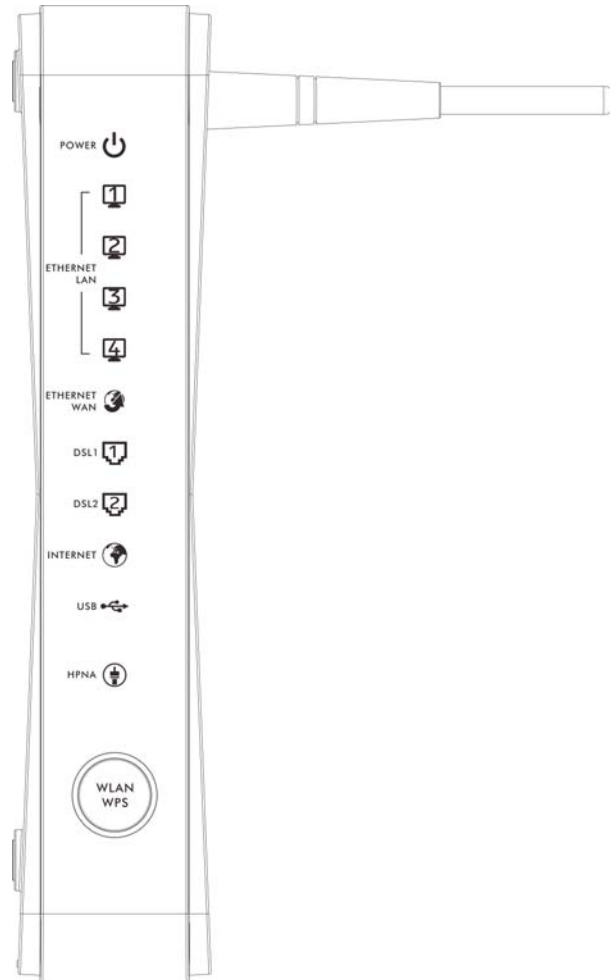
Figure 4 USB Media Server Application



1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 5 LEDs on the Device



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

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The Device is receiving power and ready for use.
		Blinking	The Device is self-testing.
	Red	On	The Device detected an error while self-testing, or there is a device malfunction.
		Off	The Device is not receiving power.
		Blinking	Firmware upgrade is in progress.
ETHERNET LAN 1-4	Green	On	The Device has a successful Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The Device is sending or receiving data to/from the LAN.
		Off	The Device does not have an Ethernet connection with the LAN.

Table 1 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
ETHERNET WAN	Green	On	The Gigabit Ethernet connection is working.
		Blinking	The Device is sending or receiving data to/from the Gigabit Ethernet link.
		Off	There is no Gigabit Ethernet link.
DSL1,2	Green	On	The ADSL line is up.
		Blinking	The Device is initializing the ADSL line.
		Off	The ADSL line is down.
	Orange	On	The VDSL line is up.
		Blinking	The Device is initializing the VDSL line.
		Off	The VDSL line is down.
INTERNET	Green	On	The 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 Device is sending or receiving IP traffic.
		Off	There is no Internet connection or the gateway is in bridged mode.
USB	Green	On	The Device recognizes a USB connection.
		Blinking	The Device is sending/receiving data to /from the USB device connected to it.
		Off	The Device does not detect a USB connection.
MoCA	Green	On	The Device has proper MoCA network link.
		Blinking	The Device has LAN activity.
		Off	The device does not have MoCA network.
HPNA	Green	On	The Device is connected to an HPNA-equipped device through the coaxial cable. ^A
		Blinking	Data is transmitting over the HPNA cable.
		Off	No HPNA device is connected.
WLAN/WPS	Green	On	The wireless network is activated.
		Blinking	The Device is communicating with other wireless clients.
	Green and Orange	Blinking	The Device is setting up a WPS connection.
		Off	The wireless network is not activated.

A. HPNA-equipped models only.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

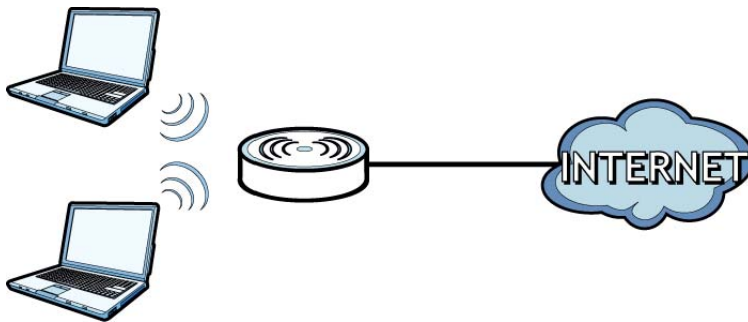
- 1 Make sure the **POWER** LED is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the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

1.7 Wireless Access

The Device is a wireless Access Point (AP) for wireless clients, such as notebook computers or PDAs and iPads. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables.

You can configure your wireless network in either the built-in Web Configurator, or using the WPS button.

Figure 6 Wireless Access Example



1.7.1 Using the WLAN/WPS Button

If the wireless network is turned off, press the **WLAN/WPS** button at the back of the Device for one second. Once the **WLAN/WPS** LED turns green, the wireless network is active.

You can also use the **WLAN/WPS** button to quickly set up a secure wireless connection between the 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 **WLAN/WPS** button for five seconds and release it.
- 3 Press the WPS button on another WPS-enabled device within range of the Device. The **WLAN/WPS** LED flashes orange while the Device sets up a WPS connection with the other wireless device.
- 4 Once the connection is successfully made, the **WLAN/WPS** LED shines green.

To turn off the wireless network, press the **WLAN/WPS** button on the front of the Device for one to five seconds. The **WLAN/WPS** LED turns off when the wireless network is off.

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions or Mozilla Firefox 3 and later versions or Safari 2.0 and later versions [or Google Chrome](#). 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 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).

See [Appendix C on page 323](#) if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

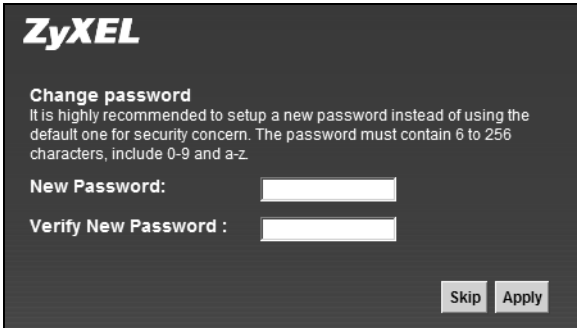
- 1 Make sure your Device hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser. If the Device does not automatically re-direct you to the login screen, go to <http://192.168.1.1>.
- 3 A password screen displays. To access the administrative web configurator and manage the Device, type the default username **admin** and password **1234** in the password screen and click **Login**. If advanced account security is enabled (see [Section 26.2 on page 259](#)) the number of dots that appears when you type the password changes randomly to prevent anyone watching the password field from knowing the length of your password. If you have changed the password, enter your password and click **Login**.

Figure 7 Password Screen



- 4 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the main menu if you do not want to change the password now.

Figure 8 Change Password Screen



- 5 The **Quick Start Wizard** screen appears. You can configure the Device's time zone, basic Internet access, and wireless settings. See [Chapter 3 on page 33](#) for more information.
- 6 After you finished or closed the **Quick Start Wizard** screen, the **Network Map** page appears.

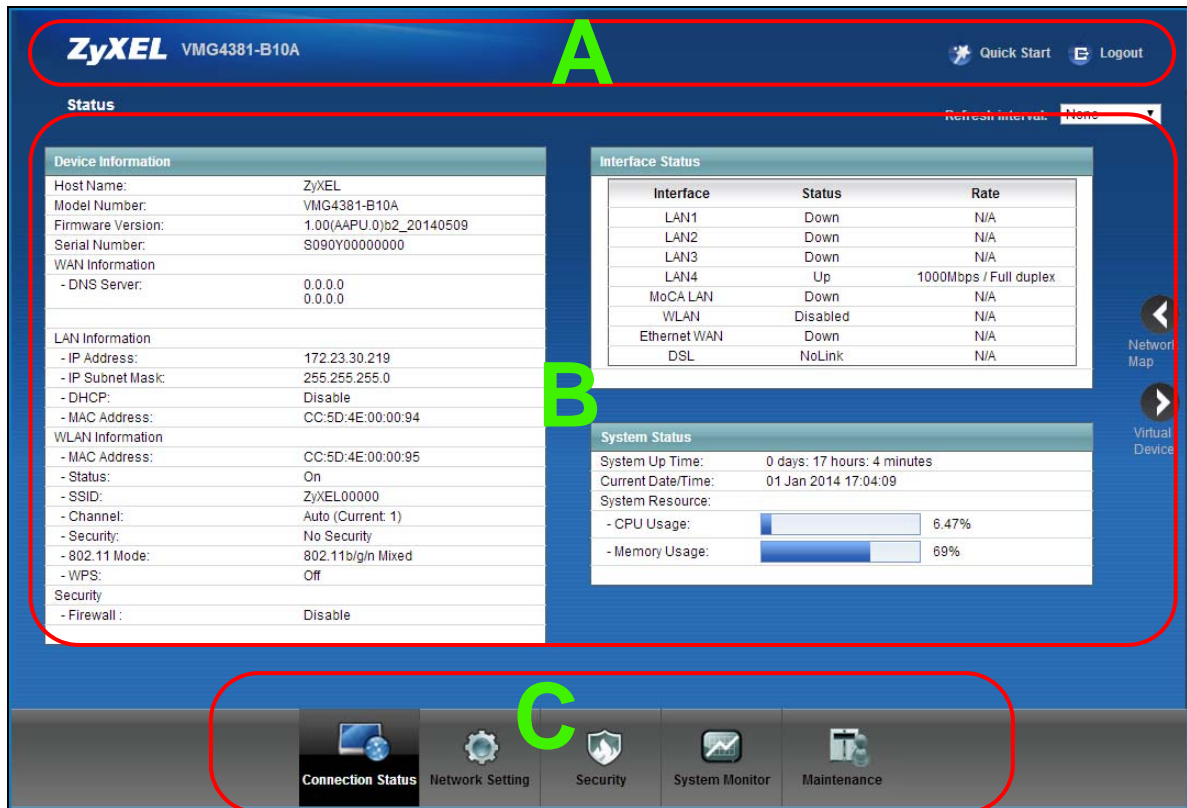
Figure 9 Network Map



- 7 Click **Status** to display the **Status** screen, where you can view the Device's interface and system information.

2.2 Web Configurator Layout

Figure 10 Screen Layout



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

- **A** - title bar
- **B** - main window
- **C** - navigation panel

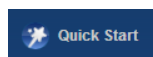

2.2.1 Title Bar

The title bar provides some icons in the upper right corner.



The icons provide the following functions.

Table 2 Web Configurator Icons in the Title Bar

ICON	DESCRIPTION
	Quick Start: Click this icon to open screens where you can configure the Device's time zone Internet access, and wireless settings.
	Logout: Click this icon to log out of the web configurator.

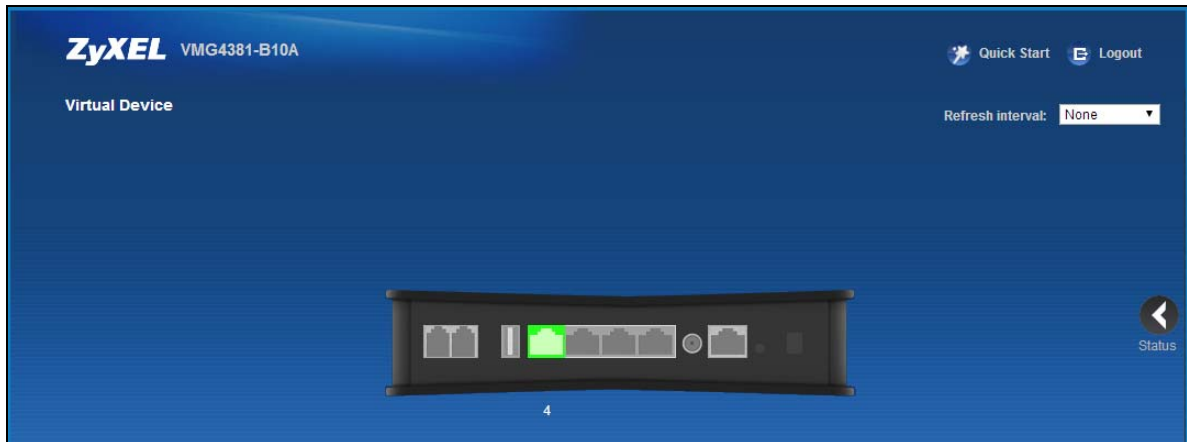
2.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

After you click **Status** on the **Connection Status** page, the **Status** screen is displayed. See [Chapter 5 on page 72](#) for more information about the **Status** screen.

If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the Device's ports. The connected ports are in color and disconnected ports are gray.

Figure 11 Virtual Device



2.2.3 Navigation Panel

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

Table 3 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the 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.
	3G 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.
	8021x	Use this screen to view and configure the IEEE 802.1x settings on the Device.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the 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).
	WDS	Use this screen to set up Wireless Distribution System (WDS) links to other access points.
	Others	Use this screen to configure advanced wireless settings.
	Channel	Use this screen to scan wireless LAN channel noises and view the results.
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 have the Device automatically create static DHCP entries for Set Top Box (STB) devices when they request IP addresses.
	5th Ethernet Port	Use this screen to configure the Ethernet WAN port as a LAN port.
Routing	Static Route	Use this screen to view and set up static routes on the Device.
	Policy Forwarding	Use this screen to configure policy routing on the Device.
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.
	Class Setup	Use this screen to define a classifier.
	Policer Setup	Use these screens to configure QoS policers.
	Monitor	Use this screen to view QoS packets statistics.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Applications	Use this screen to configure servers behind the Device.
	Port Triggering	Use this screen to change your 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 Device's address mapping settings.
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.
Interface Group		Use this screen to map a port to a PVC or bridge group.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
USB Device	File Sharing	Use this screen to enable file sharing via the Device.
	Media Server	Use this screen to use the Device as a media server.
	Printer Server	Use this screen to enable the print server on the Device and get the model name of the associated printer.
Security Settings		
Firewall	General	Use this screen to configure the security level of your firewall.
	Service	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		Use this screen to block or allow traffic from devices of certain MAC addresses to the Device.
Parental Control		Use this screen to block web sites with the specific URL.
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.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Device. You can export or e-mail the logs.
	Security Log	Use this screen to view the login record of the Device. You can export or e-mail the logs.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Device.
ARP Table		Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
IGMP Group Status		Use this screen to view the status of all IGMP settings on the Device.
xDSL Statistics		Use this screen to view the Device's xDSL traffic statistics.
Maintenance		
User Account		Use this screen to change user password on the Device.
Remote MGMT		Use this screen to enable specific traffic directions for network services.
TR-069 Client		Use this screen to configure the Device to be managed by an Auto Configuration Server (ACS).
TR-064 Client		Use this screen to enable management via TR-064 on the LAN.
Time		Use this screen to change your Device's time and date.
Email Notification		Use this screen to configure up to two mail servers and sender addresses on the Device.
Log Setting		Use this screen to change your Device's log settings.
Firmware Upgrade		Use this screen to upload firmware to your device.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Configuration		Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Reboot		Use this screen to reboot the 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.
	OAM Ping	Use this screen to view information to help you identify problems with the DSL connection.

Quick Start

3.1 Overview

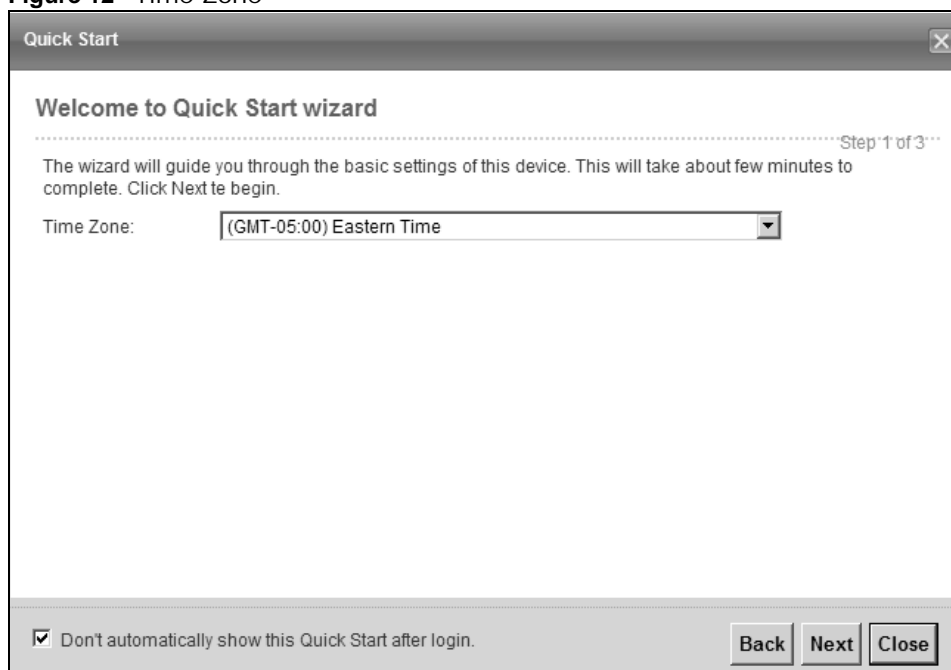
Use the Quick Start screens to configure the Device's time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on [page 69](#)) for background information on the features in this chapter.

3.2 Quick Start Setup

- 1 The Quick Start Wizard appears automatically after login. Or you can click the **Click Start** icon in the top right corner of the web configurator to open the quick start screens. Select the time zone of the Device's location and click **Next**.

Figure 12 Time Zone



- 2 Enter your Internet connection information in this screen. The screen and fields to enter may vary depending on your current connection type. Click **Next**. Click **Next**.

Figure 13 Internet Connection

Quick Start

Internet Connection

.....Step 2 of 3.....

The current connection type is set to PPPoE and needs a user name and password to get online.

User Name:

Password:

Is there specific IP address information from your Internet Service Provider (ISP)?

Yes No

Then the IP Address information will be dynamically assigned to you from your ISP.

Don't automatically show this Quick Start after login.

Back Next Close

- 3 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 Device. Click **Save**.

Figure 14 Internet Connection

Quick Start

Wireless Setting

.....Step 3 of 3.....

The following settings are the current wireless settings which your wireless client devices need in order to get connected to this device.

Wireless Service: Enable Disable

Wireless Network Name (SSID):

Security: WPA-PSK

Password: A9C6F3A24538A8C5EFA7

Don't automatically show this Quick Start after login.

Back Save Close

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

4.1 Overview

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

- [Setting Up an ADSL PPPoE Connection](#), see page 35
- [Setting Up a Secure Wireless Network](#), see page 38
- [Setting Up Multiple Wireless Groups](#), see page 44
- [Configuring Static Route for Routing to Another Network](#), see page 47
- [Configuring QoS Queue and Class Setup](#), see page 50
- [Access the Device Using DDNS](#), see page 53
- [Configuring the MAC Address Filter](#), see page 54
- [Access Your Shared Files From a Computer](#), see page 56
- [Using the Media Server Feature](#), see page 57
- [Using the Print Server Feature](#), see page 62

4.2 Setting Up an ADSL PPPoE Connection

This tutorial shows you how to set up your 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 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**.

Add new WAN Interface												
#	Name	Type	Mode	Encaps...	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	N	N	
2	VDSL_...	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
3	Etherne...	Ethernet	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	

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

General	
Name	MyDSLConnection
Type	ADSL

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!
PPPoE Service Name	MyDSL
Static IP Address	192.168.1.32
Others	PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enabled

- 3 Select the **Active** check box. 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 **IPv6/IPv4 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.

General	
Active	<input type="checkbox"/>
Name :	<input type="text" value="MyDSLConnection"/>
Type :	<input type="text" value="ADSL over ATM"/>
Mode :	<input type="text" value="Routing"/>
Encapsulation:	<input type="text" value="PPPoE"/>
IPv6/IPv4 Mode:	<input type="text" value="IPv4 Only"/>
ATM PVC Configuration	
VPI [0-255]:	<input type="text" value="36"/>
VCI [32-65535]:	<input type="text" value="48"/>
DSL Link Type:	<input type="text" value="EoA"/>
Encapsulation Mode:	<input type="text" value="LLC/SNAP-BRIDGING"/>
Service Category:	<input type="text" value="UBR Without PCR"/>
PPP Information	
PPP User Name :	<input type="text" value="1234@DSL-Ex.com"/>
PPP Password :	<input type="text" value="ABCDEF!"/>
PPP Auto Connect :	<input type="checkbox"/>
IDLE Timeout [minutes]:	<input type="text"/>
PPPoE Service Name :	<input type="text" value="MyDSL"/>
PPPoE Passthrough :	<input type="checkbox"/>
IP Address	
<input type="radio"/> Obtain an IP Address Automatically	
<input checked="" type="radio"/> Static IP Address	
IP Address :	<input type="text" value="192.168.1.32"/>
Subnet Mask :	<input type="text" value="0.0.0.0"/>
Gateway IP address :	<input type="text" value="0.0.0.0"/>
Routing Feature	
NAT Enable :	<input checked="" type="checkbox"/>
FullFeature NAT Enable :	<input type="checkbox"/>
NatSet:	<input type="text" value="1"/>
IGMP Proxy Enable :	<input checked="" type="checkbox"/>
Apply as Default Gateway :	<input checked="" type="checkbox"/>
DNS server	
DNS :	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static
DNS Server 1 :	<input type="text" value="192.168.5.6"/>
DNS Server 2 :	<input type="text" value="192.168.5.7"/>
Tunnel	
Enable 6RD :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
6RD Type :	<input checked="" type="radio"/> DHCP <input type="radio"/> Static
6RD Border Relay Server IP :	<input type="text"/>
6RD IPv6 Prefix :	<input type="text"/>
QoS	
Egress Traffic Rate Limit :	<input type="text"/> (kbps)
MTU	
MTU Size :	<input type="text" value="1492"/> MTU [68-1492]
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	VLAN Proxy	NAT	Default Gateway	IPv6	MD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
2	MyDSLConnection	ATM	Routing	PPPoE	N/A	N/A	Y	Y	N	N	N	
3	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
4	ETHoWAN	Ethernet	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
5	MyETHER	Ethernet	Routing	PPPoE	0	1	N	Y	N	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 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 Device. Then he can set up a wireless network using WPS (Section 4.3.2 on page 40) or manual configuration (Section 4.3.3 on page 43).

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 38). Click **Apply**.

Wireless Network Setup

Wireless: Enable Disable (settings are invalid when disabled)

Band: 2.4GHz

Channel: Auto Current: 10 [more...](#)

Wireless Network Settings

Wireless Network Name (SSID): Example

Max clients for all SSID: 64

Hide SSID

Client Isolation

MBSSID/LAN Isolation

Enhanced Multicast Forwarding

Maximum Bandwidth: Kbps

BSSID: CC:5D:4E:00:00:95

Security Level

No Security Basic **More Secure (Recommended)**

Security Mode: WPA2-PSK

Generate password automatically

Enter 8-63 characters (a-z, A-Z, 0-9 and '~!@#%&^&*()_-' special characters), other characters are not allowed.

Password: 868F3440CB [more...](#)

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

Wireless Advanced Setup

RTS/CTS Threshold: 2347

Fragmentation Threshold: 2346

Auto Channel Timer: 0 min

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

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the Device (see [Section 4.3.2 on page 40](#)). He can also use the notebook's wireless client to search for the Device (see [Section 4.3.3 on page 43](#)).

4.3.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the Device as the AP and ZyXEL NWD210N as the wireless client which connects to the notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCMCIA card).

There are two WPS methods to set up the wireless client settings:

- **Push Button Configuration (PBC)** - simply press a button. This is the easier of the two methods.
- **PIN Configuration** - configure a Personal Identification Number (PIN) on the Device. A wireless client must also use the same PIN in order to download the wireless network settings from the Device.

Push Button Configuration (PBC)

- 1 Make sure that your Device is turned on and your notebook is within the cover range of the wireless signal.
- 2 Make sure that you have installed the wireless client driver and utility in your notebook.
- 3 In the wireless client utility, go to the WPS setting page. Enable WPS and press the WPS button (**Start** or **WPS** button).
- 4 Push and hold the **WPS** button located on the Device's front panel for more than 5 seconds. Alternatively, you may log into Device's web configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function and click **Apply**. Then click the **Connect** button.

WPS Setup

WPS: Enable Disable (The settings in this screen are invalid if you select this.)

Method 1	Method 2	Method 3
<p>Push Button Configuration</p> <p>1. Click "Connect".</p> <p>Connect</p> <p>2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".</p>	<p>Register Wireless Client's PIN Number</p> <p>1. Enter the PIN of your wireless client and click "Register"</p> <p><input type="text"/> Register</p> <p>2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".</p>	<p>Enter AP's PIN Number in Wireless Client</p> <p>Current state: Unconfigured</p> <p>1. Enter current PIN 19838588 on your wireless client</p> <p>Generate New PIN Number</p>

Notes:

1. This function only works on the first SSID.
2. Click the "Release Configuration" button to have the WPS status changed to "Unconfigured". Otherwise, WPS status is in "Configured" mode.

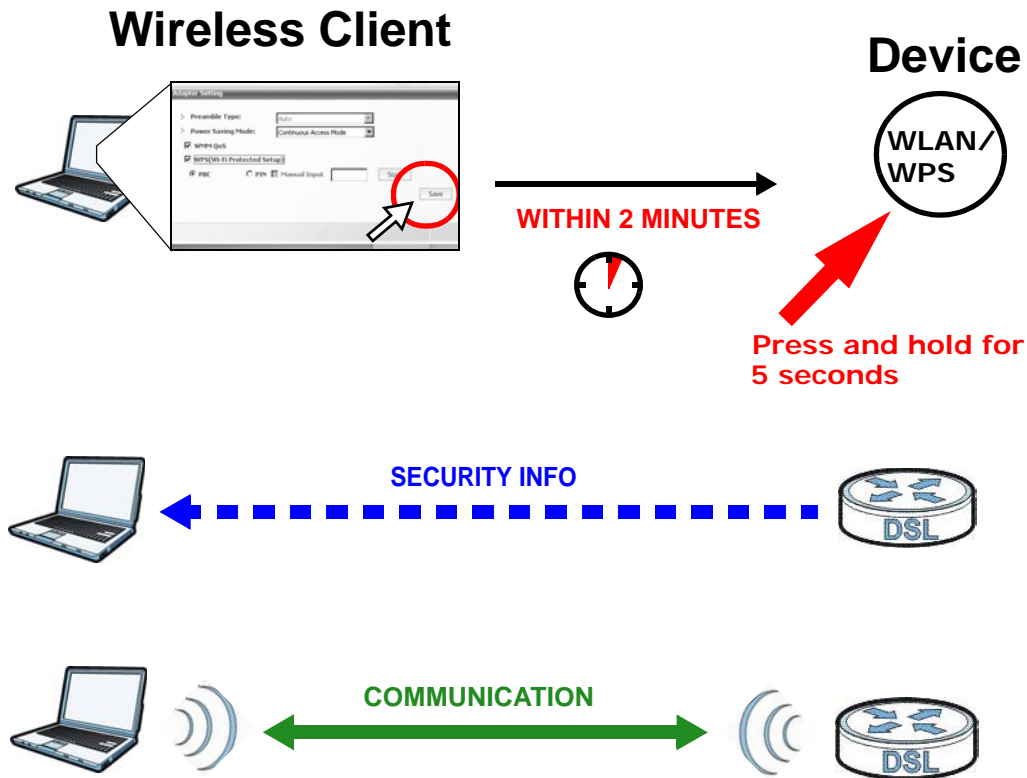
Apply **Cancel**

Note: Your Device has a WPS button located on its front 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 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 Device securely.

The following figure shows you an example of how to set up a wireless network and its security by pressing a button on both Device and wireless client.






PIN Configuration

When you use the PIN configuration method, you need to use both the Device's web configurator and the wireless client's utility.

- 1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
- 2 Log into Device's web configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function and click **Apply**.

WPS Setup

WPS: **Enable** Disable (The settings in this screen are invalid if you select this.)

 Method 1	 Method 2	 Method 3
Push Button Configuration 1. Click "Connect". <input type="button" value="Connect"/> 2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".	Register Wireless Client's PIN Number 1. Enter the PIN of your wireless client and click <input type="button" value="Register"/> 2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".	Enter AP's PIN Number in Wireless Client Current state: Unconfigured 1. Enter current PIN 19838588 on your wireless client <input type="button" value="Generate New PIN Number"/>

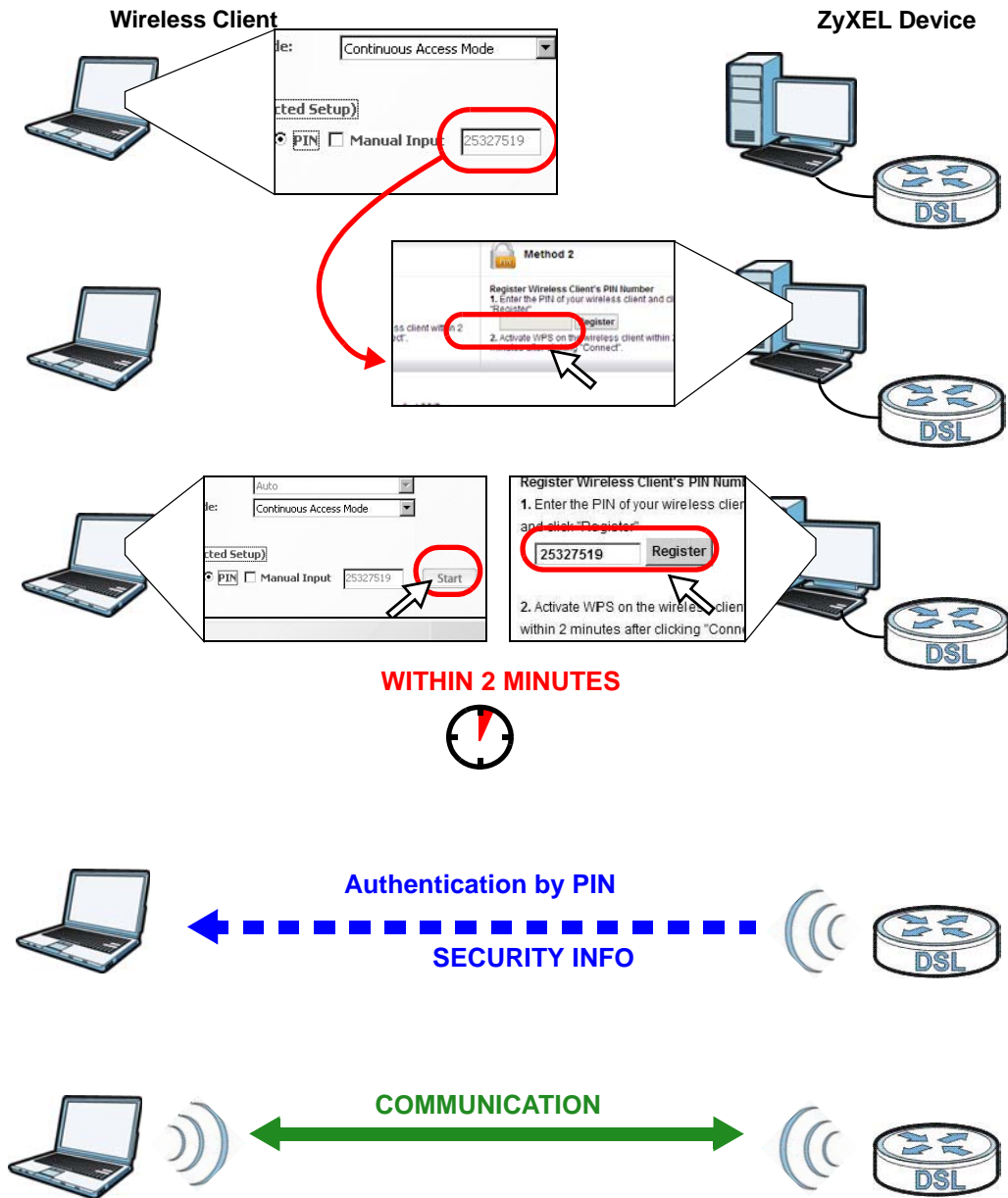
Notes:

1. This function only works on the first SSID.
2. Click the "Release Configuration" button to have the WPS status changed to "Unconfigured". Otherwise, WPS status is in "Configured" mode.

- 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 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 Device securely.

The following figure shows you how to set up a wireless network and its security on a Device and a wireless client by using PIN method.



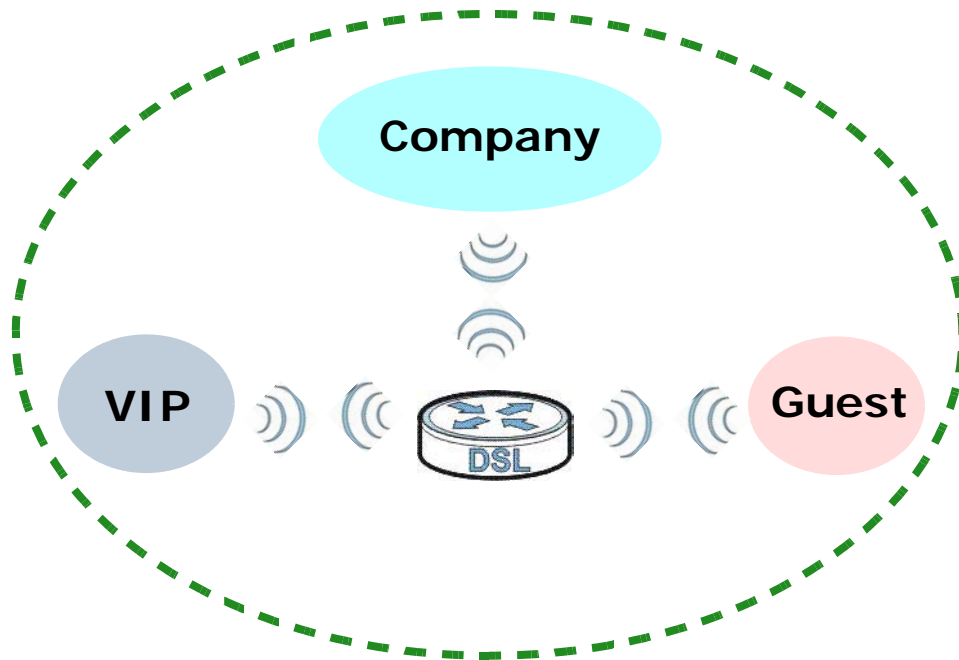
4.3.3 Without WPS

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 an wireless Internet connection.

Note: The 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 lower security mode.

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	Basic
Security Mode	WPA2-PSK	WPA2-PSK	Static WEP
Pre-Shared Key	ForCompanyOnly	ForVIPOnly	Guest12345678

- 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**.

Wireless Network Setup

Wireless Enable Disable (settings are invalid when disabled)

Band: 2.4GHz

Channel: Auto Current: 9 [more...](#)

Wireless Network Settings

Wireless Network Name (SSID): Company

Max clients for all SSID: 64

Hide SSID

Client Isolation

MBSSID/LAN Isolation

Enhanced Multicast Forwarding

Maximum Bandwidth: Kbps

BSSID: CC:5D:4E:00:00:95

Security Level

No Security Basic **More Secure (Recommended)**

Security Mode: WPA2-PSK

Generate password automatically

Enter 8-63 characters (a-z, A-Z, 0-9 and ~!@#%&*()-_ special characters), other characters are not allowed.

Password:

Show password [more...](#)

- 2 Click **Network Setting > Wireless > More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group. The following screen does not apply to VMG4381.

#	Status	SSID	Security	Guest WLAN	Modify
1	💡	ZyXEL5F5B4_Guest1	WPA-PSK	N/A	
2	💡	ZyXEL5F5B4_Guest2	WPA-PSK	N/A	
3	💡	ZyXEL5F5B4_Guest3	WPA-PSK	N/A	

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

Wireless Network Setup

Wireless : Enable Disable (The settings in this screen are invalid if you select this.)

Wireless Network Settings

Wireless Network Name(SSID):

Max clients:

Hide SSID

Enhanced Multicast Forwarding

Guest WLAN

Max. Upstream Bandwidth : Kbps

Max. Downstream Bandwidth : Kbps

Notes:

1. Max. Upstream Bandwidth: This field allows user to configure the maximum bandwidth of this SSID to WAN.
2. Max. Downstream Bandwidth: This field allows user to configure the maximum bandwidth of WAN to this SSID.
3. If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

Security Level

No Security Basic **More Secure (Recommended)**

Security Mode: Generate password automatically

Enter 8-63 characters (a-z, A-Z, 0-9, '-', '_', and '!'), other characters are not allowed.

Password: [more..](#)

4 In the **More AP** screen, click the **Edit** icon to configure the third wireless network group.

#	Status	SSID	Security	Guest WLAN	Modify
1		VIP	WPA2-PSK	N/A	
2		Guest2	WPA-PSK	N/A	
3		Guest3	WPA-PSK	N/A	

5 Configure the screen using the provided parameters and click **Apply**.

Wireless Network Setup

Wireless : Enable Disable (The settings in this screen are invalid if you select this.)

Wireless Network Settings

Wireless Network Name (SSID):

Max clients:

Hide SSID

Enhanced Multicast Forwarding

Guest WLAN

Max. Upstream Bandwidth : Kbps

Max. Downstream Bandwidth : Kbps

Notes:

1. Max. Upstream Bandwidth: This field allows user to configure the maximum bandwidth of this SSID to WAN.
2. Max. Downstream Bandwidth: This field allows user to configure the maximum bandwidth of WAN to this SSID.
3. If Max. Upstream/Downstream Bandwidth is empty, the CPE sets the value automatically.

BSSID: 62:7B:EF:75:F5:B7

Security Level

No Security Basic More Secure (Recommended)

Security Mode: WEP

Generate password automatically

64-bit: Enter 5 ASCII characters or 10 hex characters ("0-9", "A-F")

128-bit: Enter 13 ASCII characters or 26 hex characters ("0-9", "A-F")

Select one password as your active password

Password 1: 1ED1C8BEB5388CF95AB2935277 [less](#)







Password 2:

Password 3:

Password 4:

WEP Encryption:

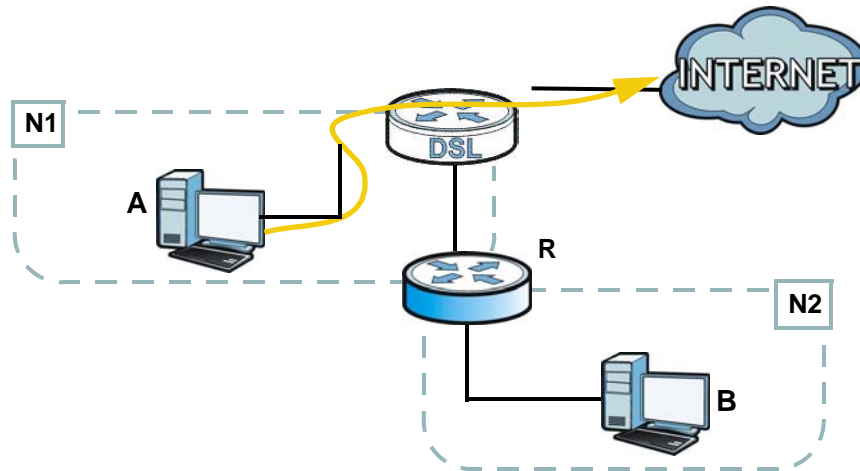
- 6 Check the status of **VIP** and **Guest** in the **More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.

#	Status	SSID	Security	Guest WLAN	Modify
1		VIP	WPA2-PSK	N/A	
2		Guest	WEP	N/A	
3		Guest3	WPA-PSK	N/A	

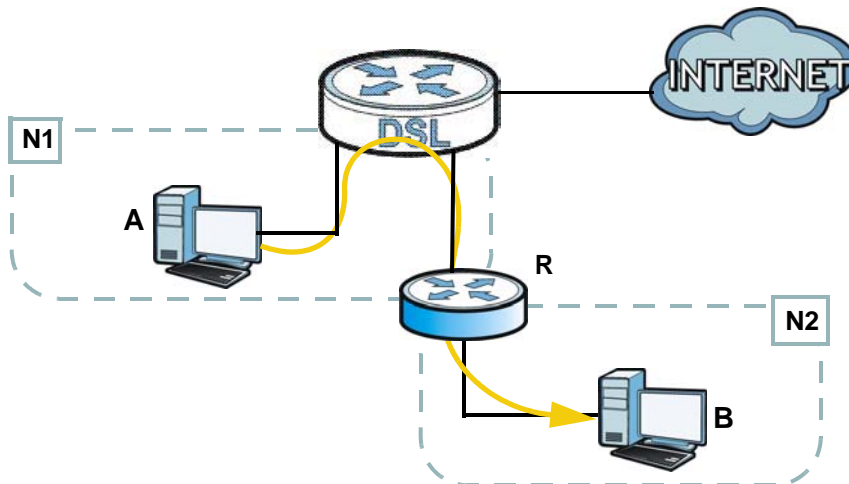
4.5 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the 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 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 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 Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 4 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The Device's WAN	172.16.1.1
The Device's LAN	192.168.1.1
IP Type	IPv4
Use Interface	ADSL/atm0
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 Device's Web Configurator in advanced mode.
- 2 Click **Network Setting > Routing**.
- 3 Click **Add new static route** in the **Static Route** screen.

#	Status	Name	Destination IP	Subnet Mask	Gateway	Interface	Modify
1		test	192.168.0.0	255.255.0.0	192.168.1.23	ADSL	

- 4 Configure the **Static Route Setup** screen using the following settings:
 - 4a Select the **Active** check box. Enter the **Route Name** as **R**.
 - 4b Set **IP Type** to **IPv4**.
 - 4c Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.
 - 4d Select **Enable** in the **Use Gateway IP Address** field. Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.
 - 4e Select **ADSL/atm0** as the **Use Interface**.

<input checked="" type="checkbox"/> Active	
Route Name :	<input type="text" value="R"/>
IP Type:	<input type="text" value="IPv4"/>
Destination IP Address :	<input type="text" value="192.168.10.0"/>
IP Subnet Mask :	<input type="text" value="255.255.255.0"/>
Use Gateway IP Address :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Gateway IP Address :	<input type="text" value="192.168.1.253"/>
Use Interface :	<input type="text" value="ADSL/atm0"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- 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.

4.6 Configuring QoS Queue and Class Setup

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

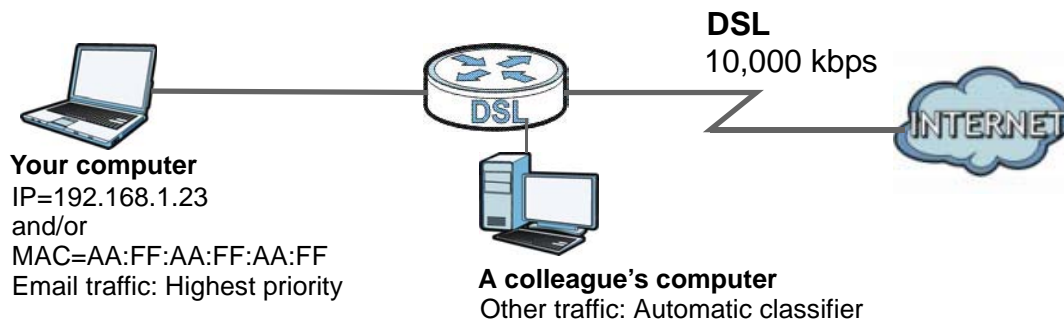
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues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

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



- 1 Click **Network Setting > QoS > General** and select **Enable**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Device automatically determine this figure). Click **Apply**.

QoS Enable Disable (settings are invalid when disabled)

WAN Managed Upstream Bandwidth : (kbps)

LAN Managed Downstream Bandwidth : (kbps)

Upstream traffic priority Assigned by:

Note:

You can assign the upstream bandwidth manually. If the field is empty, the CPE sets the value automatically.
 If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
 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.

- 2 Click **Queue Setup > Add new Queue** to create a new queue. In the screen that opens, check **Active** and enter or select the following values:

- **Name:** E-mail
- **Interface:** WAN
- **Priority:** 1 (High)
- **Weight:** 8
- **Rate Limit:** 5,000 (kbps)

Active

Name :

Interface :

Priority :

Weight :

Buffer Management :

Rate Limit : (kbps)

- 3 Click **Class Setup > Add new Classifier** to create a new class. Check **Active** and follow the settings as shown in the screen below.

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 need to be managed by this QoS rule

▪ **Basic**

From Interface :

Ether Type :

▪ **Source**

Address Subnet Netmask Exclude

Port Range ~ Exclude

MAC MAC Mask Exclude

▪ **Destination**

Address Subnet Netmask Exclude

Port Range ~ Exclude

MAC MAC Mask Exclude

▪ **Others**

Service Exclude

IP protocol Exclude

DHCP Exclude

Packet Length ~ Exclude

DSCP (0~63) Exclude

802.1P Exclude

VLAN ID (0~4094) Exclude

TCP ACK Exclude

Step3: Packet modification

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

DSCP Mark : (0~63)

802.1P Mark :

VLAN ID : (0~4094)

Step4: Policy Forwarding

This module can route or bridge packets to certain interface according to the class settings:

Forward To Interface :

Step5: Outgoing queue selection

Outgoing queue decide the priority of the traffic and how traffic should be shaped in the WAN interface. Choose "None" if you don't want to apply outgoing queue

To Queue Index :

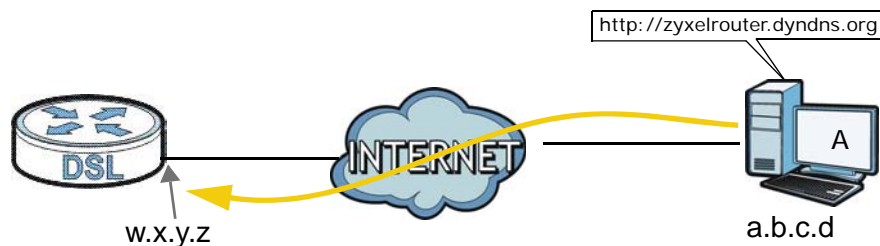
Class Name	Give a class name to this traffic, such as E-mail in this example.
From Interface	This is the interface from which the traffic will be coming from. Select LAN1 for this example.
Ether Type	Select IP to identify the traffic source by its IP address or MAC address.
IP Address	Type the IP address 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 Verify that the queue setup works by checking **Network Setting > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.

4.7 Access the Device Using DDNS

If you connect your 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 Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the 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 Device](#)
- [Testing the DDNS Setting](#)

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

4.7.1 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 Device is currently using. You can find the IP address on the Device's Web Configurator **Status** page.

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

4.7.2 Configuring DDNS on Your 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**).

Dynamic DNS Setup

Dynamic DNS Enable Disable (settings are invalid when disabled)

Service Provider :

Hostname :

Username :

Password :

Email :

Key :

Click **Apply**.

4.7.3 Testing the DDNS Setting

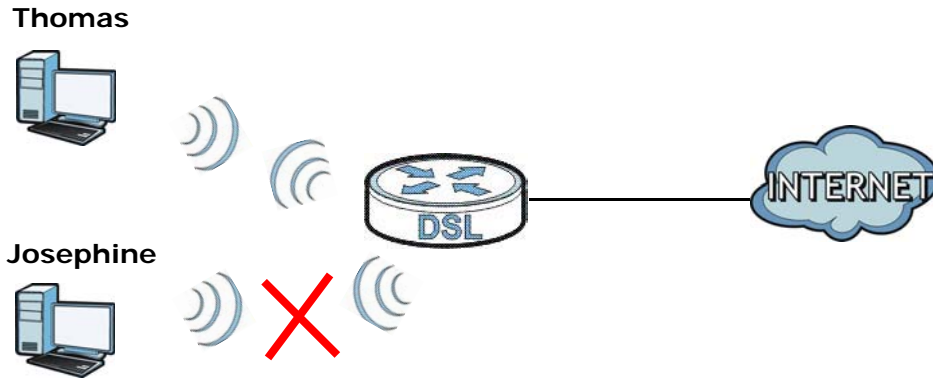
Now you should be able to access the Device from the Internet. To test this:

- 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 Device's login page should appear. You can then log into the Device and manage it.

4.8 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 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**. Then enter the host name and MAC address of Thomas' computer in this screen. Click **Apply**.

MAC Address Filter : Enable Disable (settings are invalid when disabled)

Set	Allow	Host name	MAC Address
1	<input checked="" type="checkbox"/>	Thomas	00:24:21:AB:1F:00
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
2	<input type="checkbox"/>		
30	<input type="checkbox"/>		
31	<input type="checkbox"/>		
32	<input type="checkbox"/>		

Note:
Only devices listed here are granted access to the network.

Apply Cancel

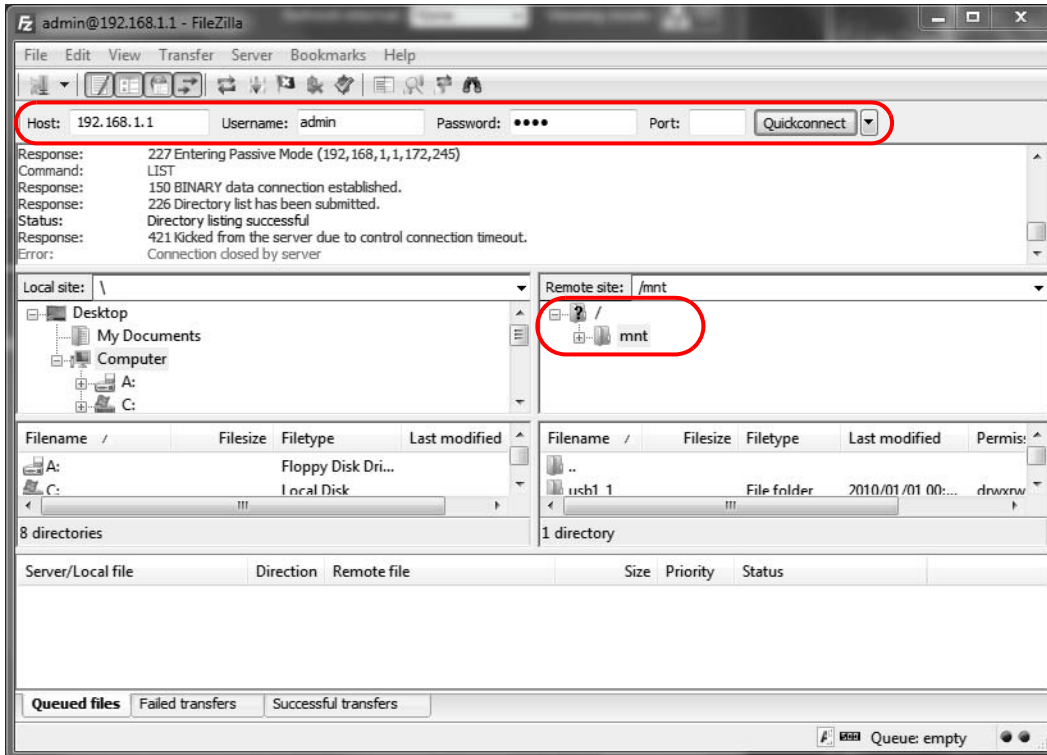
Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the Device.

4.9 Access Your Shared Files From a Computer

Here is how to use an FTP program to access a file storage device connected to the 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 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.

4.10 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 Vista and 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 Device.

4.10.1 Configuring the Device

Note: The Media Server feature is enabled by default.

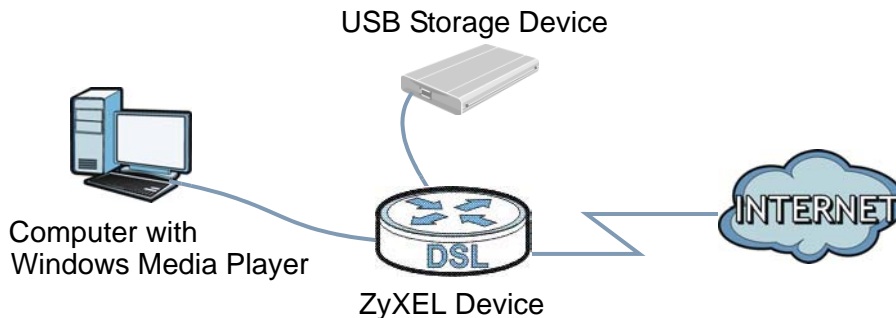
To use your Device as a media server, click **Network Setting > Home Networking > Media Server**.



Check **Enable Media Server** and click **Apply**. This enables DLNA-compliant media clients to play the video, music and image files in your USB storage device.

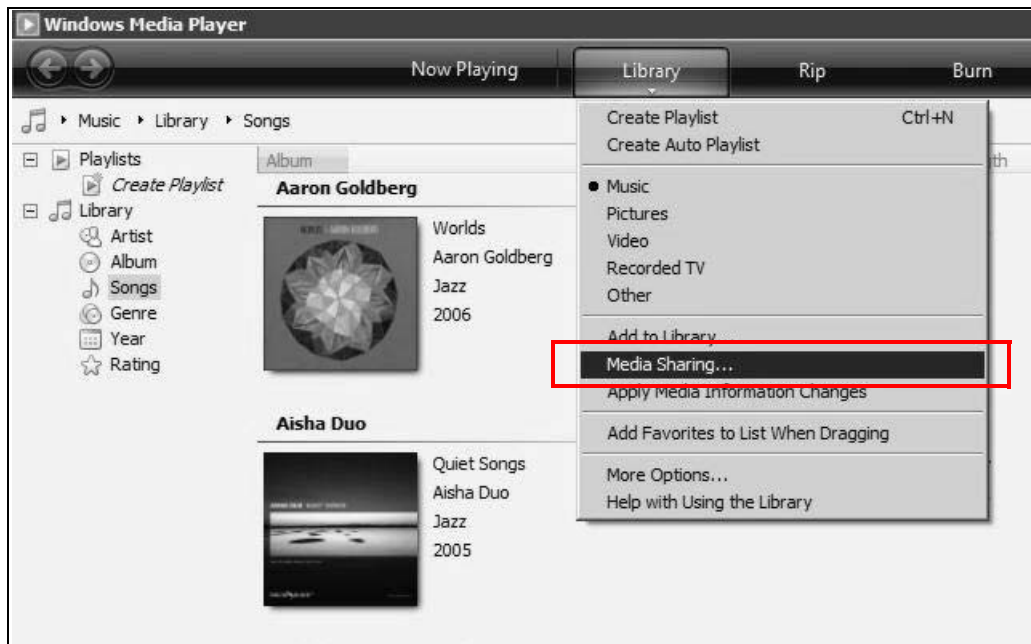
4.10.2 Using Windows Media Player

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

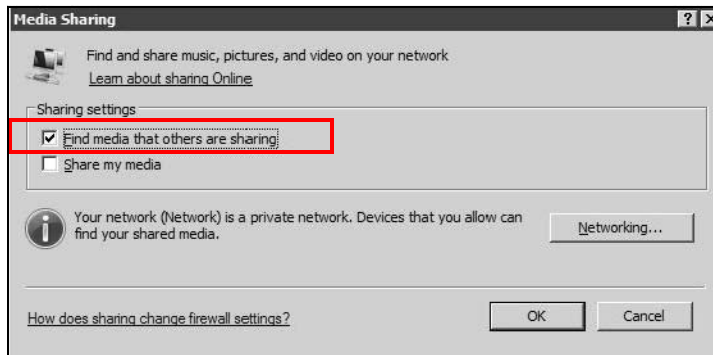


Windows Vista

- 1 Open Windows Media Player and click **Library > Media Sharing** as follows.



- 2 Check **Find media that others are sharing** in the following screen and click **OK**.



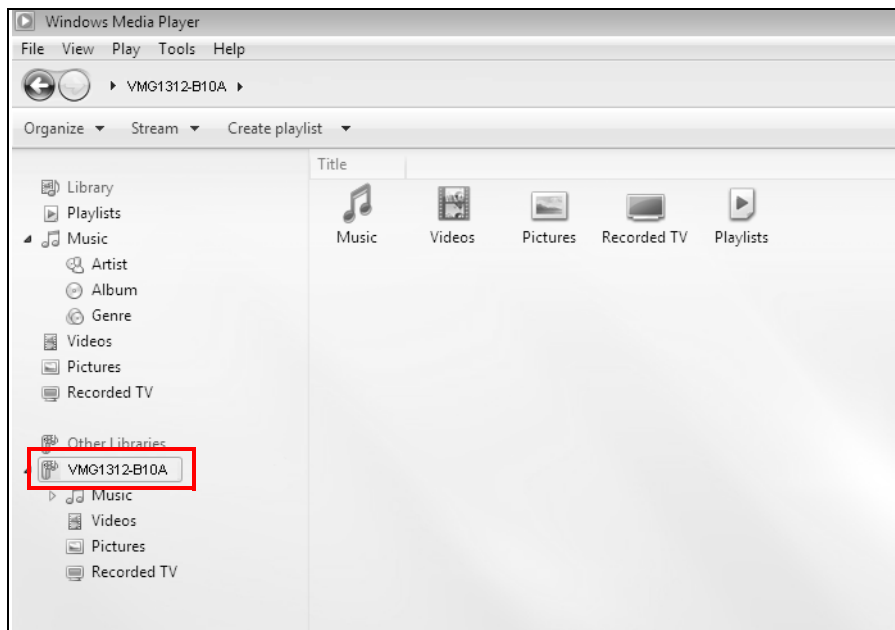
- 3 In the **Library** screen, check the left panel. The Windows Media Player should detect the Device.



The Device displays as a playlist. Clicking on the category icons in the right panel shows you the media files in the USB storage device attached to your Device.

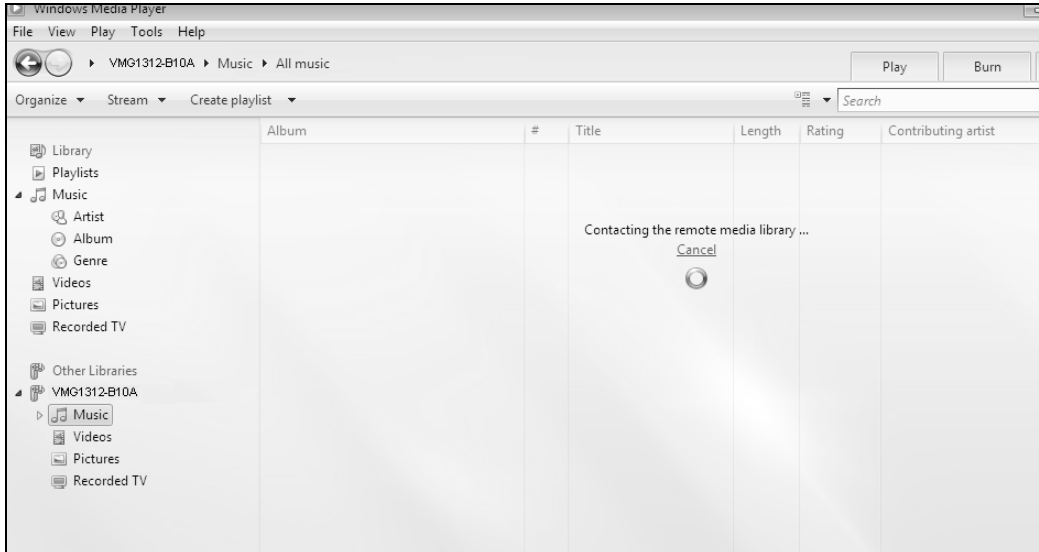
Windows 7

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

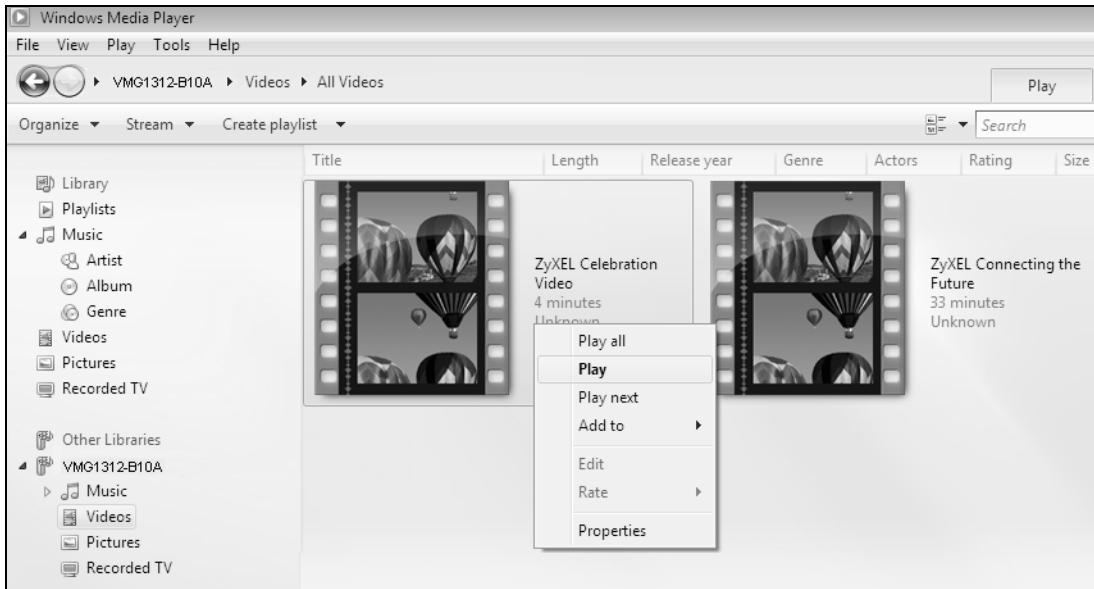


If you cannot see the Device in the left panel as shown above, right-click **Other Libraries** > **Refresh Other Libraries**.

- 2 Select a category in the left panel and wait for Windows Media Player to connect to the Device.



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

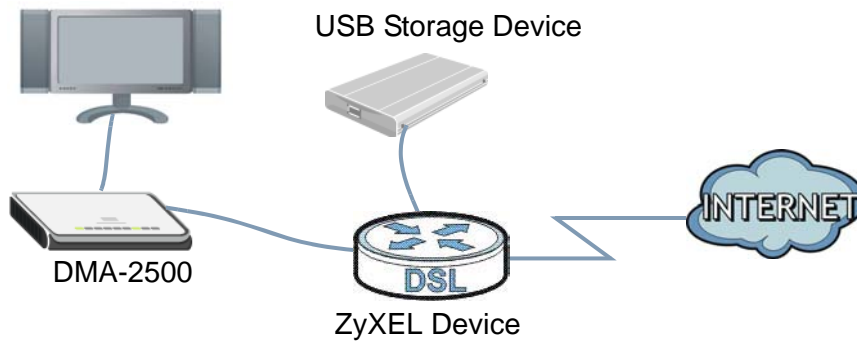


4.10.3 Using a Digital Media Adapter

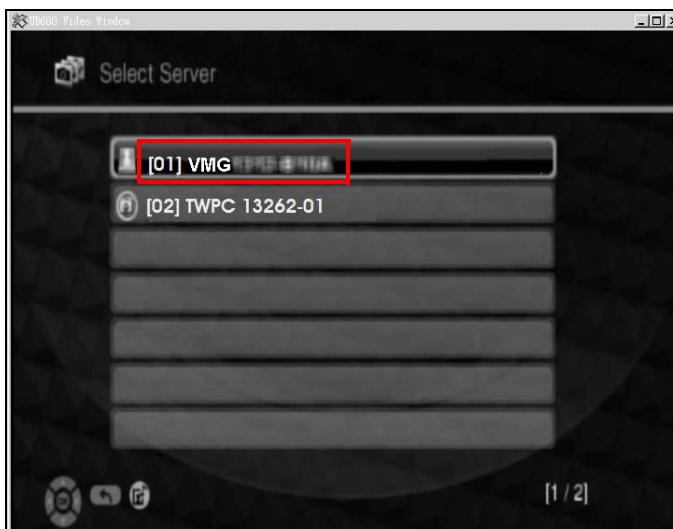
This section shows you how you can use the Device with a ZyXEL DMA-2500 to play media files stored in the USB storage device in your TV screen.

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 Device.



- 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 Device as your media server.

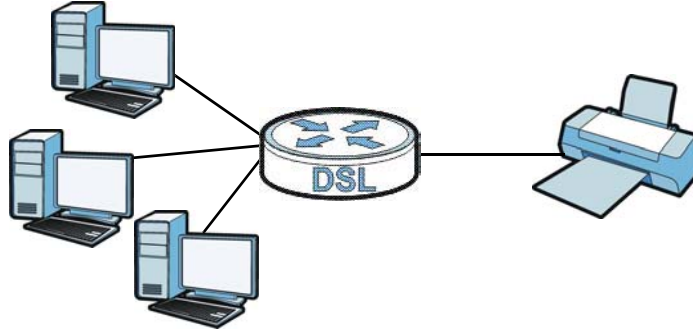


- The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button in the remote control.



4.11 Using the Print Server Feature

The Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the Device and then adding the printer on the computers connected to your network.



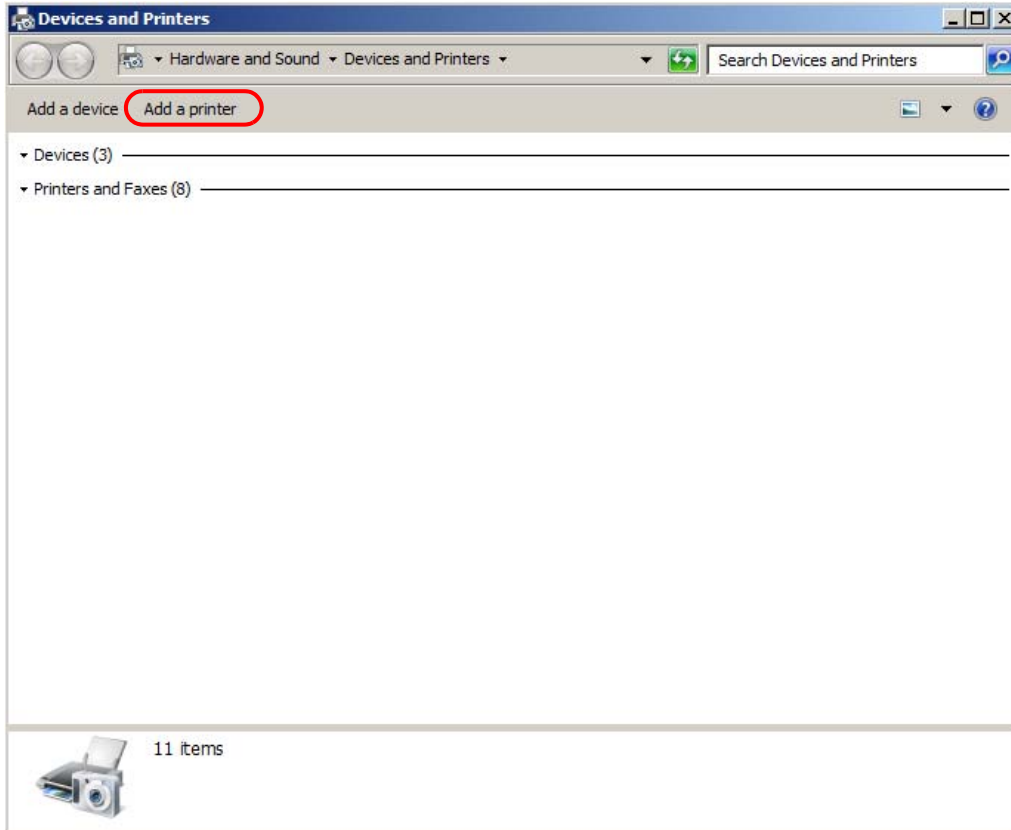
In this section you can:

- Add a New Printer Using Windows
- Add a New Printer Using Macintosh OS X

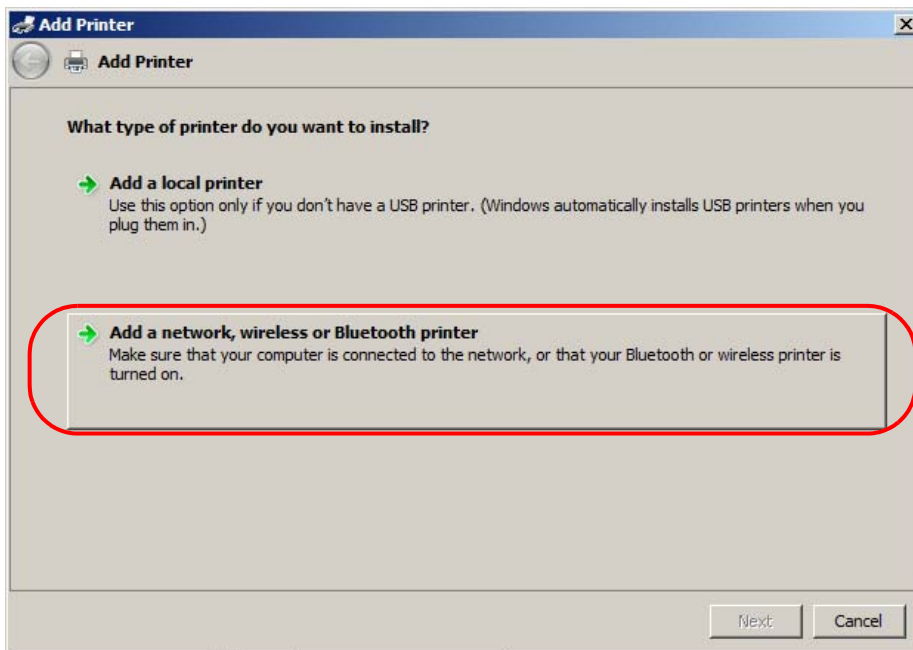
Add a New Printer Using Windows

This example shows how to connect a printer to your Device using the Windows 7 operating system. Some menu items may look different on your operating system.

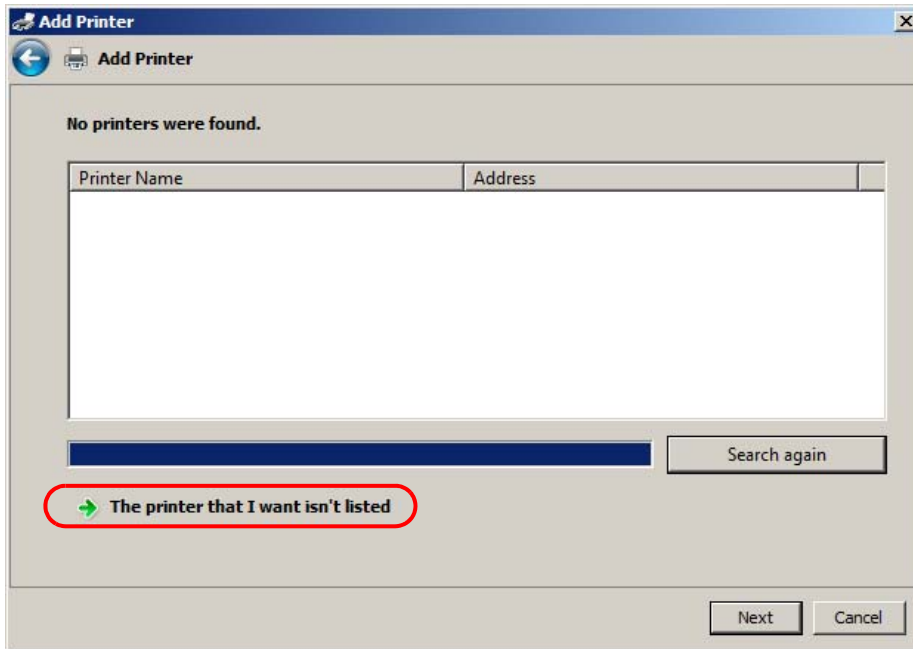
- 1 Click **Start > Control Panel > Devices and Printers** to open the **Devices and Printers** screen. Click **Add a printer**.



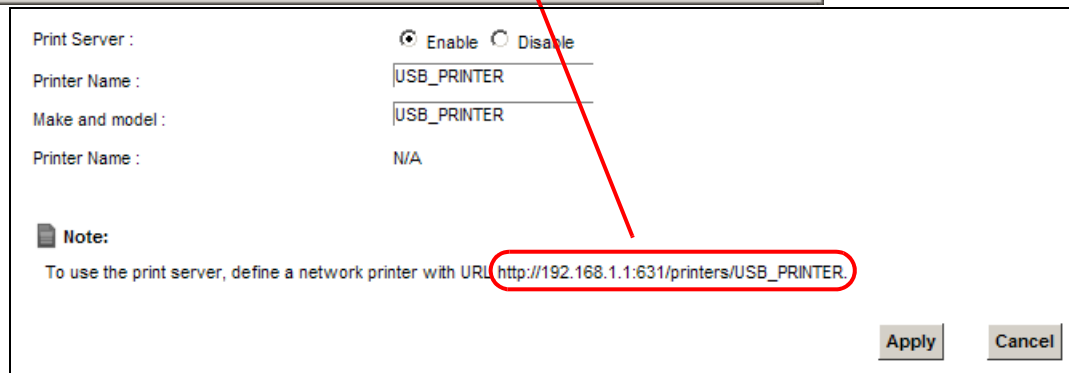
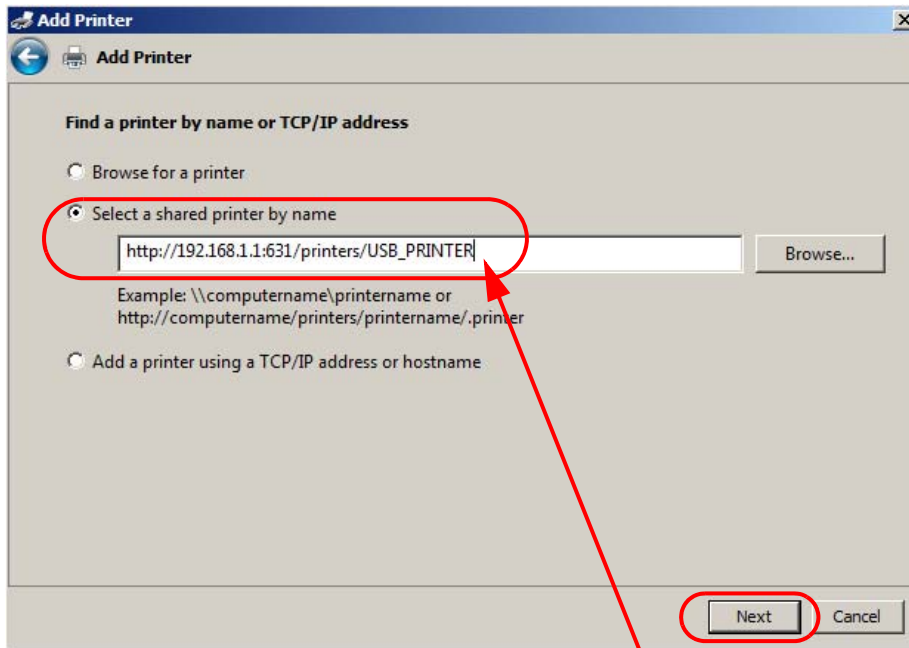
- 2 The **Add Printer** wizard screen displays. Click **Add a network, wireless or Bluetooth printer**.



- 3 Click **The printer that I want isn't listed**.




- 4 Select the **Select a shared printer by name** option. Enter the URL for your printer, **http://192.168.1.1:631/printers/USB_PRINTER**, in this example. This URL can be found in the Device's Web Configurator on the **Network Setting > USB Service > Printer Server** screen. Click **Next**.

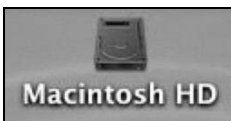


- 5 Install the printer driver. Please check the Windows CD if it includes the printer driver. If not, please install the driver from the CD included with your printer or by downloading it from the printer vendor's website.
- 6 After the printer driver installs successfully, choose if you want to set this printer to be the default.

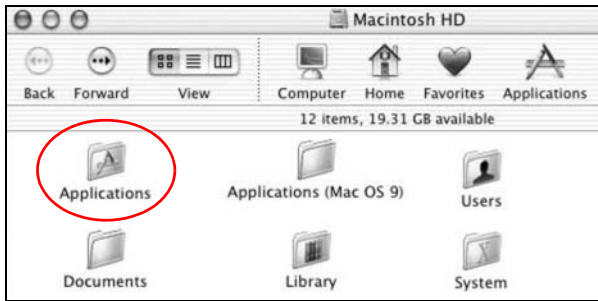
Add a New Printer Using Macintosh OS X

Complete the following steps to set up a print server driver on your Macintosh computer.

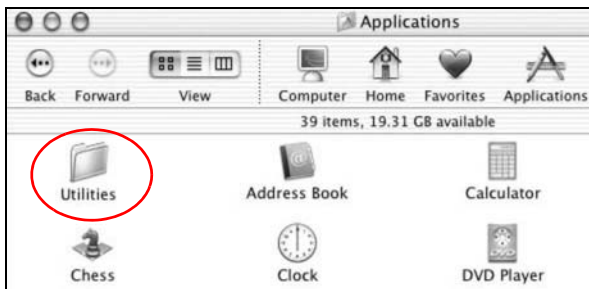
- 1 Click the **Print Center** icon  located in the Macintosh Dock (a place holding a series of icons/shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.
- 2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.



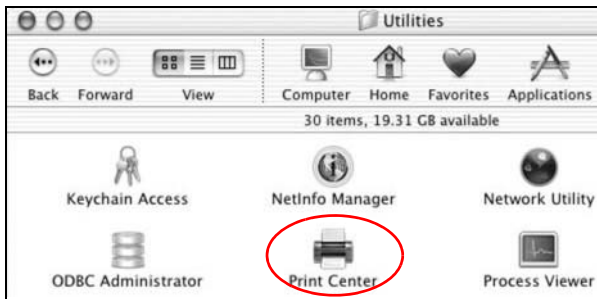
- 3 Double-click the **Applications** folder.



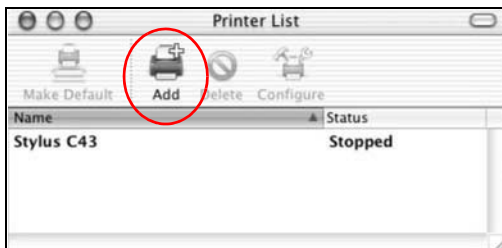
- 4 Double-click the **Utilities** folder.



- 5 Double-click the **Print Center** icon.



- 6 Click the **Add** icon at the top of the screen.

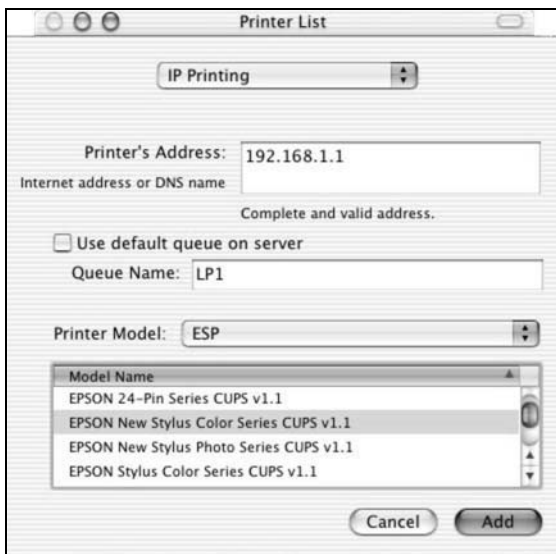


- 7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.
- 8 In the **Printer's Address** field, type the IP address of your Device.
- 9 Deselect the **Use default queue on server** check box.
- 10 Type **LP1** in the **Queue Name** field.

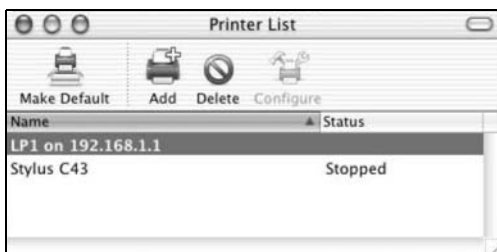
- 11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.



- 12 Click **Add** to select a printer model, save and close the **Printer List** configuration screen.



- 13 The **Name LP1 on 192.168.1.1** displays in the **Printer List** field. The default printer **Name** displays in bold type.



Your Macintosh print server driver setup is complete. You can now use the Device's print server to print from a Macintosh computer.

PART II

Technical Reference

Network Map and Status Screens

5.1 Overview

After you log into the Web Configurator, the **Network Map** screen appears. This shows the network connection status of the Device and clients connected to it.

You can use the **Status** screen to look at the current status of the Device, system resources, and interfaces (LAN, WAN, and WLAN).

5.2 The Network Map Screen

Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

If you prefer to view the status in a list, click **List View** in the **Viewing Mode** selection box. You can configure how often you want the Device to update this screen in **Refresh Interval**.

Figure 15 Network Map: Icon Mode



Figure 16 Network Map: List Mode

#	Device Name	IP Address	MAC Address	Address Source	Connection Type
1	unknown	172.23.30.10	00:1e:0b:24:f8:93	Static	Ethernet
2	unknown	172.23.30.20	10:78:d2:c5:19:cd	Static	Ethernet
3	unknown	172.23.30.31	74:d4:35:68:dd:4d	Static	Ethernet

In **Icon Mode**, if you want to view information about a client, click the client's name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change icon/name**.



In **List Mode**, you can also view the client's information.

5.3 The Status Screen

Use this screen to view the status of the Device. Click **Status** to open this screen.

Figure 17 Status Screen

ZyXEL VMG4381-B10A Quick Start Logout

Refresh interval: None

Status

Device Information	
Host Name:	ZyXEL
Model Number:	VMG4381-B10A
Firmware Version:	1.00(AAPU.0)b2_20140509
Serial Number:	S090Y00000000
WAN Information	
- DNS Server:	0.0.0.0 0.0.0.0
LAN Information	
- IP Address:	172.23.30.219
- IP Subnet Mask:	255.255.255.0
- DHCP:	Disable
- MAC Address:	CC:5D:4E:00:00:94
WLAN Information	
- MAC Address:	CC:5D:4E:00:00:95
- Status:	On
- SSID:	ZyXEL00000
- Channel:	Auto (Current: 1)
- Security:	No Security
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Off
Security	
- Firewall :	Disable

Interface Status		
Interface	Status	Rate
LAN1	Down	N/A
LAN2	Down	N/A
LAN3	Down	N/A
LAN4	Up	1000Mbps / Full duplex
MoCA LAN	Down	N/A
WLAN	Disabled	N/A
Ethernet WAN	Down	N/A
DSL	NoLink	N/A

System Status	
System Up Time:	0 days: 17 hours: 4 minutes
Current Date/Time:	01 Jan 2014 17:04:09
System Resource:	
- CPU Usage:	6.47%
- Memory Usage:	69%

Network Map Virtual Device

Connection Status Network Setting Security System Monitor Maintenance

Each field is described in the following table.

Table 5 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen.
Device Information	
Host Name	This field displays the Device system name. It is used for identification.
Model Number	This shows the model number of your Device.
Firmware Version	This is the current version of the firmware inside the Device.
WAN Information (These fields display when you have a WAN connection.)	
WAN Type	This field displays the current WAN connection type.
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) Address of your Device.
IP Address	This field displays the current IP address of the Device in the WAN. Click Release to release your IP address to 0.0.0.0. If you want to renew your IP address, click Renew .
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Encapsulation	This field displays the current encapsulation method.
LAN Information	
IP Address	This is the current IP address of the Device in the LAN.
IP Subnet Mask	This is the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the Device is providing to the LAN. Choices are: Server - The Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay - The Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. None - The Device is not providing any DHCP services to the LAN.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your Device.
WLAN Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of your Device.
Status	This displays whether WLAN is activated.
SSID	This is the descriptive name used to identify the Device in a wireless LAN.
Channel	This is the channel number used by the Device now.
Security	This displays the type of security mode the Device is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the Device is using in the wireless LAN.
WPS	This displays whether WPS is activated.
Security	
Firewall	This displays the firewall's current security level.
System Status	
System Up Time	This field displays how long the Device has been running since it last started up. The Device starts up when you plug it in, when you restart it (Maintenance > Reboot), or when you reset it.
Current Date/Time	This field displays the current date and time in the Device. You can change this in Maintenance > Time Setting .

Table 5 Status Screen (continued)

LABEL	DESCRIPTION
System Resource	
CPU Usage	This field displays what percentage of the Device's processing ability is currently used. When this percentage is close to 100%, the Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 10 on page 163).
Memory Usage	This field displays what percentage of the Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the Device is probably becoming unstable, and you should restart the device. See Section 34.2 on page 279 , or turn off the device (unplug the power) for a few seconds.

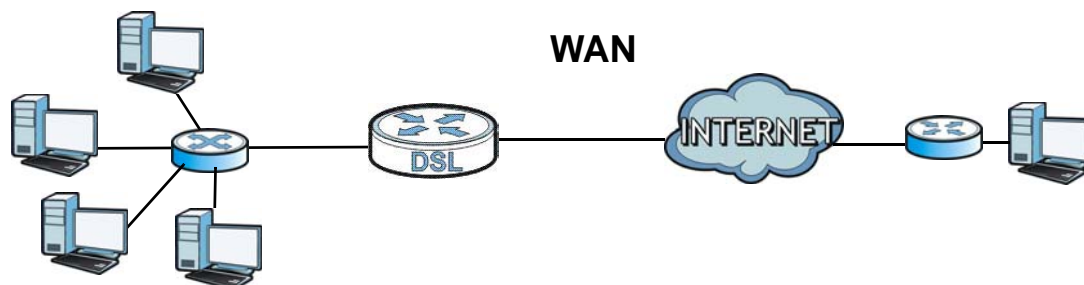
Broadband

6.1 Overview

This chapter discusses the Device's **Broadband** screens. Use these screens to configure your 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 18 LAN and WAN



3G (third generation) standards for the sending and receiving of voice, video, and data in a mobile environment.

You can attach a 3G wireless adapter to the USB port and set the Device to use this 3G connection as your WAN or a backup when the wired WAN connection fails.

Figure 19 3G WAN Connection



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 Device for Internet access ([Section 6.2 on page 79](#)).
- Use the **3G Backup** screen to configure 3G WAN connection ([Section 6.3 on page 89](#)).

- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions ([Section 6.4 on page 93](#)).
- Use the **8021x** screen to view and configure the IEEE 802.1x settings on the Device ([Section 6.5 on page 95](#)).

Table 6 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
ADSL over ATM	EoA	Routing	PPPoE/PPPOA	ATM PCV configuration, PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE/IPoA	ATM PCV configuration, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	ATM PCV configuration, and QoS

6.1.2 What You Need to Know

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

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

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

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

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 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

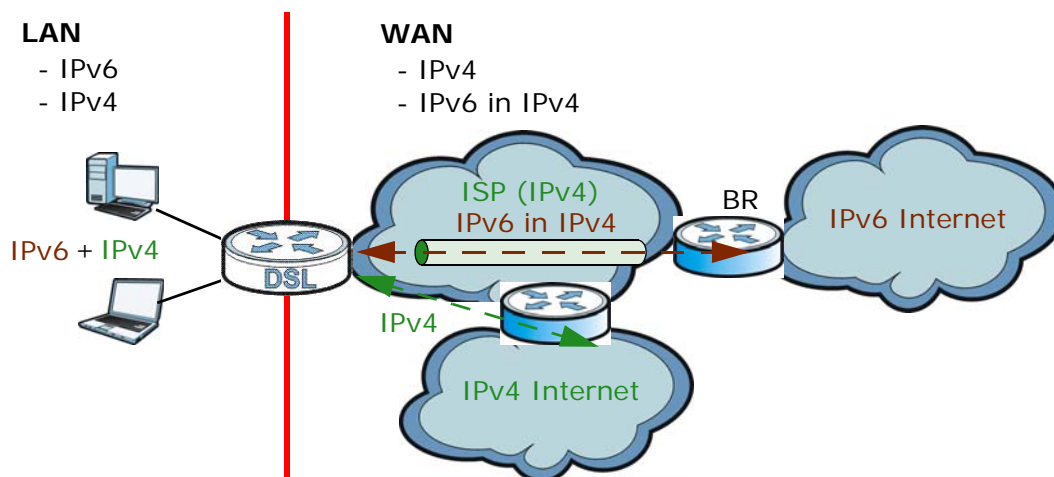
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, 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 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 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 Device uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 20 IPv6 Rapid Deployment

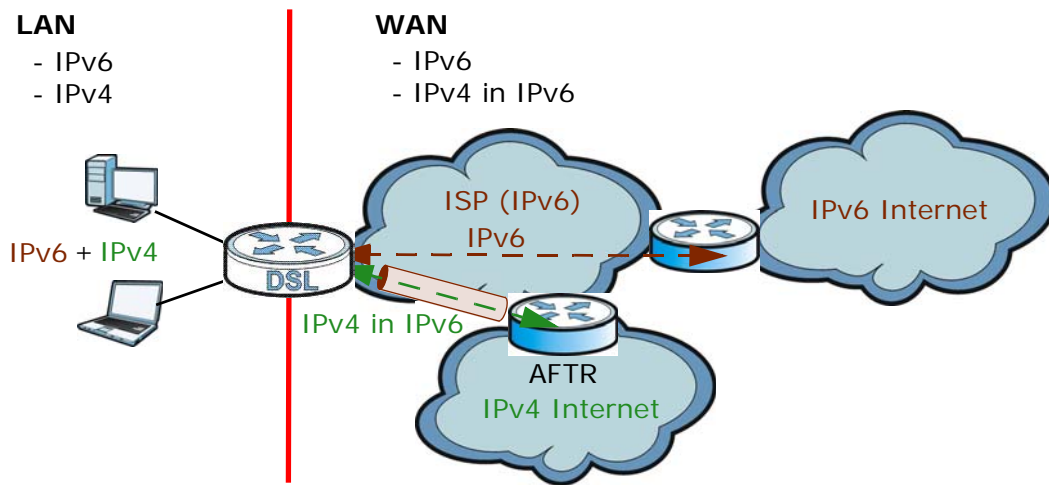


Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the 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 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 VDSL Router uses its configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 21 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 Device's Internet access settings. Click **Network Setting > Broadband** from the menu. The summary table shows you the configured WAN services (connections) on the Device.

Figure 22 Network Setting > Broadband

#	Name	Type	Mode	Encaps...	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	N	N	
2	VDSL_...	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
3	Etherne...	Ethernet	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	

The following table describes the labels in this screen.

Table 7 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, PTM, or Ethernet connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.

Table 7 Network Setting > Broadband (continued)

LABEL	DESCRIPTION
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 Device act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the 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 23 Routing Mode

The screenshot shows a configuration window for a WAN connection in Routing Mode. The 'General' section includes fields for Name, Type (set to 'ADSL over ATM'), Mode (set to 'Routing'), Encapsulation (set to 'PPPoE'), and IPv6/IPv4 Mode (set to 'IPv6/IPv4 DualStack'). The 'ATM PVC Configuration' section includes VPI (0), VCI (33), DSL Link Type (EoA), Encapsulation Mode (LLC/SNAP-BRIDGING), and Service Category (Non Realtime VBR). The 'PPP Information' section includes fields for PPP User Name, PPP Password, PPP Auto Connect, IDLE Timeout (5 minutes), PPPoE Service Name, and PPPoE Passthrough. The 'IP Address' section has radio buttons for 'Obtain an IP Address Automatically' (selected) and 'Static IP Address', with fields for IP Address, Subnet Mask, and Gateway IP address. The 'Routing Feature' section includes checkboxes for NAT Enable, IGMP Proxy Enable, and Apply as Default Gateway. The 'DNS server' section has radio buttons for Dynamic (selected) and Static, with fields for DNS Server 1 and DNS Server 2. The 'IPv6 Address' section has radio buttons for Automatic (selected) and Static, with a checkbox for 'Get IPv6 Address From DHCPv6 Server'. The 'IPv6 Routing Feature' section includes checkboxes for MLD Proxy Enable and Apply as Default Gateway. The 'IPv6 DNS Server' section has radio buttons for Dynamic (selected) and Static, with fields for IPv6 DNS Server 1 and IPv6 DNS Server 2. The 'QoS' section includes a Rate Limit field (in kbps). The 'MTU' section includes an MTU Size field (1492) and a range [68-1492]. At the bottom right, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 8 Routing Mode

LABEL	DESCRIPTION
General	
Active	Select this to activate the WAN configuration settings.
Name	Specify a descriptive name for this connection.

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
Type	<p>Select whether it is ADSL/VDSL over PTM, ADSL over ATM, or Ethernet connection.</p> <ul style="list-style-type: none"> • ADSL/VDSL over PTM: The Device uses the VDSL technology for data transmission over the DSL port. • ADSL over ATM: The Device uses the ADSL technology for data transmission over the DSL port. • Ethernet: The Device transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.
Mode	<p>Select Routing if your ISP give you one IP address only and you want multiple computers to share an Internet account.</p>
Encapsulation	<p>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.</p> <ul style="list-style-type: none"> • PPP over Ethernet (PPPoE): PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access. • IP over Ethernet (IPoE): In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. • PPP over ATM (PPPoA): PPPoA allows just one PPPoA connection over a PVC. • IP over ATM (IPoA): IPoA allows just one RFC 1483 routing connection over a PVC. <p>If your connection type is ADSL/VDSL over PTM or Ethernet, the choices are PPPoE and IPoE.</p> <p>If your connection type is ADSL over ATM, the choices are PPPoE, PPPoA, IPoE and IPoA.</p>
IPv6/IPv4 Mode	<p>Select IPv4 Only if you want the Device to run IPv4 only.</p> <p>Select IPv6/IPv4 DualStack to allow the Device to run IPv4 and IPv6 at the same time.</p> <p>Select IPv6 Only if you want the Device to run IPv6 only.</p>
ATM PVC Configuration (These fields appear when the Type is set to ADSL over ATM .)	
VPI	<p>The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.</p>
VCI	<p>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.</p>
DSL Link Type	<p>This field is not editable. The selection depends on the setting in the Encapsulation field.</p> <p>EoA (Ethernet over ATM) uses an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. EoA supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods.</p> <p>PPPoA (PPP over ATM) allows just one PPPoA connection over a PVC.</p> <p>IPoA (IP over ATM) allows just one RFC 1483 routing connection over a PVC.</p>

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
Encapsulation Mode	<p>Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:</p> <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 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. • LLC/ENCAPSULATION: More than one protocol can be carried over the same VC. This is available only when you select PPPoA in the Encapsulation field. • LLC/SNAP-ROUTING: In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select IPoA in the Encapsulation field.
Service Category	<p>Select UBR Without PCR or UBR With PCR for applications that are non-time sensitive, such as e-mail.</p> <p>Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
Peak Cell Rate	<p>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. This field is not available when you select UBR Without PCR.</p>
Sustainable Cell Rate	<p>The Sustainable 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.</p> <p>This field is available only when you select Non Realtime VBR or Realtime VBR.</p>
Maximum Burst Size	<p>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.</p> <p>This field is available only when you select Non Realtime VBR or Realtime VBR.</p>
PPP Information	<p>This is available only when you select PPPoE or PPPoA in the Mode field.</p>
PPP User Name	<p>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.</p>
PPP Password	<p>Enter the password associated with the user name above.</p>
PPP Auto Connect	<p>Select this option if you do not want the connection to time out.</p>
IDLE Timeout	<p>This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.</p> <p>This field is not configurable if you select PPP Auto Connect.</p>
PPPoE Service Name	<p>Enter the name of your PPPoE service here.</p>

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
PPPoE Passthrough	<p>This field is available when you select PPPoE encapsulation.</p> <p>In addition to the 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 Device. Each host can have a separate account and a public WAN IP address.</p> <p>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>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.</p>
IP Address	This is available only when you select IPv4 Only or IPv6/IPv4 DualStack in the IPv6/IPv4 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.
Routing Feature	This is available only when you select IPv4 Only or IPv6/IPv4 DualStack in the IPv6/IPv4 Mode field.
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	<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>Select this option to have the Device act as an IGMP proxy on this connection. This allows the 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	Select this option to have the Device use the WAN interface of this connection as the system default gateway.
DNS Server	This is available only when you select IPv4 Only or IPv6/IPv4 DualStack in the IPv6/IPv4 Mode field.
DNS	<p>Select Dynamic if you want the Device use the DNS server addresses assigned by your ISP.</p> <p>Select Static if you want the Device use the DNS server addresses you configure manually.</p>
DNS Server 1	Enter the first DNS server address assigned by the ISP.
DNS Server 2	Enter the second DNS server address assigned by the ISP.
IPv6 Address	This is available only when you select IPv6/IPv4 DualStack or IPv6 Only in the IPv6/IPv4 Mode field.
IPv6 Address	<p>Select Automatic if you want to have the Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.</p> <p>Select the Get IPv6 Address From DHCPv6 Server checkbox if you want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Device using the IPv6 prefix from an RA. This option is available only when you choose to get your IPv6 address automatically.</p> <p>Select Static if you have a fixed IPv6 address assigned by your ISP.</p>
WAN IPv6 Address	Enter the IPv6 address assigned by your ISP.

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Next Hop	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Device's interface(s). The gateway helps forward packets to their destinations.
IPv6 Routing Feature	You can enable IPv6 routing features in the following section.
MLD Proxy Enable	Select this checkbox to have the Device act as an MLD proxy on this connection. This allows the 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 Device use the WAN interface of this connection as the system default gateway.
IPv6 DNS Server	Configure the IPv6 DNS server in the following section.
IPv6 DNS	Select Dynamic to have the Device get the IPv6 DNS server addresses from the ISP automatically. Select Static to have the Device use the IPv6 DNS server addresses you configure manually.
IPv6 DNS Server 1	Enter the first IPv6 DNS server address assigned by the ISP.
IPv6 DNS Server 2	Enter the second IPv6 DNS server address assigned by the ISP.
Tunnel	The IPv6 rapid deployment fields display when you set the IPv6/IPv4 Mode field to IPv4 Only . See IPv6 Rapid Deployment on page 78 for more information.
Enable 6RD	Enable IPv6 rapid deployment to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
6RD Type	Select Static if you have the IPv4 address of the relay server, otherwise select DHCP to have the Device detect it automatically through DHCP.
6RD Border Relay Server IP	When you set the 6RD Type to Static , specify the relay server IPv4 address.
6RD IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's Border Relay router and connecting to the native IPv6 Internet.
Tunnel	The Dual Stack Lite fields display when you set the IPv6/IPv4 Mode field to IPv6 Only . Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 78 for more information.
Enable DS-Lite	Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
VLAN	These fields appear when the Type is set to ADSL/VDSL over PTM .
Active	Select this option to add the VLAN tag (specified below) to the outgoing traffic through this connection.
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.

Table 8 Routing Mode (continued)

LABEL	DESCRIPTION
QoS	
Rate Limit	Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection.
MTU	
MTU Size	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to exit this screen without saving.

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** as the interface type, the following screen appears.

Figure 24 Bridge Mode (ADSL/VDSL over PTM)

The following table describes the fields in this screen.

Table 9 Bridge Mode (ADSL/VDSL over PTM)

LABEL	DESCRIPTION
General	
Active	Select this to activate the WAN configuration settings.
Name	Enter a service name of the connection.
Type	Select ADSL/VDSL over PTM as the interface that you want to configure. The 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).

Table 9 Bridge Mode (ADSL/VDSL over PTM) (continued)

LABEL	DESCRIPTION
VLAN	This section is available only when you select ADSL/VDSL over PTM in the Type field.
Active	Select this to add the VLAN Tag (specified below) to the outgoing traffic through this connection.
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.
QoS	
Rate Limit	Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

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

Figure 25 Bridge Mode (ADSL over ATM)

The following table describes the fields in this screen.

Table 10 Bridge Mode (ADSL over ATM)

LABEL	DESCRIPTION
General	
Active	Select this to activate the WAN configuration settings.
Name	Enter a service name of the connection.
Type	Select ADSL over ATM as the interface for which you want to configure here. The Device uses the ADSL technology for data transmission over the DSL port.

Table 10 Bridge Mode (ADSL over ATM) (continued)

LABEL	DESCRIPTION
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	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	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.
DSL Link Type	<p>This field is not editable. The selection depends on the setting in the Encapsulation field.</p> <p>EoA (Ethernet over ATM) uses an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. EoA supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods.</p> <p>PPPoA (PPP over ATM) allows just one PPPoA connection over a PVC.</p> <p>IPoA (IP over ATM) allows just one RFC 1483 routing connection over a PVC.</p>
Encapsulation Mode	<p>Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:</p> <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 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. • LLC/ENCAPSULATION: More than one protocol can be carried over the same VC. This is available only when you select PPPoA in the Encapsulation field. • LLC/SNAP-ROUTING: In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select IPoA in the Encapsulation field.
Service Category	<p>Select UBR Without PCR or UBR With PCR for applications that are non-time sensitive, such as e-mail.</p> <p>Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
Peak Cell Rate	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. This field is not available when you select UBR Without PCR .
Sustainable Cell Rate	<p>The Sustainable 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.</p> <p>This field is available only when you select Non Realtime VBR or Realtime VBR.</p>
Maximum Burst Size	<p>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.</p> <p>This field is available only when you select Non Realtime VBR or Realtime VBR.</p>
QoS	

Table 10 Bridge Mode (ADSL over ATM) (continued)

LABEL	DESCRIPTION
Rate Limit	Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.3 The 3G Backup Screen

Use this screen to configure your 3G settings. Click **Network Setting > Broadband > 3G Backup**.

Note: The actual data rate you obtain varies depending the 3G card you use, the signal strength to the service provider's base station, and so on.

Figure 26 Network Setting > Broadband > 3G Backup

General

3G Backup Enable Disable (settings are invalid when disabled)

Trigger by ETHER WAN Down (trigger 3G backup when physical link of primary WAN is down)

Ping Check Enable Disable

Check Cycle: Every (5-30 Sec.)

Consecutive Fail: (2-5 times)

Ping Default Gateway

Ping the Host (Host Name or IP address)

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

3G Connection Settings

Card description: N/A

Username: (Optional)

Password: (Optional)

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

IP Address:

Obtain DNS info dynamically

Use the following static DNS IP address

Primary DNS server:

Secondary DNS server:

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

Budget Setup

Enable Budget Control Enable Disable

Time Budget: hours per month

Data Budget: Mbytes per month

Data Budget: kPackets per month

Reset all budget counters on day of per month

Actions before over budget:

Enable % of time budget

Enable % of data budget (Mbytes)

Enable % of data budget (Packets)

Actions when over budget:

Current 3G connection

Actions:

Enable Email Notification

Mail Server:

Over Budget Email Title:

Send Notification to Email:

Interval: minute(s)

Enable Log: Interval minute(s)

The following table describes the labels in this screen.

Table 11 Network Setting > Broadband > 3G Backup

LABEL	DESCRIPTION
General	
3G Backup	Select Enable to have the Device use the 3G connection as your WAN or a backup when the wired WAN connection fails.
Ping Check	Select Enable if you want the Device to ping check the connection status of your WAN. You can configure the frequency of the ping check and number of consecutive failures before triggering 3G backup.
Check Cycle	Enter the frequency of the ping check in this field.
Consecutive Fail	Enter how many consecutive failures are required before 3G backup is triggered.
Ping Default Gateway	Select this to have the Device ping the WAN interface's default gateway IP address.
Ping the Host	Select this to have the Device ping the particular host name or IP address you typed in this field.
3G Connection Settings	
Card description	This field displays the manufacturer and model name of your 3G card if you inserted one in the 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.
PIN	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. 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 3G card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, leave this field blank.
Dial string	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. For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan.
APN	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. You can enter up to 32 ASCII printable characters. Spaces are allowed.
Connection	Select Nailed UP if you do not want the connection to time out. 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.
Max Idle Timeout	This value specifies the time in minutes that elapses before the Device automatically disconnects from the ISP.
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected Use the following static IP address .

Table 11 Network Setting > Broadband > 3G Backup (continued)

LABEL	DESCRIPTION
Obtain DNS info dynamically	Select this to have the Device get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the Device 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.
Advanced	Click this to show the advanced 3G backup settings.
Budget Setup	
Enable Budget Control	Select Enable to set a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The Device takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the 3G connection can be used within one month. If you change the value after you configure and enable budget control, the Device resets the statistics.
Data Budget (Mbytes)	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month. Select Download/Upload to set a limit on the total traffic in both directions. Select Download to set a limit on the downstream traffic (from the ISP to the Device). Select Upload to set a limit on the upstream traffic (from the Device to the ISP). If you change the value after you configure and enable budget control, the Device resets the statistics.
Data Budget (kPackets)	Select this and specify how much downstream and/or upstream data (in k Packets) can be transmitted via the 3G connection within one month. Select Download/Upload to set a limit on the total traffic in both directions. Select Download to set a limit on the downstream traffic (from the ISP to the Device). Select Upload to set a limit on the upstream traffic (from the Device to the ISP). If you change the value after you configure and enable budget control, the Device resets the statistics.
Reset all budget counters on	Select the date on which the Device resets the budget every month. Select last if you want the Device to reset the budget on the last day of the month. Select specific and enter the number of the date you want the Device to reset the budget
Reset time and data budget counters	Click this button to reset the time and data budgets immediately. The count starts over with the 3G 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.
Actions before over budget	Specify the actions the Device takes before the time or data limit exceeds.
Enable % of time budget/data budget (Mbytes)/data budget (kPackets)	Select Enable 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 Device resets the statistics.

Table 11 Network Setting > Broadband > 3G Backup (continued)

LABEL	DESCRIPTION
Actions when over budget	Specify the actions the Device takes when the time or data limit is exceeded.
Current 3G connection	Select Keep to maintain an existing 3G connection or Drop to disconnect it.
Enable Email Notification	Select this to enable the e-mail notification function. The Device will e-mail you a notification when there over budget occurs.
Mail Server	Select a mail server for the e-mail address specified below. If you do not select a mail server, e-mail notifications cannot be sent via e-mail. You must have configured a mail server already in the Maintenance > Email Notification screen.
Over Budget Email Title	Type a title that you want to be in the subject line of the e-mail notifications that the 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 Device to e-mail you.
Enable Log	Select this to activate the logging function at the interval you set in this field.
Basic	Click this to hide the advanced settings of 3G backup.
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to return to the previous configuration.

6.4 The Advanced Screen

Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M, and DSL PhyR functions. The 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.

6.4.1 DSL Bonding

If the DSLAM of your ISP supports DSL bonding, you can connect the two DSL ports on the Device to two separate telephone jacks and enable the bonding feature in the **Advanced** screen.

DSL signals have distance limitations. VDSL2 (profile 17a) supports greater speed but offer shorter distances (within 3000 ft). The farther away the subscribers are from the DSLAM, the slower the speed. VDSL (profile 12a) provides longer distance range (over 3000 ft) but at lower speeds. DSL bonding allows subscribers to use data streams spread over two DSL lines in order to (almost) double the speed at longer distances. You may choose to use DSL bonding if the DSLAM supports it and there are two DSL lines to the DSLAM.

The total available bandwidth for the subscriber then becomes the sum of the bandwidth available for each of the subscriber's line connections. The data rate depends on the DSL type, its standard/profile, and the standard/profile that the DSLAM supports. The table below shows the transmission data rate for single DSL line and DSL bonding.

Table 12 Comparison Table for Single DSL line and DSL Bonding

ITEM	VDSL2	VDSL BONDING	ADSL2+	ADSL(2+) BONDING
PROFILE/ STANDARD	G993.2 Profile 17a	G993.2 Profile 12a	G.992.5	G.992.5
MAX. DOWNSTREAM/ UPSTREAM	100/60 Mbps	50/25 x 2 = 100/50 Mbps	25/1 Mbps	25/1 x 2 = 50/2 Mbps
DISTANCE	within 3000 ft	over 3000 ft	over 5000 ft	5000 to 7000 ft

For a single VDSL2 line, the profile is 17a, which provides a maximum data rate of 100/60 Mbps (downstream/upstream). A VDSL2 17a bonding profile can reach 200Mbps/100Mbps. If VDSL bonding is used, the supported profile is 12a, which provides a maximum data rate of 50/25 Mbps for each VDSL line. The ideal total data rate for the bonded connection is 100/50 Mbps.

For a single ADSL line, the standard with the highest data rate supported is ADSL2+, which provides 25/1 Mbps data rate. When ADSL bonding is used, the data rate doubles to 50/2 Mbps.

In addition, DSL bonding supports ADSL bonding fallback. If a VDSL connection cannot be established, the Device tries to use ADSL. If the VDSL connection is re-established, the Device automatically switches back to VDSL. You must enable DSL bonding in order to use ADSL fallback.

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

Figure 27 Network Setting > Broadband > Advanced

DSL Bonding

State: Enable Disable

xDSL setup

PTM over ADSL: Enable Disable

Annex M: Enable Disable

PhyR US: Enable Disable

PhyR DS: Enable Disable

The following table describes the labels in this screen.

Table 13 Network Setting > Network Setting > Broadband

LABEL	DESCRIPTION
State	Select Enable to use the DSL bonding and ADSL fallback features. Make sure your ISP supports these functions.
PTM over ADSL	Select Enable to use PTM over ADSL. Since PTM has less overhead than ATM, some ISPs use PTM over ADSL for better performance.
Annex M	You can enable Annex M for the Device to use double upstream mode to increase the maximum upstream transfer rate.

Table 13 Network Setting > Network Setting > Broadband (continued)

LABEL	DESCRIPTION
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.
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to return to the previous configuration.

6.5 The 8021x Screen

You can view and configure the 802.1x authentication settings in the **8021x** screen. Click **Network Setting > Broadband > 8021x** to display the following screen.

Figure 28 Network Setting > Broadband > 8021x

802.1x Authentication List.								
#	Status	Interface	EAP Identity	EAP method	Bidirectional Au...	Certificate	Trusted CA	Modify
1		N/A	N/A	EAP-TLS	NO	N/A	N/A	
2		N/A	N/A	EAP-TLS	NO	N/A	N/A	

Note:
You need to add the WAN interface first before you can modify the authentication rules.

The following table describes the labels in this screen.

Table 14 Network Setting > Network Setting > 8021x

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field displays whether the authentication is active or not. A yellow bulb signifies that this authentication is active. A gray bulb signifies that this authentication is not active.
Interface	This is the interface that uses the authentication. This displays N/A when there is no interface assigned.
EAP Identity	This shows the EAP identity of the authentication. This displays N/A when there is no EAP identity assigned.
EAP method	This shows the EAP method used in the authentication. This displays N/A when there is no EAP method assigned.
Bidirectional Authentication	This shows whether bidirectional authentication is allowed.
Certificate	This shows the certificate used for this authentication. This displays N/A when there is no certificate assigned.
Trusted CA	This shows the Trusted CA used for this authentication. This displays N/A when there is no Trusted CA assigned.
Apply	Click Apply to save your changes back to the Device.
Cancel	Click Cancel to return to the previous configuration.

6.5.1 Edit 802.1x Settings

Use this screen to edit a 802.1x authentication's settings. Click the **Edit** icon next to the rule you want to edit. The screen shown next appears.

Figure 29 802.1x: Add/Edit

The following table describes the labels in this screen.

Table 15 802.1x: Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate the authentication. Select this to enable the authentication. Clear this to disable this authentication without having to delete the entry.
Interface	Select the interface that uses the authentication.
EAP Identity	Enter the EAP identity of the authentication.
EAP method	This is the EAP method used for this authentication.
Enable Bidirectional Authentication	Select this to allow bidirectional authentication.
Certificate	Select the certificate you want to assign to the authentication. You need to import the certificate in the Security > Certificates > Local Certificates screen.
Trusted CA	Select the Trusted CA you want to assign to the authentication. You need to import the certificate in the Security > Certificates > Trusted CA screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.6 Technical Reference

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

Encapsulation

Be sure to use the encapsulation method required by your ISP. The Device can work in bridge mode or routing mode. When the 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 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 Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

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 Device queries all directly connected networks to gather group membership. After that, the 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 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 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.

7.1 Overview

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

7.1.1 What You Can Do in this Chapter

This section describes the Device's **Wireless** screens. Use these screens to set up your 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 102](#)).
- Use the **More AP** screen to set up multiple wireless networks on your Device ([Section 7.3 on page 109](#)).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the Device ([Section 7.4 on page 111](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 7.5 on page 112](#)).
- 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 114](#)).
- Use the **WDS** screen to set up a Wireless Distribution System, in which the Device acts as a bridge with other ZyXEL access points ([Section 7.7 on page 114](#)).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold ([Section 7.8 on page 116](#)).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results ([Section 7.9 on page 118](#)).

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 118](#) for advanced technical information on wireless networks.

7.2 The General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the Device from a computer connected to the wireless LAN and you change the 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 Device’s new settings.

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

Figure 30 Network Setting > Wireless > General

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

Table 16 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can Enable or Disable the wireless LAN in this field.
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.
Channel	Set the channel depending on your particular region. Select a channel or use Auto to have the Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the Device is currently using then displays next to this field.
more.../less	Click more... to show more information. Click less to hide them.

Table 16 Network Setting > Wireless > General (continued)

LABEL	DESCRIPTION
Bandwidth	<p>Select whether the Device uses a wireless channel width of 20MHz or 40MHz.</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>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	<p>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.</p>
Passphrase Type	<p>If you set security for the wireless LAN and have the Device generate a password, the setting in this field determines how the Device generates the password.</p> <p>Select None to set the Device's password generation to not be based on a passphrase.</p> <p>Select Fixed to use a 16 character passphrase for generating a password.</p> <p>Select Variable to use a 16 to 63 character passphrase for generating a password.</p>
Passphrase Key	<p>For a fixed type passphrase enter 16 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.</p> <p>For a variable type passphrase enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.</p>
Wireless Network Settings	
Wireless Network Name (SSID)	<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>
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>
Client Isolation	<p>Select this to keep the wireless clients in this SSID from communicating with each other through the Device.</p>
MBSSID/LAN Isolation	<p>Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or wired LAN devices through the Device.</p> <p>Select both Client Isolation and MBSSID/LAN Isolation to allow this SSID's wireless clients to only connect to the Internet through the Device.</p>
Enhanced Multicast Forwarding	<p>Select this check box to allow the Device to convert wireless multicast traffic into wireless unicast traffic.</p>
BSSID	<p>This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.</p>
Maximum Bandwidth	<p>Specify the maximum rate for wireless traffic in kilobits per second (Kbps).</p>
Security Level	
Security Mode	<p>Select Basic (WEP) or More Secure (WPA(2)-PSK, WPA(2)) 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 Device. When you select to use a security, additional options appears in this screen.</p> <p>Or you can select No Security to allow any client to associate this network without any data encryption or authentication.</p> <p>See the following sections for more details about this field.</p>

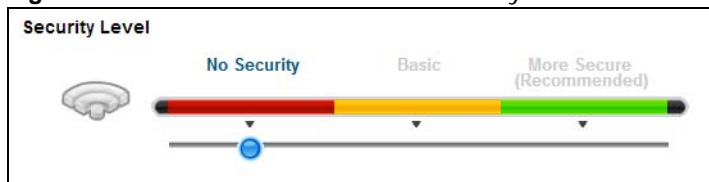
Table 16 Network Setting > Wireless > General (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

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 Device, your network is accessible to any wireless networking device that is within range.

Figure 31 Wireless > General: No Security

The following table describes the labels in this screen.

Table 17 Wireless > General: No Security

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

7.2.2 Basic (WEP Encryption)

WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK if all your wireless devices support it, or use WPA or WPA2 if your wireless devices support it and you have a RADIUS server. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

Your Device allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption, click **Network Setting > Wireless** to display the **General** screen, then select **Basic** as the security level.

Figure 32 Wireless > General: Basic (WEP)

Security Level

No Security **Basic** More Secure (Recommended)

Security Mode: WEP

Generate password automatically

64-bit: Enter 5 ASCII characters or 10 hex characters ("0-9", "A-F")
 128-bit: Enter 13 ASCII characters or 26 hex characters ("0-9", "A-F")
 Select one password as your active password.

Password 1: 533C4B868F344
 0CB527590DEF1 [less](#)

Password 2: 1234567890123

Password 3: 1234567890123

Password 4: 1234567890123

WEP Encryption: 128-bit ▼

The following table describes the labels in this screen.

Table 18 Wireless > General: Basic (WEP)

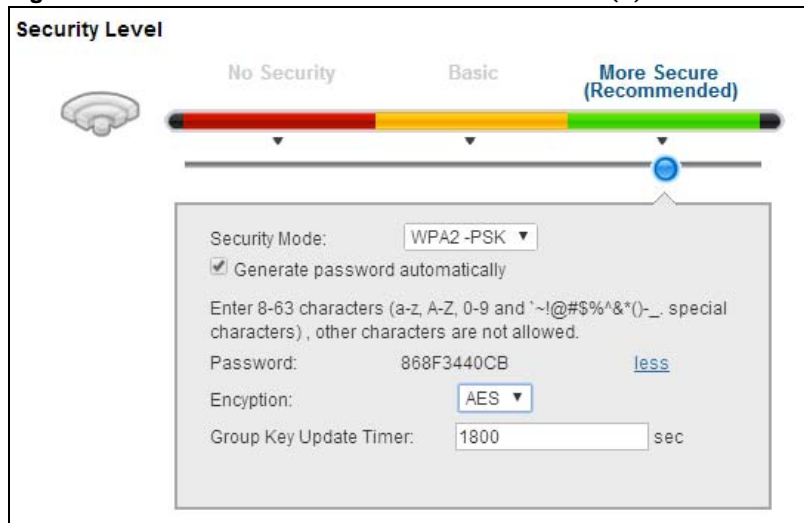
LABEL	DESCRIPTION
Security Level	Select Basic to enable WEP data encryption.
Generate password automatically	Select this option to have the Device automatically generate a password. The password field will not be configurable when you select this option.
Password 1~4	The password (WEP keys) are used to encrypt data. Both the Device and the wireless stations must use the same password (WEP key) for data transmission. If you chose 64-bit WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one password, only one password can be activated at any one time. The default password is Password 1 .
more.../less	Click more... to show more fields in this section. Click less to hide them.
WEP Encryption	Select 64-bits or 128-bits . This dictates the length of the security key that the network is going to use.

7.2.3 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 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-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 33 Wireless > General: More Secure: WPA(2)-PSK



The following table describes the labels in this screen.

Table 19 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 or WPA2-PSK from the drop-down list box.
Generate password automatically	Select this option to have the Device automatically generate a password. The password field will not be configurable when you select this option.
Password	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. If you did not select Generate password automatically , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
more.../less	Click more... to show more fields in this section. Click less to hide them.
WPA-PSK Compatible	This field appears when you choose WPA-PSK2 as the Security Mode . Check this field to allow wireless devices using WPA-PSK security mode to connect to your Device. The Device supports WPA-PSK and WPA2-PSK simultaneously.

Table 19 Wireless > General: More Secure: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
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.
Group Key Update Timer	The Group Key Update Timer is the rate at which the RADIUS server sends a new group key out to all clients.

7.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

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

Figure 34 Wireless > General: More Secure: WPA(2)

The screenshot shows a configuration interface for wireless security. At the top, a 'Security Level' slider is positioned at 'More Secure (Recommended)'. Below this, the 'Security Mode' is set to 'WPA2'. The 'Authentication Server' section includes fields for 'IP Address' (0.0.0.0), 'Port Number' (1812), and 'Shared Secret'. There is a 'Show password' checkbox and a 'less' link. The 'WPA Compatible' section has radio buttons for 'Enable' and 'Disable', with 'Disable' selected. The 'Encryption' dropdown is set to 'AES'. The 'WPA2 Pre-authentication' section has radio buttons for 'Enable' and 'Disable', with 'Disable' selected. The 'Network Re-auth Interval' is set to 36000 seconds, and the 'Group Key Update Timer' is set to 1800 seconds.

The following table describes the labels in this screen.

Table 20 Wireless > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Level	Select More Secure to enable WPA(2)-PSK data encryption.
Security Mode	Choose WPA or WPA2 from the drop-down list box.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.

Table 20 Wireless > General: More Secure: WPA(2) (continued)

LABEL	DESCRIPTION
Port Number	Enter the port number of the external authentication server. The default port number is 1812 . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the Device. The key must be the same on the external authentication server and your Device. The key is not sent over the network.
more.../less	Click more... to show more fields in this section. Click less to hide them.
WPA Compatible	This field is only available for WPA2. Select this if you want the Device to support WPA and WPA2 simultaneously.
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.
WPA2 Pre-Authentication	This field is available only when you select WPA2 . 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. Select Enabled to turn on preauthentication in WAP2. Otherwise, select Disabled .
Network Re-auth Interval	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The Group Key Update Timer is the rate at which the RADIUS server sends a new group key out to all clients.

7.3 The More AP Screen

[This screen is not applicable to VMG4381.](#)

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the Device.

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

Figure 35 Network Setting > Wireless > More AP

#	Status	SSID	Security	Guest WLAN	Modify
1		ZyXEL5F5B4_Guest1	WPA-PSK	N/A	
2		ZyXEL5F5B4_Guest2	WPA-PSK	N/A	
3		ZyXEL5F5B4_Guest3	WPA-PSK	N/A	

The following table describes the labels in this screen.

Table 21 Network Setting > Wireless > 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. A gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the 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.
Modify	Click the Edit icon to configure the SSID profile.

7.3.1 Edit More AP

[This screen is not applicable to VMG4381.](#) Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 36 More AP: Edit

The following table describes the fields in this screen.

Table 22 More AP: Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can Enable or Disable the wireless LAN in this field.

Table 22 More AP: Edit (continued)

LABEL	DESCRIPTION
Passphrase Type	<p>If you set security for the wireless LAN and have the Device generate a password, the setting in this field determines how the Device generates the password.</p> <p>Select None to set the Device's password generation to not be based on a passphrase.</p> <p>Select Fixed to use a 16 character passphrase for generating a password.</p> <p>Select Variable to use a 16 to 63 character passphrase for generating a password.</p>
Passphrase Key	<p>For a fixed type passphrase enter 16 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.</p> <p>For a variable type passphrase enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.</p>
Wireless Network Settings	
Wireless Network Name (SSID)	<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>
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.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or LAN devices.
Enhanced Multicast Forwarding	Select this check box to allow the Device to convert wireless multicast traffic into wireless unicast traffic.
Maximum Bandwidth	Specify the maximum rate for wireless traffic in kilobits per second (Kbps).
Security Level	
Security Mode	<p>Select Basic (WEP) or More Secure (WPA(2)-PSK, WPA(2)) 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 Device. After you select to use a security, additional options appears in this screen.</p> <p>Or you can select No Security to allow any client to associate this network without any data encryption or authentication.</p> <p>See Section 7.2.1 on page 105 for more details about this field.</p>
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

7.4 MAC Authentication

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**). 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 devices to configure this screen.

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

Figure 37 Wireless > MAC Authentication

General
 SSID :
 ZyXEL5F5B4_Guest1
 MAC Restrict Mode : Disable Allow Deny

MAC address List
 Add new MAC address

#	MAC Address	Modify

Notes:
 If mode of first SSID 'allow' is choosed and MAC list is empty, WPS will be disabled.

Apply Cancel

The following table describes the labels in this screen.

Table 23 Wireless > MAC Authentication

LABEL	DESCRIPTION
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 Device. MAC addresses not listed will be allowed to access the Device. Select Allow to permit access to the Device. MAC addresses not listed will be denied access to the Device.
Add new MAC address	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 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 Device.
Modify	Click the Delete icon to delete the entry.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

7.5 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See [Section 7.10.9.3 on page 127](#) for more information about WPS.

Note: The Device applies the security settings of the **SSID1** profile (see [Section 7.2 on page 102](#)). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network Setting > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 38 Network Setting > Wireless > WPS

WPS Setup

WPS: Enable Disable (The settings in this screen are invalid if you select this.)

Method 1	Method 2	Method 3
<p>Push Button Configuration</p> <p>1. Click "Connect".</p> <p>Connect</p> <p>2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".</p>	<p>Register Wireless Client's PIN Number</p> <p>1. Enter the PIN of your wireless client and click "Register".</p> <p><input type="text"/> Register</p> <p>2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".</p>	<p>Enter AP's PIN Number in Wireless Client</p> <p>Current state: Unconfigured</p> <p>1. Enter current PIN 19838588 on your wireless client.</p> <p>Generate New PIN Number</p>

Notes:

- This function only works on the first SSID.
- Click the "Release Configuration" button to have the WPS status changed to "Unconfigured". Otherwise, WPS status is in "Configured" mode.

Apply **Cancel**

The following table describes the labels in this screen.

Table 24 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
WPS	Select Enable to activate WPS on the Device.
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
Connect	Click this button to add another WPS-enabled wireless device (within wireless range of the 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 Connect 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 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 Device.
Method 3	Use this section to set up a WPS wireless network by entering the PIN of the Device into the client.
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 Device.
Generate New PIN Number	The PIN (Personal Identification Number) of the 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 Number button to have the Device create a new PIN.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.6 The WMM Screen

Use this screen to enable Wi-Fi MultiMedia (WMM) and WMM Power Save in wireless networks for multimedia applications.

Click **Network Setting > Wireless > WMM**. The following screen displays.

Figure 39 Network Setting > Wireless > WMM

WMM : Enable Disable
 WMM Automatic Power Save Delivery (APSD) : Enable Disable

Apply Cancel

The following table describes the labels in this screen.

Table 25 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM	Select On to have the Device automatically give a service 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.
WMM Automatic Power Save Delivery	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Device until the Device "wakes up". The Device wakes up periodically to check for incoming data. Note: Note: This works only if the wireless device to which the Device is connected also supports this feature.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.7 The WDS Screen

An AP using the Wireless Distribution System (WDS) can function as a wireless network bridge allowing you to wirelessly connect two wired network segments. The **WDS** screen allows you to configure the Device to connect to two or more APs wirelessly when WDS is enabled.

Use this screen to set up your WDS (Wireless Distribution System) links between the Device and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made.

Note: WDS security is independent of the security settings between the Device and any wireless clients.

Note: At the time of writing, WDS is compatible with other ZyXEL APs only. Not all models support WDS links. Check your other AP's documentation.

Click **Network Setting > Wireless > WDS**. The following screen displays.









Figure 40 Network Setting > Wireless > WDS

Wireless Bridge Setup

AP Mode: ▾

Bridge Restrict: Enable Disable

Remote Bridges MAC Address

#	MAC Address	Modify	Scan
1		 	
2		 	
3		 	
4		 	

Notes:

1. The WDS function only works when the security mode is set to No Security, WEP, WPA-PSK and WPA2-PSK.
2. The WDS connection security mode is based on the settings configured in the Wireless > General screen.
3. The WDS function only works with the first SSID.
4. If the AP mode is Wireless Bridge, WPS will be disabled.
5. The SSID should be the same in both WPA-PSK or WPA-PSK2 security modes.

The following table describes the labels in this screen.

Table 26 Network Setting > Wireless > WDS

LABEL	DESCRIPTION
Wireless Bridge Setup	
AP Mode	Select the operating mode for your Device. <ul style="list-style-type: none"> • Access Point - The Device functions as a bridge and access point simultaneously. • Wireless Bridge - The Device acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the Device wirelessly.
Bridge Restrict	This field is available only when you set operating mode to Access Point . Select Enabled to turn on WDS and enter the peer device's MAC address manually in the table below. Select Disable to turn off WDS.
Remote Bridge MAC Address	You can enter the MAC address of the peer device by clicking the Edit icon under Modify .
#	This is the index number of the entry.
MAC Address	This shows the MAC address of the peer device. You can connect to up to 4 peer devices.
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 remove this entry.
Scan	Click the Scan icon to search and display the available APs within range.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.7.1 WDS Scan

You can click the **Scan** icon in **Wireless > WDS** to have the Device automatically search and display the available APs within range. Select an AP and click **Apply** to have the Device establish a wireless link with the selected wireless device.

Figure 41 WDS: Scan

#	SSID	BSSID
<input checked="" type="radio"/>	5200-LOC24G-PSK	00:13:49:FE:11:01
<input type="radio"/>	5200-LOC24G-WPA2	06:13:49:FE:11:01
<input type="radio"/>	EddyLab	00:13:49:31:63:06

The following table describes the labels in this screen.

Table 27 WDS: Scan

LABEL	DESCRIPTION
Wireless Bridge Scan Setup	
Refresh	Click Refresh to update the table.
#	This is the index number of the entry.
SSID	This shows the SSID of the available wireless device within range.
BSSID	This shows the MAC address of the available wireless device within range.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.8 The Others Screen

Use this screen to configure advanced wireless settings. Click **Network Setting > Wireless > Others**. The screen appears as shown.

See [Section 7.10.2 on page 120](#) for detailed definitions of the terms listed in this screen.

Figure 42 Network Setting > Wireless > Others

The following table describes the labels in this screen.

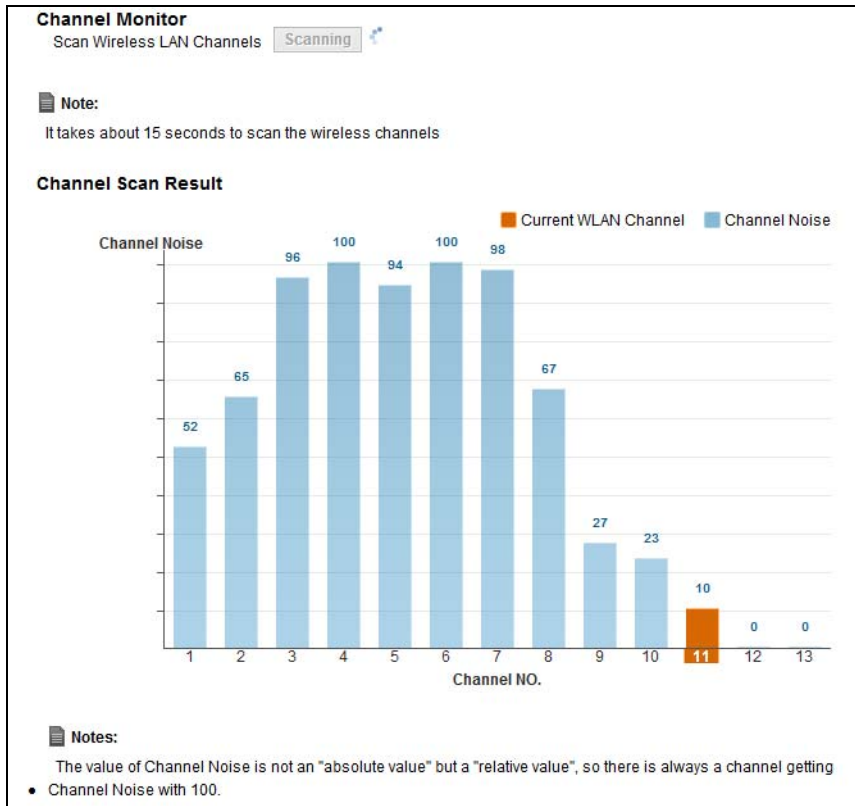
Table 28 Network Setting > Wireless > Others

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.
Auto Channel Timer	If you set the channel to Auto in the Network Setting > Wireless > General screen, specify the interval in minutes for how often the Device scans for the best channel. Enter 0 to disable the periodical scan.
Output Power	Set the output power of the 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 20ms 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 100.
802.11 Mode	Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the Device. Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the Device. Select 802.11n Only to allow only IEEE 802.11n compliant WLAN devices to associate with the Device. Select 802.11b/g Mixed to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Device. The transmission rate of your 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 Device. The transmission rate of your Device might be reduced.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select Off to disable 802.11 protection. The transmission rate of your Device might be reduced in a mixed-mode network. This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only .
Preamble	Select a preamble type from the drop-down list box. Choices are Long or Short . See Section 7.10.7 on page 124 for more information. This field is configurable only when you set 802.11 Mode to 802.11b .
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.9 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 43 Network Setting > Wireless > Channel Status



7.10 Technical Reference

This section discusses wireless LANs in depth. For more information, see [Appendix D on page 331](#).

7.10.1 Wireless Network Overview

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

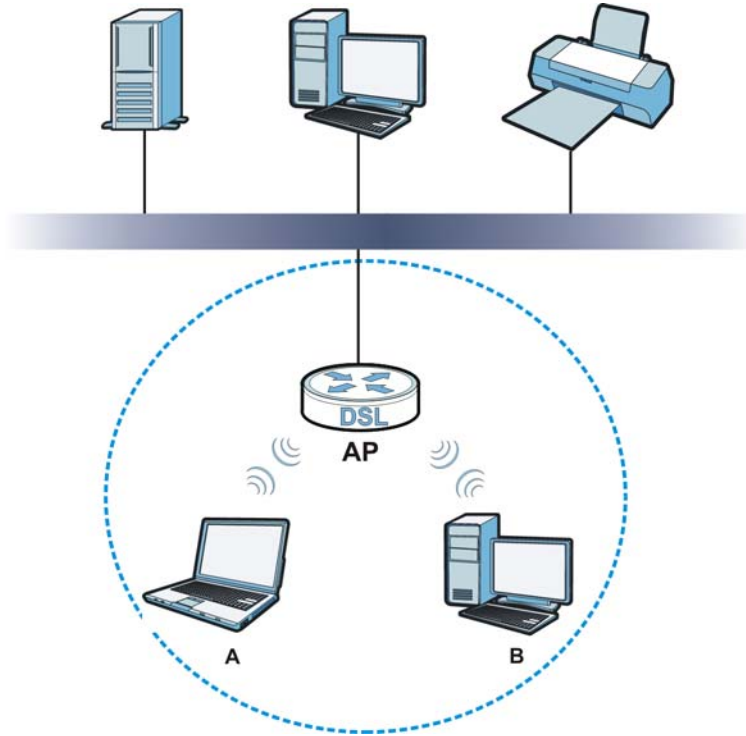
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, 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 44 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 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 Device's Web Configurator.

Table 29 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>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.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the Device. The lower the value, the more often the devices must get permission.</p> <p>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 Device.</p>
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 Device does, it cannot communicate with the 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 Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the 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 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

-
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.


wireless users to get a 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 121](#) for information about this.)

Table 30 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest 	No Security	WPA
	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

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, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

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.

When you select **WPA2** or **WPA2-PSK** in your Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the Device.

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

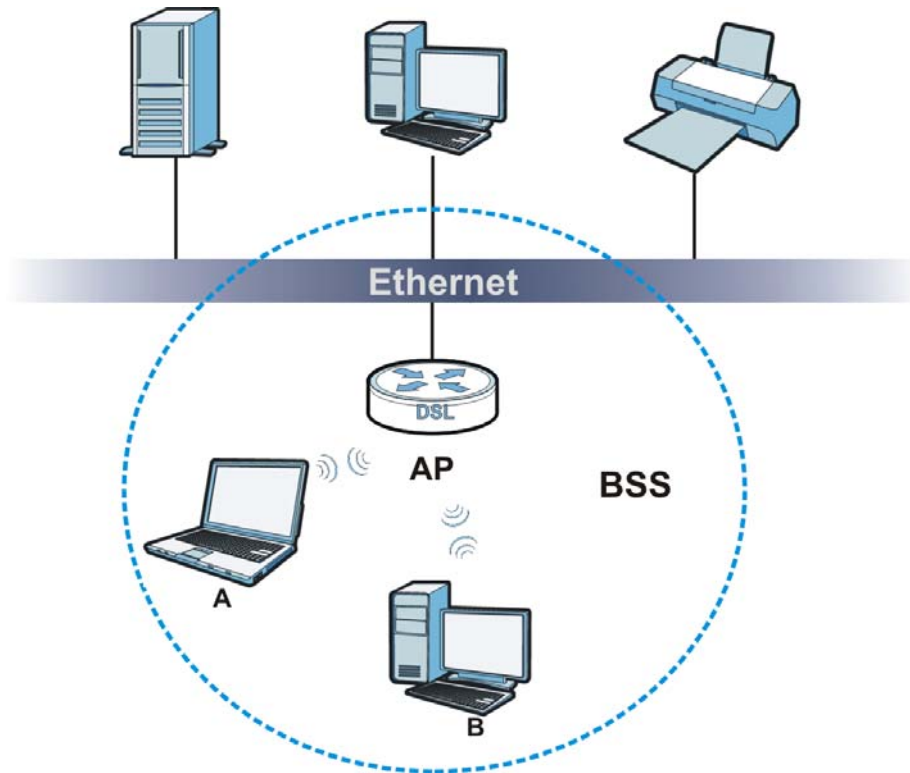
coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

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 45 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 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 Device uses long preamble.

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

7.10.8 Wireless Distribution System (WDS)

The Device can act as a wireless network bridge and establish WDS (Wireless Distribution System) links with other APs. You need to know the MAC addresses of the APs you want to link to. Once the security settings of peer sides match one another, the connection between devices is made.

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

The following figure illustrates how WDS link works between APs. Notebook computer **A** is a wireless client connecting to access point **AP 1**. **AP 1** has no wired Internet connection, but it can establish a WDS link with access point **AP 2**, which has a wired Internet connection. When **AP 1** has a WDS link with **AP 2**, the notebook computer can access the Internet through **AP 2**.

Figure 46 WDS Link Example



7.10.9 WiFi Protected Setup (WPS)

Your 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.

7.10.9.1 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 Device, see [Section 7.6 on page 114](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the Device you must press the WPS button for more than three 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.

7.10.9.2 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.

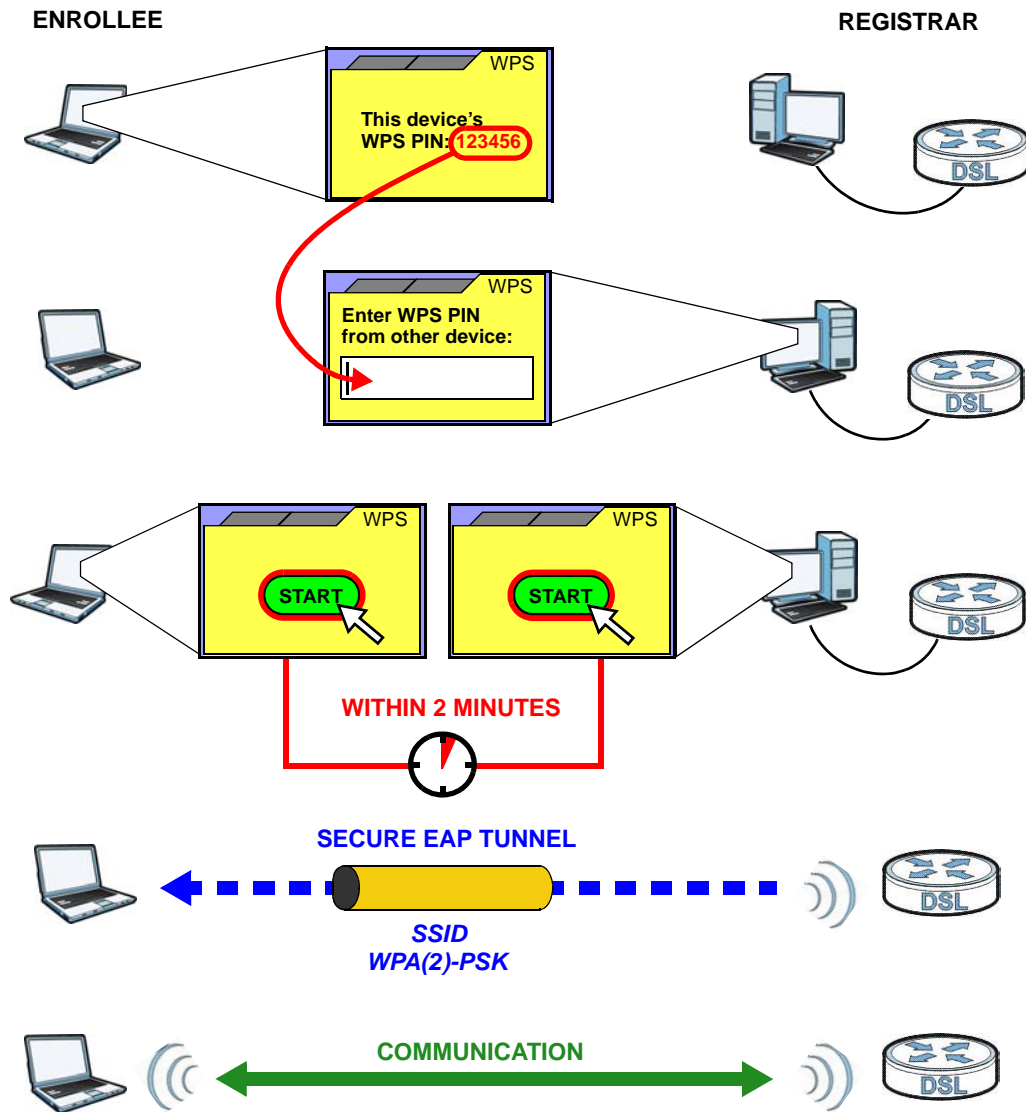
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 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 Device, see [Section 7.5 on page 112](#)).
- 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 47 Example WPS Process: PIN Method

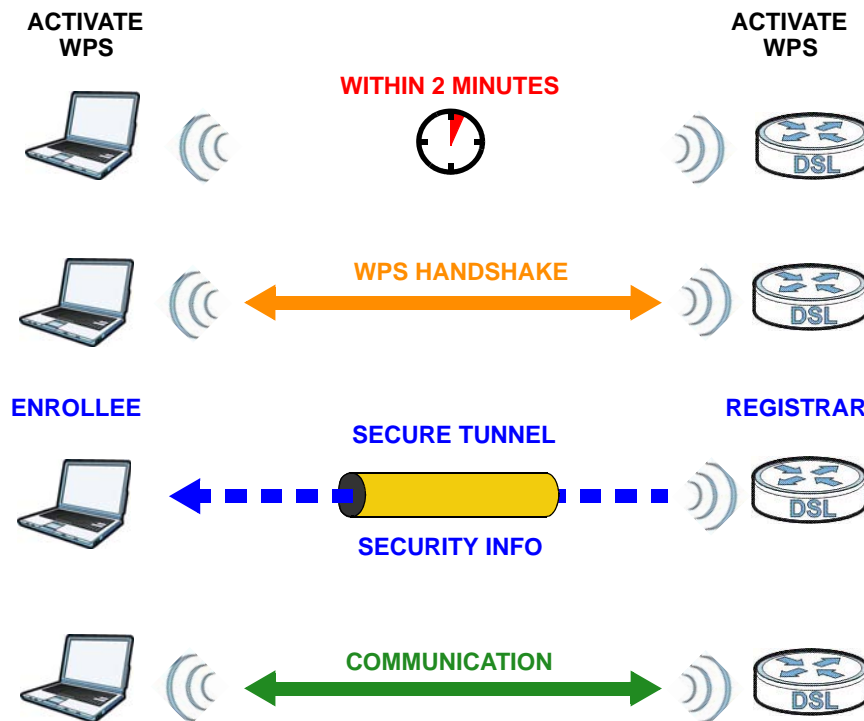


7.10.9.3 How WPS Works

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 48 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.

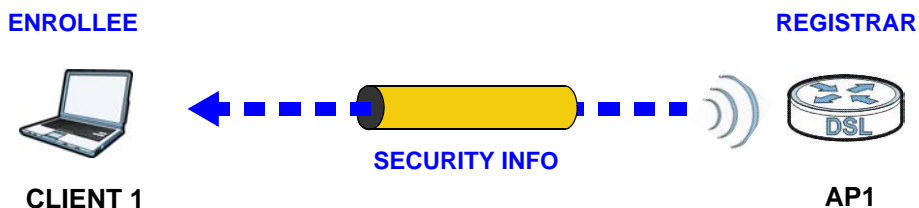
By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled 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.

7.10.9.4 Example WPS Network Setup

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

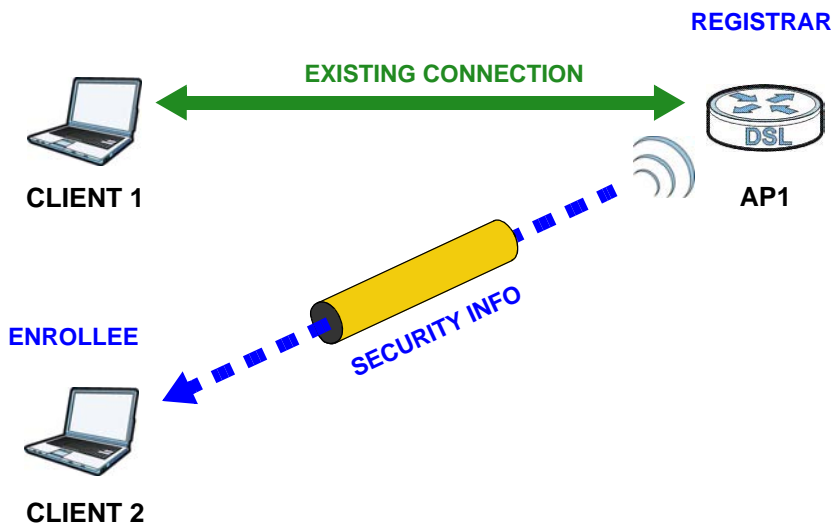
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 49 WPS: Example Network Step 1

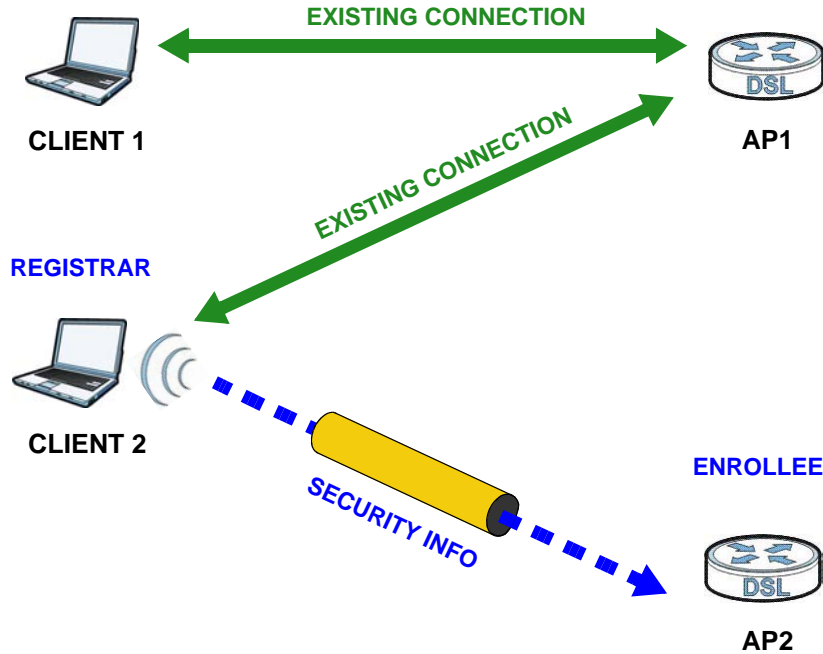


In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 50 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 51 WPS: Example Network Step 3

7.10.9.5 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

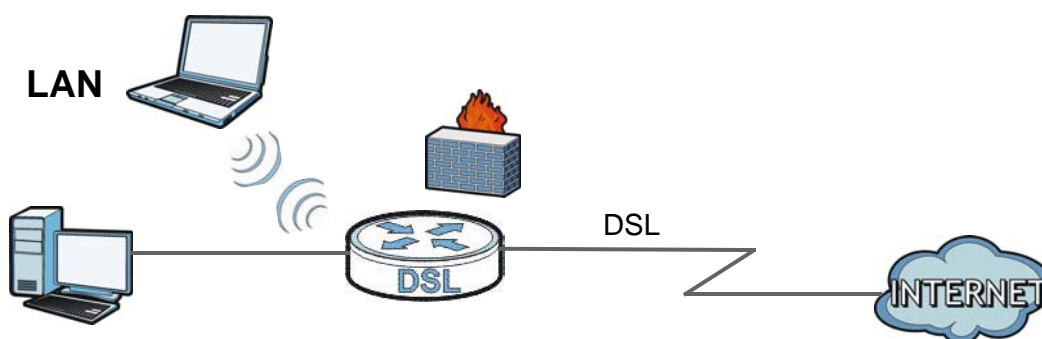
access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

Home Networking

8.1 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 Device ([Section 8.2 on page 135](#)).
- 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 138](#)).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the Device ([Section 8.4 on page 140](#)).
- Use the **Additional Subnet** screen to configure IP alias and public static IP ([Section 8.5 on page 141](#)).
- Use the **STB Vendor ID** screen to have the Device automatically create static DHCP entries for Set Top Box (STB) devices when they request IP addresses ([Section 8.8 on page 150](#)).
- Use the **5th Ethernet Port** screen to configure the Ethernet WAN port as a LAN port ([Section 8.9 on page 150](#)).
- [Use the MoCA screen to set the MoCA Privacy, and enable multimedia and home networking over coaxial cable \(Section 8.10 on page 151\).](#)
- Use the **LAN VLAN** screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent out through individual LAN ports ([Section 8.11 on page 152](#)).
- [Use the TFTP Server Name screen to access the TFTP server using DHCP option 66 \(Section 8.12 on page 152\).](#)

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 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 181](#) 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 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 8.5 on page 141](#) for examples of installing and using UPnP.

Finding Out More

See [Section 8.13 on page 153](#) 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 Device. 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 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 52 Network Setting > Home Networking > LAN Setup

The following table describes the fields in this screen.

Table 31 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 13 on page 201 for how to create a new interface group.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your 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 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	
Status	Select the Enable IGMP Snooping checkbox to allows the Device to passively learn multicast group.
IGMP Mode	Select Standard Mode to have the Device 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 have the Device block all unknown multicast packets from the WAN.
DHCP Server State	
DHCP	Select Enable to have the Device act as a DHCP server or DHCP relay agent. Select Disable to stop the DHCP server on the Device. Select DHCP Relay to have the Device forward DHCP request to the DHCP server.

Table 31 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DHCP Relay Server Address	This field is only available when you select DHCP Relay in the DHCP field.
IP Address	Enter the 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.
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 Dynamic DNS service provider. Select Dynamic if you have the Dynamic DNS service. Select Static if you have the Static DNS service.
DNS Server 1 DNS Server 2	Enter the first and second DNS (Domain Name System) server IP address the Device passes to the DHCP clients.
LAN IPv6 Mode Setup	
IPv6 State	Select Enable to activate the IPv6 mode and configure IPv6 settings on the Device.
LAN IPv6 Address 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 Device's LAN IPv6 address.
ULA IPv6 Address Setup	
IPv6 Address	If you select static IPv6 address, enter the IPv6 address prefix that the Device uses for the LAN IPv6 address.
Prefix Length	If you select static IPv6 address, enter the IPv6 prefix length that the Device uses to generate the LAN IPv6 address. An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
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. Select Enable MLD Snooping to activate MLD Snooping on the Device. This allows the Device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.

Table 31 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: <ul style="list-style-type: none"> • stateless + DNS send by RADVD: The Device uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. (See page 134 for more information on RADVD.) • stateless + DNS send by DHCPv6: The Device uses IPv6 stateless autoconfiguration. The DNS is provided by a DHCPv6 server. • stateful + DHCPv6 server: The Device uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Device act as a DHCPv6 server and pass IPv6 addresses, DNS server and domain name information to DHCPv6 clients. • stateful + DHCPv6 relay: The Device uses IPv6 stateful autoconfiguration. DHCPv6 Relay is enabled to have the Device relay client DHCPv6 requests.
DHCPv6 Configuration	
DHCPv6 State	This shows the status of the DHCPv6.
IPv6 DNS Values	
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 Device passes to the DHCP clients. Select None if you do not want to configure IPv6 DNS servers.
IPv6 Address Values	
IPv6 Start Address	If DHCPv6 is enabled, specify the first IPv6 address in the pool of addresses that can be assigned to DHCPv6 clients.
IPv6 End Address	If DHCPv6 is enabled, specify the last IPv6 address in the pool of addresses that can be assigned to DHCPv6 clients.
IPv6 Domain Name	If DHCPv6 is enabled, specify the domain name to be assigned to DHCPv6 clients.
IPv6 Router Advertisement State	
RADVD State	This shows the status of RADVD.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

8.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific 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 Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 53 Network Setting > Home Networking > Static DHCP

Add new static lease				
#	Status	MAC Address	IP Address	Modify
1		00:24:21:7E:20:96	172.23.30.1	

The following table describes the labels in this screen.

Table 32 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Add new static lease	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 Device.
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 **Add new static lease** in the **Static DHCP** screen or the Edit icon next to a static DHCP entry, the following screen displays.

Figure 54 Static DHCP: Add/Edit

<input type="checkbox"/> Active	
Group Name :	Default
Select Device Info:	Manual Input
MAC Address :	_____ : _____ : _____ : _____ : _____ : _____
IP Address :	_____
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

Table 33 Static DHCP: Add/Edit

LABEL	DESCRIPTION
Active	Select this to activate the connection between the client and the Device.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See Chapter 13 on page 201 for how to create a new interface group.
Select Device Info	If you select Manual Input , you can manually type in the MAC address and IP address of a computer on your LAN. You can also choose the name of a computer from the drop list and have the MAC Address and IP Address auto-detected.
MAC Address	If you select Manual Input , enter the MAC address of a computer on your LAN.

Table 33 Static DHCP: Add/Edit (continued)

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

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. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See [page 134](#) for more information on UPnP.

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

Figure 55 Network Setting > Home Networking > UPnP

UPnP State
UPnP: Enable Disable

UPnP NAT-T State
UPnP NAT-T: Enable Disable

Note:
UPnP NAT-T only work when NAT is enable

#	Description	IP ADDRESS	External Port	Internal Port	Protocol
---	-------------	------------	---------------	---------------	----------

Apply Cancel

The following table describes the labels in this screen.

Table 34 Network Setting > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP	Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Device's IP address (although you must still enter the password to access the web configurator).
UPnP NAT-T	Select Enable to allow UPnP-enabled applications to automatically configure the Device so that they can communicate through the Device by using NAT traversal. 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.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

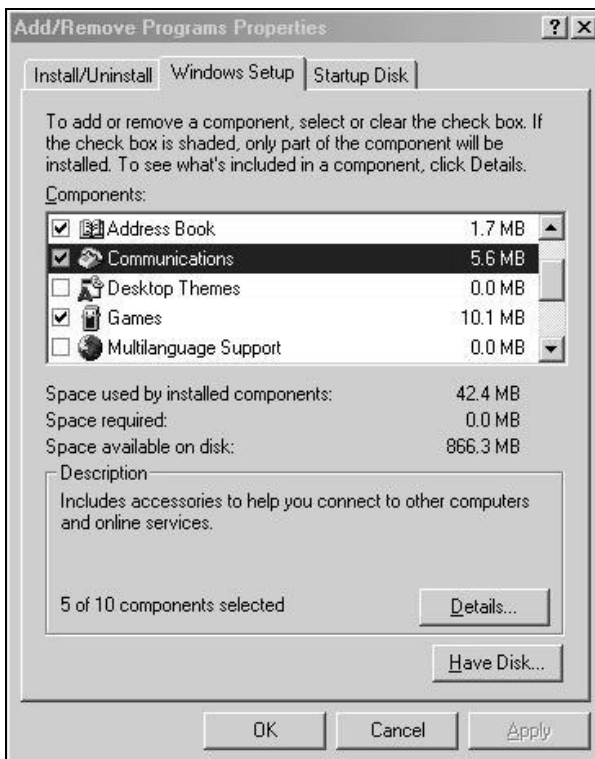
8.5 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

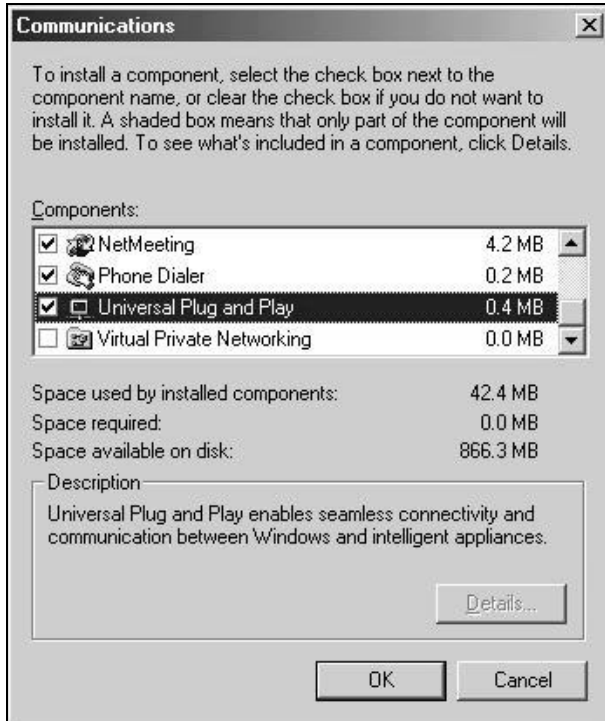
Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

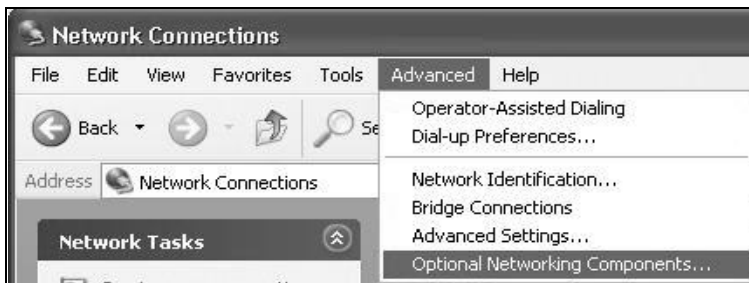


- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

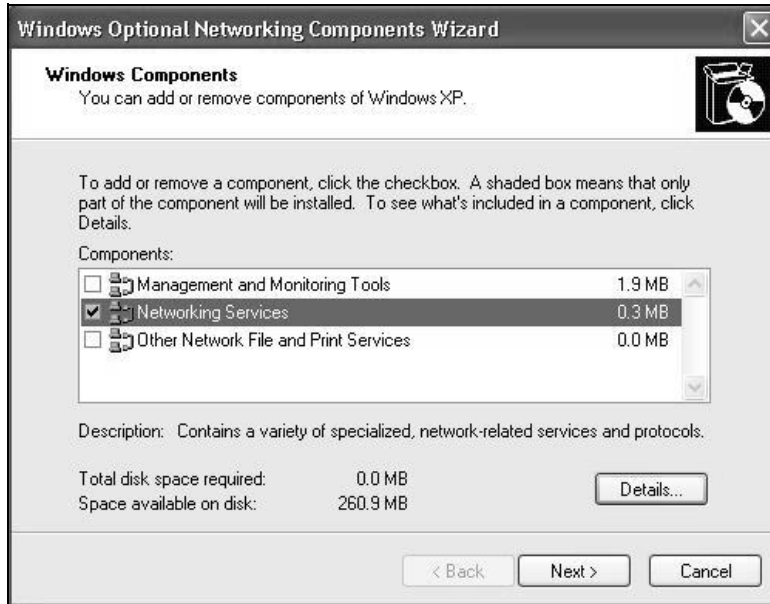
Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

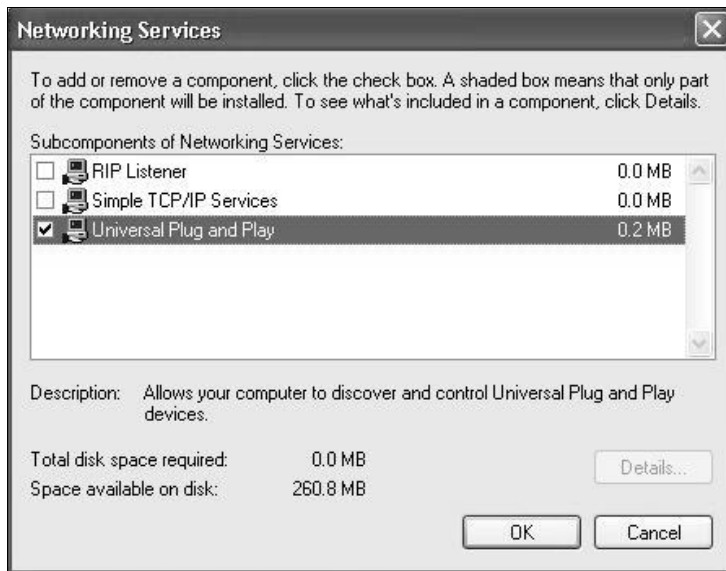
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**



- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.



- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

8.6 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Device.

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

Auto-discover Your UPnP-enabled Network Device

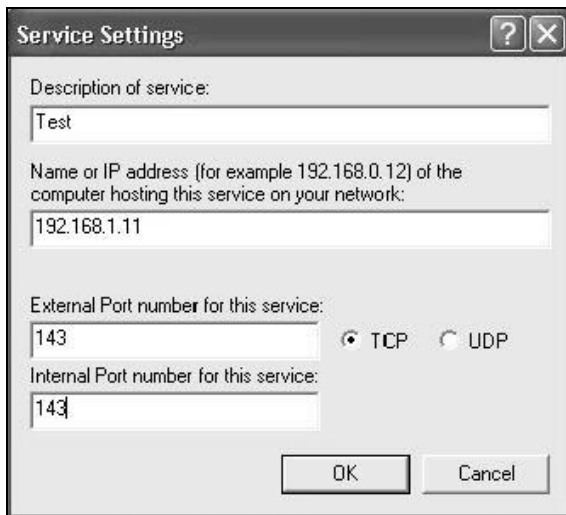
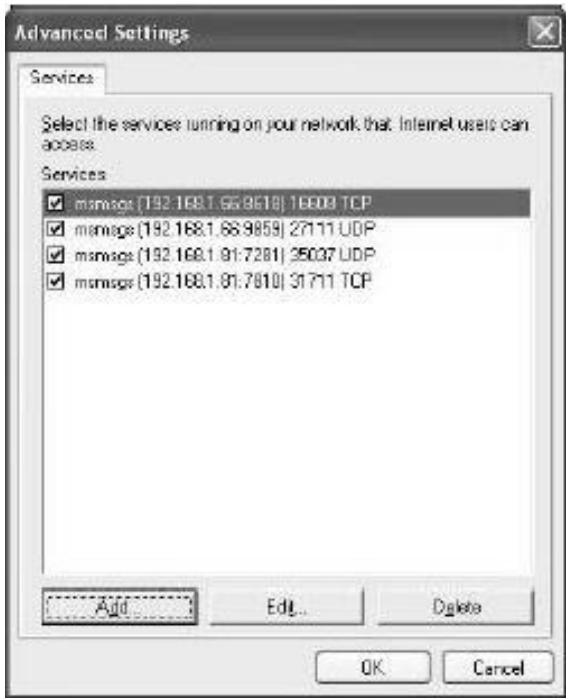
- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.



- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.



- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.



- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.
- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.



- 7 Double-click on the icon to display your current Internet connection status.

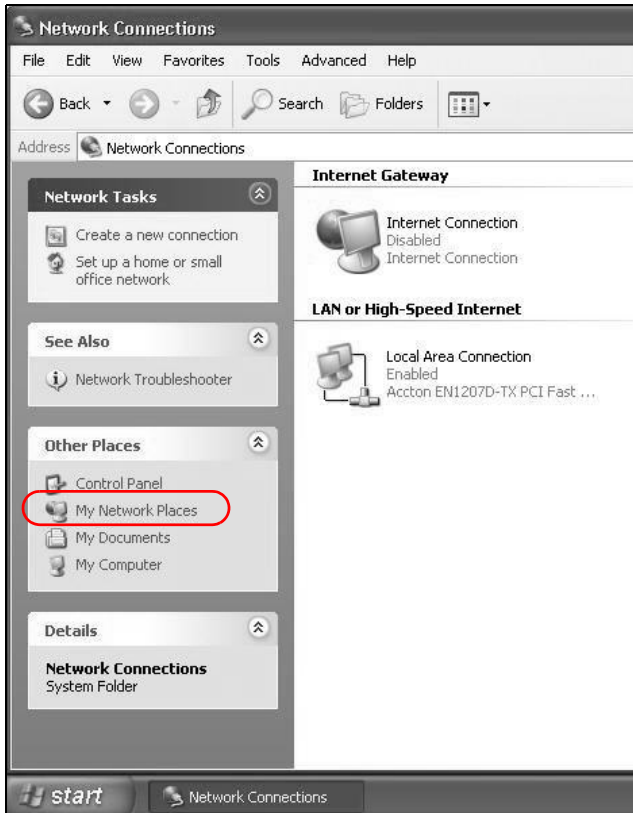


Web Configurator Easy Access

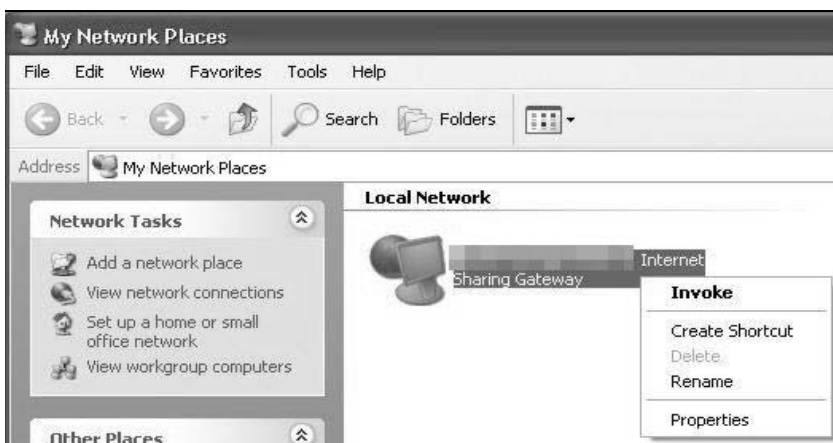
With UPnP, you can access the web-based configurator on the Device without finding out the IP address of the Device first. This comes helpful if you do not know the IP address of the Device.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click on the icon for your Device and select **Invoke**. The web configurator login screen displays.



- 6 Right-click on the icon for your Device and select **Properties**. A properties window displays with basic information about the Device.



8.7 The Additional Subnet Screen

Use the **Additional Subnet** 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 Device supports multiple logical LAN interfaces via its physical Ethernet interface with the 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 Device may use an LAN IP address that can be accessed from the WAN.

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

Figure 56 Network Setting > Home Networking > Additional Subnet

IP Alias Setup

Group Name :

Active

IP Address :

IP Subnet Mask :

Public LAN

Active

IP Address :

IP Subnet Mask :

Offer Public IP by DHCP :

Enable ARP Proxy :

The following table describes the labels in this screen.

Table 35 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 13 on page 201 for how to create a new interface group.
Active	Select the checkbox to configure a LAN network for the Device.
IP Address	Enter the IP address of your Device in dotted decimal notation.
IP Subnet Mask	Your Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Device.
Public LAN	
Active	Select the checkbox to enable the Public LAN feature. Your ISP must support Public LAN and Static IP.
IP Address	Enter the public IP address provided by your ISP.
IP Subnet Mask	Enter the public IP subnet mask provided by your ISP.

Table 35 Network Setting > Home Networking > Additional Subnet (continued)

LABEL	DESCRIPTION
Offer Public IP by DHCP	Select the checkbox to enable the Device to provide public IP addresses by DHCP server.
Enable ARP Proxy	Select the checkbox to enable the ARP (Address Resolution Protocol) proxy.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.8 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 list the Vendor IDs of connected STBs to have the Device 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 57 Network Setting > Home Networking > STB Vendor ID

Please enter Vendor ID for STB:

Vendor ID 1: _____

Vendor ID 2: _____

Vendor ID 3: _____

Vendor ID 4: _____

Vendor ID 5: _____

Apply Cancel

The following table describes the labels in this screen.

Table 36 Network Setting > Home Networking > STB Vendor ID

LABEL	DESCRIPTION
Vendor ID 1 ~ 5	Enter the STB's vendor ID.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.9 The 5th Ethernet Port Screen

If you are using DSL connection, you can configure your Ethernet WAN port as an extra LAN port. This fifth Ethernet port is a Gigabit port. Click **Network Settings > Home Networking > 5th Ethernet Port** to open this screen.