



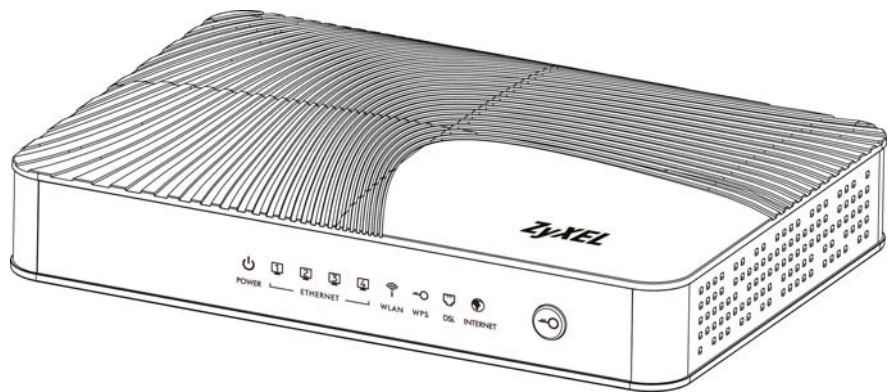
AMG1302-TSeries

Wireless N ADSL2+ 4-port Gateway

AMG1202-TSeries

Wireless N-lite ADSL2+ 4-port Gateway

Version 2.00(AAJC.0)
Edition 2, 5/2013



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 shows how to connect the AMG1302/AMG1202-TSeries and access the Web Configurator. It contains information on setting up your wireless network.

Contents Overview

User's Guide	13
Introduction	15
Introducing the Web Configurator	21
Internet / Wireless Setup Wizard.....	29
Tutorials	37
Technical Reference	65
Connection Status and System Info Screens	67
Broadband	73
Wireless LAN	91
Home Networking	121
Static Route	135
Quality of Service (QoS)	139
Network Address Translation (NAT)	151
Port Binding	161
Dynamic DNS Setup	165
Filters	167
Firewall	173
Parental Control	191
Certificate	195
Logs	201
Traffic Status	203
User Account	207
TR-069 Client	209
System Settings	213
Firmware Upgrade	217
Backup/Restore	219
Remote Management	223
Diagnostic	235
Troubleshooting	239

Table of Contents

Contents Overview	3
Table of Contents	5
Part I: User's Guide	13
Chapter 1	
Introduction.....	15
1.1 Overview	15
1.2 Ways to Manage the AMG1302/AMG1202-TSeries	15
1.3 Good Habits for Managing the AMG1302/AMG1202-TSeries	15
1.4 Applications for the AMG1302/AMG1202-TSeries	16
1.4.1 Internet Access	16
1.4.2 Wireless Access	16
1.5 General Hardware Features	17
1.6 Using the WPS Button	18
1.7 The RESET Button	19
1.7.1 Using the Reset Button	19
1.8 Ways to Manage the AMG1302/AMG1202-TSeries	19
Chapter 2	
Introducing the Web Configurator	21
2.1 Overview	21
2.1.1 Accessing the Web Configurator	21
2.2 The Web Configurator Layout	23
2.2.1 Title Bar	24
2.2.2 Main Window	25
2.2.3 Navigation Panel	25
Chapter 3	
Internet / Wireless Setup Wizard	29
3.1 Overview	29
3.2 Internet / Wireless Wizard Setup	29
Chapter 4	
Tutorials.....	37
4.1 Overview	37
4.2 Setting Up Your DSL Connection	37

4.3 IPv6 Address Configuration 39

4.4 Setting Up a Secure Wireless Network 40

 4.4.1 Configuring the Wireless Network Settings 40

 4.4.2 Using WPS 41

 4.4.3 Connecting Wirelessly to your AMG1302/AMG1202-TSeries 45

4.5 Configuring the MAC Address Filter for Restricting Wireless Internet Access 47

4.6 Setting Up NAT Forwarding for a Game Server 48

 4.6.1 Port Forwarding 49

4.7 Configuring Firewall Rules to Allow a Specified Service 50

4.8 Configuring Static Route for Routing to Another Network 53

4.9 Port Binding Configuration 55

 4.9.1 Configuring ATM QoS for Multiple WAN Connections 55

 4.9.2 Configuring Port Binding 58

4.10 Configuring QoS to Prioritize Traffic 59

4.11 Access the AMG1302/AMG1202-TSeries from the Internet Using DDNS 62

 4.11.1 Registering a DDNS Account on www.dyndns.org 62

 4.11.2 Configuring DDNS on Your AMG1302/AMG1202-TSeries 63

 4.11.3 Testing the DDNS Setting 63

Part II: Technical Reference..... 65

Chapter 5

Connection Status and System Info Screens 67

5.1 Overview 67

5.2 The Connection Status Screen 67

5.3 The System Info Screen 68

Chapter 6

Broadband..... 73

6.1 Overview 73

 6.1.1 What You Can Do in the WAN Screens 73

 6.1.2 What You Need to Know About WAN 73

 6.1.3 Before You Begin 74

6.2 The Internet Connection Screen 74

 6.2.1 Advanced Setup 79

6.3 The More Connections Screen 81

 6.3.1 More Connections Edit 82

 6.3.2 Configuring More Connections Advanced Setup 85

6.4 WAN Technical Reference 86

 6.4.1 Encapsulation 86

 6.4.2 Multiplexing 87

6.4.3 VPI and VCI	87
6.4.4 IP Address Assignment	87
6.4.5 Nailed-Up Connection (PPP)	88
6.4.6 NAT	88
6.5 Traffic Shaping	88
6.5.1 ATM Traffic Classes	89
Chapter 7	
Wireless LAN.....	91
7.1 Overview	91
7.1.1 What You Can Do in the Wireless LAN Screens	91
7.1.2 What You Need to Know About Wireless	92
7.1.3 Before You Start	92
7.2 The General Screen	92
7.2.1 No Security	94
7.2.2 Basic (WEP Encryption)	94
7.2.3 More Secure (WPA(2)-PSK)	95
7.2.4 WPA(2) Authentication	96
7.3 The More AP Screen	98
7.3.1 More AP Edit	98
7.4 The MAC Authentication Screen	100
7.5 The WPS Screen	101
7.6 The WDS Screen	103
7.7 The WMM Screen	104
7.8 The Scheduling Screen	105
7.9 The Advanced Screen	106
7.10 Wireless LAN Technical Reference	107
7.10.1 Wireless Network Overview	107
7.10.2 Additional Wireless Terms	109
7.10.3 Wireless Security Overview	109
7.10.4 Signal Problems	111
7.10.5 BSS	112
7.10.6 MBSSID	112
7.10.7 Wireless Distribution System (WDS)	113
7.10.8 WiFi Protected Setup (WPS)	113
Chapter 8	
Home Networking.....	121
8.1 Overview	121
8.1.1 What You Can Do in the LAN Screens	121
8.1.2 What You Need To Know	121
8.1.3 Before You Begin	123
8.2 The LAN Setup Screen	123

8.3 The Static DHCP Screen	125
8.4 The UPnP Screen	126
8.5 The IP Alias Screen	126
8.5.1 Configuring the LAN IP Alias Screen	127
8.6 The IPv6 LAN Setup Screen	127
8.7 Home Networking Technical Reference	131
8.7.1 LANs, WANs and the AMG1302/AMG1202-TSeries	131
8.7.2 DHCP Setup	131
8.7.3 DNS Server Addresses	131
8.7.4 LAN TCP/IP	132
8.7.5 RIP Setup	133
8.7.6 Multicast	133
Chapter 9	
Static Route	135
9.1 Overview	135
9.1.1 What You Can Do in the Static Route Screens	136
9.2 The Static Route Screen	136
9.2.1 Static Route Add/Edit	136
9.3 IPv6 Static Route	137
9.3.1 IPv6 Static Route Edit	138
Chapter 10	
Quality of Service (QoS).....	139
10.1 Overview	139
10.1.1 What You Can Do in the QoS Screens	139
10.1.2 What You Need to Know About QoS	140
10.2 The Quality of Service General Screen	140
10.3 The Queue Screen	141
10.3.1 Adding a QoS Queue	142
10.4 The Class Setup Screen	143
10.4.1 Class Setup Add/Edit	143
10.5 The QoS Game List Screen	147
10.6 QoS Technical Reference	148
10.6.1 IEEE 802.1p	148
10.6.2 IP Precedence	148
10.6.3 Automatic Priority Queue Assignment	149
Chapter 11	
Network Address Translation (NAT).....	151
11.1 Overview	151
11.1.1 What You Can Do in the NAT Screens	151
11.1.2 What You Need To Know About NAT	151

11.2 The NAT General Screen	152
11.3 The Port Forwarding Screen	153
11.3.1 Configuring the Port Forwarding Screen	153
11.3.2 Port Forwarding Rule Add/Edit	154
11.4 The DMZ Screen	156
11.5 NAT Technical Reference	156
11.5.1 NAT Definitions	156
11.5.2 What NAT Does	157
11.5.3 How NAT Works	157
11.5.4 NAT Application	158
11.5.5 NAT Mapping Types	158
Chapter 12	
Port Binding	161
12.1 Overview	161
12.1.1 What You Can Do in the Port Binding Screens	162
12.2 The Port Binding General Screen	162
12.3 The Port Binding Screen	162
12.3.1 Port Binding Summary Screen	163
Chapter 13	
Dynamic DNS Setup	165
13.1 Overview	165
13.1.1 What You Can Do in the DDNS Screen	165
13.1.2 What You Need To Know About DDNS	165
13.2 The Dynamic DNS Screen	165
Chapter 14	
Filters	167
14.1 Overview	167
14.1.1 What You Can Do in the Filter Screens	167
14.1.2 What You Need to Know About Filtering	167
14.2 The IP/MAC Filter Screen	167
14.3 IPv6/MAC Filter	170
Chapter 15	
Firewall	173
15.1 Overview	173
15.1.1 What You Can Do in the Firewall Screens	173
15.1.2 What You Need to Know About Firewall	174
15.2 The Firewall General Screen	175
15.3 The Default Action Screen	176
15.4 The Rules Screen	178

15.4.1 The Rules Add Screen	179
15.4.2 Customized Services	181
15.4.3 Customized Service Add/Edit	182
15.5 The DoS Screen	184
15.5.1 The DoS Advanced Screen	184
15.5.2 Configuring Firewall Thresholds	185
15.6 Firewall Technical Reference	186
15.6.1 Firewall Rules Overview	186
15.6.2 Guidelines For Enhancing Security With Your Firewall	187
15.6.3 Security Considerations	188
15.6.4 Triangle Route	188
Chapter 16	
Parental Control	191
16.1 Overview	191
16.2 The Parental Control Screen	191
16.2.1 Add/Edit Parental Control Rule	192
Chapter 17	
Certificate	195
17.1 Overview	195
17.1.1 What You Can Do in this Chapter	195
17.2 What You Need to Know	195
17.3 Local Certificates	195
17.4 The Trusted CA Screen	197
17.5 Trusted CA Import	197
17.6 View Certificate	198
Chapter 18	
Logs	201
18.1 Overview	201
18.1.1 What You Can Do in this Chapter	201
18.1.2 What You Need To Know	201
18.2 The System Log Screen	202
Chapter 19	
Traffic Status	203
19.1 Overview	203
19.1.1 What You Can Do in this Chapter	203
19.2 The WAN Status Screen	203
19.3 The LAN Status Screen	204
19.4 The NAT Screen	205

Chapter 20	
User Account	207
20.1 Overview	207
20.2 The User Account Screen	207
Chapter 21	
TR-069 Client.....	209
21.1 Overview	209
21.2 The TR-069 Client Screen	209
Chapter 22	
System Settings.....	213
22.1 Overview	213
22.1.1 What You Can Do in the System Settings Screens	213
22.2 The System Screen	213
22.3 The Time Screen	213
Chapter 23	
Firmware Upgrade	217
23.1 Overview	217
23.2 The Firmware Screen	217
Chapter 24	
Backup/Restore	219
24.1 Overview	219
24.2 The Backup/Restore Screen	219
24.3 The Reboot Screen	221
Chapter 25	
Remote Management.....	223
25.1 Overview	223
25.1.1 What You Can Do in the Remote Management Screens	223
25.1.2 What You Need to Know About Remote Management	224
25.2 The WWW Screen	224
25.2.1 Configuring the WWW Screen	224
25.3 The Telnet Screen	226
25.4 The FTP Screen	226
25.5 The SNMP Screen	227
25.5.1 Configuring SNMP	228
25.6 The DNS Screen	230
25.7 The ICMP Screen	230
25.8 The SSH Screen	231
25.8.1 SSH Example	232

Chapter 26	
Diagnostic	235
26.1 Overview	235
26.1.1 What You Can Do in the Diagnostic Screens	235
26.2 The General Screen	235
26.3 The DSL Line Screen	236
Chapter 27	
Troubleshooting.....	239
27.1 Power, Hardware Connections, and LEDs	239
27.2 AMG1302/AMG1202-TSeries Access and Login	240
27.3 Internet Access	242
Appendix A Setting up Your Computer's IP Address.....	245
Appendix B IP Addresses and Subnetting.....	265
Appendix C Pop-up Windows, JavaScripts and Java Permissions	273
Appendix D Wireless LANs.....	281
Appendix E IPv6	295
Appendix F Services.....	305
Appendix G Legal Information	309
Index	313

PART I

User's Guide

Introduction

1.1 Overview

The AMG1302/AMG1202-TSeries are ADSL2+ routers. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The AMG1302/AMG1202-TSeries are also a complete security solution with a robust firewall and content filtering.

Only use firmware for your AMG1302/AMG1202-TSeries's specific model. Refer to the label on the bottom of your AMG1302/AMG1202-TSeries.

Note: Not all models have all of the features shown in this User's Guide.

1.2 Ways to Manage the AMG1302/AMG1202-TSeries

Use any of the following methods to manage the AMG1302/AMG1202-TSeries.

- Web Configurator. This is recommended for everyday management of the AMG1302/AMG1202-TSeries using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the AMG1302/AMG1202-TSeries

Do the following things regularly to make the AMG1302/AMG1202-TSeries more secure and to manage the AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the AMG1302/AMG1202-TSeries. You could simply restore your last configuration.

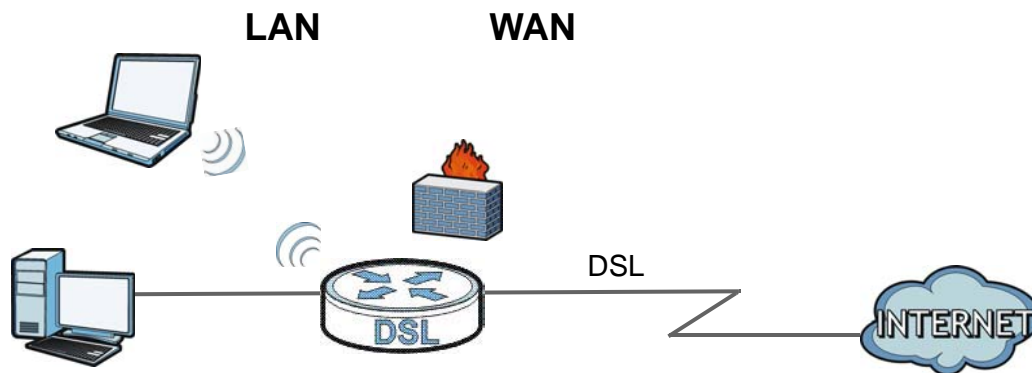
1.4 Applications for the AMG1302/AMG1202-TSeries

Here are some example uses for which the AMG1302/AMG1202-TSeries is well suited.

1.4.1 Internet Access

Your AMG1302/AMG1202-TSeries provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the AMG1302/AMG1202-TSeries's Ethernet ports (or wirelessly).

Figure 1 AMG1302/AMG1202-TSeries's Router Features



You can also configure firewall and filtering feature on the AMG1302/AMG1202-TSeries for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked 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.

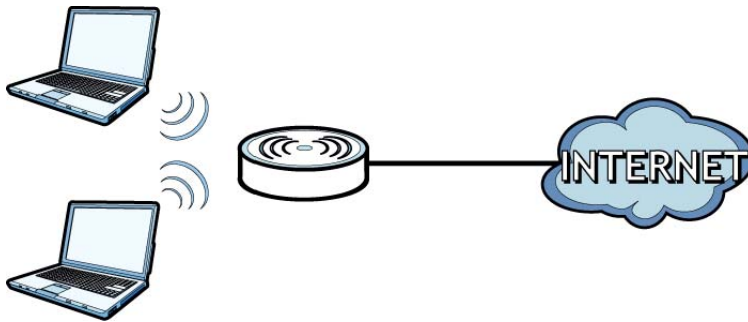
Use the filtering feature to block access to specific web sites or Internet applications such as MSN or Yahoo Messenger. You can also configure IP/MAC filtering rules for incoming or outgoing traffic.

Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the AMG1302/AMG1202-TSeries gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.4.2 Wireless Access

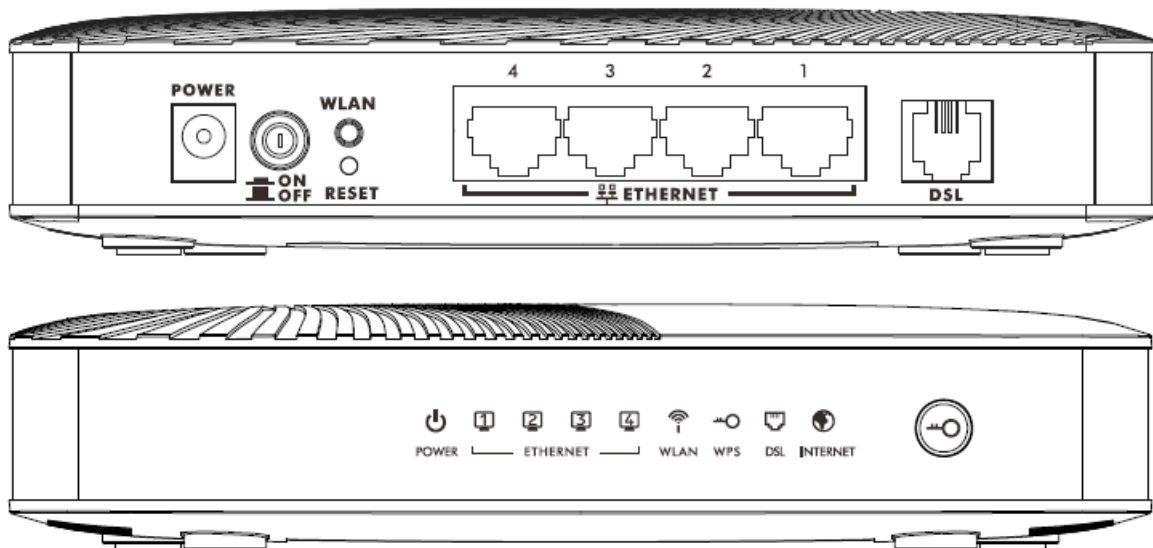
The ZyXEL Device is a wireless Access Point (AP) for IEEE 802.11b/g/n compliant clients, such as notebook computers or PDAs and iPads. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

Figure 2 Wireless Access Example



1.5 General Hardware Features

Figure 3 General Hardware Features



The following table describes the LEDs..

Table 1 LED Descriptions





LED	COLOR	STATUS	DESCRIPTION
 (POWER)	Green	On	The AMG1302/AMG1202-TSeries is receiving power and ready for use.
		Blinking	The AMG1302/AMG1202-TSeries is self-testing.
	Red	On	The AMG1302/AMG1202-TSeries detected an error while self-testing, or there is a device malfunction.
		Off	The AMG1302/AMG1202-TSeries is not receiving power.
Ethernet 1-4	Green	On	The AMG1302/AMG1202-TSeries has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The AMG1302/AMG1202-TSeries is sending/receiving data to / from the LAN.
	Off	The AMG1302/AMG1202-TSeries does not have an Ethernet connection with the LAN.	

Table 1 LED Descriptions

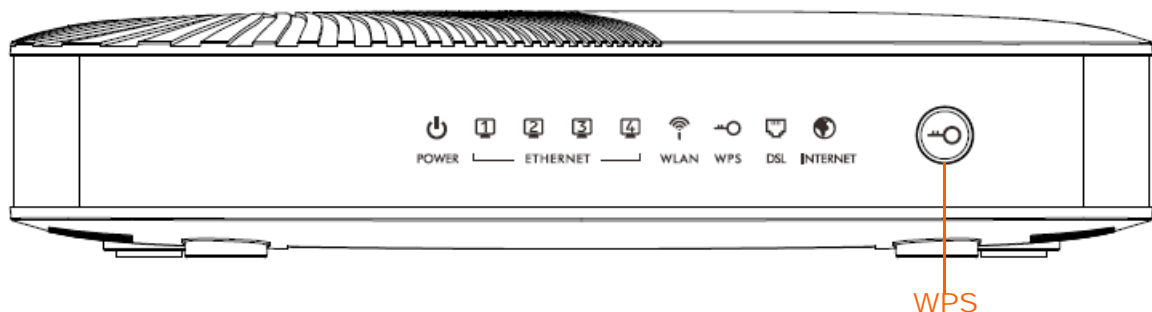
LED	COLOR	STATUS	DESCRIPTION
 (WPS/WLAN)	Green	On	The wireless network is activated.
		Blinking	The AMG1302/AMG1202-TSeries is communicating with other wireless clients.
	Green	Blinking	The AMG1302/AMG1202-TSeries is setting up a WPS connection.
		Off	The wireless network is not activated.
 (DSL)	Green	On	The DSL line is up.
		Blinking	The AMG1302/AMG1202-TSeries is initializing the DSL line.
		Off	The DSL line is down.
 (INTERNET)	Green	On	The AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries is sending or receiving IP traffic.
	Red	On	The AMG1302/AMG1202-TSeries attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The AMG1302/AMG1202-TSeries does not have an IP connection.

1.6 Using the WPS Button

You can also use the **WPS** button to quickly set up a secure wireless connection between the AMG1302/AMG1202-TSeries and a WPS-compatible client by adding one device at a time.

To activate WPS:

- 1 Make sure the **POWER** LED is on and not blinking.
- 2 Press the **WPS** button for 1-5 seconds and release it. See below for WPS button location.



- 3 Press the WPS button on another WPS-enabled device within range of the AMG1302/AMG1202-TSeries. The **WPS** LED should flash while the AMG1302/AMG1202-TSeries sets up a WPS connection with the other wireless device.
- 4 Once the connection is successfully made, the **WPS** LED shines green.

1.7 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 user name and password will be reset to the default.

1.7.1 Using the Reset Button

- 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.

1.8 Ways to Manage the AMG1302/AMG1202-TSeries

Use any of the following methods to manage the AMG1302/AMG1202-TSeries.

- Web Configurator. This is recommended for everyday management of the AMG1302/AMG1202-TSeries using a (supported) web browser.
- FTP for firmware upgrades and configuration backup/restore.

Introducing 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, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

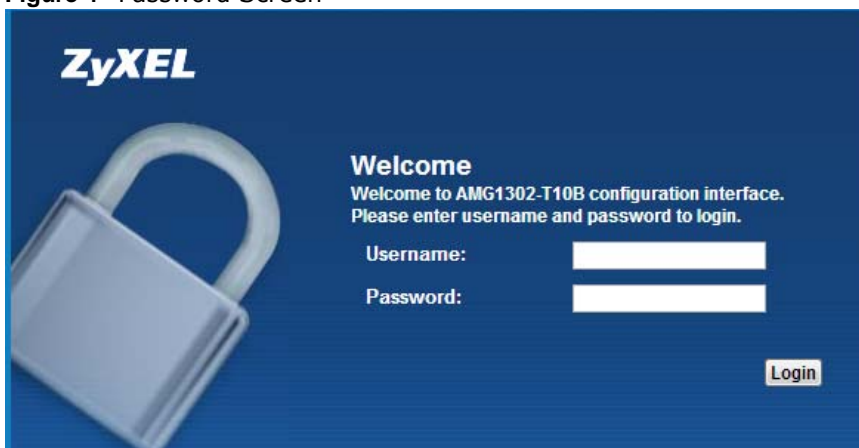
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See [Appendix C on page 273](#) if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

- 1 Make sure your AMG1302/AMG1202-TSeries hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.
- 4 A password screen displays. Type "admin" (default) as the username and "1234" as the password, and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 4 Password Screen



Note: For security reasons, the AMG1302/AMG1202-TSeries automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

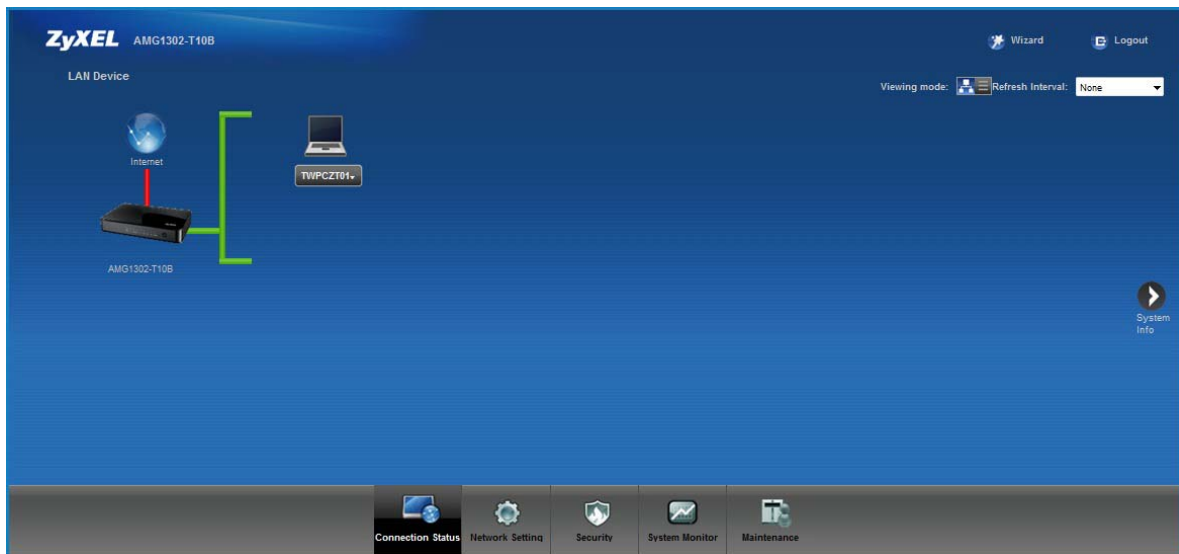
- The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the Connection Status screen if you do not want to change the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

Figure 5 Change Password Screen



- The **Connection Status** screen appears.

Figure 6 Connection Status



- Click **System Info** to display the **System Info** screen, where you can view the AMG1302/AMG1202-TSeries's interface and system information.

2.2 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen.

Figure 7 Web Configurator Layout Screen

ZyXEL AMG1302-T10B A Wizard Logout

system info Refresh Interval: None

Device Information

Host Name: admin

Model Name: AMG1302-T10B

MAC Address: FC:F5:28:E2:06:A0

Firmware Version: V2.00(AAJC.0)b1

DSL Version: FwVer:3.20.3.0_A_TC3087
HwVer:T14.F7_11.2

WAN Information:

- DSL Mode: N/A
- Annex Type: ANNEX A
- IPv6/IPv4 Dual Stack: DualStack
- IP Address: 0.0.0.0
- IP Subnet Mask: N/A
- Default Gateway: 0.0.0.0
- Primary DNS: 0.0.0.0
- Secondary DNS: 0.0.0.0
- IPv6 Global IP: ::
- IPv6 Prefix Length: 0
- IPv6 Gateway: ::
- IPv6 WAN DNS1: ::
- IPv6 WAN DNS2: ::
- Link-Local Address: ::
- IPv4/IPv6 MTU: 0 / 33

LAN Information:

- IP Address: 192.168.1.153
- IP Subnet Mask: 255.255.255.0
- DHCP: None
- IPv6 Address: ::
- Link-local IPv6 Address: fe80::1
- IPv6 Prefix: 0
- Preferred/Valid Time(sec): 3600/7200
- DHCPv6: Server
- Radvd State: Enable
- IPv6 LAN DNS1: fe80::1
- IPv6 LAN DNS2: ::

WLAN Information:

- Status: On
- SSID: ZyXEL_06A0
- Channel: 6
- Security Mode: WPA-PSK/WPA2-PSK
- WPS: Unconfigured
- Scheduling: Disable
- WiFi MAC: FC:F5:28:E2:06:A0-FC:F5:28:E2:06:A3

Security:

- Firewall: Enable

Interface Status

Interface	Status	Rate
ADSL WAN	Down	N/A
LAN1	Down	N/A
LAN2	Down	N/A
LAN3	Up	100 Mbps/Full Duplex
LAN4	Down	N/A
WLAN	Active	300M

System Status

DSL Up Time: N/A

System Up Time: 2 days 17 hours 3 minutes

Current Date/Time: Sun Jan 3 17:03:04 UTC 2010

PPPoE Up Time: 0

System Resource:

- CPU Usage: 2%
- Memory Usage: 52%
- DSL Down Bandwidth Usage: 0%
- DSL Up Bandwidth Usage: 0%

LAN Device
Virtual Device

B


C

Connection Status Network Setting Security System Monitor Maintenance

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 shows the following icon in the upper right corner: 

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 **System Info** on the **Connection Status** screen, the **System Info** screen is displayed. See [Chapter 5 on page 68](#) for more information about the **System Info** screen.

If you click **LAN Device** on the **System Info** screen, the **Connection Status** screen appears. See [Chapter 5 on page 67](#) for more information about the **Connection Status** screen.

If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the AMG1302/AMG1202-TSeries's ports. The connected ports are in color and disconnected ports are gray.

2.2.3 Navigation Panel

Use the menu items on the navigation panel to open screens to configure AMG1302/AMG1202-TSeries features. The following table describes each menu item.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the AMG1302/AMG1202-TSeries and computers/devices connected to it.
Network Setting		
Broadband	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
	More Connections	Use this screen to configure additional WAN connections.
Wireless	General	Use this screen to turn the wireless connection on or off, specify the SSID(s) and configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the AMG1302/AMG1202-TSeries.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the AMG1302/AMG1202-TSeries.
	WPS	Use this screen to use WPS (Wi-Fi Protected Setup) to establish a wireless connection.
	WDS	Use this screen to set up Wireless Distribution System (WDS) links to other access points.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Scheduling	Use this screen to configure when the AMG1302/AMG1202-TSeries enables or disables the wireless LAN.
	Advanced	Use this screen to configure advanced wireless settings such as output power.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
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.
	IP Alias	Use this screen to partition your LAN interface into different logical networks.
	UPnP	Use this screen to enable the UPnP function.
	IPv6 LAN Setup	Use this screen to configure the IPv6 settings on the AMG1302/AMG1202-TSeries's LAN interface.
Static Route	Static Route	Use this screen to view and set up static routes on the AMG1302/AMG1202-TSeries.
	IPv6 Static Route	Use this screen to configure IPv6 static routes.
QoS	General	Use this screen to enable QoS and decide allowable bandwidth using QoS.
	Queue	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
	Game List	Use this screen to give priority to traffic for specific games.
NAT	General	Use this screen to activate/deactivate NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen.
Port Binding	General	Use this screen to activate/deactivate port binding.
	Port Binding	Use this screen to configure and view port binding groups.
Dynamic DNS	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Security		
Filter	IP/MAC Filter	Use this screen to configure IPv4/MAC filtering rules for incoming or outgoing traffic.
	IPv6/MAC Filter	Use this screen to configure IPv6/MAC filtering rules for incoming or outgoing traffic.
Firewall	General	Use this screen to activate/deactivate the firewall.
	Default Action	Use this screen to set the default action that the firewall takes on packets that do not match any of the firewall rules.
	Rules	Use this screen to view the configured firewall rules and add, edit or remove a firewall rule.
	Dos	Use this screen to set the thresholds that the AMG1302/AMG1202-TSeries uses to determine when to start dropping sessions that are not fully established (half-open sessions).
Parental Control	Parental Control	Use this screen to define time periods and days during which the AMG1302/AMG1202-TSeries performs parental control and/or block web sites with the specific URL.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Certificates	Local Certificates	Use this screen to export self-signed certificates or certification requests and import the AMG1302/AMG1202-TSeries's CA-signed certificates.
	Trusted CA	Use this screen to save CA certificates to the AMG1302/AMG1202-TSeries.
System Monitor		
Log	Log	Use this screen to view the logs for the level that you selected. 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 AMG1302/AMG1202-TSeries.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the AMG1302/AMG1202-TSeries.
	NAT	Use this screen to view the status of NAT sessions on the AMG1302/AMG1202-TSeries.
Maintenance		
Users Account	Users Account	Use this screen to configure the passwords your user accounts.
TR-069 Client	TR-069 Client	Use this screen to configure the AMG1302/AMG1202-TSeries to be managed by an Auto Configuration Server (ACS).
System	System	Use this screen to configure management inactivity time-out setting.
Time	Time Setting	Use this screen to change your AMG1302/AMG1202-TSeries's time and date.
Log Setting	Log Setting	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the AMG1302/AMG1202-TSeries without turning the power off.
Remote MGMT	WWW, Telnet, FTP, SNMP, DNS, ICMP, SSH	Use this screen to enable specific traffic directions for specific network service.
Diagnostic	Ping	Use this screen to test the connections to other devices.
	DSL Line	Use this screen to identify problems with the DSL connection.


Internet / Wireless Setup Wizard

3.1 Overview

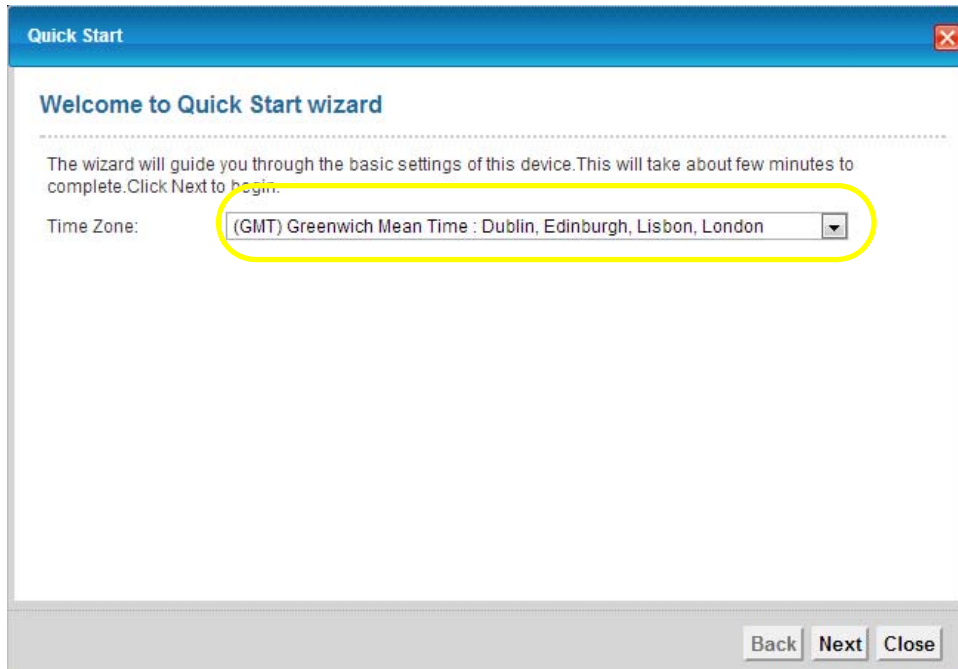
Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.

Note: See the advanced menu chapters for background information on these fields.

3.2 Internet / Wireless Wizard Setup

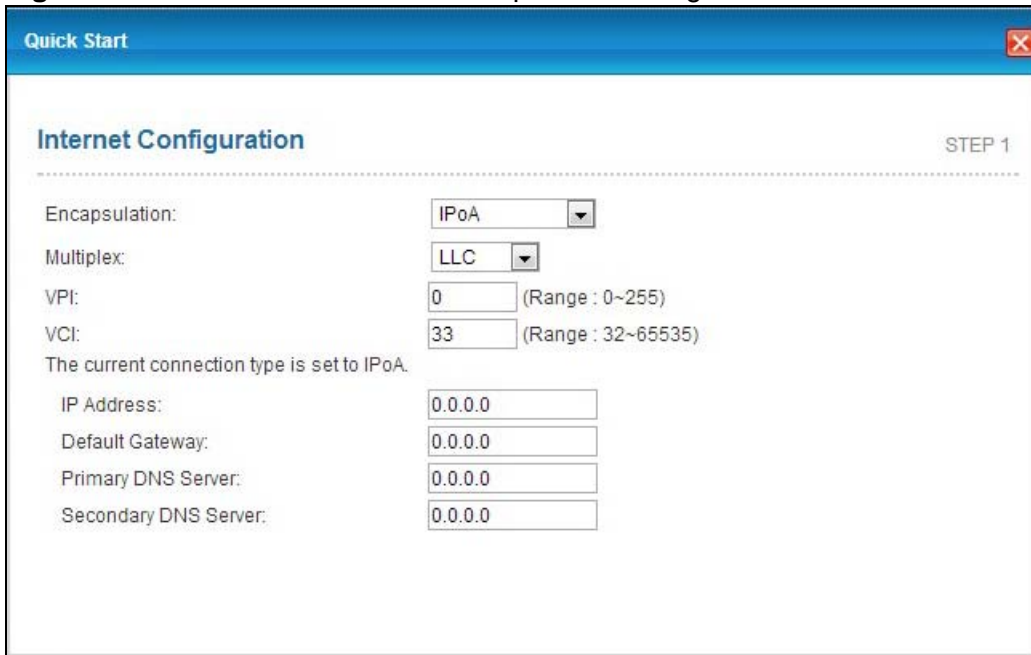
- 1 After you enter the password to access the web configurator, click the Wizard icon () in the top right corner of the web configurator to go to the Wizard.
- 2 Click **INTERNET/WIRELESS SETUP** to configure the system for Internet access and wireless connection.

- 3 Select your **Time Zone** from the drop-down menu, and click **Next**.

Figure 8 Wizard Welcome

Enter your Internet access information in the wizard screen exactly as your service provider gave it to you. Leave the defaults in any fields for which you were not given information.

- 4 Configure the field and click **Next** to continue. See [Section 3.2 on page 29](#) for wireless connection wizard setup.

Figure 9 Internet Access Wizard Setup: IPoA Configuration

The following table describes the fields in this screen.

Table 3 Internet Access Wizard Setup: IPoA Configuration

LABEL	DESCRIPTION
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box: IPoA , ENET ENCAP , PPPoA , or PPPoE .
Multiplex	Select the multiplexing method used by your ISP from the Multiplex drop-down list box either VC-based or LLC-based.
VPI	Enter the Virtual Path Identifier (VPI) assigned to you. This field may already be configured.
VCI	Enter the Virtual Channel Identifier (VCI) assigned to you. This field may already be configured.
IP Address	Enter the IP address of the AMG1302/AMG1202-TSeries.
Default Gateway	Enter the default gateway of the ZyXEL Device.
Primary DNS Server	Enter the primary DNS server IP address for the AMG1302/AMG1202-TSeries.
Secondary DNS Server	Enter the secondary DNS server IP address for the AMG1302/AMG1202-TSeries.
Back	Click this to return to the previous screen without saving.
Next	Click this to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.
Exit	Click this to close the wizard screen without saving.

Note: Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) define a virtual circuit.

Figure 10 Internet Connection with ENET ENCAP

The screenshot shows a window titled "Quick Start" with a sub-header "Internet Configuration" and "STEP 1" in the top right corner. The form contains the following fields and options:

- Encapsulation:** A dropdown menu set to "ENET ENCAP".
- Multiplex:** A dropdown menu set to "LLC".
- VPI:** A text input field containing "0" with a range of "(Range : 0~255)".
- VCI:** A text input field containing "33" with a range of "(Range : 32~65535)".
- Is there specific IP address information from your Internet Service Provider (ISP)?** Two radio buttons: "Yes" (selected) and "No".
- IP Address:** A text input field containing "0.0.0.0".
- Subnet Mask:** A text input field containing "255.0.0.0".
- Default Gateway:** A text input field containing "0.0.0.0".
- Primary DNS Server:** A text input field containing "0.0.0.0".
- Secondary DNS Server:** A text input field containing "0.0.0.0".

At the bottom right of the form are three buttons: "Back", "Next", and "Close".

The following table describes the fields in this screen.

Table 4 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box: IPoA , ENET ENCAP , PPPoA , or PPPoE .
Multiplex	Select the multiplexing method used by your ISP from the Multiplex drop-down list box either VC-based or LLC-based.
VPI	Enter the Virtual Path Identifier (VPI) assigned to you. This field may already be configured.
VCI	Enter the Virtual Channel Identifier (VCI) assigned to you. This field may already be configured.
Select Yes to enter specific IP information from your Internet service provider. Enter your Internet access information exactly as your service provider gave it to you.	
IP Address	Enter the IP address of the AMG1302/AMG1202-TSeries.
Subnet Mask	Enter the subnet mask in dotted decimal notation. Refer to the appendix to calculate a subnet mask if you are implementing subnetting.
Default Gateway	You must specify a gateway IP address (supplied by your ISP) when you use ENET ENCAP in the Encapsulation field in the previous screen.
Primary DNS Server	Enter the primary DNS server IP address for the AMG1302/AMG1202-TSeries.
Secondary DNS Server	Enter the secondary DNS server IP address for the AMG1302/AMG1202-TSeries.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Exit	Click this to close the wizard screen without saving.

Figure 11 Internet Connection with PPPoA

Quick Start STEP 1

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

Encapsulation:

User Name:

Password:

Multiplex:

VPI: (Range : 0~255)

VCI: (Range : 32~65535)

IP Address:

Primary DNS Server:

Secondary DNS Server:

The following table describes the fields in this screen.

Table 5 Internet Connection with PPPoA

LABEL	DESCRIPTION
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box: IPoA , ENET ENCAP , PPPoA , or PPPoE .
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Multiplex	Select the multiplexing method used by your ISP from the Multiplex drop-down list box either VC-based or LLC-based.
VPI	Enter the Virtual Path Identifier (VPI) assigned to you. This field may already be configured.
VCI	Enter the Virtual Channel Identifier (VCI) assigned to you. This field may already be configured.
IP Address	Enter the IP address of the AMG1302/AMG1202-TSeries.
Primary DNS Server	Enter the primary DNS server IP address for the AMG1302/AMG1202-TSeries.
Secondary DNS Server	Enter the secondary DNS server IP address for the AMG1302/AMG1202-TSeries.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Exit	Click this to close the wizard screen without saving.

Figure 12 Internet Connection with PPPoE

The following table describes the fields in this screen.

Table 6 Internet Connection with PPPoE

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Multiplex	Select the multiplexing method used by your ISP from the Multiplex drop-down list box either VC-based or LLC-based.
VPI	Enter the Virtual Path Identifier (VPI) assigned to you. This field may already be configured.
VCI	Enter the Virtual Channel Identifier (VCI) assigned to you. This field may already be configured.
Select Yes to enter specific IP information from your Internet service provider. Enter your Internet access information exactly as your service provider gave it to you.	
IP Address	Enter the IP address of the AMG1302/AMG1202-TSeries.
Primary DNS Server	Enter the primary DNS server IP address for the AMG1302/AMG1202-TSeries.
Secondary DNS Server	Enter the secondary DNS server IP address for the AMG1302/AMG1202-TSeries.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Exit	Click this to close the wizard screen without saving.

- If the user name and/or password you entered for PPPoE or PPPoA connection are not correct, you are prompted to enter the correct information.

- If the Internet connection fails, check to see if your account is activated.

After you configure the Internet access information, use the following screen to set up your wireless LAN.

- 5 Check the **Wireless Service** box to enable wireless connection on the ZyXEL device.
- 6 Configure your wireless settings in this screen. Click **Next**.

Figure 13 Wireless Setup

The following table describes the labels in this screen.

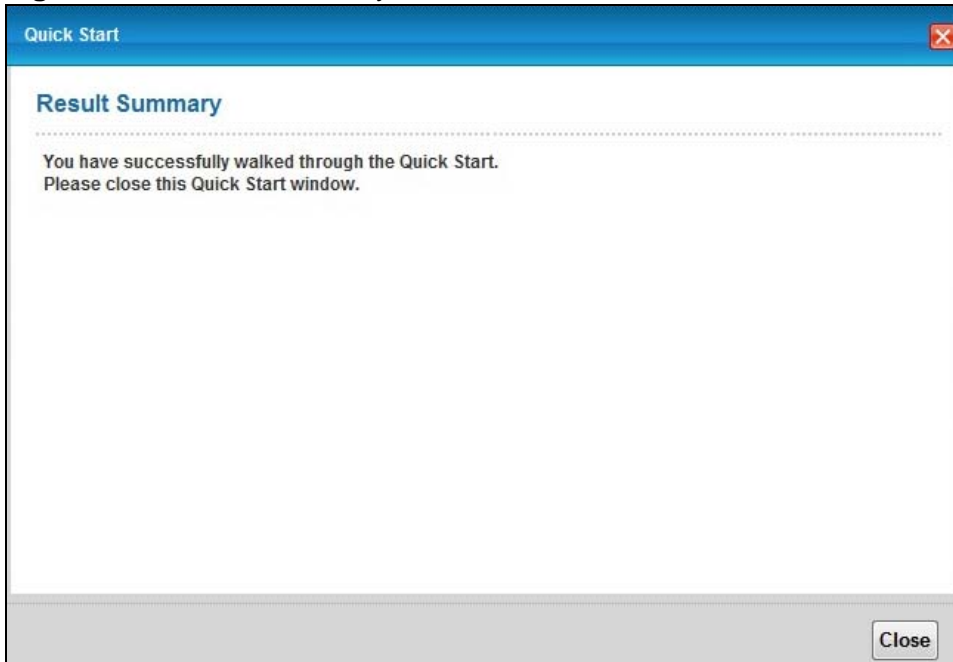
Table 7 Wireless Setup

LABEL	DESCRIPTION
Wireless Service	Click this to enable or disable wireless service on the ZyXEL device.
Wireless Network Name(SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the AMG1302/AMG1202-TSeries, make sure all wireless stations use the same SSID in order to access the network.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel ID that is not already in use by a neighboring device.
Security	Displays the security setting. To modify, see Section 7.2 on page 92 .
Pre-Shared Key	Enter a set of characters (8 to 63 characters or 64 hexadecimal digits [a-f, A-F, and 0-9]) for the shared security key.
Back	Click this to return to the previous screen without saving.
Next	Click this to continue to the next wizard screen.
Exit	Click this to close the wizard screen without saving.

Note: The wireless stations and AMG1302/AMG1202-TSeries must use the same SSID and channel ID for wireless communication.

- 7 The configuration settings are saved and applied. Click **Close** to complete the Internet / Wireless setup.

Figure 14 Results Summary



- 8 Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of AMG1302/AMG1202-TSeries features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.

4.1 Overview

This chapter shows you how to use the AMG1302/AMG1202-TSeries's various features.

- [Setting Up Your DSL Connection](#), see page 37
- [IPv6 Address Configuration](#), see page 39
- [Setting Up a Secure Wireless Network](#), see page 40
- [Configuring the MAC Address Filter for Restricting Wireless Internet Access](#), see page 47
- [Setting Up NAT Forwarding for a Game Server](#), see page 48
- [Setting Up NAT Forwarding for a Game Server](#), see page 48
- [Configuring Firewall Rules to Allow a Specified Service](#), see page 50
- [Configuring Static Route for Routing to Another Network](#), see page 53
- [Port Binding Configuration](#), see page 55
- [Configuring QoS to Prioritize Traffic](#), see page 59
- [Access the AMG1302/AMG1202-TSeries from the Internet Using DDNS](#), see page 62

4.2 Setting Up Your DSL Connection

This tutorial shows you how to set up your Internet connection using the web configurator.

If you connect to the Internet through a DSL connection, use the information from your Internet Service Provider (ISP) to configure the AMG1302/AMG1202-TSeries. Do the following steps:

- 1 Connect the AMG1302/AMG1202-TSeries properly. Refer to the Quick Start Guide for details on the AMG1302/AMG1202-TSeries's hardware connection.
- 2 Connect one end of a DSL cable to the DSL port of your AMG1302/AMG1202-TSeries. The other end should be connected to the DSL port in your house or a DSL router/modem provided by your ISP.
- 3 Connect one end of Ethernet cable to an Ethernet port on the AMG1302/AMG1202-TSeries and the other end to a computer that you will use to access the web configuration.
- 4 Connect the AMG1302/AMG1202-TSeries to a power source, turn it on and wait for the **POWER** LED to become a steady green.

Account Configuration

For this example, the interface type is ADSL and the connection has the following information.

General	
Mode	Router
Encapsulation	PPPoE
User Name	1234@DSL-Ex.com
Password	ABCDEF!
Service Name	My DSL
Multiplex	LLC
IPv6/IPv4 Dual Stack	Enabled
PPP Authentication	Auto
VPI	0
VCI	33
Others	IP Address: Obtain IP Address Automatically DNS Server: Obtained From ISP IPv6 Address: Obtain IPv6 Address Automatically DHCP IPv6: DHCP DHCP PD: Enable WAN Identifier Type: EUI64

Go to **Network Setting > Broadband**, enter or select these values and click **Apply**.

Line

Type

General

Mode

Encapsulation

User Name

Password

Multiplex

IPv6/IPv4 Dual Stack:

PPP Authentication

Virtual Circuit ID

VPI (Range : 0~255)

VCI (Range : 32~65535)

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

DNS Server

Primary DNS

Secondary DNS

IPv6 Address

Obtain an IP Address Automatically

Static IP Address

DHCP IPv6 DHCP SLAAC Auto

DHCP PD Enable Disable

WAN Identifier Type Manual EUI64

WAN Identifier

Connection

Keep Alive

Connect on Demand Sec

This completes your DSL WAN connection setting.

4.3 IPv6 Address Configuration

If the ISP's network supports IPv6, the ISP may assign an IPv6 address to the AMG1302/AMG1202-TSeries automatically.



In the **Network Setting > Broadband** screen's **IPv6 Address** configuration section, select **Obtain an IP Address Automatically**. In the **DHCP IPv6** field select **DHCP** to obtain an IPv6 address from a DHCPv6 server. In the **DHCP PD** field select **Enable** to have the AMG1302/AMG1202-TSeries pass the WAN prefix to LAN hosts. The LAN hosts can then use the prefix to generate their IPv6 addresses.

IPv6 Address

Obtain an IP Address Automatically

Static IP Address

DHCP IPv6 DHCP SLAAC Auto

DHCP PD Enable Disable

WAN Identifier Type Manual EUI64

WAN Identifier

4.4 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 AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries. Then he can set up a wireless network using WPS ([Section 4.4.2 on page 41](#)) or manual configuration ([Section 4.4.3 on page 45](#)).

4.4.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a wireless network. In the client, choose the AP with the SSID configured here. When prompted for a key, use the Pre-Shared Key configured here.

SSID	SecureWirelessNetwork
Security Mode	WPA2-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b+g+n

- 1 Click **Network Setting > Wireless** to open the **General** screen. Configure the screen using the provided parameters (see [page 40](#)). Click **Apply**.

Wireless Network Setup

Wireless Enable Wireless LAN

Wireless Network Settings

Wireless Network Name (SSID):

Hide SSID

Client Isolation

MBSSID/LAN Isolation

Channel Selection :

Operating Channel : 6

Security Level

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

Security Mode :

Enter 8-63 characters or 64 hexadecimal digits (a-f, A-F, and 0-9).

Pre-Shared Key [more...](#)

- 2 Click **Network Setting > Wireless > Advanced** and make sure **802.11b+g+n** is selected in the **802.11 Mode** field. Click **Apply**.

Fragmentation Threshold: (256 ~ 2346, even numbers only)

Output Power :

Preamble :

802.11 Mode :

Channel Width :

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the AMG1302/AMG1202-TSeries (see [Section 4.4.2 on page 41](#)). He can also use the notebook's wireless client to search for the AMG1302/AMG1202-TSeries (see [Section 4.4.3 on page 45](#)).

4.4.2 Using WPS

This section shows you how to set up a wireless network using WPS. WPS is a way to automatically set up a secure wireless network connection between an AP and a notebook. Limitations of using WPS are that it must be done two devices at a time and within two minutes. It uses the AMG1302/

AMG1202-TSeries as the AP and ZyXEL NWD210N as the wireless client which connects to the notebook.

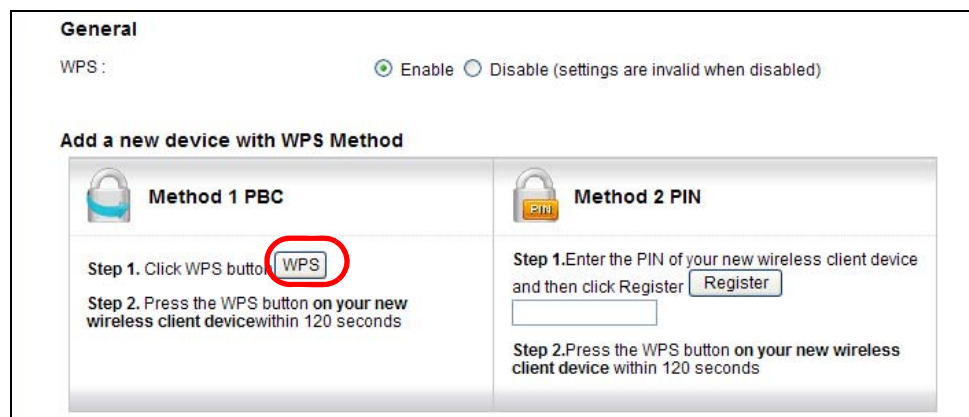
Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCMCIA card).

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 AMG1302/AMG1202-TSeries. A wireless client must also use the same PIN in order to download the wireless network settings from the AMG1302/AMG1202-TSeries.

Push Button Configuration (PBC)

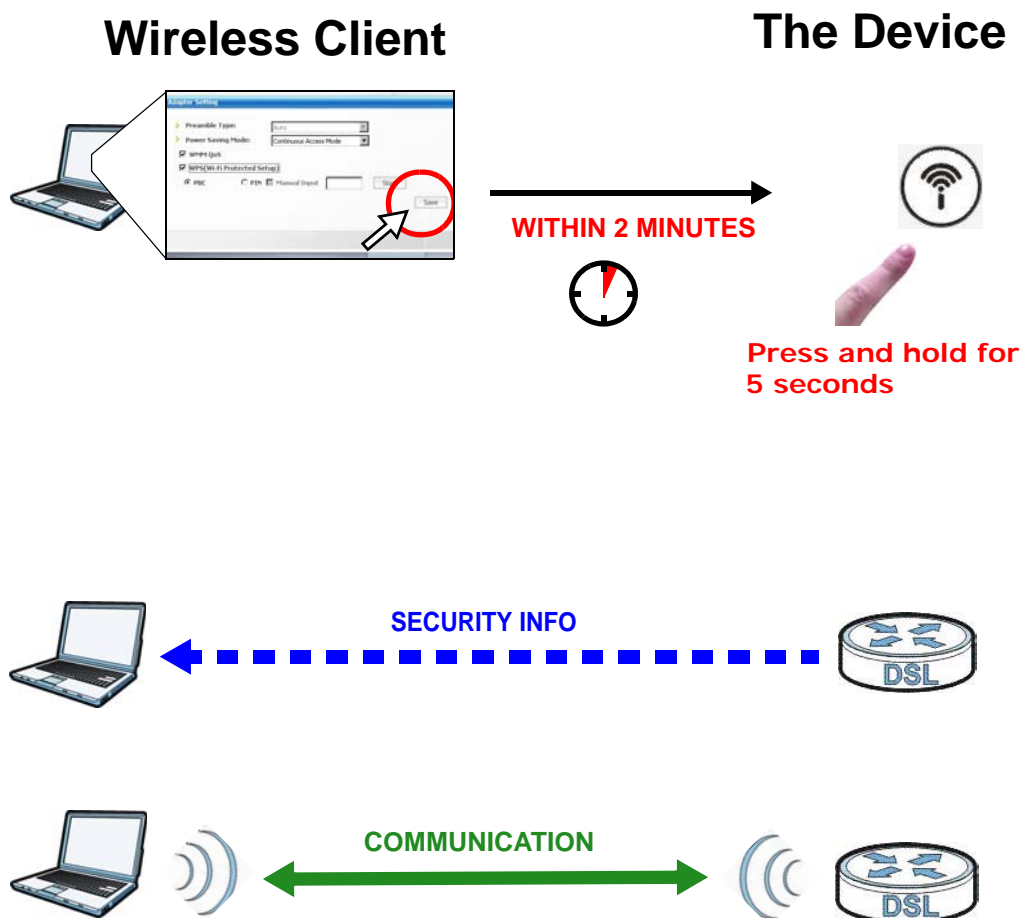
- 1 Make sure that your AMG1302/AMG1202-TSeries is turned on and your notebook is within the cover range of the wireless signal.
- 2 Make sure that you have installed the wireless client driver and utility in your notebook.
- 3 Make sure wireless LAN is enabled and the wireless security mode is set to **WPA-PSK2** or **No Security** in the **Network Setting > Wireless > General** screen.
- 4 In the wireless client utility, go to the WPS setting page. Enable WPS and press the WPS button (**Start** or **WPS** button).
- 5 Push and hold the **WPS** button on the AMG1302/AMG1202-TSeries for 1-2 seconds. Alternatively, you may log into AMG1302/AMG1202-TSeries's web configuration, enable WPS and click the **WPS** button in the **Network Setting > Wireless > WPS** screen.



Note: It doesn't matter which button (on the client or the AMG1302/AMG1202-TSeries) is pressed first. You must press the second button within two minutes of pressing the first one.

The AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries and wireless client.



PIN Configuration



When you use the PIN configuration method, you need to use both the AMG1302/AMG1202-TSeries's web configuration utility 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 Enter the PIN number in the **PIN** section in the **Network Setting > Wireless > WPS** screen on the AMG1302/AMG1202-TSeries.

General

WPS : Enable Disable (settings are invalid when disabled)

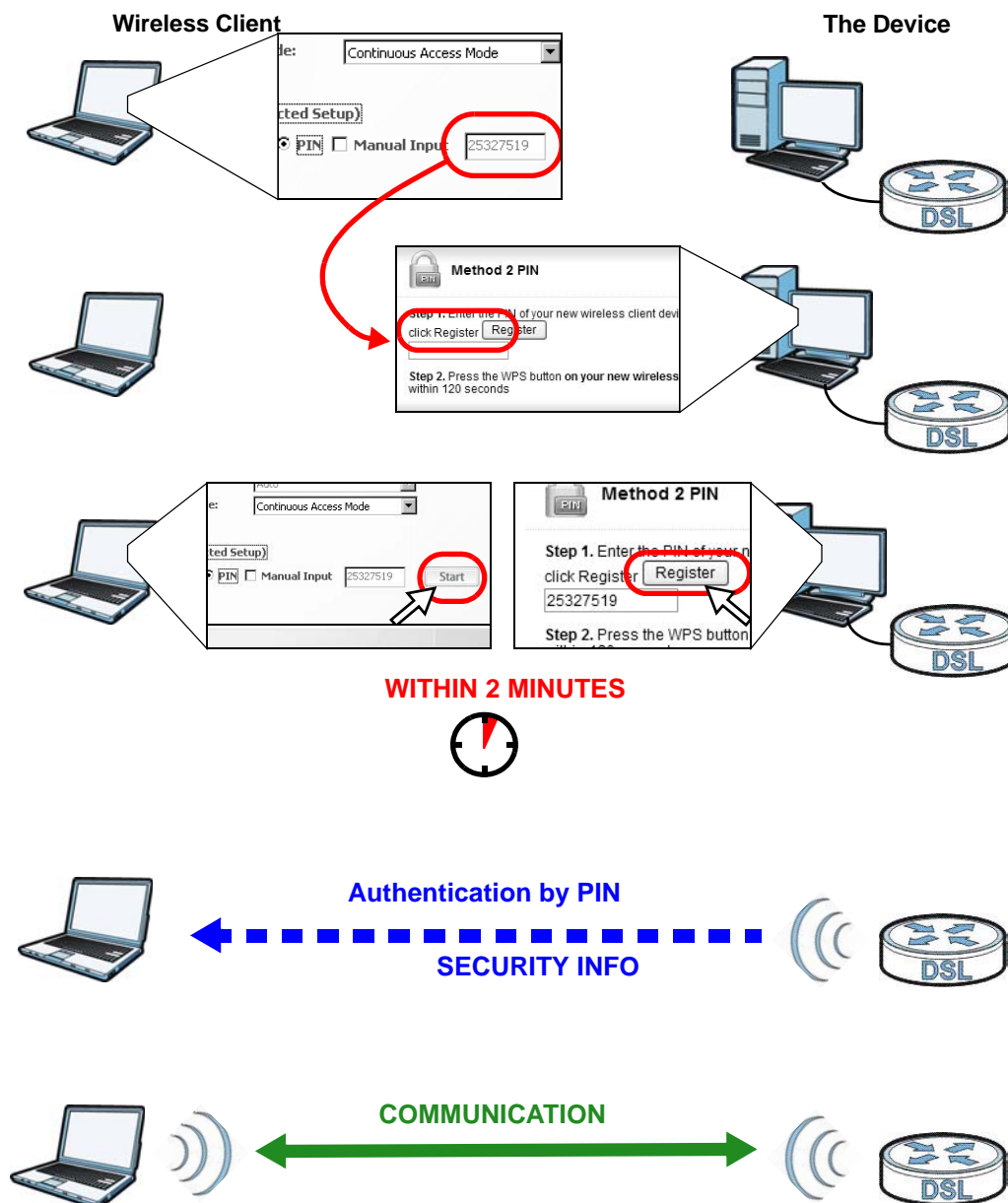
Add a new device with WPS Method

 Method 1 PBC	 Method 2 PIN
<p>Step 1. Click WPS button <input type="button" value="WPS"/></p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>	<p>Step 1. Enter the PIN of your new wireless client device and then click Register <input type="button" value="Register"/></p> <p><input type="text"/></p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>

- 3 Click the **Start** and **Register** buttons (or the button next to the PIN field) on both the wireless client utility screen and the AMG1302/AMG1202-TSeries's **WPS** screen within two minutes.

The AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries securely.

The following figure shows you how to set up a wireless network and its security on a AMG1302/AMG1202-TSeries and a wireless client by using PIN method.



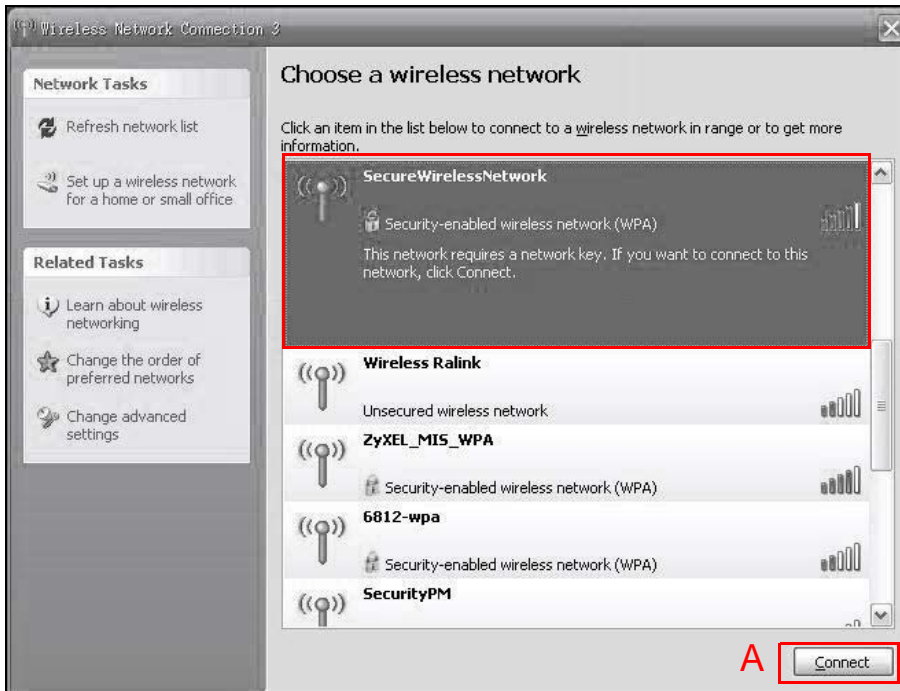
4.4.3 Connecting Wirelessly to your AMG1302/AMG1202-TSeries

This section describes how to connect wirelessly to your AMG1302/AMG1202-TSeries. The connection procedure is shown here using Windows XP as an example.

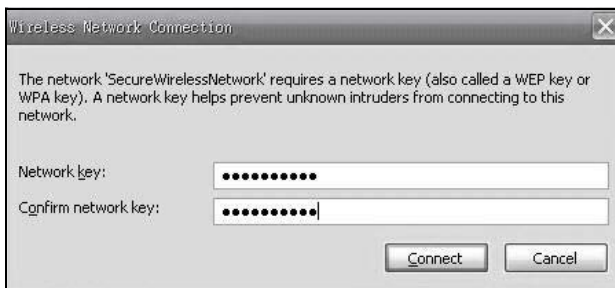
- 1 Right-click the wireless adapter icon which appears in the bottom right of your computer monitor. Click **View Available Wireless Networks**.



- 2 Select the AMG1302/AMG1202-TSeries’s **SSID** name and click **Connect (A)**. The SSID “SecureWirelessNetwork” is given here as an example.



- 3 You are prompted to enter a password. Enter it and click **Connect**.



- 4 You may have to wait several minutes while your computer connects to the wireless network.
- 5 You should now be securely connected wirelessly to the AMG1302/AMG1202-TSeries.



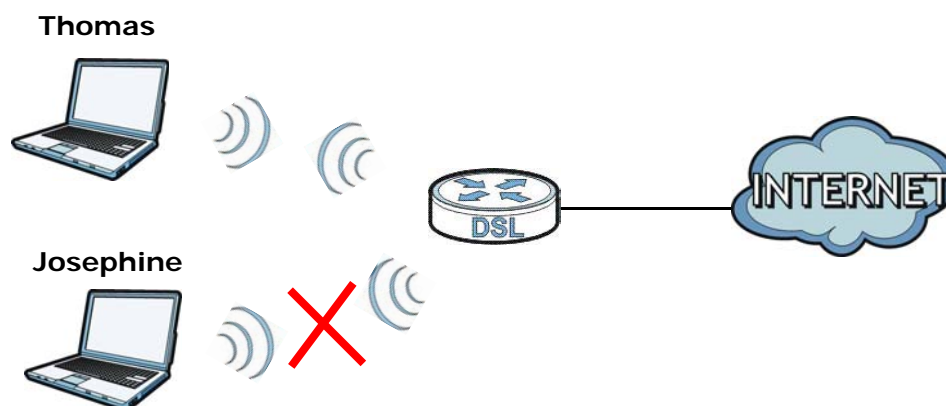
Congratulations! Your computer is now ready to connect to the Internet wirelessly through your AMG1302/AMG1202-TSeries.

Note: If you cannot connect wirelessly to the AMG1302/AMG1202-TSeries, check you have selected the correct SSID and entered the correct security key. If that does not work, ensure your wireless network adapter is enabled by clicking on the wireless adapter icon and clicking Enable.

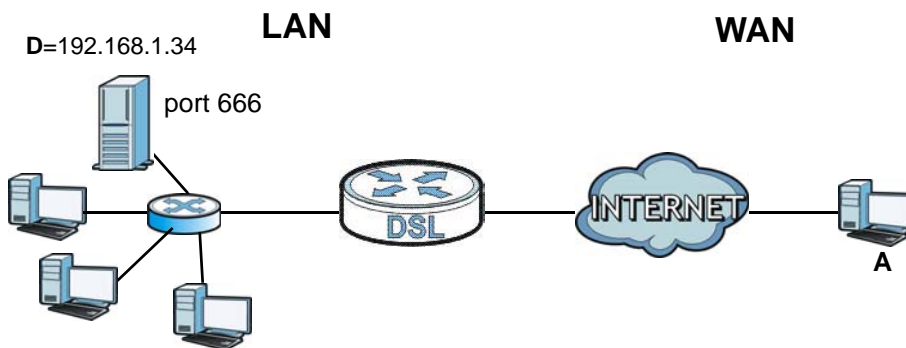
4.5 Configuring the MAC Address Filter for Restricting Wireless Internet Access

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 AMG1302/AMG1202-TSeries. Thomas can deny access to the wireless network using the MAC address of Josephine's computer.



- 1 Check the MAC address (physical address) of the wireless card on Josephine's computer using the "ipconfig /all" command in a Command Prompt.



4.6.1 Port Forwarding

Thomas needs to configure the port settings and IP address on the AMG1302/AMG1202-TSeries. Traffic should be forwarded to port 666 of the Doom server computer which has an IP address of 192.168.1.34.

Thomas may set up the port settings by configuring the port settings for the Doom server computer (see [Section 11.3 on page 153](#) for more information).

- 1 Activate NAT in the **Network Setting > NAT > General** screen. Click **Apply**.

Active

Max NAT/Firewall Session Per User

Note:

Maximum number of NAT/firewall sessions for the router is 8192. To remove the per user limit, set to 8192.

Apply Cancel

- 2 Click **Network Setting > NAT > Port Forwarding**. Select **PVC0** as the WAN interface and click **Add new rule**.

WAN Interface

Add new rule

#	Active	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify

Note:

The TCP port 7547 is reserved for TR069 connection request port.

- 3 Configure the screen with the following values:

Service Name	Select User Define .
Start/End Ports	Enter 666 as the Start and End port.
Server IP Address	Enter the IP address of the Doom server (192.168.1.34 for this example).

The screen should look as follows. Click **Apply**.

- The port forwarding settings you configured appear in the table. The AMG1302/AMG1202-TSeries forwards port 666 traffic to the computer with IP address 192.168.1.34.

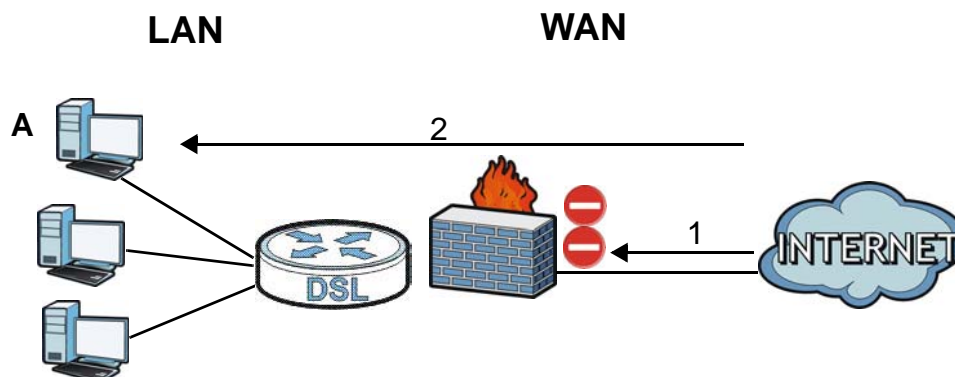
#	Active	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify
1		User Define	666	666	666	666	192.168.1.34	

Note :
The TCP port 7547 is reserved for TR069 connection request port.

Players on the Internet then can have access to Thomas' Doom server.

4.7 Configuring Firewall Rules to Allow a Specified Service

By default the firewall will block traffic originating from the WAN (1). However, if you are running a server or other service, you may need to allow access from the WAN (2). The following tutorial will show how to allow traffic from WAN to LAN if it matches a specified port number.



- 1 Click **Security > Firewall** and select **Custom**. Click **Apply** to save your settings.

Firewall

High
This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, FTP, HTTP, HTTPS, DNS, POP3, SMTP) is permitted.

Medium
This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.

Low
This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server.

Custom
This setting allows the customer to create and edit individual firewall rules.

Off
This setting is not recommended. It disables firewall protection for your network and could potentially expose your network to significant security risks. This option should only be used for troubleshooting or if you intend using another firewall in conjunction with your ZyXEL router.

- 2 Click the **Rules** tab. In the **Packet Direction** field select **WAN to LAN** and click **Add**.

Rules

Firewall Rules Storage Space in Use (0%)

0% 100%

Packet Direction WAN to LAN

Create a new rule after rule number 0

#	Active	Source IP Address	Destination IP Address	Service	Action	Source Interface	Destination Interface	Modify	Order

- 3 The **Add New Firewall Rule** screen will appear. Click the **Edit Customized Services** button to access the following screen. Click **Add** and configure the following settings. In this tutorial, a hypothetical port 123 is allowed. Click **OK**.

Service Name	My_Service
Service Type	TCP
Port Number	123

Config

Service Name:

Service Type:

Port Configuration

Type: Single Port Range

Port Number: From To

- 4 In the **Add New Firewall Rule** screen, select **Active**. In the **Available Services** field, select the service you configured, **My_Service**. Click **OK**.

Add New Firewall Rule

Edit Rule

Active

Action for Matched Packets:

IP Version Type:

Rate Limit: packets/second

Maximum Burst Number: (packets)

Log(Log Level:DEBUG)

Rules

Source Address

Address Type:

Start IP Address:

End IP Address:

Subnet Mask:

Source Mac Address:

Source Interface:

Destination Address

Address Type:

Start IP Address:

End IP Address:

Subnet Address:

Destination Interface:

Service

Available Services:

TCP Flag: (SYN,ACK,FIN,RST,URG,PSH,ALL,NONE)

Schedule

Day to Apply

Everyday

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Apply:(24-Hour Format)

All Day

Start hour minute End hour minute

- 5 The firewall rule you configured appears in the table. The AMG1302/AMG1202-TSeries allows traffic from the WAN to LAN if it matches port 123.

Rules
Firewall Rules Storage Space in Use (2%)
0%  100%

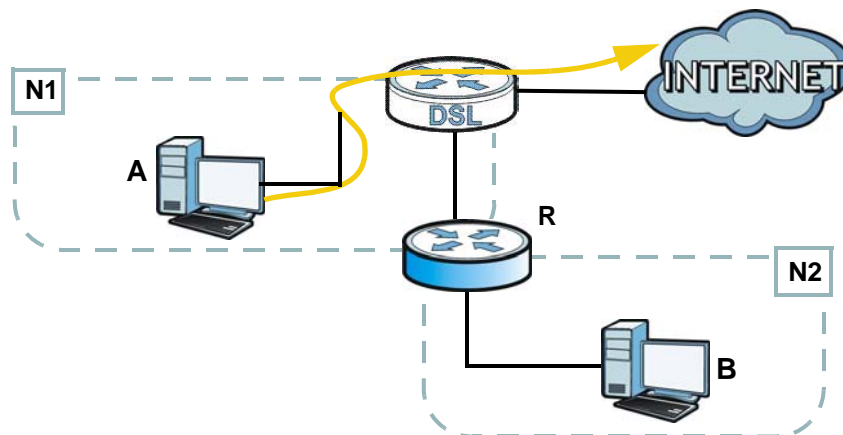
Packet Direction: WAN to LAN
Create a new rule after rule number: 0

#	Active	Source IP Address	Destination IP Address	Service	Action	Source Interface	Destination Interface	Modify	Order
1	Yes	Any	Any	My_Ser...	Permit		N/A	  	

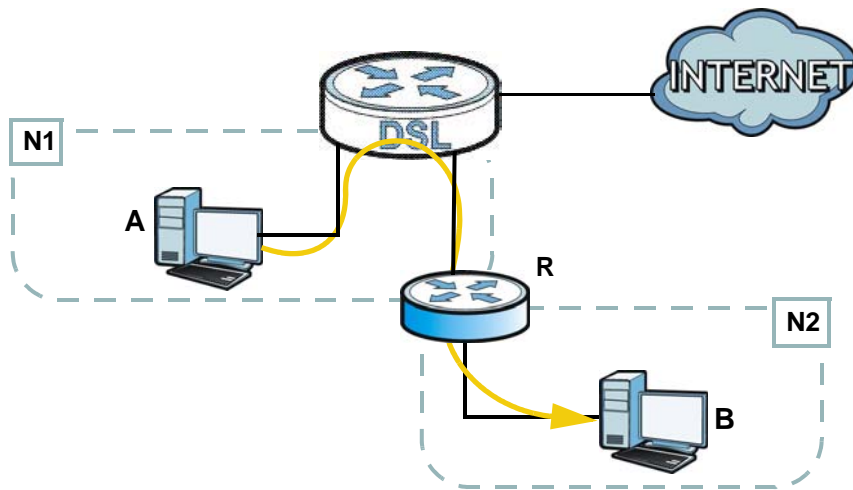
4.8 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the AMG1302/AMG1202-TSeries'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 AMG1302/AMG1202-TSeries'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 AMG1302/AMG1202-TSeries'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 AMG1302/AMG1202-TSeries to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the AMG1302/AMG1202-TSeries routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 8 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The AMG1302/AMG1202-TSeries's WAN	172.16.1.1
The AMG1302/AMG1202-TSeries's LAN	192.168.1.1
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 AMG1302/AMG1202-TSeries's Web Configurator.
- 2 Click **Network Setting > Static Route**.
- 3 Click **Edit** on a new rule in the **Static Route** screen.



- 4 Configure the **Static Route Setup** screen using the following settings:
 - 4a Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.
 - 4b Type **192.168.1.253** (**R's N1** address) in the **Gateway IP Address** field.
 - 4c Enter **1** in the **Metric** field.

4d 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.

4.9 Port Binding Configuration

This tutorial shows you how to configure port binding for WAN connections with different ATM QoS settings for different types of traffic. The port binding feature is used to group each WAN connection with specific LAN ports and WLANs. In this example ATM QoS settings are configured for a WAN PVC for time sensitive Media-On-Demand (MOD) traffic. ATM QoS settings are also configured for another WAN PVC for non-time sensitive data traffic.

4.9.1 Configuring ATM QoS for Multiple WAN Connections

This example shows an application for multiple WAN connections with different ATM QoS Settings.

More than one WAN connection on the AMG1302/AMG1202-TSeries may be configured to record traffic statistics or calculate service charges.

Three WAN connections are configured over the ADSL line:

- The connection with VPI/VCI, **0/33**, is dedicated for general data transmission.
- The connection with VPI/VCI, **0/34**, is dedicated for VoIP service.
- The connection with VPI/VCI, **0/35**, is dedicated for Media-On-Demand (MOD) service.

To configure bandwidth for the WAN connections, access the WAN configuration **Advanced Setup** screen by clicking **Network Setting** > **Broadband**. Click **Advanced Setup**.

Line
ADSL Mode: Auto Sync-Up

General
 Mode: Router
 Encapsulation: PPPoE
 User Name: ChangeMe
 Password: ••••••••
 Service Name:
 Multiplex: LLC
 IPv6/IPv4 Dual Stack: IPv4/IPv6
 PPP Authentication: Auto
 Virtual Circuit ID
 VPI: 0 (Range : 0~255)
 VCI: 33 (Range : 32~65535)

IP Address
 Obtain an IP Address Automatically
 Static IP Address
 IP Address: 0.0.0.0

DNS Server
 Primary DNS: Obtained From ISP 0.0.0.0
 Secondary DNS: Obtained From ISP 0.0.0.0

IPv6 Address
 Obtain an IP Address Automatically
 Static IP Address
 DHCP IPv6: DHCP SLAAC Auto
 DHCP PD: Enable Disable
 WAN Identifier Type: Manual EUI64
 WAN Identifier:

Connection
 Keep Alive
 Connect on Demand Max Idle Time: 0 Sec

EXAMPLE

To configure bandwidth for the data connection, select **UBR with PCR** in the **ATM QoS Type** field. Click **Apply**.

RIP & Multicast Setup	
RIP Direction	None
RIP Version	RIP1
Multicast	None
MLD Proxy	None
ATM QoS	
ATM QoS Type	UBR With PCR
Peak Cell Rate	0 cell/sec
Sustain Cell Rate	0 cell/sec
Maximum Burst Size	0 cell
PPPoE Passthrough	No
MTU	
MTU	1492
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>	

To configure dedicated bandwidth of 400 kbps for the VoIP connection, select **CBR** in the **ATM QoS Type** field and enter the **Peak Cell Rate** as **943** (divide the bandwidth 400000 bps by 424). Click **Apply** to save the settings.

RIP & Multicast Setup	
RIP Direction	None
RIP Version	RIP1
Multicast	None
MLD Proxy	None
ATM QoS	
ATM QoS Type	CBR
Peak Cell Rate	943 cell/sec
Sustain Cell Rate	0 cell/sec
Maximum Burst Size	0 cell
PPPoE Passthrough	No
MTU	
MTU	1492
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>	

To configure variable bandwidth of 2 Mbps for MOD data connection, select **Realtime VBR** in the **ATM QoS Type** field. Set the **Peak Cell Rate** as **4717** (divide the bandwidth 2mbps by 424) and set both the **Sustain Cell Rate** and **Maximum Burst Size** as **4716** (which is less than the peak cell rate). Click **Apply** to save the settings.

RIP & Multicast Setup

RIP Direction: None

RIP Version: RIP1

Multicast: None

MLD Proxy: None

ATM QoS

ATM QoS Type: Realtime VBR

Peak Cell Rate: 4717 cell/sec

Sustain Cell Rate: 4716 cell/sec

Maximum Burst Size: 4716 cell

PPPoE Passthrough: No

MTU

MTU: 1492

Apply Cancel Advanced Setup

Configured WAN connections can be viewed by clicking the **More Connections** tab under **Network Setting > Broadband**. See the WAN Setup chapter ([Chapter 6 on page 73](#)) for more information on configuring WAN connections and ATM QoS settings.

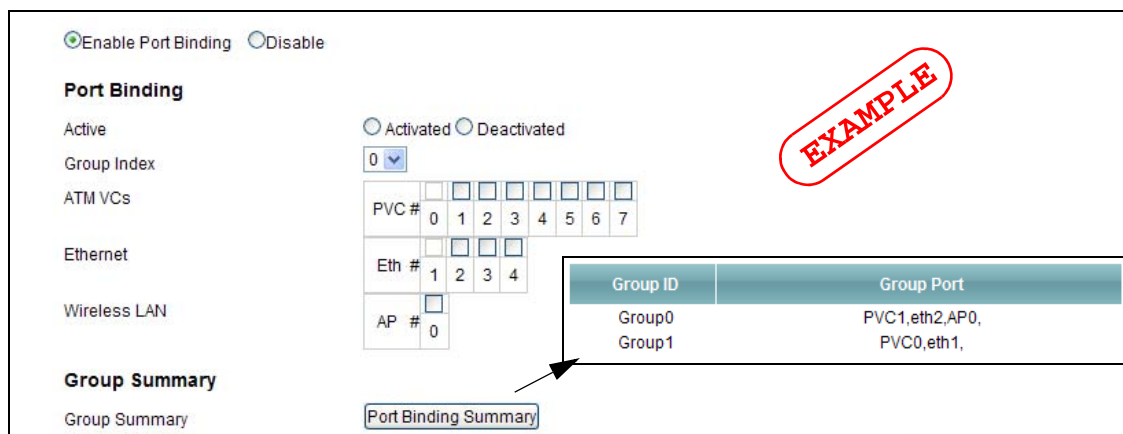
4.9.2 Configuring Port Binding

You can then group specific WAN PVCs with LAN ports or WLANs, so traffic from these ports is forwarded through specific WAN PVCs. In the configuration shown below, the WAN connections set up in the previous section are bound as follows:

Table 9 Port Binding Groups

GROUP INDEX	WAN CONNECTION	LAN PORT
0	PVC0 - for Data	eth1, eth2, APO
1	PVC1 - for VoIP	eth3
2	PVC2 - for MOD	eth4

- 1 Access the port binding screen by clicking **Network Setting > Port Binding**, and select **Activated Port Binding** to turn on the port binding feature.
- 2 Click the **Port Binding** tab, specify the **Group Index** and select the ports to include in the port binding group. Click **Apply**.



- The configured groups can be viewed by clicking the Port Binding Summary button. See the Port Binding chapter ([Chapter 12 on page 161](#)) for more details on configuring port binding.

4.10 Configuring QoS to Prioritize Traffic

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

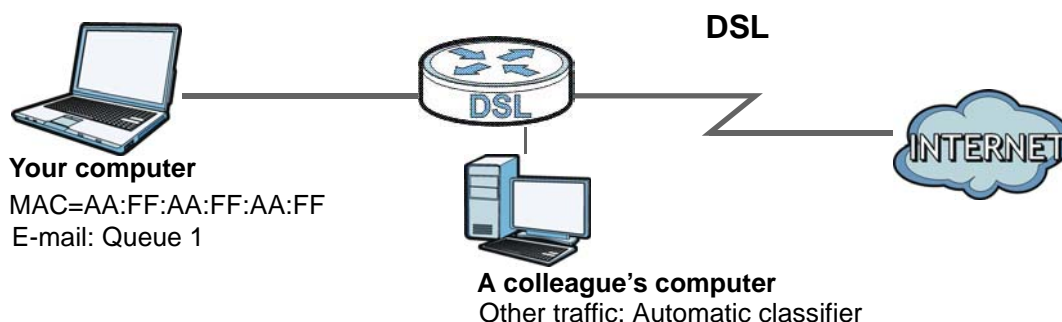
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues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

In the following figure you want to configure QoS so that e-mail traffic gets the highest priority. You can do the following:

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

Note: QoS is applied to traffic flowing out of the AMG1302/AMG1202-TSeries.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the AMG1302/AMG1202-TSeries.



- 1 Click **Network Setting > QoS** and check **Active QoS**. Click **Apply**.

- 2 Go to **Network Setting > QoS > Queue Setup**. Click the **Edit** icon next to an entry to configure a queue.

Inde	Status	Name	Interface	Priority	Weight	Rate Limit	Modify
1	💡	N/A	N/A	N/A	N/A	N/A N/A	
2	💡	N/A	N/A	N/A	N/A	N/A N/A	
3	💡	N/A	N/A	N/A	N/A	N/A N/A	
4	💡	N/A	N/A	N/A	N/A	N/A N/A	

Note :
If queue is deleted, then related classifiers will be removed too.

- 3 Select **Active** and give it a name (**Queue1** in this example). Select **WAN** in the **Interface** field and **1** in the **Priority** and **Weight** fields. Then click **OK**.

- 4 Go to **Network Setting > QoS > Class Setup** and click **Add new Classifier**.

Index	Status	From Interface	Classification Criteria	DSCP(Traffic Class) Mark	802.1P/1Q Mark	To Queue	Modify
-------	--------	----------------	-------------------------	--------------------------	----------------	----------	--------

- 5 Select **Active** and follow the settings as shown in the screen below. Then click **OK**. Note that you have to select **TCP** in the **IP Protocol** field first, then you can configure the source port range setting.

Add new Classifier

Rule Index

Class Configuration

Active

Ether Type

Interface

To Queue

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 LAN1 LAN2 LAN3 LAN4 ra0 ra1 ra2 ra3

▪ **Source**

IP Address IP Subnet Mask Exclude

Port Range ~ Exclude

MAC Address MAC Mask Exclude

▪ **Destination**

IP Address IP Subnet Mask Exclude

Port Range ~ Exclude

MAC Address MAC Mask Exclude

▪ **Others**

Service

IP Protocol Exclude

TCP ACK Exclude

DHCP Exclude

Packet Length ~ Exclude

IPP/DS Field IPP/TOS DSCP

IP Precedence Range ~ Exclude

Type of Service Exclude

DSCP Range(0 ~ 63) ~ Exclude

802.1P ~ Exclude

VLAN ID ~ (Value Range: 1 ~ 4094) Exclude

Action

Forward to

IPP/DS Field IPP/TOS DSCP

IP Precedence Mark

Type Of Service Mark

DSCP Mark(0 ~ 63)

802.1Q Tag

- Ethernet Priority

- VLAN ID (Value Range: 1 ~ 4094)

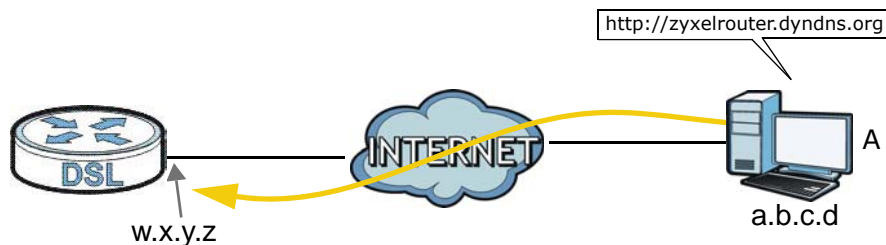
OK Cancel

Interface	Select From LAN .
To Queue	Link this to a queue created in the Network Setting > QoS > Queue Setup screen, which is the 1 queue created in this example.
Source MAC Address	Type the MAC address of your computer - AA:FF:AA:FF:AA:FF . Type the Source Mac Netmask if you know it.
Source Port Range	Enter the port number to which the rule should be applied - 25 for SMTP.
Protocol ID	Select the IP protocol type - TCP .

This maps e-mail traffic to queue 1 created in the previous screen (see the **Source Port Range** field). This also maps your computer's MAC address to queue 1 (see the **Source MAC Address** field).

4.11 Access the AMG1302/AMG1202-TSeries from the Internet Using DDNS

If you connect your AMG1302/AMG1202-TSeries to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The AMG1302/AMG1202-TSeries's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the AMG1302/AMG1202-TSeries using a domain name.



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

This tutorial shows you how to:

- [Registering a DDNS Account on \[www.dyndns.org\]\(http://www.dyndns.org\)](#)
- [Configuring DDNS on Your AMG1302/AMG1202-TSeries](#)
- [Testing the DDNS Setting](#)

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

4.11.1 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 AMG1302/AMG1202-TSeries is currently using. You can find the IP address on the AMG1302/AMG1202-TSeries's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the AMG1302/AMG1202-TSeries later.

4.11.2 Configuring DDNS on Your AMG1302/AMG1202-TSeries

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

- Select **Active Dynamic DNS**.
- Select **www.dyndns.org** in the **Service Provider** field.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).

Dynamic DNS Configuration

Dynamic DNS Enable Disable

Service Provider:

Host Name:

Username:

Password:

Click **Apply**.

4.11.3 Testing the DDNS Setting

Now you should be able to access the AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries's login page should appear. You can then log into the AMG1302/AMG1202-TSeries and manage it.

PART II

Technical Reference

Connection Status and System Info Screens

5.1 Overview

After you log into the web configurator, the **Connection Status** screen appears. This shows the network connection status of the AMG1302/AMG1202-TSeries and clients connected to it.

Use the **System Info** screen to look at the current status of the device, system resources and interfaces (LAN, WAN, WLAN).

5.2 The Connection Status 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 AMG1302/AMG1202-TSeries to update this screen in **Refresh Interval**.

Figure 15 Connection Status: Icon View

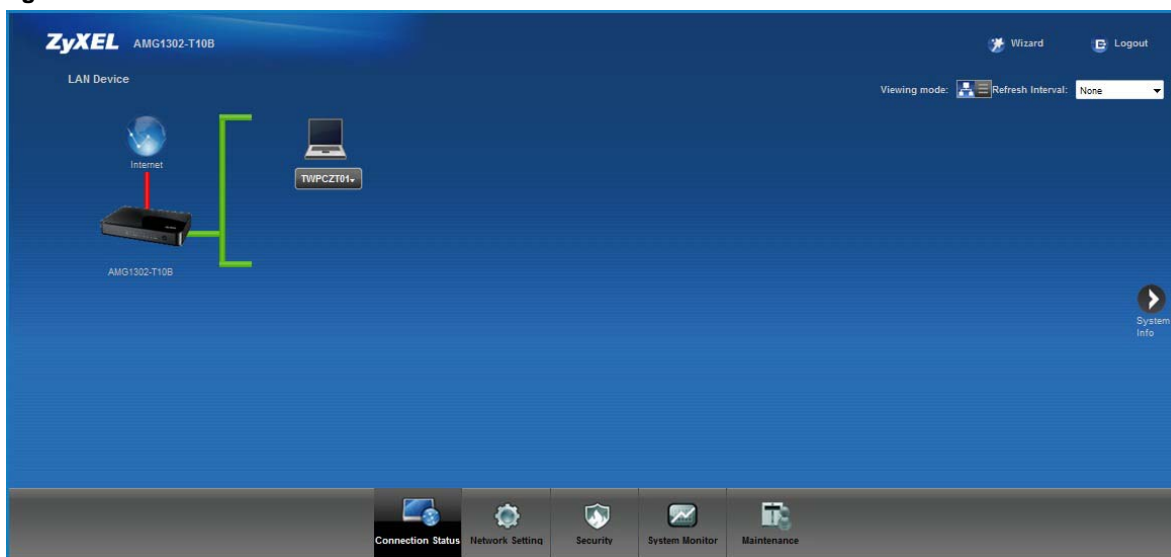


Figure 16 Connection Status: List View

#	Device Name	IP Address	Link-local IPv6 Address	Global IPv6 Address	MAC Address	Reserve
1	Unknown	192.168.1.60	N/A	N/A	6C:F0:49:70:12:C5	<input type="checkbox"/>
2	Unknown	192.168.1.11	N/A	N/A	00:24:1D:7F:34:05	<input type="checkbox"/>

In **Icon View**, if you want to view information about a client, click the client’s name and then click on **Info**.

In **List View**, you can also view the client’s information.

5.3 The System Info Screen

Click **Connection Status > System Info** to open this screen.

Figure 17 System Info Screen

ZyXEL AMG1302-T10B

System Info

Refresh Interval: None

Device Information	
Host Name:	admin
Model Name:	AMG1302-T10B
MAC Address:	FC:F5:28:E2:06:A0
Firmware Version:	V2.00(AAJC.0)b1
DSL Version:	FwVer:3.20.3.0_A_TC3087 HwVer:T14.F7_11.2
WAN Information:	
- DSL Mode:	N/A
- Annex Type:	ANNEX A
- IPv6/IPv4 Dual Stack:	DualStack
- IP Address:	0.0.0.0
- IP Subnet Mask:	N/A
- Default Gateway:	0.0.0.0
- Primary DNS:	0.0.0.0
- Secondary DNS:	0.0.0.0
- IPv6 Global IP:	::
- IPv6 Prefix Length:	0
- IPv6 Gateway:	::
- IPv6 WAN DNS1:	::
- IPv6 WAN DNS2:	::
- Link-Local Address:	::
- IPv4/IPv6 MTU:	::
- VPI/VCI:	0 / 33
LAN Information:	
- IP Address:	192.168.1.153
- IP Subnet Mask:	255.255.255.0
- DHCP:	None
- IPv6 Address:	::
- Link-local IPv6 Address:	fe80::1
- IPv6 Prefix:	0

Interface Status		
Interface	Status	Rate
ADSL WAN	Down	N/A
LAN1	Down	N/A
LAN2	Down	N/A
LAN3	Up	100 Mbps/Full Duplex
LAN4	Down	N/A
WLAN	Active	300M

System Status	
DSL Up Time:	N/A
System Up Time:	2 days: 17 hours: 3 minutes
Current Date/Time:	Sun Jan 3 17:03:04 UTC 2010
PPPoE Up Time:	0
System Resource:	
- CPU Usage:	2%
- Memory Usage:	52%
- DSL Down Bandwith Usage:	0%
- DSL Up Bandwith Usage:	0%

Each field is described in the following table.

Table 10 System Info Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the AMG1302/AMG1202-TSeries to update this screen from the drop-down list box.
Device Information	
Host Name	This field displays the AMG1302/AMG1202-TSeries system name. It is used for identification.
Model Name	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your AMG1302/AMG1202-TSeries.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Go to the Maintenance > Firmware Upgrade screen to change it.
DSL Version	This is the current version of the AMG1302/AMG1202-TSeries's DSL modem code.
WAN Information	
DSL Mode	This is the method of encapsulation used by your ISP.
Annex Type	This is the ADSL Annex Type that your AMG1302/AMG1202-TSeries is using.
IP Address	This field displays the current IP address of the AMG1302/AMG1202-TSeries in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
Default Gateway	This is the IP address of the default gateway, if applicable.
Primary/Secondary DNS	This is the primary/secondary DNS server IP address assigned to the AMG1302/AMG1202-TSeries.
IPv6 Global IP	This is the current IPv6 address of the AMG1302/AMG1202-TSeries in the WAN. Click this to go to the screen where you can change it.
IPv6 Prefix Length	This is the current IPv6 prefix length in the WAN.
IPv6 Gateway	This is the IPv6 address of the default gateway, if applicable.
IPv6 WAN DNS1/2	This is the primary/secondary DNS server IPv6 address assigned to the AMG1302/AMG1202-TSeries.
Link-Local Address	This is the link local address assigned to the AMG1302/AMG1202-TSeries within the LAN.
IPv4/IPv6 MTU	This is the MTU (Maximum Transmission Unit) for IPv4 and IPv6 packets passing through the WAN interface.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the Network Setting > Broadband > Internet Connection screen.
LAN Information	
IP Address	This field displays the current IP address of the AMG1302/AMG1202-TSeries in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
IPv6 Address	This is the current IPv6 address of the AMG1302/AMG1202-TSeries in the LAN. Click this to go to the screen where you can change it.
IPv6 Prefix Length	This is the current IPv6 prefix length in the LAN.
IPv6 Prefix	This is the current IPv6 prefix in the LAN.
IPv6 Global IP	This is the current global IPv6 address of the AMG1302/AMG1202-TSeries.

LABEL	DESCRIPTION
DHCP	<p>This field displays what DHCP services the AMG1302/AMG1202-TSeries is providing to the LAN. Choices are:</p> <p>Server - The AMG1302/AMG1202-TSeries is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p>Relay - The AMG1302/AMG1202-TSeries acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.</p> <p>None - The AMG1302/AMG1202-TSeries is not providing any DHCP services to the LAN.</p>
IPv6 LAN DNS1/2	This is the first/second DNS server IPv6 address the AMG1302/AMG1202-TSeries passes to the DHCP clients.
WLAN Information	
Status	This displays whether wireless LAN is turned on or off.
SSID	This is the descriptive name used to identify the AMG1302/AMG1202-TSeries in the wireless LAN.
Channel	This is the channel number used by the AMG1302/AMG1202-TSeries now.
Security Mode	This displays the type of security the AMG1302/AMG1202-TSeries is using in the wireless LAN.
WPS	Configured displays when the WPS security settings have been configured and wireless clients can connect with the device through WPS. Unconfigured displays when the device has not been configured and wireless clients can't establish a link with the device through WPS.
Scheduling	This displays whether WLAN scheduling is activated.
WiFi MAC	This is the MAC (Media Access Control) of the WiFi interface.
Security	
Firewall	This displays whether or not the AMG1302/AMG1202-TSeries's firewall is activated. Click this to go to the screen where you can change it.
Interface Status	
Interface	This column displays each interface the AMG1302/AMG1202-TSeries has.
Status	<p>This field indicates whether or not the AMG1302/AMG1202-TSeries is using the interface.</p> <p>For the DSL interface, this field displays Down (line is down), Up (line is up or connected), Initializing (line is initializing), Establishing Link (line is establishing a link) if you're using Ethernet encapsulation and Down (line is down), Up (line is up or connected), Idle (line ppp idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE encapsulation.</p> <p>For the LAN interface, this field displays Up when the AMG1302/AMG1202-TSeries is connected through an Ethernet cable to a computer or a HUB. It displays Down when the AMG1302/AMG1202-TSeries's Ethernet port is disconnected.</p> <p>For the WLAN interface, it displays Active when WLAN is enabled or InActive when WLAN is disabled.</p>
Rate	<p>For the LAN interface, this displays the port speed.</p> <p>For the WAN interface, this displays the DSL link rate downstream and upstream.</p> <p>For the DSL interface, it displays the downstream and upstream transmission rate.</p> <p>For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or N/A when WLAN is disabled.</p>
System Status	
DSL Up Time	This field displays how long the DSL connection has been active.

LABEL	DESCRIPTION
System Up Time	This field displays how long the AMG1302/AMG1202-TSeries has been running since it last started up. The AMG1302/AMG1202-TSeries starts up when you plug it in, when you restart it (Maintenance > Reboot), or when you reset it (see Chapter 1 on page 19).
Current Date/Time	This field displays the current date and time in the AMG1302/AMG1202-TSeries. You can change this in Maintenance > Time Setting .
System Resource	
CPU Usage	This field displays what percentage of the AMG1302/AMG1202-TSeries's processing ability is currently used. When this percentage is close to 100%, the AMG1302/AMG1202-TSeries 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.
Memory Usage	This field displays what percentage of the AMG1302/AMG1202-TSeries's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100% and remains like that for a high period of time, the AMG1302/AMG1202-TSeries may become unstable and you should restart it. See Chapter 24 on page 221 , or turn off the device (unplug the power) for a few seconds.

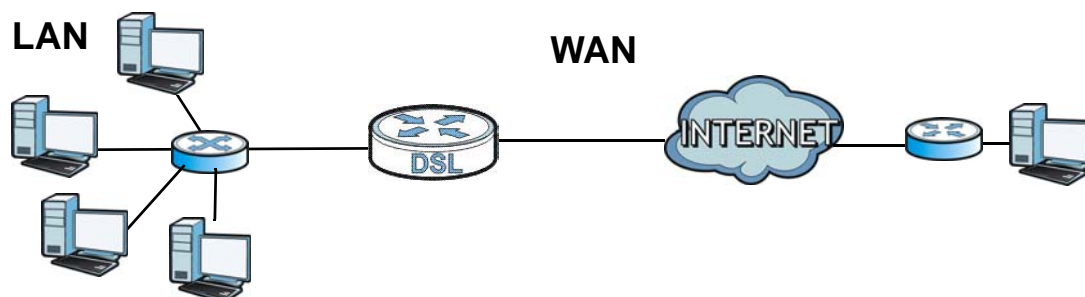
Broadband

6.1 Overview

This chapter describes the AMG1302/AMG1202-TSeries's **Broadband** screens. Use these screens to configure your AMG1302/AMG1202-TSeries 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



6.1.1 What You Can Do in the WAN Screens

- Use the **Internet Connection** screen ([Section 6.2 on page 74](#)) to configure the WAN settings on the AMG1302/AMG1202-TSeries for Internet access.
- Use the **More Connections** screen ([Section 6.3 on page 81](#)) to set up additional Internet access connections.

6.1.2 What You Need to Know About WAN

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) or PPPoA, 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 AMG1302/AMG1202-TSeries, which makes it accessible from an outside network. It is used by the AMG1302/AMG1202-TSeries to communicate with other

devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the AMG1302/AMG1202-TSeries 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) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

Multicast

Traditionally, IP packets are transmitted in one of either 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 one.

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

IPv6

IPv6 (Internet Protocol version 6), is designed to increase IP address space and enhance features. The AMG1302/AMG1202-TSeries supports IPv4/IPv6 dual stack and can connect to IPv4 and IPv6 networks. See ([Appendix E on page 295](#)) for more information about IPv6.

Finding Out More

See [Section 6.4 on page 86](#) for technical background information on WAN.

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 Internet Connection Screen

Use this screen to change your AMG1302/AMG1202-TSeries's WAN settings. Click **Network Setting > Broadband > Internet Connection**. The screen differs by the WAN type and encapsulation you select.

Figure 19 Network Setting > Broadband > Internet Connection > Auto Sync Up

Line	
Type	Auto Sync-Up ▾
General	
Mode	Router ▾
Encapsulation	PPPoA ▾
User Name	ChangeMe
Password	*****
Multiplex	LLC ▾
IPv6/IPv4 Dual Stack:	IPv4/IPv6 ▾
PPP Authentication	Auto ▾
Virtual Circuit ID	
VPI	0 (Range : 0~255)
VCI	33 (Range : 32~65535)
IP Address	
<input checked="" type="radio"/> Obtain an IP Address Automatically	
<input type="radio"/> Static IP Address	
IP Address	0.0.0.0
DNS Server	
Primary DNS	Obtained From ISP ▾ 0.0.0.0
Secondary DNS	Obtained From ISP ▾ 0.0.0.0
IPv6 Address	
<input checked="" type="radio"/> Obtain an IP Address Automatically	
<input type="radio"/> Static IP Address	
DHCP IPv6	<input checked="" type="radio"/> DHCP <input type="radio"/> SLAAC <input type="radio"/> Auto
DHCP PD	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Identifier Type	<input type="radio"/> Manual <input checked="" type="radio"/> EUI64
WAN Identifier	
Connection	
<input checked="" type="radio"/> Keep Alive	
<input type="radio"/> Connect on Demand	
Max Idle Time	0 Sec
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Advanced Setup"/>	

Figure 20 Network Setting > Broadband > Internet Connection > Ethernet(ETH1)

Line

Type Ethernet(ETH1) ▼

General

Mode Router ▼

Encapsulation PPPoE ▼

User Name ChangeMe

Password *****

Service Name

IPv6/IPv4 Dual Stack: IPv4/IPv6 ▼

PPP Authentication Auto ▼

Enable VLAN

802.1Q VLAN ID [5-4094]

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

DNS Server

Primary DNS Obtained From ISP ▼ 0.0.0.0

Secondary DNS Obtained From ISP ▼ 0.0.0.0

IPv6 Address

Obtain an IP Address Automatically

Static IP Address

DHCP IPv6 DHCP SLAAC Auto

DHCP PD Enable Disable

WAN Identifier Type Manual EUI64

WAN Identifier

Connection

Keep Alive

Connect on Demand Max Idle Time Sec

The following table describes the labels in this screen.

Table 11 Network Setting > Broadband > Internet Connection

LABEL	DESCRIPTION
Line	
Type	<p>Select the DSL mode supported by your ISP.</p> <p>Use Auto Sync-Up if you are not sure which mode to choose from. The AMG1302/AMG1202-TSeries dynamically diagnoses the mode supported by the ISP and selects the best compatible one for your connection.</p> <p>Other options are ADSL2+, ADSL2, G.DMT, T1.413 and G.lite.</p> <p>The P-1302-T10B device supports Ethernet (ETH1) mode. To select this mode, connect a modem or router to the WAN port and select Ethernet (ETH1).</p> <p>Note: The ZyXEL Device reboots when transferring to and from Ethernet (ETH1) type.</p>
General	
Mode	<p>Select Router (default) from the drop-down list box if your ISP gives you one IP address only and you want multiple computers to share an Internet account. 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 Firewall, DHCP server and NAT on the AMG1302/AMG1202-TSeries.</p>
Encapsulation	<p>Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field.</p> <p>If you select Router in the Mode field, select PPPoA, RFC 1483, ENET ENCAP or PPPoE.</p> <p>If you select Bridge in the Mode field, method of encapsulation is not available.</p>
User Name	<p>(PPPoA and PPPoE encapsulation only) 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>
Password	<p>(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.</p>
Service Name	<p>(PPPoE only) Type the name of your PPPoE service here.</p>
Multiplex	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC.</p>
IPv6/IPv4 Dual Stack	<p>If you select Enable, the AMG1302/AMG1202-TSeries can connect to IPv4 and IPv6 networks and choose the protocol for applications according to the address type. If you select Disable, the AMG1302/AMG1202-TSeries will operate in IPv4 mode.</p>
PPP Authentication	<p>The AMG1302/AMG1202-TSeries supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.</p> <p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p>AUTO - Your AMG1302/AMG1202-TSeries accepts either CHAP or PAP when requested by this remote node.</p> <p>CHAP - Your AMG1302/AMG1202-TSeries accepts CHAP only.</p> <p>PAP - Your AMG1302/AMG1202-TSeries accepts PAP only.</p>
Virtual Circuit ID	<p>VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.</p>
VPI	<p>This option is available if you select Router in the Mode field.</p> <p>The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.</p>

Table 11 Network Setting > Broadband > Internet Connection (continued)

LABEL	DESCRIPTION
VCI	This option is available if you select Router in the Mode field. 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.
Enable VLAN	This option is available if you select Ethernet(ETH1) in the Line->Type field. The AMG1302/AMG1202-TSeries supports Ether WAN function: DSL users must connect an RJ11 cable to the DSL port (Default), while EtherWAN users must connect an RJ45 cable into LAN port 1.
802.1Q VLAN ID	The valid range for the VLAN ID (as assigned by your provider) is 5 to 4094.
IP Address	
Obtain an IP Address Automatically	This option is available if you select Router in the Mode field. 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 Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field and a gateway IP address (supplied by your ISP) below.
DNS Server - This section is not available when you select Bridge in the Mode field.	
Obtain DNS info Automatically	Select this to have the AMG1302/AMG1202-TSeries get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the AMG1302/AMG1202-TSeries 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.
IPv6 Address	
Obtain an IP Address Automatically	Select this option if you want to have the AMG1302/AMG1202-TSeries use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
DHCP IPv6	Select DHCP 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 AMG1302/AMG1202-TSeries using the IPv6 prefix from an RA. Select SLAAC (Stateless address autoconfiguration) to have the AMG1302/AMG1202-TSeries use the prefix to automatically generate a unique IP address that does not need to be maintained by a DHCP server. Select Auto to have the AMG1302/AMG1202-TSeries indicate to hosts for IPv6 address generation depending on the M/O (Managed/Other) flag values in the router advertisements sending to hosts. <ul style="list-style-type: none"> • If M flag is 1, the AMG1302/AMG1202-TSeries will indicate to hosts to obtain network settings (such as WAN IP, LAN prefix and DNS settings) through DHCPv6. • If M flag is 0, the AMG1302/AMG1202-TSeries will check O flag. • If O flag is 1, the AMG1302/AMG1202-TSeries will indicate to hosts to obtain DNS information and LAN prefix through DHCPv6. • If O flag is 0, the AMG1302/AMG1202-TSeries will not get information through DHCPv6.
DHCP PD	Select Enable to use DHCP PD (Prefix Delegation) to allow the AMG1302/AMG1202-TSeries to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses.

Table 11 Network Setting > Broadband > Internet Connection (continued)

LABEL	DESCRIPTION
WAN Identifier Type	Select Manual to manually enter a WAN Identifier as the interface ID to identify the WAN interface. The WAN Identifier is appended to the IPv6 address prefix to create the routable global IPv6 address. Select EUI 64 to use the EUI-64 format to generate an interface ID from the MAC address of the WAN interface.
WAN Identifier	If you selected Manual , enter the WAN Identifier in this field. The WAN identifier should be unique and 64 bits in hexadecimal form. Every 16 bit block should be separated by a colon as in XXXX:XXXX:XXXX:XXXX where X is a hexadecimal character. Blocks of zeros can be represented with double colons as in XXXX:XXXX::XXXX.
Connection (PPPoA and PPPoE encapsulation only)	
Keep Alive	Select Keep Alive when you want your connection up all the time. The AMG1302/AMG1202-TSeries will try to bring up the connection automatically if it is disconnected.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the Advanced WAN Setup screen and edit more details of your WAN setup. Click this button again to display less fields in this screen.

6.2.1 Advanced Setup

Use this screen to edit your AMG1302/AMG1202-TSeries's advanced WAN settings. Click the **Advanced Setup** button in the **Internet Connection** screen. The screen appears as shown.

Figure 21 Network Setting > Broadband > Internet Connection: Advanced Setup

RIP & Multicast Setup

RIP Direction:

RIP Version:

Multicast:

MLD Proxy:

ATM QoS

ATM QoS Type:

Peak Cell Rate: cell/sec

Sustain Cell Rate: cell/sec

Maximum Burst Size: cell

PPPoE Passthrough:

MTU

MTU:

The following table describes the labels in this screen.















Table 12 Network Setting > Broadband > Internet Connection: Advanced Setup















LABEL	DESCRIPTION
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Use this field to control how much routing information the AMG1302/AMG1202-TSeries sends and receives on the subnet.</p> <p>Select the RIP direction from None, Both, In Only and Out Only.</p>
RIP Version	<p>This field is not configurable if you select None in the RIP Direction field.</p> <p>Select the RIP version from RIP-1, RIP2-B and RIP2-M.</p>
Multicast	<p>Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).</p> <p>Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group. The AMG1302/AMG1202-TSeries supports IGMP-v1, IGMP-v2 and IGMP-v3. Select None to disable it.</p>
MLD Proxy	<p>Select the version of MLD proxy (v1 or v2) to have the AMG1302/AMG1202-TSeries act as for this connection. This allows the AMG1302/AMG1202-TSeries to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly. Select None to turn off MLD proxy.</p>
ATM QoS	
ATM QoS Type	<p>Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR With PCR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select Realtime VBR (real-time Variable Bit Rate) type for applications with bursty connections that require closely controlled delay and delay variation. Select Non Realtime VBR (non real-time Variable Bit Rate) type for connections that do not 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.</p>
Sustain Cell Rate	<p>The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.</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>
PPPoE Passthrough	<p>If encapsulation type is PPPoE, select this to enable PPPoE Passthrough. In addition to the Device's built-in PPPoE client, you can select this to allow 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>
MTU	
MTU	<p>The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.</p> <p>For ENET ENCAP, the MTU value is 1500.</p> <p>For PPPoE, the MTU value is 1492.</p> <p>For PPPoA and RFC 1483, the MTU is 65535.</p>

6.3 The More Connections Screen

The AMG1302/AMG1202-TSeries allows you to configure more than one Internet access connection. To configure additional Internet access connections click **Network Setting > Broadband > More Connections**. The screen differs by the encapsulation you select. When you use the **Broadband > Internet Connection** screen to set up Internet access, you are configuring the first WAN connection.

Figure 22 Network Setting > Broadband > More Connections

#	Active	Node Name	VPI/VCI	Encapsulation	Modify
1	<input checked="" type="checkbox"/>	Wan_PVC0	0/33	PPPoA LLC	
2	<input type="checkbox"/>	N/A	--/--	--	 
3	<input type="checkbox"/>	N/A	--/--	--	 
4	<input type="checkbox"/>	N/A	--/--	--	 
5	<input type="checkbox"/>	N/A	--/--	--	 
6	<input type="checkbox"/>	N/A	--/--	--	 
7	<input type="checkbox"/>	N/A	--/--	--	 
8	<input type="checkbox"/>	N/A	--/--	--	 

Ethernet Connections Table					
#	Active	Node Name	VID	Encapsulation	Modify
1	<input checked="" type="checkbox"/>	Ethernet_WAN0	--	PPPoE	
2	<input type="checkbox"/>	N/A	--	--	 
3	<input type="checkbox"/>	N/A	--	--	 
4	<input type="checkbox"/>	N/A	--	--	 
5	<input type="checkbox"/>	N/A	--	--	 
6	<input type="checkbox"/>	N/A	--	--	 
7	<input type="checkbox"/>	N/A	--	--	 
8	<input type="checkbox"/>	N/A	--	--	 

The following table describes the labels in this screen.

Table 13 Network Setting > Broadband > More Connections

LABEL	DESCRIPTION
ADSL Connections Table	
#	This is an index number indicating the number of the corresponding connection.
Active	This field indicates whether the connection is active or not. Clear the check box to disable the connection. Select the check box to enable it.
Node Name	This is the name you gave to the Internet connection.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	The first (ISP) connection is read-only in this screen. Use the Broadband > Internet Connection screen to edit it. Click the Edit icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup. Click the Remove icon to delete the Internet access setup from your connection list.
Ethernet Connections Table	

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

LABEL	DESCRIPTION
#	This is an index number indicating the number of the corresponding connection.
Active	This field indicates whether the connection is active or not. Clear the check box to disable the connection. Select the check box to enable it.
Node Name	This is the name you gave to the Internet connection.
VID	This field displays the VLAN ID number used by this connection.
Encapsulation	This field indicates the encapsulation method of the Internet connection.
Modify	The first (ISP) connection is read-only in this screen. Use the Broadband > Internet Connection screen to edit it. Click the Edit icon to edit the Internet connection settings. Click this icon on an empty configuration to add a new Internet access setup. Click the Remove icon to delete the Internet access setup from your connection list.

6.3.1 More Connections Edit

Use this screen to configure a connection. Click the edit icon in the **More Connections** screen to display the following screen.

Figure 23 Network Setting > Broadband > More Connections: Edit

General

Active

Node Name

Mode

Encapsulation

Multiplex

IPv6/IPv4 Dual Stack

VPI (Range : 0-255)

VCI (Range : 32-65535)

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Subnet Mask

Gateway IP Address

Primary DNS

Secondary DNS

NAT

None

SUA Only

Advanced Setup ▲

RIP & Multicast Setup

RIP Direction

RIP Version

Multicast

ATM QoS

ATM QoS Type

Peak Cell Rate cell/sec

Sustain Cell Rate cell/sec

Maximum Burst Size cell

MTU

MTU

The following table describes the labels in this screen.

Table 14 Network Setting > Broadband > More Connections: Edit

LABEL	DESCRIPTION
General	
Active	Select the check box to activate or clear the check box to deactivate this connection.

Table 14 Network Setting > Broadband > More Connections: Edit (continued)

LABEL	DESCRIPTION
Node Name	Enter a unique, descriptive name of up to 13 ASCII characters for this connection.
Mode	<p>Select Router from the drop-down list box if your ISP allows multiple computers to share an Internet account.</p> <p>If you select Bridge, the AMG1302/AMG1202-TSeries will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.</p>
Encapsulation	<p>Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field.</p> <p>If you select Router in the Mode field, select PPPoA, RFC 1483, ENET ENCAP or PPPoE.</p> <p>If you select Bridge in the Mode field, method of encapsulation is not available.</p>
Multiplex	<p>Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC.</p> <p>By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol.</p> <p>For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.</p>
IPv6/IPv4 Dual Stack	If you select Enable , the AMG1302/AMG1202-TSeries can connect to IPv4 and IPv6 networks and choose the protocol for applications according to the address type. If you select Disable , the AMG1302/AMG1202-TSeries will operate in IPv4 mode.
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.
IP Address	<p>This option is available if you select Router in the Mode field.</p> <p>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.</p> <p>If you use the encapsulation type except RFC 1483, select Obtain an IP Address Automatically when you have a dynamic IP address; otherwise select Static IP Address and type your ISP assigned IP address in the IP Address field below.</p> <p>If you use RFC 1483, enter the IP address given by your ISP in the IP Address field.</p>
Subnet Mask	Enter a subnet mask in dotted decimal notation.
Gateway IP Address	Specify a gateway IP address (supplied by your ISP).
Primary DNS	Enter the primary DNS server's address for the AMG1302/AMG1202-TSeries.
Secondary DNS	Enter the secondary DNS server's address for the AMG1302/AMG1202-TSeries.
NAT	<p>SUA Only is available only when you select Router in the Mode field.</p> <p>Select SUA Only if you have one public IP address and want to use NAT. Otherwise, select None to disable NAT.</p>
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.
Advanced Setup	Click this to display more fields in this screen to configure more details of your WAN settings.

6.3.2 Configuring More Connections Advanced Setup

Use this screen to edit your AMG1302/AMG1202-TSeries's advanced WAN settings. Click the **Advanced Setup** arrow icon in the **More Connections Edit** screen. The screen appears as shown.

Figure 24 Network Setting > Broadband > More Connections: Edit: Advanced Setup

Advanced Setup ▲

RIP & Multicast Setup

RIP Direction: Both

RIP Version: RIP1

Multicast: None

ATM QoS

ATM QoS Type: UBR With PCR

Peak Cell Rate: 0 cell/sec

Sustain Cell Rate: 0 cell/sec

Maximum Burst Size: 0 cell

MTU

MTU: 1500

Apply Cancel

The following table describes the labels in this screen.

Table 15 Network Setting > Broadband > More Connections: Edit: Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	Select the RIP Direction from None , Both , In Only and Out Only .
RIP Version	This field is not configurable if you select None in the RIP Direction field. Select the RIP Version from RIP-1 , RIP2-B and RIP2-M .
Multicast	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group. The AMG1302/AMG1202-TSeries supports IGMP-v1 , IGMP-v2 and IGMP-v3 . Select None to disable it.
ATM QoS	
ATM QoS Type	Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select nrtVBR (Variable Bit Rate-non Real Time) or rtVBR (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
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.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	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.
MTU	

Table 15 Network Setting > Broadband > More Connections: Edit: Advanced Setup (continued)

LABEL	DESCRIPTION
MTU	<p>The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.</p> <p>For ENET ENCAP, the MTU value is 1500.</p> <p>For PPPoE, the MTU value is 1492.</p> <p>For PPPoA and RFC, the MTU is 100-1500.</p>
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

6.4 WAN Technical Reference

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

6.4.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The AMG1302/AMG1202-TSeries supports the following methods.

6.4.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. 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. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Gateway IP Address** field in the wizard or WAN screen. You can get this information from your ISP.

6.4.1.2 PPP over Ethernet

The AMG1302/AMG1202-TSeries supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.

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 AMG1302/AMG1202-TSeries (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the AMG1302/

AMG1202-TSeries does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

6.4.1.3 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 AMG1302/AMG1202-TSeries 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 Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

6.4.1.4 RFC 1483

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

6.4.2 Multiplexing

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

VC-based Multiplexing

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

LLC-based Multiplexing

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

6.4.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

6.4.4 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 ENET ENCAP gateway.

IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a **Static IP Address** assigned by your ISP, then they should also assign you a **Subnet Mask** and a **Gateway IP Address**.

IP Assignment with RFC 1483 Encapsulation

In this case the IP address assignment must be static.

IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **Gateway IP Address** fields as supplied by your ISP. However for a dynamic IP, the AMG1302/AMG1202-TSeries acts as a DHCP client on the WAN port and so the **IP Address** and **Gateway IP Address** fields are not applicable (N/A) as the DHCP server assigns them to the AMG1302/AMG1202-TSeries.

6.4.5 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The AMG1302/AMG1202-TSeries does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the AMG1302/AMG1202-TSeries will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

6.4.6 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

6.5 Traffic Shaping

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

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

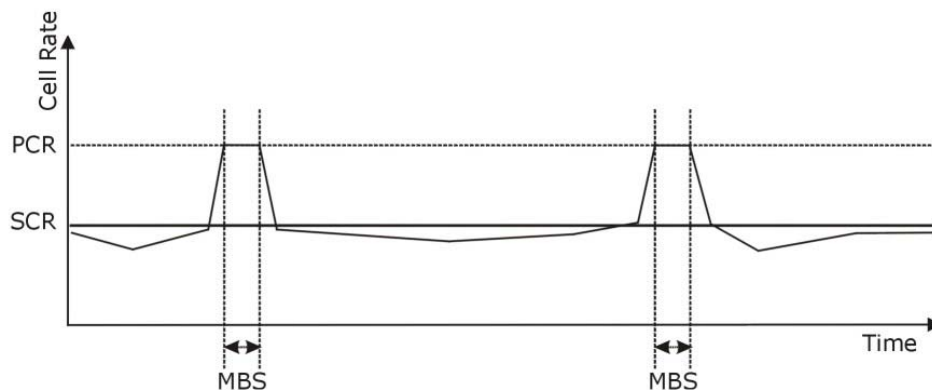
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

Figure 25 Example of Traffic Shaping



6.5.1 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 a 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.

Wireless LAN

7.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Setting up multiple wireless networks.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.
- Performing other performance-related wireless tasks.

7.1.1 What You Can Do in the Wireless LAN Screens

This section describes the AMG1302/AMG1202-TSeries's **Network Setting > Wireless** screens. Use these screens to set up your AMG1302/AMG1202-TSeries'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 92](#)).
- Use the **More AP** screen (see [Section 7.3 on page 98](#)) to set up multiple wireless networks on your AMG1302/AMG1202-TSeries.
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the AMG1302/AMG1202-TSeries ([Section 7.4 on page 100](#)).
- Use the **WPS** screen (see [Section 7.5 on page 101](#)) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the AMG1302/AMG1202-TSeries's WPS status.
- Use the **WDS** screen (see [Section 7.6 on page 103](#)) to set up a Wireless Distribution System, in which the AMG1302/AMG1202-TSeries acts as a bridge with other ZyXEL access points.
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications ([Section 7.7 on page 104](#)).
- Use the **Scheduling** screen (see [Section 7.8 on page 105](#)) to configure the dates/times to enable or disable the wireless LAN.
- Use the **Advanced** screen to configure wireless advanced features ([Section 7.9 on page 106](#)).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and security in the **General** screen.

7.1.2 What You Need to Know About Wireless

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

7.1.3 Before You Start

Before you start using these screens, ask yourself the following questions. See [Section 7.1.2 on page 92](#) if some of the terms used here are not familiar to you.

- What wireless standards do the other wireless devices in your network support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices in your network support (WPA-PSK, for example)? What is the strongest security option supported by all the devices in your network?
- Do the other wireless devices in your network support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.

- What advanced options do you want to configure, if any? If you want to configure advanced options such as Quality of Service, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them as they are.

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 AMG1302/AMG1202-TSeries from a computer connected to the wireless LAN and you change the AMG1302/AMG1202-TSeries'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 AMG1302/AMG1202-TSeries's new settings.

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

Figure 26 Network Setting > Wireless > General

Wireless Network Setup

Wireless Enable Wireless LAN

Wireless Network Settings

Wireless Network Name(SSID):

Hide SSID

Client Isolation

MBSSID/LAN Isolation

Channel Selection :

Operating Channel 6

Security Level

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

Security Mode :

Enter 8-63 characters or 64 hexadecimal digits (a-f, A-F, and 0-9).

Pre-Shared Key [more...](#)

The following table describes the labels in this screen.

Table 16 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select Enable Wireless LAN to activate wireless LAN.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other through the AMG1302/AMG1202-TSeries.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or wired LAN devices through the AMG1302/AMG1202-TSeries. Select both Client Isolation and MBSSID/LAN Isolation to allow this SSID's wireless clients to only connect to the Internet through the AMG1302/AMG1202-TSeries.
Channel Selection	Set the operating channel manually by selecting a channel from the Channel Selection list or use Auto to have it automatically determine a channel to use.
Operating Channel	This field displays the channel the AMG1302/AMG1202-TSeries is currently using.
Security Level	

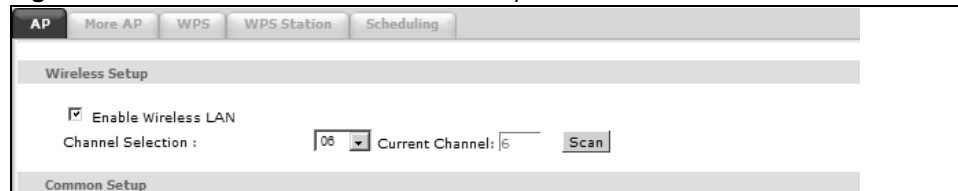
Table 16 Network Setting > Wireless > General

LABEL	DESCRIPTION
Security Mode	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 AMG1302/AMG1202-TSeries. When you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Apply	Click this to save your changes.
Cancel	Click this 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 AMG1302/AMG1202-TSeries, your network is accessible to any wireless networking device that is within range.

Figure 27 Wireless > General: No Security

7.2.2 Basic (WEP Encryption)

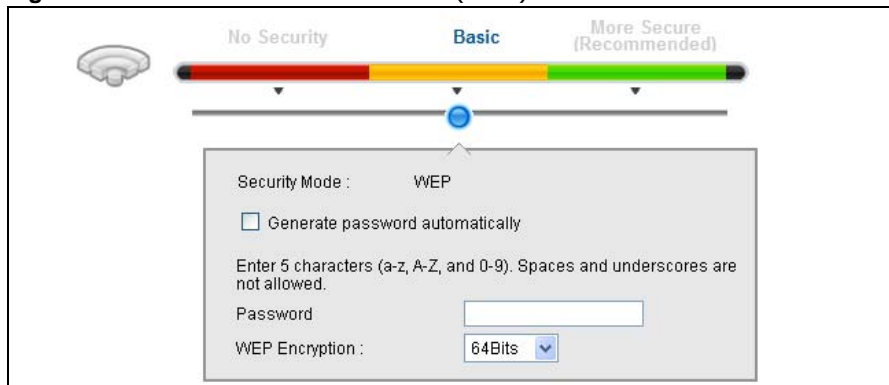
WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

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 AMG1302/AMG1202-TSeries allows you to configure one 64-bit or 128-bit WEP key.

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 28 Wireless > General: Basic (WEP)



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

Table 17 Wireless > General: Basic (WEP)

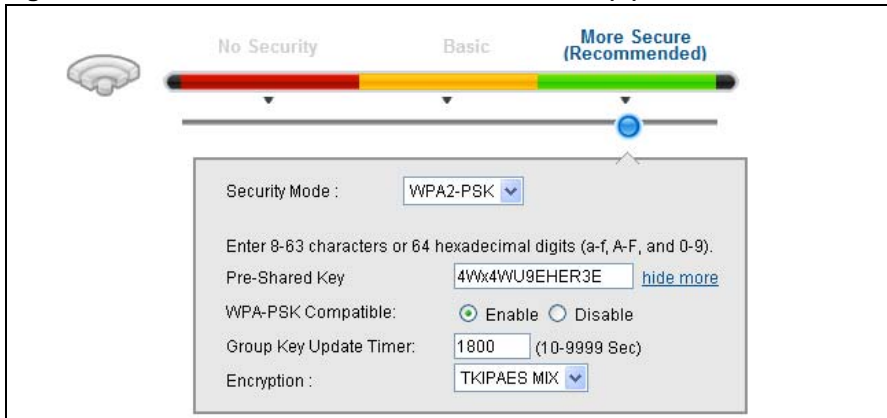
LABEL	DESCRIPTION
Security Level	Select Basic to enable WEP data encryption.
Generate password automatically	Select this option to have the AMG1302/AMG1202-TSeries automatically generate a password. The password field will not be configurable when you select this option.
Password	The password (WEP key) are used to encrypt data. Both the AMG1302/AMG1202-TSeries 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").
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 AMG1302/AMG1202-TSeries 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 29 Wireless > General: More Secure: WPA(2)-PSK



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

Table 18 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.
Pre-Shared Key	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. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
more.../hide more	Click more... to show more fields in this section. Click hide more to hide them.
WPA-PSK Compatible	This field appears when you choose WPA-PSK2 as the Security Mode . Select Enable to allow wireless devices using WPA-PSK security mode to connect to your AMG1302/AMG1202-TSeries. The AMG1302/AMG1202-TSeries supports WPA-PSK and WPA2-PSK simultaneously. Otherwise, select Disable .
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.
Encryption	This field displays the encryption type for data encryption. If you choose WPA-PSK as the security mode, the AMG1302/AMG1202-TSeries uses TKIP for data encryption. If you choose WPA2-PSK as the security mode and enable WPA-PSK Compatible, the AMG1302/AMG1202-TSeries uses either TKIP and AES (TKIPAES MIX) for data encryption. If you choose WPA2-PSK as the security mode but disable WPA-PSK Compatible, the AMG1302/AMG1202-TSeries uses AES for data encryption.

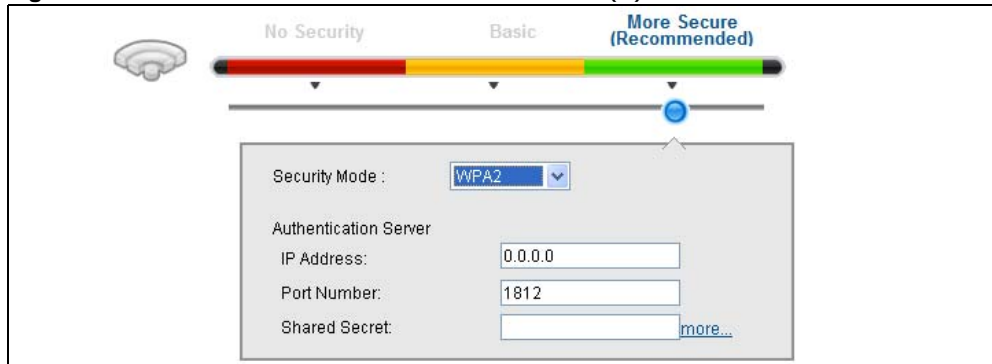
7.2.4 WPA(2) Authentication

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 30 Wireless > General: More Secure: WPA(2)



The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
Security Level	Select More Secure to enable WPA(2) 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.
Port Number	Enter the port number of the external authentication server. 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 AMG1302/AMG1202-TSeries. The key must be the same on the external authentication server and your AMG1302/AMG1202-TSeries. The key is not sent over the network.
more.../hide more	Click more... to show more fields in this section. Click hide more to hide them.
ReAuthentication Timer	Enter how often the external authentication server requires a connected wireless client to reauthenticate itself to the server again.
Network Re-auth Interval	Specify how often wireless stations have to resend user names and passwords in order to stay connected. This field is available only when you select WPA2 as security mode. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
WPA Compatible	This field is only available for WPA2. Select this if you want the AMG1302/AMG1202-TSeries to support WPA and WPA2 simultaneously.

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

LABEL	DESCRIPTION
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.
Encryption	Select the encryption type for data encryption. If you choose WPA as the security mode, the AMG1302/AMG1202-TSeries uses TKIP for data encryption. If you choose WPA2 as the security mode and enable WPA-PSK Compatible, the AMG1302/AMG1202-TSeries uses either TKIP and AES (TKIPAES MIX) for data encryption. If you choose WPA2 as the security mode but disable WPA-PSK Compatible, the AMG1302/AMG1202-TSeries uses AES for data encryption.

7.3 The More AP Screen

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the AMG1302/AMG1202-TSeries.

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

Figure 31 Network Setting > Wireless > More AP

#	Active	SSID	Security	Modify
1		N/A	N/A	
2		N/A	N/A	
3		N/A	N/A	

The following table describes the labels in this screen.

Table 20 Network Setting > Wireless > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Active	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 AMG1302/AMG1202-TSeries'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 More AP Edit

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 32 More AP: Edit

The following table describes the fields in this screen.

Table 21 More AP: Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select Enable Wireless LAN to activate wireless LAN.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other through the AMG1302/AMG1202-TSeries.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or wired LAN devices through the AMG1302/AMG1202-TSeries. Select both Client Isolation and MBSSID/LAN Isolation to allow this SSID's wireless clients to only connect to the Internet through the AMG1302/AMG1202-TSeries.
Security Level	

Table 21 More AP: Edit

LABEL	DESCRIPTION
Security Mode	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 AMG1302/AMG1202-TSeries. After you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

7.4 The MAC Authentication Screen

This screen allows you to configure the AMG1302/AMG1202-TSeries to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the AMG1302/AMG1202-TSeries (**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 AMG1302/AMG1202-TSeries's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wireless > MAC Authentication**. The screen appears as shown.

Figure 33 Network Setting > Wireless > MAC Authentication

The following table describes the labels in this screen.

Table 22 Network Setting > Wireless > MAC Authentication

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC List	Define the filter action for the list of MAC addresses in the MAC Address table. Select Disable to turn off MAC filtering. Select Allow to permit access to the AMG1302/AMG1202-TSeries. MAC addresses not listed will be denied access to the AMG1302/AMG1202-TSeries. Select Deny to block access to the AMG1302/AMG1202-TSeries. MAC addresses not listed will be allowed to access the AMG1302/AMG1202-TSeries.

Table 22 Network Setting > Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
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 AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries.
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 AMG1302/AMG1202-TSeries.

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 7.10.8.3 on page 115](#) for more information about WPS.

Note: The AMG1302/AMG1202-TSeries applies the security settings configured in the General screen (see [Section 7.2 on page 92](#)). If you want to use the WPS feature, make sure you have set the security mode to **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 34 Network Setting > Wireless > WPS

General

WPS: Enable Disable (settings are invalid when disabled)

Add a new device with WPS Method

<p> Method 1 PBC</p> <p>Step 1. Click WPS button <input type="button" value="WPS"/></p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>	<p> Method 2 PIN</p> <p>Step 1. Enter the PIN of your new wireless client device and then click Register <input type="button" value="Register"/></p> <p><input type="text"/></p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>
---	--

WPS Configuration Summary

AP PIN: 08186324

Status: Unconfigured

Lock Status: Unlocked

802.11 Mode: 802.11b+g+n

SSID: ZyXEL_7DC8

Security: WPA-PSK/WPA2-PSK

Pre-Shared Key: 4Wx4WU9EHER3E

Note:

- If you enable WPS, it will be turned on UPnP service automatically.
- This feature is available only when WPA2-PSK, WPA-PSK/WPA2-PSK or No Security mode is configured.

The following table describes the labels in this screen.

Table 23 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Select Enable to activate WPS on the AMG1302/AMG1202-TSeries. Otherwise, select Disable to deactivate WPS.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the AMG1302/AMG1202-TSeries) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the WPS button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS wireless network by entering the PIN of the client into the AMG1302/AMG1202-TSeries.

Table 23 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
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 AMG1302/AMG1202-TSeries.
WPS Configuration Summary	
AP PIN	The PIN (Personal Identification Number) of the AMG1302/AMG1202-TSeries is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the Generate New PIN button to have the AMG1302/AMG1202-TSeries create a new PIN.
Status	This displays Configured when the AMG1302/AMG1202-TSeries has connected to a wireless network using WPS or Enable WPS is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays Unconfigured if WPS is disabled and there is no wireless or wireless security changes on the AMG1302/AMG1202-TSeries or you click Release to remove the configured wireless and wireless security settings.
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 AMG1302/AMG1202-TSeries.
802.11 Mode	This field displays the AMG1302/AMG1202-TSeries's wireless mode that only allows the compliant WLAN devices to associate with it.
SSID	This field displays the SSID the AMG1302/AMG1202-TSeries is currently using.
Security	This field displays the security mode the AMG1302/AMG1202-TSeries is currently using.
Pre-Shared Key	This field displays the pre-shared key the AMG1302/AMG1202-TSeries uses when the security mode is set to WPA(2)-PSK.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.6 The WDS Screen

An AP using the Wireless Distribution System (WDS) can function as a wireless network bridge allowing you to wirelessly connect wired network segments. The **WDS** screen allows you to configure the AMG1302/AMG1202-TSeries to connect to other APs wirelessly when WDS is enabled.

Use this screen to set up your WDS (Wireless Distribution System) links between the AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries 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 35 Network Setting > Wireless > WDS

#	Active	Remote Bridge MAC Address	PSK
1	<input type="checkbox"/>	00:00:00:00:00:00	
2	<input type="checkbox"/>	00:00:00:00:00:00	
3	<input type="checkbox"/>	00:00:00:00:00:00	
4	<input type="checkbox"/>	00:00:00:00:00:00	

The following table describes the labels in this screen.

Table 24 Network Setting > Wireless > WDS

LABEL	DESCRIPTION
WDS Security	Select the type of the key used to encrypt data between APs. All the wireless APs (including the AMG1302/AMG1202-TSeries) must use the same pre-shared key for data transmission. The option is available only when you set the security mode to WPA(2) or WPA(2)-PSK in the Wireless > General screen.
TKIP	Select this to use TKIP (Temporal Key Integrity Protocol) encryption.
AES	Select this to use AES (Advanced Encryption Standard) encryption.
#	This is the index number of the individual WDS link.
Active	Select this to activate the link between the AMG1302/AMG1202-TSeries and the peer device to which this entry refers. When you do not select the check box this link is down.
Remote Bridge MAC Address	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).
PSK	Enter a Pre-Shared Key (PSK) from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.7 The WMM Screen

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

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

Figure 36 Network Setting > Wireless > WMM

The following table describes the labels in this screen.

Table 25 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
Enable WMM of SSID1~4	Use the checkboxes to determine whether to have the AMG1302/AMG1202-TSeries automatically give a service a priority level according to the ToS value in the IP header of packets it sends for a wireless network. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.8 The Scheduling Screen

Use the wireless LAN scheduling to configure the days you want to enable or disable the wireless LAN. Click **Network Setting > Wireless > Scheduling**. The following screen displays.

Figure 37 Network Setting > Wireless > Scheduling

The following table describes the labels in this screen.

Table 26 Network Setting > Wireless > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	Select Enable or Disable to activate or deactivate wireless LAN scheduling on your AMG1302/AMG1202-TSeries.
State	Select On or Off to enable or disable the wireless LAN.
Day	Check the day(s) you want to turn the wireless LAN on or off.

Table 26 Network Setting > Wireless > Scheduling

LABEL	DESCRIPTION
Time (24-Hour Format)	Specify a time frame during which the schedule would apply. For example, if you set the time range from 12:00 to 23:00, the wireless LAN will be turned on only during this time period.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.9 The Advanced Screen

Use this screen to configure advanced wireless settings. Click **Network Setting > Wireless > Advanced**, the screen appears as shown.

See [Section 7.10.2 on page 109](#) for detailed definitions of the terms listed in this screen.

Figure 38 Network Setting > Wireless> Advanced

The following table describes the labels in this screen.

Table 27 Network Setting > Wireless> Advanced

LABEL	DESCRIPTION
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the AMG1302/AMG1202-TSeries. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: 100% , 75% , 50% or 25% .
Preamble	Select a preamble type from the drop-down list menu. Choices are Long or Short . See the Appendix D on page 285 for more information.

Table 27 Network Setting > Wireless> Advanced

LABEL	DESCRIPTION
802.11 Mode	<p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the AMG1302/AMG1202-TSeries.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the AMG1302/AMG1202-TSeries.</p> <p>Select 802.11b+g to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the AMG1302/AMG1202-TSeries. The transmission rate of your AMG1302/AMG1202-TSeries might be reduced.</p> <p>Select 802.11n to allow only IEEE 802.11n compliant WLAN devices to associate with the AMG1302/AMG1202-TSeries.</p> <p>Select 802.11g+n to allow either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the AMG1302/AMG1202-TSeries. The transmission rate of your AMG1302/AMG1202-TSeries might be reduced.</p> <p>Select 802.11b+g+n to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the AMG1302/AMG1202-TSeries. The transmission rate of your AMG1302/AMG1202-TSeries might be reduced.</p>
Channel Width	<p>Select whether the AMG1302/AMG1202-TSeries uses a wireless channel width of 20MHz or Auto. If Auto is selected, the AMG1302/AMG1202-TSeries will use 40MHz if it is supported.</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> <p>This field is available only when you set the 802.11 Mode to 802.11n or 802.11b+g+n in the Advanced Setup screen.</p>
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

7.10 Wireless LAN Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

7.10.1 Wireless Network Overview

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

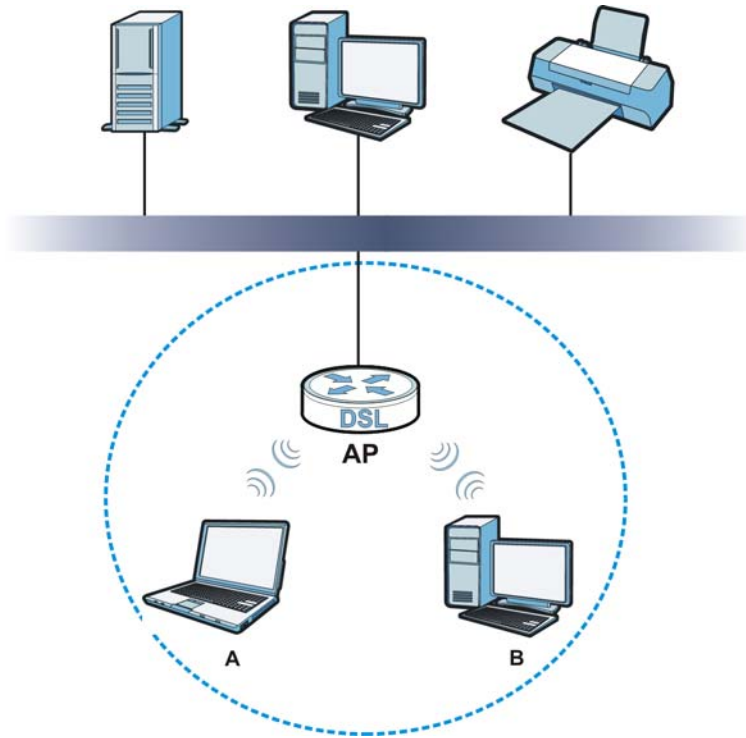
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, 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 39 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 AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries's Web Configurator.

Table 28 Additional Wireless Terms

TERM	DESCRIPTION
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 AMG1302/AMG1202-TSeries does, it cannot communicate with the AMG1302/AMG1202-TSeries.
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 AMG1302/AMG1202-TSeries acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

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

7.10.3.3 User Authentication

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

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

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


-
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.

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 110](#) for information about this.)

Table 29 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 AMG1302/AMG1202-TSeries 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-PSK. 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 AMG1302/AMG1202-TSeries, 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 AMG1302/AMG1202-TSeries.

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.

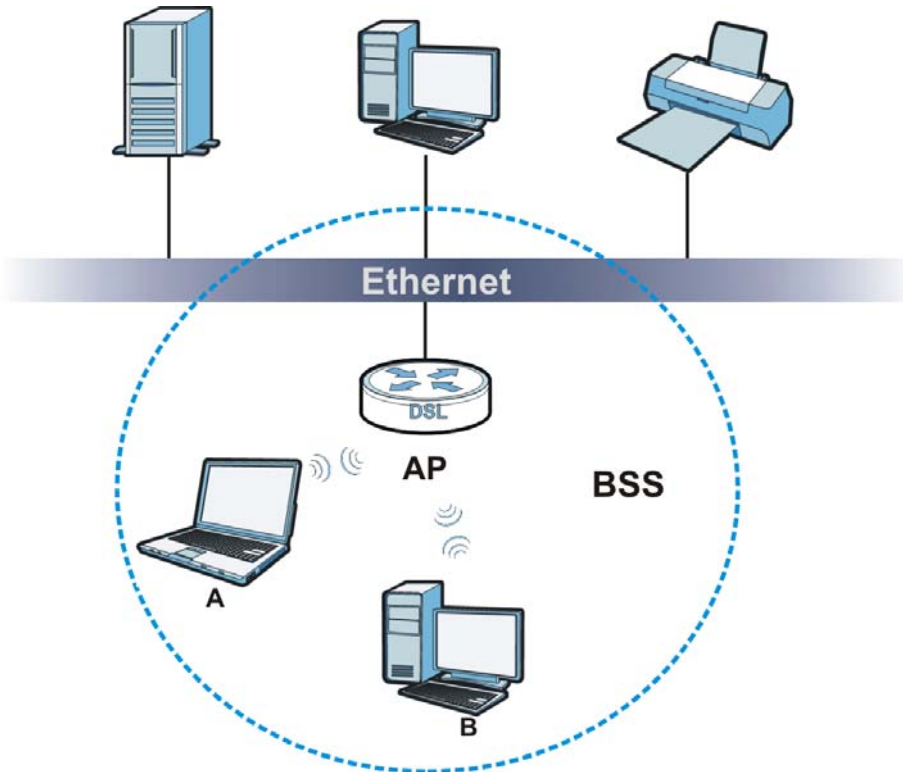
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters 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 40 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 AMG1302/AMG1202-TSeries'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 Wireless Distribution System (WDS)

The AMG1302/AMG1202-TSeries 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 41 WDS Link Example



7.10.8 WiFi Protected Setup (WPS)

Your AMG1302/AMG1202-TSeries supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

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

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

7.10.8.1 Push Button Configuration

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

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

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

- 1 Ensure that the two devices you want to set up are within wireless range of one another.

- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the AMG1302/AMG1202-TSeries, see [Section 7.6 on page 103](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the AMG1302/AMG1202-TSeries 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.

7.10.8.2 PIN Configuration

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

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

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

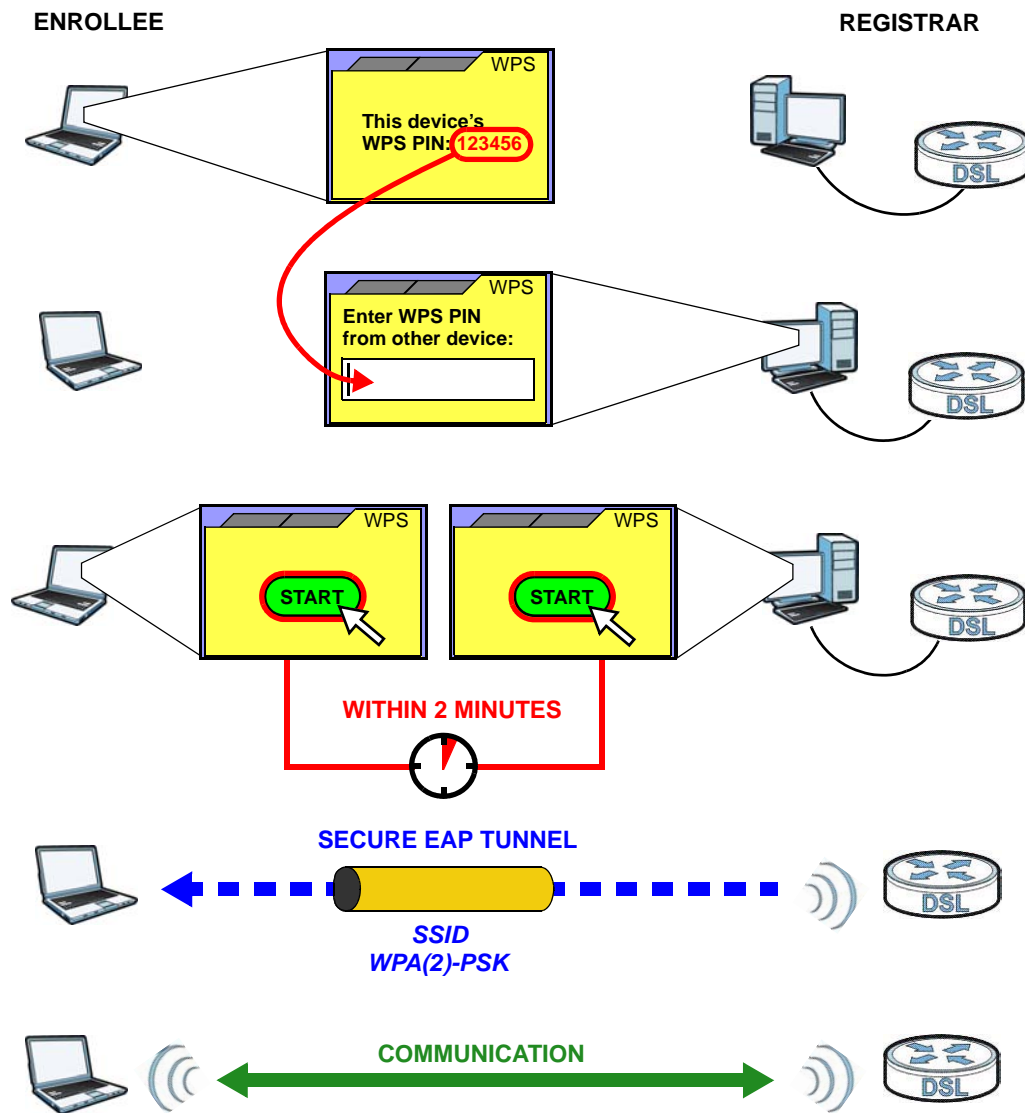
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the AMG1302/AMG1202-TSeries, see [Section 7.5 on page 101](#)).
- 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 42 Example WPS Process: PIN Method

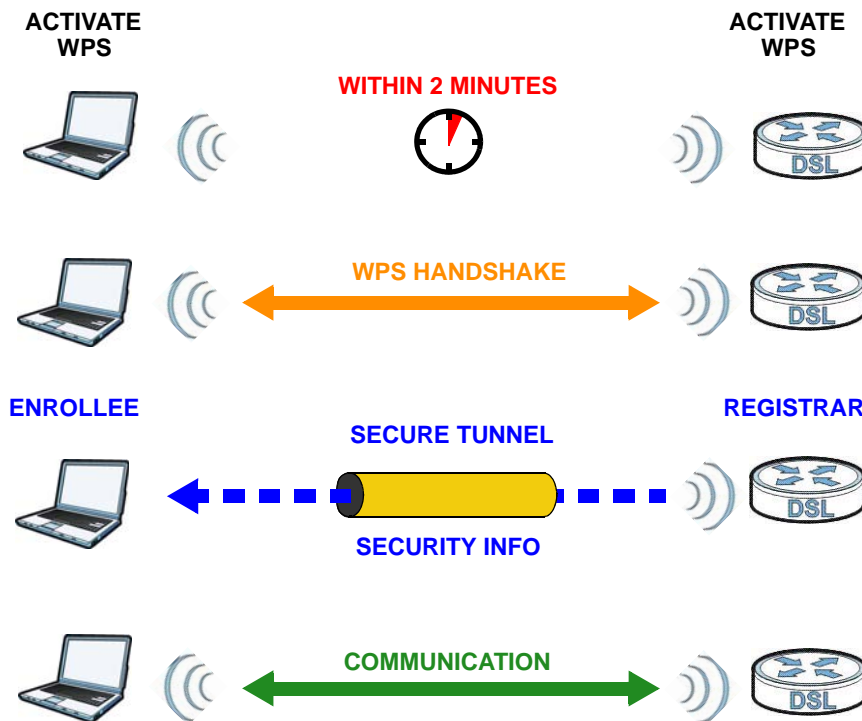


7.10.8.3 How WPS Works

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

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

Figure 43 How WPS works



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

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

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

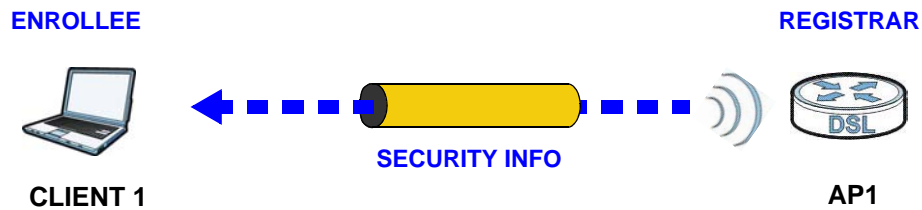
By default, a WPS device is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

7.10.8.4 Example WPS Network Setup

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

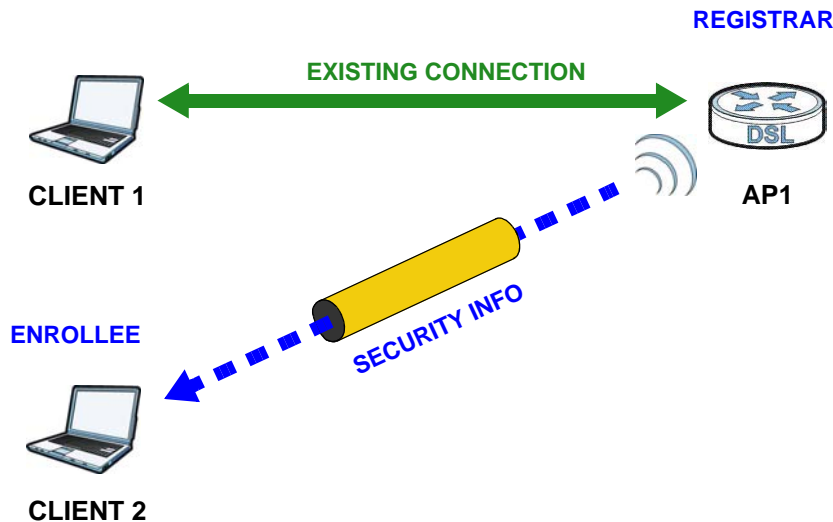
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 44 WPS: Example Network Step 1



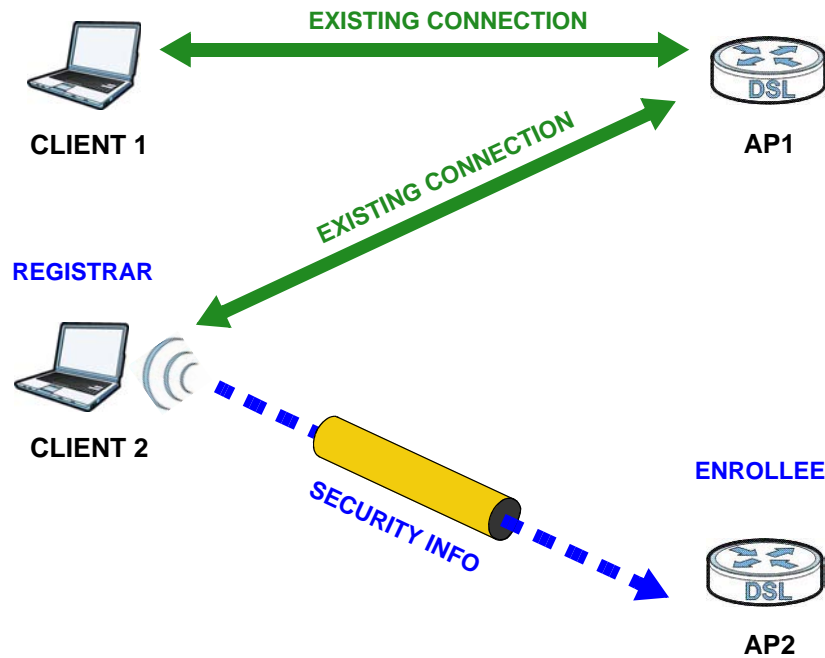
In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 45 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 46 WPS: Example Network Step 3



7.10.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

WPS works by automatically issuing a randomly-generated WPA2-PSK pre-shared key from the registrar device to the enrollee devices. 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 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

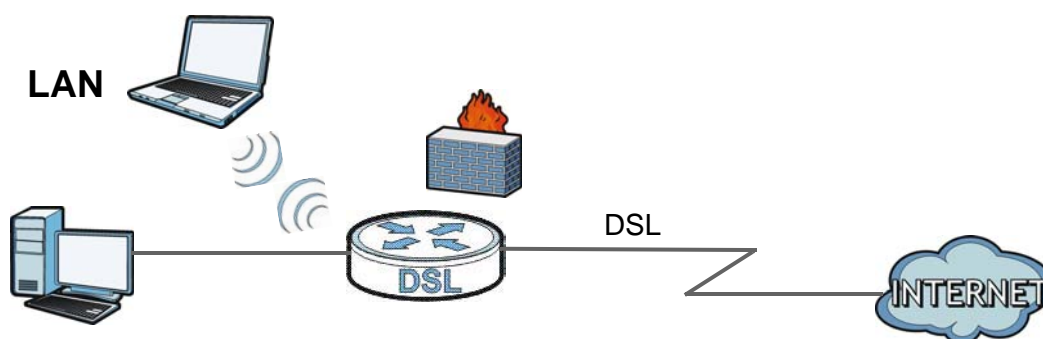
access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an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

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your AMG1302/AMG1202-TSeries ([Section 8.2 on page 123](#)).
- 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 125](#)).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the AMG1302/AMG1202-TSeries ([Section 8.4 on page 126](#)).
- Use the **IP Alias** screen ([Section 8.5 on page 126](#)) to change your AMG1302/AMG1202-TSeries's IP alias settings.
- Use the **IPv6 LAN Setup** screen ([Section 8.6 on page 127](#)) to configure the IPv6 settings on your AMG1302/AMG1202-TSeries's LAN interface.

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 AMG1302/AMG1202-TSeries 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.

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 151](#) 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 AMG1302/AMG1202-TSeries 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

Sexual 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.

Finding Out More

See [Section 8.7 on page 131](#) 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, subnet mask and advanced networking settings such as RIP, multicast of your AMG1302/AMG1202-TSeries. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Figure 47 Network Setting > Home Networking > LAN Setup

The screenshot displays the LAN Setup configuration interface, organized into several sections:

- LAN IP Setup:**
 - IP Address: 192.168.1.153
 - Subnet Mask: 255.255.255.0
 - RIP Version: RIP1 (dropdown), Direction: None (dropdown)
 - Multicast: IGMP v1/IGMP v2/IGMP v3 (dropdown)
 - IGMP Snooping: Disabled Enabled
- DHCP Server State:**
 - DHCP: Disable Enable DHCP Relay
- IP Addressing Values:**
 - IP Pool Starting Address: 192.168.1.33
 - Pool Size: 32
- DHCP Server Lease Time:**
 - Lease Time: 259200 seconds
- DNS Values:**
 - DNS Server 1: DNS Proxy (dropdown), 192.168.1.153
 - DNS Server 2: None (dropdown), 0.0.0.0

At the bottom right, there are **Apply** and **Cancel** buttons.

The following table describes the fields in this screen.

Table 30 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries 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.
Dynamic Route	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. Select the RIP version from RIP1 and RIP2 .
Direction	Use this field to control how much routing information the VDSL Router sends and receives on the subnet. Select the RIP Direction from None , Both , IN Only and OUT Only .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The AMG1302/AMG1202-TSeries supports IGMP v1/IGMP v2/IGMP v3 . Select None to disable it.
IGMP Snooping	Select Enabled to activate IGMP Snooping. This allows the AMG1302/AMG1202-TSeries to passively learn memberships in multicast groups. Otherwise, select Disabled to deactivate it.
DHCP Server State	
DHCP	<p>If set to Enable, your AMG1302/AMG1202-TSeries can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to Disable, the DHCP server will be disabled.</p> <p>If set to DHCP Relay, the AMG1302/AMG1202-TSeries acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Server Lease Time	
Lease Time	This field specifies the lease time in seconds of an IP address assigned by the DHCP server.
DNS Values	
DNS	<p>Select Dynamic to have the AMG1302/AMG1202-TSeries pass a DNS (Domain Name System) server IP address to the DHCP clients.</p> <p>Select Static and enter the DNS server IP address(es) in the fields below, if you know the IP address.</p>
DNS Server 1/2	Enter the IP address of your primary/secondary DNS server.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.
Advanced Setup	Click this to display the Advanced LAN Setup screen and edit more details of your LAN setup.

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 AMG1302/AMG1202-TSeries's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 48 Network Setting > Home Networking > Static DHCP



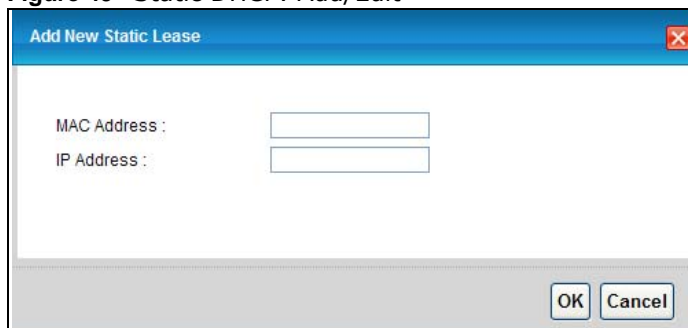
The following table describes the labels in this screen.

Table 31 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.
Active	This field displays whether the client is connected to the AMG1302/AMG1202-TSeries.
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 49 Static DHCP: Add/Edit



The following table describes the labels in this screen.

Table 32 Static DHCP: Add/Edit

LABEL	DESCRIPTION
MAC Address	If you select Manual Input in the Select Device Info field, enter the MAC address of a computer on your LAN.
IP Address	If you select Manual Input in the Select Device Info field, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
OK	Click OK 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 122](#) for more information on UPnP.

Use the following screen to enable or disable the UPnP function on your AMG1302/AMG1202-TSeries. Click **Network Setting > Home Networking > UPnP** to display the screen shown next.

Figure 50 Network Setting > Home Networking > UPnP



The following table describes the labels in this screen.

Table 33 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 AMG1302/AMG1202-TSeries's IP address (although you must still enter the password to access the web configurator). Otherwise, select Disable to deactivate UPnP.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.5 The IP Alias Screen

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The AMG1302/AMG1202-TSeries supports multiple logical LAN interfaces via its physical Ethernet interface with the AMG1302/AMG1202-TSeries 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).

8.5.1 Configuring the LAN IP Alias Screen

Use this screen to change your AMG1302/AMG1202-TSeries's IP alias settings. Click **Network Setting > Home Networking > IP Alias** to open the following screen.

Figure 51 Network Setting > Home Networking > IP Alias

The following table describes the labels in this screen.

Table 34 Network Setting > Home Networking > IP Alias

LABEL	DESCRIPTION
IP Alias	Select Enable to configure a LAN network for the AMG1302/AMG1202-TSeries.
IP Address	Enter the IP address of your AMG1302/AMG1202-TSeries in dotted decimal notation.
IP Subnet Mask	Your AMG1302/AMG1202-TSeries 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 AMG1302/AMG1202-TSeries.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

8.6 The IPv6 LAN Setup Screen

Use this screen to configure the IPv6 settings for your AMG1302/AMG1202-TSeries's LAN interface. See [Appendix E on page 295](#) for background information about IPv6.

Figure 52 Network Setting > Home Networking > IPv6 LAN Setup

IPv6 LAN Setup

Link Local Address Type : Manual EUI64

IPv6 Address :

Prefix :

MLD Snooping : Enabled Disabled

Lan Global Identifier Type : Manual EUI64

Lan Identifier :

IPv6 ULA Address Type : Auto Generate Manual

IPv6 ULA Address :

LAN IPv6 Address Setting

Delegate prefix from WAN Static

Static IPv6 Address Prefix :

Prefix length :

Preferred Lifetime :

Valid Lifetime :

LAN IPv6 Address Assign Setup:

LAN IPv6 DNS Assign Setup:

DHCPv6

DHCPv6 Server : Disable Enable

DNSv6 Mode: Proxy Relay Manual

Primary DNS :

Secondary DNS :

Information refresh time :

DNS Query Mode :

The following table describes the labels in this screen.

Table 35 Network Setting > Home Networking > IPv6 LAN Setup

LABEL	DESCRIPTION
IPv6 LAN Setup	
Link Local Address Type	Select Manual to manually enter a link local address. Select EUI64 to use the EUI-64 format to generate a link local address from the Ethernet MAC address.
IPv6 Address	If you selected Manual in the Link Local Address Type field, enter the LAN IPv6 address you want to assign to your AMG1302/AMG1202-TSeries in hexadecimal notation, for example, fe80::1 (factory default).
Prefix	Enter the address prefix to specify how many most significant bits in an IPv6 address compose the network address.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. Select Enabled to activate MLD Snooping on the AMG1302/AMG1202-TSeries. This allows the AMG1302/AMG1202-TSeries to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.

LABEL	DESCRIPTION
Lan Global Identifier Type	Select Manual to manually enter a LAN Identifier as the interface ID to identify the LAN interface. The LAN Identifier is appended to the IPv6 address prefix to create the routable global IPv6 address. Select EUI 64 to use the EUI-64 format to generate an interface ID from the Ethernet MAC address.
Lan Identifier	If you selected Manual , enter the LAN Identifier in this field. The LAN identifier should be unique and 64 bits in hexadecimal form. Every 16 bit block should be separated by a colon as in XXXX:XXXX:XXXX:XXXX where X is a hexadecimal character. Blocks of zeros can be represented with double colons as in XXXX:XXXX::XXXX.
LAN IPv6 Address Setting	
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 AMG1302/AMG1202-TSeries's LAN IPv6 address.
Static IPv6 Address Prefix	If you select static IPv6 address, enter the IPv6 address prefix that the AMG1302/AMG1202-TSeries uses for the LAN IPv6 address.
Prefix length	If you select static IPv6 address, enter the IPv6 prefix length that the AMG1302/AMG1202-TSeries 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.
Preferred Lifetime	Enter the preferred lifetime for the prefix.
Valid Lifetime	Enter the valid lifetime for the prefix.
RADVD Setup	
Send RA on	Select this to have the AMG1302/AMG1202-TSeries send router advertisement messages to the LAN hosts. Router advertisement is a response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters, such as IPv6 prefix and DNS information. Router solicitation is a request from a host to locate a router that can act as the default router and forward packets. Note: The LAN hosts neither generate global IPv6 addresses nor communicate with other networks if you disable this feature.
Delegate M/O flag from WAN	Select this to have the AMG1302/AMG1202-TSeries obtain the M/O (Managed/Other) flag setting from the service provider or uplink router.
Manual	Select this to specify the M/O flag setting manually.
Managed config flag on	Select this to have the AMG1302/AMG1202-TSeries indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the AMG1302/AMG1202-TSeries indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Other config flag on	Select this to have the AMG1302/AMG1202-TSeries indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the AMG1302/AMG1202-TSeries indicate to hosts that DNS information is not available in this network.
Advertisement interval option on	Select this to have the Router Advertisement messages the VDSL Router sends specify the allowed interval between Router Advertisement messages.
Hop limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0. Possible value for this field are 0-255.

LABEL	DESCRIPTION
Router Lifetime	Enter the time in seconds that hosts should consider the AMG1302/AMG1202-TSeries to be the default router. Possible values for this field are 0-9000.
Router Preference	Select the router preference (Low , Medium or High) for the AMG1302/AMG1202-TSeries. The AMG1302/AMG1202-TSeries sends this preference in the router advertisements to tell hosts what preference they should use for the AMG1302/AMG1202-TSeries. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
Reachable Time (ms)	Enter the time in milliseconds that can elapse before a neighbor is detected. Possible values for this field are 0-3600000.
Retrans Timer (ms)	Enter the time in milliseconds between neighbor solicitation packet retransmissions. Possible values for this field are 1000-4294967295.
RA Interval	Enter the time in seconds between router advertisement messages. Possible values for this field are 4-1800.
Delegate MTU from WAN	Select this to have the AMG1302/AMG1202-TSeries obtain the MTU setting from the service provider or uplink router.
Manual	Select this to specify the MTU manually.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the AMG1302/AMG1202-TSeries divides it into smaller fragments.
DAD attempts	Specify the number of DAD (Duplicate Address Detection) attempts before an IPv6 address is assigned to the AMG1302/AMG1202-TSeries LAN interface. Possible values for this field are 1-7.
DHCPv6	
DHCPv6 Server	Use this field to Enable or Disable DHCPv6 server on the AMG1302/AMG1202-TSeries.
DNSv6 Mode	Select the DNS role (Proxy or Relay) that you want the AMG1302/AMG1202-TSeries to act in the IPv6 LAN network. Alternatively, select Manual and specify the DNS servers' IPv6 address in the fields below.
Primary DNS	This field is available if you choose Manual as the DNSv6 mode. Enter the first DNS server IPv6 address the AMG1302/AMG1202-TSeries passes to the DHCP clients.
Secondary DNS	This field is available if you choose Manual as the DNSv6 mode. Enter the second DNS server IPv6 address the AMG1302/AMG1202-TSeries passes to the DHCP clients.
Information refresh time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

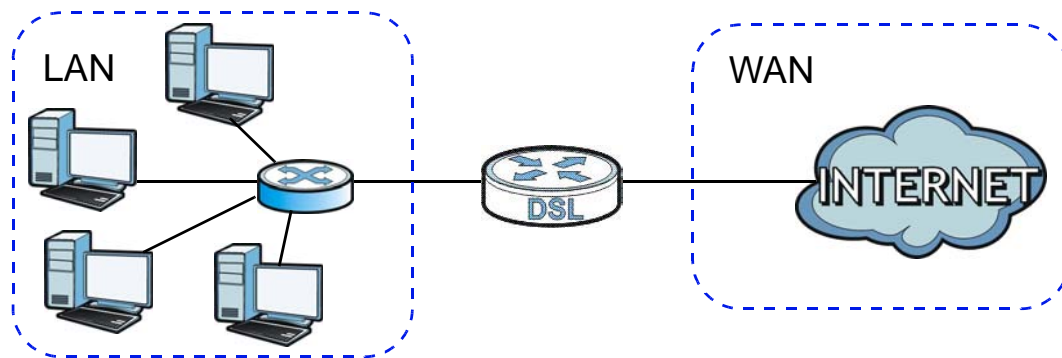
8.7 Home Networking Technical Reference

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

8.7.1 LANs, WANs and the AMG1302/AMG1202-TSeries

The actual physical connection determines whether the AMG1302/AMG1202-TSeries ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 53 LAN and WAN IP Addresses



8.7.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the AMG1302/AMG1202-TSeries as a DHCP server or disable it. When configured as a server, the AMG1302/AMG1202-TSeries provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The AMG1302/AMG1202-TSeries is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). Do not assign static IP addresses from the DHCP pool to your LAN computers.

8.7.3 DNS Server Addresses

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

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

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.

- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The AMG1302/AMG1202-TSeries supports the IPCP DNS server extensions through the DNS proxy feature.

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

8.7.4 LAN TCP/IP

The AMG1302/AMG1202-TSeries has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

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

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the AMG1302/AMG1202-TSeries. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your AMG1302/AMG1202-TSeries, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your AMG1302/AMG1202-TSeries will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the AMG1302/AMG1202-TSeries unless you are instructed to do otherwise.

Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255

- 192.168.0.0 — 192.168.255.255

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

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

8.7.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the AMG1302/AMG1202-TSeries will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the AMG1302/AMG1202-TSeries will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the AMG1302/AMG1202-TSeries will send out RIP packets but will not accept any RIP packets received.
- **None** - the AMG1302/AMG1202-TSeries will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the AMG1302/AMG1202-TSeries sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

8.7.6 Multicast

Traditionally, IP packets are transmitted in one of either 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.

IGMP (Internet Group Multicast Protocol) 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. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network. 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 AMG1302/AMG1202-TSeries queries all directly connected networks to gather group membership. After that, the AMG1302/AMG1202-TSeries periodically updates this information. IP multicasting can be enabled/disabled on the AMG1302/AMG1202-TSeries LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

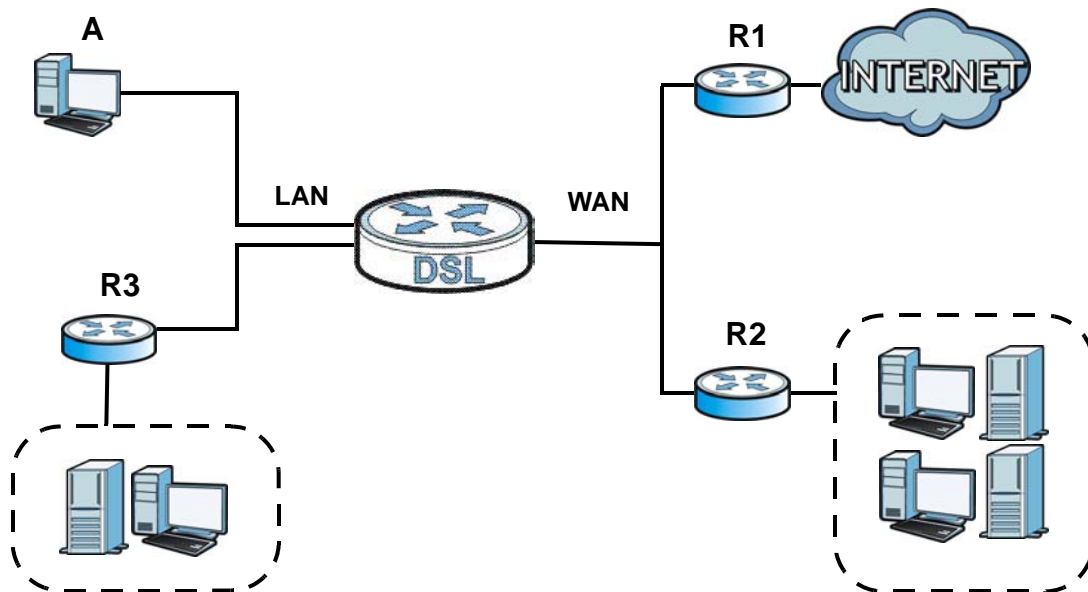
Static Route

9.1 Overview

The AMG1302/AMG1202-TSeries usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the AMG1302/AMG1202-TSeries send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the AMG1302/AMG1202-TSeries's LAN interface. The AMG1302/AMG1202-TSeries routes most traffic from **A** to the Internet through the AMG1302/AMG1202-TSeries's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 54 Example of Static Routing Topology



9.1.1 What You Can Do in the Static Route Screens

- Use the **Static Route** screens ([Section 9.2 on page 136](#)) to view and configure IP static routes on the AMG1302/AMG1202-TSeries.
- Use the **IPv6 Static Route** screens ([Section 9.3 on page 137](#)) to view and configure IPv6 static routes on the AMG1302/AMG1202-TSeries.

9.2 The Static Route Screen

Use this screen to view the static route rules. Click **Network Setting > Static Route** to open the **Static Route** screen.

Figure 55 Network Setting > Static Route



The following table describes the labels in this screen.

Table 36 Network Setting > Static Route

LABEL	DESCRIPTION
Add new static route	Click this to configure a new static route.
#	This is the number of an individual static route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Metric	This is the number of transmission hops between this AMG1302/AMG1202-TSeries and the destination.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the AMG1302/AMG1202-TSeries. Click the Delete icon to remove a static route from the AMG1302/AMG1202-TSeries. A window displays asking you to confirm that you want to delete the route.

9.2.1 Static Route Add/Edit

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

Figure 56 Network Setting > Static Route Add/Edit

The following table describes the labels in this screen.

Table 37 Network Setting > Static Route Add/Edit

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Enter the number of transmission hops (routers) that need to cross from the AMG1302/AMG1202-TSeries to the destination.
OK	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

9.3 IPv6 Static Route

Use this screen to view the IPv6 static route rules. Click **Network Setting > Static Route > IPv6 Static Route** to open the **IPv6 Static Route** screen.

Figure 57 Network Setting > Static Route > IPv6 Static Route

The following table describes the labels in this screen.

Table 38 Network Setting > Static Route > IPv6 Static Route

LABEL	DESCRIPTION
Add new static route	Click this to configure a new IPv6 static route.
#	This is the number of an individual static route.

Table 38 Network Setting > Static Route > IPv6 Static Route

LABEL	DESCRIPTION
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Prefix Length	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.
Device	This specifies the LAN or WAN PVC.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the AMG1302/AMG1202-TSeries. Click the Remove icon to remove a static route from the AMG1302/AMG1202-TSeries. A window displays asking you to confirm that you want to delete the route.

9.3.1 IPv6 Static Route Edit

Use this screen to configure the required information for an IPv6 static route. Click **Add new static route** or select an IPv6 static route index number and click **Edit**. The screen shown next appears.

Figure 58 Network Setting > Static Route > IPv6 Static Route: Add/Edit

The following table describes the labels in this screen.

Table 39 Network Setting > Static Route > IPv6 Static Route: Add/Edit

LABEL	DESCRIPTION
Destination IPv6 Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a prefix length of 128 in the prefix length field to force the network number to be identical to the host ID.
IPv6 Prefix Length	Enter the address prefix to specify how many most significant bits compose the network address.
PVC IPv6 Address	Select the interface through which the traffic is routed.
OK	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

Quality of Service (QoS)

10.1 Overview

Use the **QoS** screen to set up your AMG1302/AMG1202-TSeries to use QoS for traffic management.

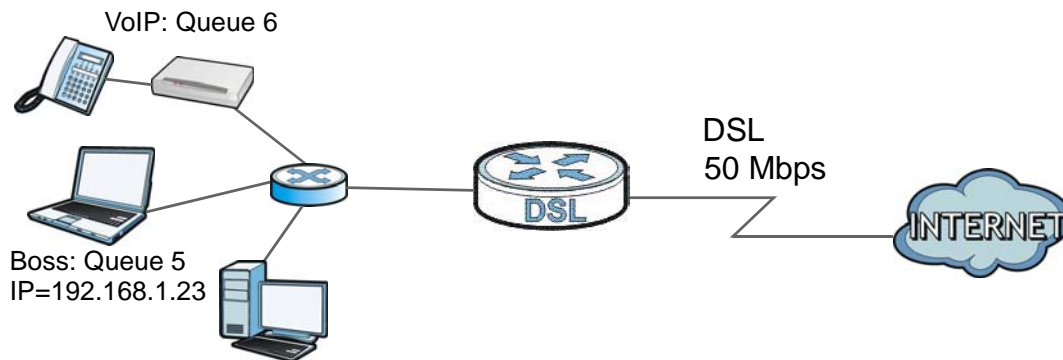
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the AMG1302/AMG1202-TSeries to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data are equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

The AMG1302/AMG1202-TSeries assigns each packet a priority and then queues the packet accordingly. Packets assigned with a high priority are processed more quickly than those with low priorities if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 5. Traffic that does not match these two classes are assigned priority queue based on the internal QoS mapping table on the AMG1302/AMG1202-TSeries.

Figure 59 QoS Example



10.1.1 What You Can Do in the QoS Screens

- Use the **General** screen ([Section 10.2 on page 140](#)) to enable QoS on the AMG1302/AMG1202-TSeries, and specify the type of scheduling.

- Use the **Queue** screen ([Section 10.3 on page 141](#)) to configure QoS settings on the AMG1302/AMG1202-TSeries.
- Use the **Class Setup** screen ([Section 10.4 on page 143](#)) to configure QoS settings on the AMG1302/AMG1202-TSeries.
- Use the **Game List** screen ([Section 10.5 on page 147](#)) to give priority to traffic for specific games.

10.1.2 What You Need to Know About QoS

802.1p

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. 802.1p is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use 802.1p to give different priorities to different packet types.

Tagging and Marking

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

Finding Out More

See [Section 10.6 on page 148](#) for advanced technical information on QoS.

10.2 The Quality of Service General Screen

Use this screen to enable or disable QoS and set the upstream bandwidth.

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

Figure 60 Network Setting > QoS > General



Active QoS

Traffic priority will be automatically assigned by None

Apply Cancel

The following table describes the labels in this screen.

Table 40 Network Setting > QoS > General













LABEL	DESCRIPTION
Active QoS	Use this field to turn on QoS to improve your network performance.
Traffic priority will be automatically assigned by	<p>Select how the AMG1302/AMG1202-TSeries assigns priorities to various incoming and outgoing traffic flows.</p> <ul style="list-style-type: none"> None: Disables auto priority mapping and has the AMG1302/AMG1202-TSeries put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. Ethernet Priority: Automatically assign priority based on the IEEE 802.1p priority level. IP Precedence: Automatically assign priority based on the first three bits of the TOS field in the IP header. Packet Length: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

10.3 The Queue Screen

Use this screen to configure QoS queue assignment disciplines and priorities.

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

Figure 61 Network Setting > QoS > Queue

Inde	Status	Name	Interface	Priority	Weight	Rate Limit	Modify
1		Queue1	WAN	1	1	N/A	 
2		N/A	N/A	N/A	N/A	N/A N/A	 
3		N/A	N/A	N/A	N/A	N/A N/A	 
4		N/A	N/A	N/A	N/A	N/A N/A	 

The following table describes the labels in this screen.

Table 41 Network Setting > QoS > Queue

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the AMG1302/AMG1202-TSeries's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.

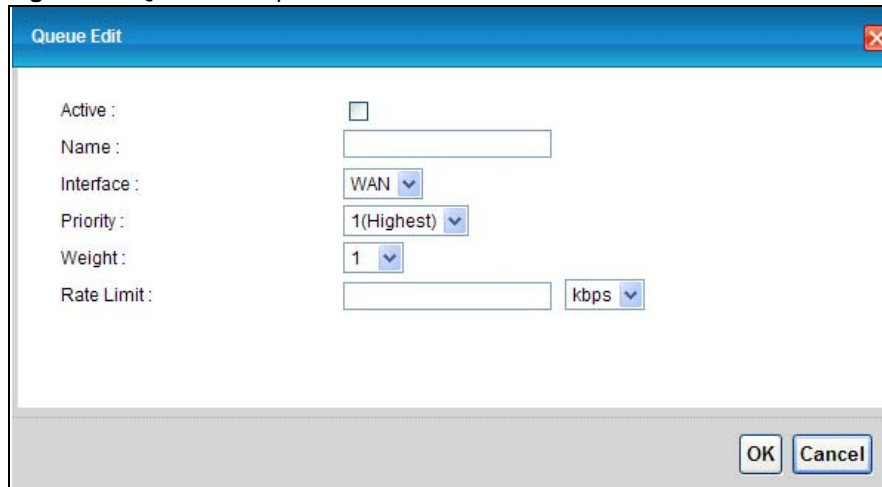
Table 41 Network Setting > QoS > Queue

LABEL	DESCRIPTION
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the Edit icon to edit the queue. Click the Delete icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

10.3.1 Adding a QoS Queue

Click the edit icon in the **Queue Setup** screen to configure a queue.

Figure 62 Queue Setup: Edit



The following table describes the labels in this screen.

Table 42 Queue Setup: Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 3) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the AMG1302/AMG1202-TSeries divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

10.4 The Class Setup Screen

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

You can give different priorities to traffic that the AMG1302/AMG1202-TSeries forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

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

Figure 63 Network Setting > QoS > Class Setup

Index	Status	From Interface	Classification Criteria	DSCP(Traffic Class) Mark	802.1P/1Q Mark	To Queue	Modify
-------	--------	----------------	-------------------------	--------------------------	----------------	----------	--------

The following table describes the labels in this screen.

Table 43 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
Index	This is the index number of the entry.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
From Interface	This shows the interface from which traffic of this class should come.
Classification Criteria	This shows criteria specified in this classifier, for example the type and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P/1Q Mark	This is the IEEE 802.1p priority level and 802.1Q VLAN tag assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the Edit icon to edit the classifier. Click the Delete icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

10.4.1 Class Setup Add/Edit

Click **Add new Classifier** in the **Network Setting > QoS > Class Setup** screen or click the **Edit** icon next to a class, the screen appears as shown next.

Figure 64 QoS > Class Setup Add/Edit

✖
Add new Classifier

Rule Index ▼

Class Configuration

Active

Ether Type IPv4 (0x0800) ▼

Interface From LAN ▼

To Queue ▼

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
 LAN1 LAN2 LAN3 LAN4 ra0 ra1 ra2 ra3

▪ **Source**

<input type="checkbox"/> IP Address	<input type="text"/>	IP Subnet Mask	<input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	<input type="text"/> ~ <input type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC Address	<input type="text"/>	MAC Mask	<input type="text"/>	<input type="checkbox"/> Exclude

▪ **Destination**

<input type="checkbox"/> IP Address	<input type="text"/>	IP Subnet Mask	<input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	<input type="text"/> ~ <input type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC Address	<input type="text"/>	MAC Mask	<input type="text"/>	<input type="checkbox"/> Exclude

▪ **Others**

<input type="checkbox"/> Service	▼			
<input type="checkbox"/> IP Protocol	▼			<input type="checkbox"/> Exclude
<input type="checkbox"/> TCP ACK				<input type="checkbox"/> Exclude
<input type="checkbox"/> DHCP	▼	<input type="text"/>		<input type="checkbox"/> Exclude
<input type="checkbox"/> Packet Length	<input type="text"/> ~ <input type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> IPP/DS Field	<input type="radio"/> IPP/TOS <input checked="" type="radio"/> DSCP			
<input type="checkbox"/> IP Precedence Range	▼ ~ ▼			<input type="checkbox"/> Exclude
<input type="checkbox"/> Type of Service	▼			<input type="checkbox"/> Exclude
<input type="checkbox"/> DSCP Range(0 ~ 63)	<input type="text"/> ~ <input type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> 802.1P	▼ ~ ▼			<input type="checkbox"/> Exclude
<input type="checkbox"/> VLAN ID	<input type="text"/> ~ <input type="text"/> (Value Range: 1 ~ 4094)			<input type="checkbox"/> Exclude

Action

Forward to Unchange ▼

IPP/DS Field IPP/TOS DSCP

IP Precedence Mark Unchange ▼ ▼

Type Of Service Mark Unchange ▼ ▼

DSCP Mark(0 ~ 63) Unchange ▼

802.1Q Tag Same ▼

- Ethernet Priority ▼ ▼

- VLAN ID ▼ (Value Range: 1 ~ 4094)

OK Cancel

The following table describes the labels in this screen.

Table 44 QoS > Class Setup Add/Edit

LABEL	DESCRIPTION
Rule Index	Select the rule's index number from the drop-down list box.
Class Configuration	
Active	Use this field to enable or disable the QoS class rule.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select IPv4 or IPv6 , you also need to configure source or destination IP address, MAC address, DHCP options, DSCP value or the protocol type. If you select ARP , you also need to configure source or destination MAC address. If you select 802.1Q , you can configure an 802.1p priority level and VLAN ID.
Interface	Select an interface if you want to classify the traffic received by it.
To Queue	Select a queue that applies to this class. You should have configured a queue in the Queue Setup screen already.
Criteria Configuration	
Basic	
From Interface	If you select From LAN in the Interface field, you can select specific interface(s) from which traffic is received. ra0 ~ ra3 means wireless interfaces WLAN0 to WLAN3. If you select From WAN in the Interface field, you can select a specific WAN connection (PVC0~PVC2) from which traffic is received.
Source	
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank IP address means any source IP address.
Subnet Netmask/ Source Prefix Length	Enter the source subnet mask if you select IPv4 as the Ether Type . Enter the source prefix length if you select IPv6 as the Ether Type .
Port Range	If you select TCP/UDP , TCP or UDP in the IP protocol field, select the check box and enter the port number(s) of the source.
MAC Address	Select the check box and enter the source MAC address of the packet.
Mac Netmask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank IP address means any destination IP address.
Subnet Netmask/ Destination Prefix Length	Enter the destination subnet mask if you select IPv4 as the Ether Type . Enter the destination prefix length if you select IPv6 as the Ether Type .
Port Range	If you select TCP/UDP , TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
MAC Address	Select the check box and enter the destination MAC address of the packet.

Table 44 QoS > Class Setup Add/Edit (continued)

LABEL	DESCRIPTION
Mac Netmask	<p>Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.</p> <p>Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.</p>
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
IP Protocol	<p>This field is available only when you select IPv4 or IPv6 in the Ether Type field.</p> <p>If you select IPv4, select this option and select the protocol (service type) from TCP/UDP, TCP, UDP or ICMP. If you select IPv6, select this option and select the protocol (service type) from TCP/UDP, TCP, UDP or ICMPv6.</p>
TCP ACK	<p>This field is available only when you select TCP in the IP protocol field.</p> <p>If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.</p>
Packet Length	<p>This field is available only when you select IPv4 or IPv6 in the Ether Type field.</p> <p>Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.</p>
IPP/DS Field	<p>Select IPP/TOS to specify an IP precedence range and type of services.</p> <p>Select DSCP to specify a DiffServ Code Point (DSCP) range.</p>
IP Precedence Range	Enter a range from 0 to 7 for IP precedence. 0 is the lowest priority and 7 is the highest.
Type of Service	<p>Select a type of service from the drop-down list box.</p> <p>Available options are: Normal service, Minimize delay, Maximize throughput, Maximize reliability and Minimize monetary cost.</p>
DSCP Range	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	<p>Select this option and select a priority level (between 0 and 7) from the drop-down list box.</p> <p>"0" is the lowest priority level and "7" is the highest.</p>
VLAN ID	Select this option and enter the source VLAN ID in this field.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Action	
Forward To	<p>Select the interface through which traffic that matches the rule is forwarded out. If you select Unchange, the AMG1302/AMG1202-TSeries forwards traffic of this class according to the default routing table.</p> <p>If traffic of this class comes from a WAN interface and is in a queue that forwards traffic through the LAN/WLAN interface, the AMG1302/AMG1202-TSeries ignores the setting here.</p>
IPP/DS Field	<p>Select IPP/TOS to specify an IP precedence range and type of services.</p> <p>Select DSCP to specify a DiffServ Code Point (DSCP) range.</p>

Table 44 QoS > Class Setup Add/Edit (continued)

LABEL	DESCRIPTION
IP Precedence Mark	Enter a range from 0 to 7 to re-assign IP precedence to matched traffic. 0 is the lowest priority and 7 is the highest.
Type Of Service Mark	Select a type of service to re-assign the priority level to matched traffic. Available options are: Normal service , Minimize delay , Maximize throughput , Maximize reliability and Minimize monetary cost .
DSCP Mark(0~63)	This field is available only when you select IP in the Ether Type field. If you select Mark , enter a DSCP value with which the AMG1302/AMG1202-TSeries replaces the DSCP field in the packets. If you select Unchange , the AMG1302/AMG1202-TSeries keep the DSCP field in the packets.
802.1Q Tag	If you select Remark , select a priority level (in the Ethernet Priority field) and enter a VLAN ID number (in the VLAN ID field) with which the AMG1302/AMG1202-TSeries replaces the IEEE 802.1p priority field and VLAN ID of the frames. If you select Remove , the AMG1302/AMG1202-TSeries deletes the VLAN ID of the frames before forwarding them out. If you select Add , the AMG1302/AMG1202-TSeries treat all matched traffic untagged and add a second priority level and VLAN ID that you specify in the Ethernet Priority and VLAN ID fields. If you select Same , the AMG1302/AMG1202-TSeries keep the Ethernet Priority and VLAN ID in the packets. To configure the Ethernet Priority, you can either select a priority number in the first drop-down list box (7 is the highest and 0 is the lowest priority) or select an application from the second drop-down list box which automatically maps to the corresponding priority number. (Key Net Traffic: 7; Voice: 6; Video: 5; IGMP: 4; Key Data: 3)
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

10.5 The QoS Game List Screen

Use this screen to give priority to traffic for specific games. Click **Network Setting > QoS > Game List** to open the screen as shown next.

Figure 65 Network Setting > QoS > Game List

Enable Game List

Call of Duty: Black Ops(PC) Call of Duty: Black Ops(PS3) Call of Duty: Black Ops(XBOX360)

Call of Duty: Modern Warfare 2(PC) Call of Duty: Modern Warfare 2(PS3) Call of Duty: World at War(PS3)

CounterStrike(PC) DiRT 2(PS3) FIFA 2010(PS3)

FIFA 2011(PS3) Pro Evolution Soccer 2011(PS3) Red Dead Redemption(PS3)

StarCraft2(PC) Uncharted 2: Among Thieves(PS3) Valve Steam Session(PC)

The following table describes the labels in this screen.

Table 45 Network Setting > QoS > Game List

LABEL	DESCRIPTION
Enable Game List	Select this to have QoS give the highest priority to traffic for the games you specify. This priority is higher than the other QoS queues. Select the games below.
Apply	Click this to save your changes.
Cancel	Click this to restore previously saved settings.

10.6 QoS Technical Reference

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

10.6.1 IEEE 802.1p

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

Table 46 IEEE 802.1p Priority Level and Traffic Type

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

10.6.2 IP Precedence

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

10.6.3 Automatic Priority Queue Assignment

If you enable QoS on the AMG1302/AMG1202-TSeries, the AMG1302/AMG1202-TSeries can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the AMG1302/AMG1202-TSeries. On the AMG1302/AMG1202-TSeries, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 47 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Network Address Translation (NAT)

11.1 Overview

This chapter discusses how to configure NAT on the AMG1302/AMG1202-TSeries. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

11.1.1 What You Can Do in the NAT Screens

- Use the **General** screen ([Section 11.2 on page 152](#)) to activate/deactivate NAT for the default WAN connection (PVC0).
- Use the **Port Forwarding** screen ([Section 11.3 on page 153](#)) to configure forward incoming service requests to the server(s) on your local network.
- Use the **DMZ** screen to configure a default server ([Section 11.4 on page 156](#)).

11.1.2 What You Need To Know About NAT

Inside/Outside

Inside/outside denotes where a host is located relative to the AMG1302/AMG1202-TSeries, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See [Section 11.5 on page 156](#) for advanced technical information on NAT.

11.2 The NAT General Screen

Use this screen to activate NAT for the default WAN connection (PVC0). Click **Network Setting > NAT** to open the following screen.

Note: You must create an IP filter rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the AMG1302/AMG1202-TSeries.

Figure 66 Network Setting > NAT > General

The screenshot shows a configuration window for NAT. At the top, there is a checked checkbox labeled 'Active'. Below it is a text input field labeled 'Max NAT/Firewall Session Per User' containing the number '3072'. A 'Note' section follows, with a document icon and the text: 'Maximum number of NAT/firewall sessions for the router is 8192. To remove the per user limit, set to 8192.' At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 48 Network Setting > NAT > General

LABEL	DESCRIPTION
Active	Select this check box to enable NAT.
Max NAT/Firewall Session Per User	<p>When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.</p> <p>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/Firewall sessions client computers can establish through the AMG1302/AMG1202-TSeries.</p> <p>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is exhausting all of the available NAT sessions.</p>
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

11.3 The Port Forwarding Screen

Use this screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

The most often used port numbers and services are shown in [Appendix F on page 305](#). Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default Server IP Address

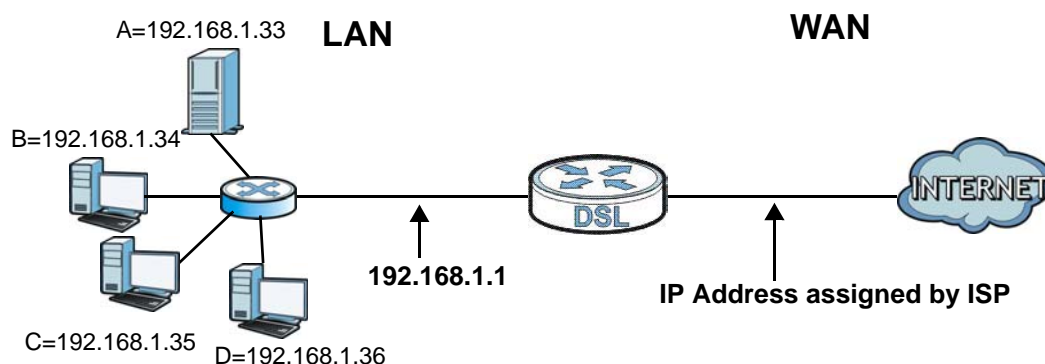
In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

Note: If you do not assign a **Default Server** IP address, the AMG1302/AMG1202-TSeries discards all packets received for ports that are not specified here or in the remote management setup.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 67 Multiple Servers Behind NAT Example



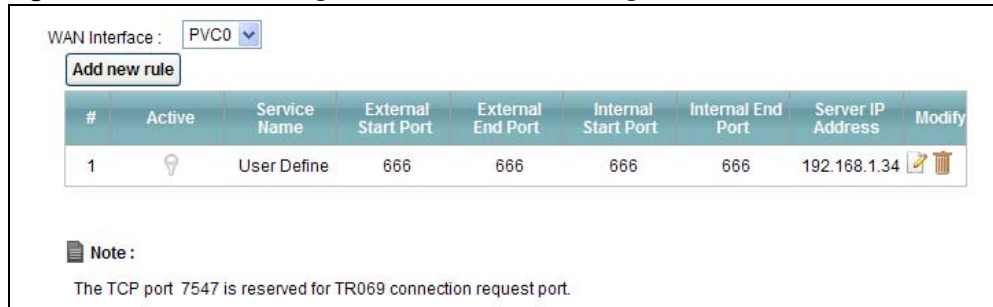
11.3.1 Configuring the Port Forwarding Screen

Click **Network Setting > NAT > Port Forwarding** to open the following screen.

See [Appendix F on page 305](#) for port numbers commonly used for particular services.

Note: Make sure NAT is activated on the WAN connection before you configure a port forwarding rule for it. For the default WAN connection (PVC0), activate NAT in the **Network Setting > NAT > General** screen. For other WAN connections (PVC1~PVC7), activate NAT for an individual WAN connection in the **Broadband > More Connections > Edit** screen.

Figure 68 Network Setting > NAT > Port Forwarding



WAN Interface : PVC0

Add new rule

#	Active	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify
1	<input checked="" type="checkbox"/>	User Define	666	666	666	666	192.168.1.34	

Note :
The TCP port 7547 is reserved for TR069 connection request port.

The following table describes the fields in this screen.

Table 49 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
WAN Interface	Select a WAN connection for which you want to configure a port forwarding rule.
Add new rule	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is a service's name.
External Start Port	This is the first port number of a port range that incoming service requests may use to access the service in your local network.
External End Port	This is the last port number of a port range that incoming service requests may use to access the service in your local network.
Internal Start Port	This is the starting port number that the device translates for the service in your local network.
Internal End Port	This is the ending port number that the device translates for the service in your local network.
Server IP Address	This is the server's IP address in your local network.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.

11.3.2 Port Forwarding Rule Add/Edit

Use this screen to add or edit a port forwarding rule. Click the **Add new rule** button or a rule's edit icon in the **Port Forwarding** screen to display the screen as shown next.

Figure 69 Network Setting > NAT > Port Forwarding: Add/Edit

The following table describes the fields in this screen.

Table 50 Network Setting > NAT > Port Forwarding: Edit

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
External Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the End Port field. To forward a series of ports, enter the start port number here and the end port number in the End Port field.
External End Port	Enter a port number in this field. To forward only one port, enter the port number in the Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port field above.
Server IP Address	Enter the IP address of the server in your local network.
Trigger Protocol	Select the protocol of the service, TCP , UDP or ALL (TCP+UDP).
Open Start Port	Enter the first port number here to which you want the device to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the device automatically calculates the last port of the translated port range.
Open End Port	Enter the last port number here to which you want the device to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the device automatically calculates the last port of the translated port range.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

11.4 The DMZ Screen

If you need to allow packets from a specific WAN connection to your local network, NAT supports a default server IP address. A default server receives packets from the specified WAN connection and the ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 70 Network Setting > NAT > DMZ

WAN Interface : PVC0

Default Server Address : 0.0.0.0

Note :
 Enter IP address and click 'Apply' to activate the DMZ host.
 Input 0.0.0.0 in IP address field and click 'Apply' to deactivate the DMZ host.

Apply Cancel

The following table describes the fields in this screen.

Table 51 Network Setting > NAT > DMZ

LABEL	DESCRIPTION
WAN Interface	Select a WAN PVC connection (PVC0~PVC7) from which you want to forward the traffic to the specified default server.
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the NAT > Port Forwarding screen. Note: If you do not assign a Default Server Address , the AMG1302/AMG1202-TSeries discards all packets received for ports that are not specified in the NAT Port Forwarding screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

11.5 NAT Technical Reference

This chapter contains more information regarding NAT.

11.5.1 NAT Definitions

Inside/outside denotes where a host is located relative to the AMG1302/AMG1202-TSeries, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in

a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 52 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

11.5.2 What NAT Does

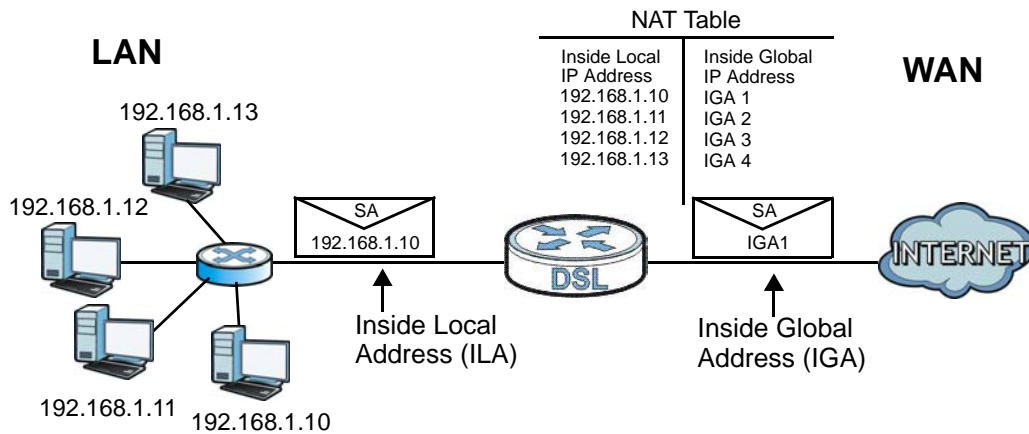
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 53 on page 159](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your AMG1302/AMG1202-TSeries filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

11.5.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The AMG1302/AMG1202-TSeries keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

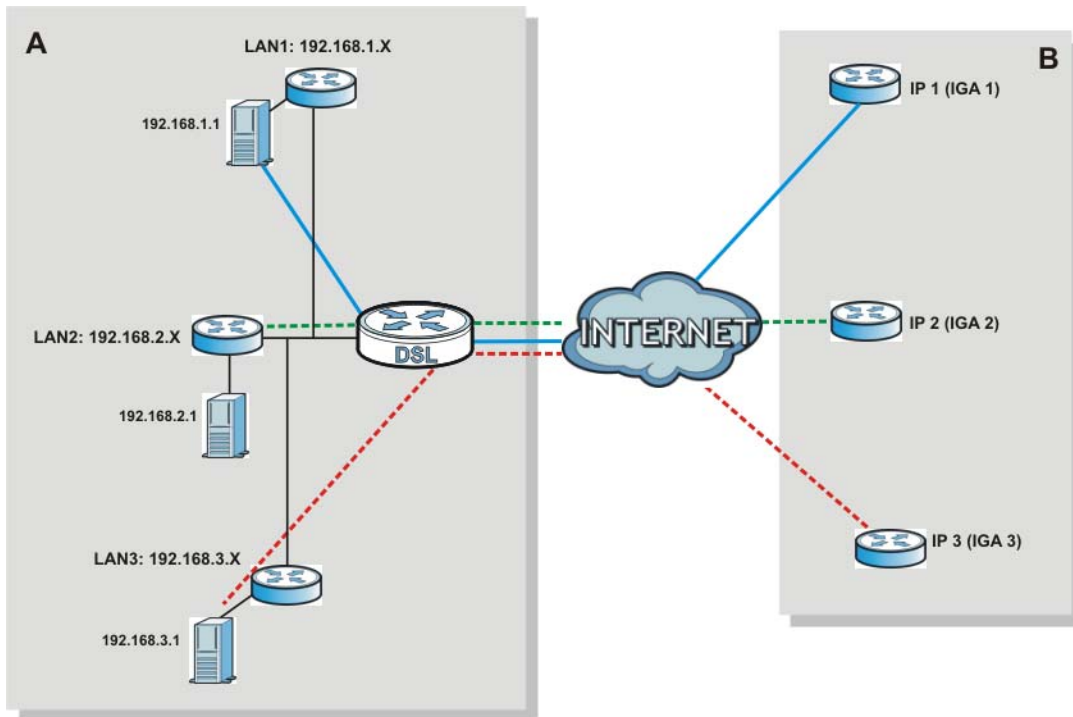
Figure 71 How NAT Works



11.5.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the AMG1302/AMG1202-TSeries can communicate with three distinct WAN networks.

Figure 72 NAT Application With IP Alias



11.5.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the AMG1302/AMG1202-TSeries maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the AMG1302/AMG1202-TSeries maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload:** In Many-to-Many Overload mode, the AMG1302/AMG1202-TSeries maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the AMG1302/AMG1202-TSeries maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 53 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1 ↔ IGA1
Many-to-One (SUA/PAT)	ILA1 ↔ IGA1 ILA2 ↔ IGA1 ...
Many-to-Many Overload	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA1 ILA4 ↔ IGA2 ...
Many-to-Many No Overload	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA3 ...
Server	Server 1 IP ↔ IGA1 Server 2 IP ↔ IGA1 Server 3 IP ↔ IGA1

