

User's Guide

VMG3312-T20A

Wireless N VDSL2 Combo WAN Gateway with USB

Default Login Details

LAN IP Address	http://192.168.1.1
Login	admin, user
Password	1234, user

Version 5.30 Edition 1, 03/2017



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the managed device.

- More Information

Go to support.zyxel.com to find other information on the VMG.



Contents Overview

User's Guide	14
Introducing the VMG	15
The Web Configurator	26
Quick Start	33
Tutorials	36
Technical Reference	65
Network Map and Status Screens	66
Broadband	70
Wireless	96
Home Networking	123
Routing	138
Quality of Service (QoS)	145
Network Address Translation (NAT)	163
Dynamic DNS Setup	179
Interface Grouping	183
USB Service	188
Firewall	193
MAC Filter	200
Parental Control	202
Scheduler Rule	207
Certificates	209
Log	216
Traffic Status	219
ARP Table	222
Routing Table	224
xDSL Statistics	226
Cellular Statistics	228
System	230
User Account	231
Remote Management	234
SNMP	237
Time Settings	239
E-mail Notification	241
Logs Setting	243
Firmware Upgrade	246
Backup/Restore	248
Diagnostic	251

Troubleshooting 253

Appendices259

Table of Contents

Contents Overview	3
Table of Contents	5
Part I: User's Guide.....	14
Chapter 1	
Introducing the VMG	15
1.1 Overview	15
1.2 Ways to Manage the VMG	15
1.3 Good Habits for Managing the VMG	15
1.4 Applications for the VMG	16
1.4.1 Internet Access	16
1.4.2 VMG's USB Support	17
1.5 Wireless Access	19
1.6 Hardware	19
1.6.1 Front Panel	19
1.6.2 LEDs (Lights)	20
1.6.3 Side Panels	21
1.6.4 Using the Wi-Fi and WPS Buttons	23
1.6.5 Rear Panel	23
1.6.6 The RESET Button	24
1.6.7 Wall Mounting	24
Chapter 2	
The Web Configurator.....	26
2.1 Overview	26
2.1.1 Accessing the Web Configurator	26
2.2 Web Configurator Layout	28
2.2.1 Title Bar	28
2.2.2 Main Window	28
2.2.3 Navigation Panel	29
Chapter 3	
Quick Start	33
3.1 Overview	33
3.2 Quick Start Setup	33

Chapter 4	
Tutorials	36
4.1 Overview	36
4.2 Setting Up an ADSL PPPoE Connection	36
4.3 Setting Up a Secure Wireless Network	39
4.3.1 Configuring the Wireless Network Settings	39
4.3.2 Using WPS	41
4.3.3 Without WPS	44
4.4 Setting Up Multiple Wireless Groups	44
4.5 Using the File Sharing Feature	48
4.5.1 Set Up File Sharing	48
4.5.2 Access Your Shared Files From a Computer	51
4.6 Using the Media Server Feature	51
4.6.1 Configuring the VMG	52
4.6.2 Using Windows Media Player	52
4.6.3 Using a Digital Media Adapter	54
4.7 Configuring Static Route for Routing to Another Network	55
4.8 Configuring QoS Queue and Class Setup	58
4.9 Access the VMG Using DDNS	61
4.9.1 Registering a DDNS Account on www.dyndns.org	61
4.9.2 Configuring DDNS on Your VMG	61
4.9.3 Testing the DDNS Setting	62
4.10 Configuring the MAC Address Filter	62
4.11 Access Your Shared Files From a Computer	63
Part II: Technical Reference	65
Chapter 5	
Network Map and Status Screens	66
5.1 Overview	66
5.2 The Network Map Screen	66
5.3 The Status Screen	67
Chapter 6	
Broadband	70
6.1 Overview	70
6.1.1 What You Can Do in this Chapter	70
6.1.2 What You Need to Know	71
6.1.3 Before You Begin	74
6.2 The Broadband Screen	74
6.2.1 Add/Edit Internet Connection	75

6.3 The Cellular Backup Screen 83
 6.4 The Advanced Screen 89
 6.5 Technical Reference 91

Chapter 7

Wireless 96

7.1 Overview 96
 7.1.1 What You Can Do in this Chapter 96
 7.1.2 What You Need to Know 96
 7.2 The General Screen 97
 7.2.1 No Security 98
 7.2.2 Basic (WEP Encryption) 99
 7.2.3 More Secure (WPA(2)-PSK) 100
 7.3 The Guest/More AP Screen 101
 7.3.1 Edit Guest/More AP 102
 7.4 The MAC Authentication Screen 104
 7.5 The WPS Screen 105
 7.6 The WMM Screen 107
 7.7 The Others Screen 108
 7.8 The Channel Status Screen 109
 7.9 Technical Reference 110
 7.9.1 Wireless Network Overview 110
 7.9.2 Additional Wireless Terms 112
 7.9.3 Wireless Security Overview 112
 7.9.4 Signal Problems 114
 7.9.5 BSS 115
 7.9.6 MBSSID 115
 7.9.7 Preamble Type 116
 7.9.8 WiFi Protected Setup (WPS) 116

Chapter 8

Home Networking 123

8.1 Overview 123
 8.1.1 What You Can Do in this Chapter 123
 8.1.2 What You Need To Know 124
 8.1.3 Before You Begin 125
 8.2 The LAN Setup Screen 125
 8.3 The Static DHCP Screen 129
 8.4 The UPnP Screen 130
 8.4.1 Turning On UPnP in Windows 7 Example 131
 8.5 The Additional Subnet Screen 133
 8.6 The STB Vendor ID Screen 134
 8.7 The Wake on LAN Screen 134

8.8 The TFTP Server Name Screen	135
8.9 Technical Reference	135
8.9.1 LANs, WANs and the VMG	135
8.9.2 DHCP Setup	136
8.9.3 DNS Server Addresses	136
8.9.4 LAN TCP/IP	137
Chapter 9	
Routing	138
9.1 Overview	138
9.2 The Routing Screen	138
9.2.1 Add/Edit Static Route	139
9.3 The DNS Route Screen	140
9.3.1 The DNS Route Add Screen	141
9.4 The Policy Route Screen	141
9.4.1 Add/Edit Policy Route	143
9.5 RIP	143
9.5.1 The RIP Screen	144
Chapter 10	
Quality of Service (QoS)	145
10.1 Overview	145
10.1.1 What You Can Do in this Chapter	145
10.2 What You Need to Know	146
10.3 The Quality of Service General Screen	147
10.4 The Queue Setup Screen	148
10.4.1 Editing a QoS Queue	150
10.5 The Classification Setup Screen	151
10.5.1 Add/Edit QoS Class	152
10.6 The QoS Shaper Setup Screen	155
10.6.1 Add/Edit a QoS Shaper	156
10.7 The QoS Policer Setup Screen	156
10.7.1 Add/Edit a QoS Policer	157
10.8 Technical Reference	158
Chapter 11	
Network Address Translation (NAT)	163
11.1 Overview	163
11.1.1 What You Can Do in this Chapter	163
11.1.2 What You Need To Know	163
11.2 The Port Forwarding Screen	164
11.2.1 Add/Edit Port Forwarding	166
11.3 The Applications Screen	167

11.3.1 Add New Application	168
11.4 The Port Triggering Screen	168
11.4.1 Add/Edit Port Triggering Rule	170
11.5 The DMZ Screen	171
11.6 The ALG Screen	172
11.7 The Address Mapping Screen	172
11.7.1 Add/Edit Address Mapping Rule	173
11.8 The Sessions Screen	174
11.9 Technical Reference	175
11.9.1 NAT Definitions	175
11.9.2 What NAT Does	176
11.9.3 How NAT Works	176
11.9.4 NAT Application	176
Chapter 12	
Dynamic DNS Setup.....	179
12.1 Overview	179
12.1.1 What You Can Do in this Chapter	179
12.1.2 What You Need To Know	179
12.2 The DNS Entry Screen	180
12.2.1 Add/Edit DNS Entry	180
12.3 The Dynamic DNS Screen	181
Chapter 13	
Interface Grouping.....	183
13.1 Overview	183
13.1.1 What You Can Do in this Chapter	183
13.2 The Interface Group Screen	183
13.2.1 Interface Group Configuration	184
13.2.2 Interface Grouping Criteria	186
Chapter 14	
USB Service.....	188
14.1 Overview	188
14.1.1 What You Can Do in this Chapter	188
14.1.2 What You Need To Know	188
14.1.3 Before You Begin	189
14.2 The File Sharing Screen	189
14.2.1 The Add New Share Screen	191
14.2.2 The Add New User Screen	192
14.3 The Media Server Screen	192
Chapter 15	
Firewall.....	193

15.1 Overview	193
15.1.1 What You Can Do in this Chapter	193
15.1.2 What You Need to Know	194
15.2 The Firewall Screen	194
15.3 The Protocol Screen	195
15.3.1 Add/Edit a Service	196
15.4 The Access Control Screen	197
15.4.1 Add/Edit an ACL Rule	197
15.5 The DoS Screen	199
Chapter 16	
MAC Filter	200
16.1 Overview	200
16.2 The MAC Filter Screen	200
Chapter 17	
Parental Control	202
17.1 Overview	202
17.2 The Parental Control Screen	202
17.2.1 Add/Edit a Parental Control Profile	203
Chapter 18	
Scheduler Rule	207
18.1 Overview	207
18.2 The Scheduler Rule Screen	207
18.2.1 Add/Edit a Schedule	207
Chapter 19	
Certificates	209
19.1 Overview	209
19.1.1 What You Can Do in this Chapter	209
19.2 What You Need to Know	209
19.3 The Local Certificates Screen	209
19.3.1 Create Certificate Request	210
19.3.2 Load Signed Certificate	212
19.4 The Trusted CA Screen	213
19.4.1 View Trusted CA Certificate	214
19.4.2 Import Trusted CA Certificate	215
Chapter 20	
Log	216
20.1 Overview	216
20.1.1 What You Can Do in this Chapter	216

20.1.2 What You Need To Know	216
20.2 The System Log Screen	217
20.3 The Security Log Screen	217
Chapter 21	
Traffic Status	219
21.1 Overview	219
21.1.1 What You Can Do in this Chapter	219
21.2 The WAN Status Screen	219
21.3 The LAN Status Screen	220
21.4 The NAT Status Screen	221
Chapter 22	
ARP Table	222
22.1 Overview	222
22.1.1 How ARP Works	222
22.2 ARP Table Screen	223
Chapter 23	
Routing Table	224
23.1 Overview	224
23.2 The Routing Table Screen	224
Chapter 24	
xDSL Statistics	226
24.1 The xDSL Statistics Screen	226
Chapter 25	
Cellular Statistics	228
25.1 Overview	228
25.2 The Cellular Statistics Screen	228
Chapter 26	
System	230
26.1 Overview	230
26.2 The System Screen	230
Chapter 27	
User Account	231
27.1 Overview	231
27.2 The User Account Screen	231
27.2.1 The User Account Add and Edit Screens	232

Chapter 28	
Remote Management	234
28.1 Overview	234
28.2 The Remote MGMT Screen	234
28.3 The Trust Domain Screen	235
28.3.1 The Add Trust Domain Screen	235
Chapter 29	
SNMP	237
29.1 Overview	237
29.2 The SNMP Screen	237
Chapter 30	
Time Settings	239
30.1 Overview	239
30.2 The Time Screen	239
Chapter 31	
E-mail Notification	241
31.1 Overview	241
31.2 The E-mail Notification Screen	241
31.2.1 E-mail Notification Edit	241
Chapter 32	
Logs Setting	243
32.1 Overview	243
32.2 The Logs Setting Screen	243
32.2.1 Example E-mail Log	244
Chapter 33	
Firmware Upgrade	246
33.1 Overview	246
33.2 The Firmware Screen	246
Chapter 34	
Backup/Restore	248
34.1 Overview	248
34.2 The Backup/Restore Screen	248
34.3 The Reboot Screen	250
Chapter 35	
Diagnostic	251
35.1 Overview	251

35.1.1 What You Can Do in this Chapter	251
35.2 What You Need to Know	251
35.3 Ping & TraceRoute & Nslookup	252
Chapter 36	
Troubleshooting.....	253
36.1 Power, Hardware Connections, and LEDs	253
36.2 VMG Access and Login	254
36.3 Internet Access	255
36.4 Wireless Internet Access	257
36.5 USB Device Connection	258
36.6 UPnP	258
Part III: Appendices	259
Appendix A Customer Support	260
Appendix B Wireless LANs.....	266
Appendix C IPv6.....	279
Appendix D Services.....	287
Appendix E Legal Information	291
Index	299

PART I

User's Guide

CHAPTER 1

Introducing the VMG

1.1 Overview

The VMG is a wireless VDSL router. It has a DSL port as well as a Ethernet WAN port for Internet access. The VMG supports both Packet Transfer Mode (PTM) and Asynchronous Transfer Mode (ATM). It is backward compatible with ADSL, ADSL2 and ADSL2+ in case VDSL is not available. The VMG also acts as an IEEE 802.11 b/g/n access point.

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

The VMG works over the analog telephone system, POTS (Plain Old Telephone Service). The VMG has one USB port for sharing files via a USB storage device or connecting a cellular dongle for a WAN backup connection.

Note: Cellular networks refer to 3G only at the time of writing.

Note: See the product page on Zyxel's website for the list of compatible cellular USB dongles.

1.2 Ways to Manage the VMG

Use any of the following methods to manage the VMG.

- Web Configurator. This is recommended for everyday management of the VMG using a (supported) web browser.

1.3 Good Habits for Managing the VMG

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

1.4 Applications for the VMG

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

1.4.1 Internet Access

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

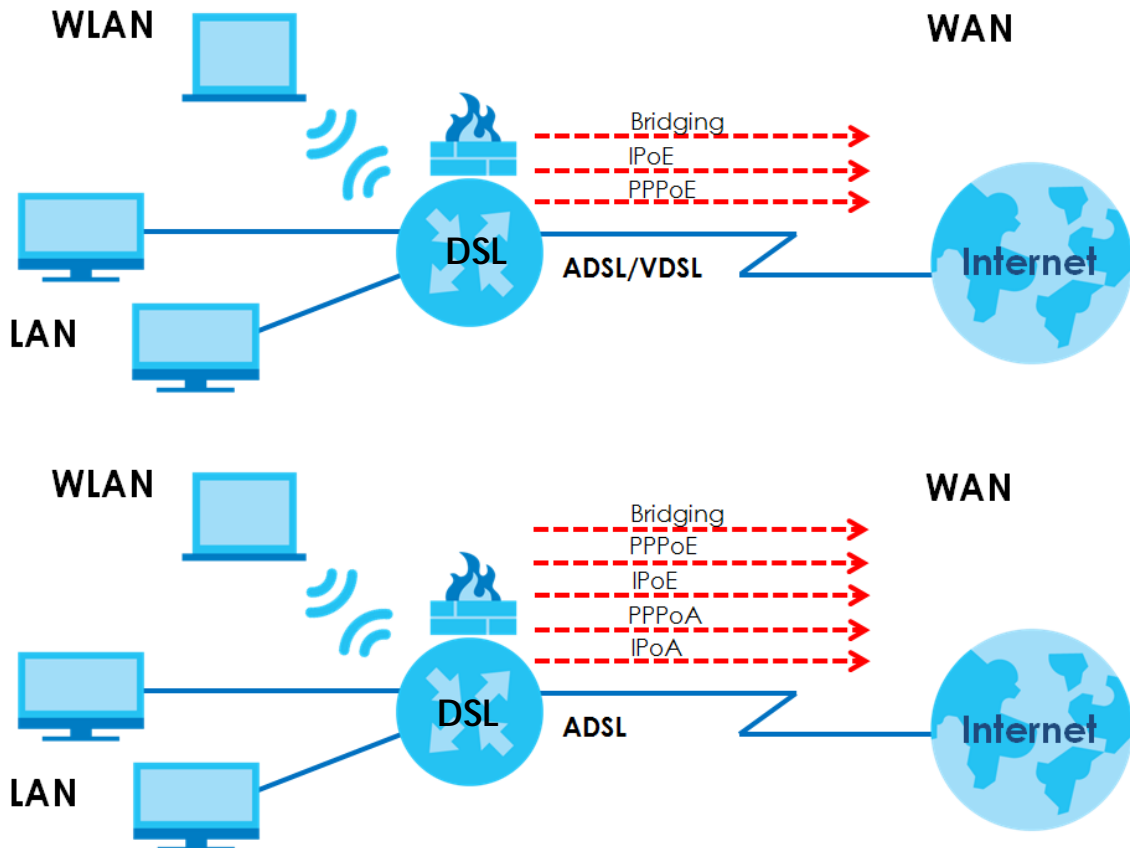
You can also configure IP filtering on the VMG for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you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

1.4.1.1 DSL

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

Note: The ADSL and VDSL lines share the same WAN (layer-2) interfaces that you configure in the VMG. Refer to [Section 6.2 on page 74](#) for the **Network Setting > Broadband** screen.

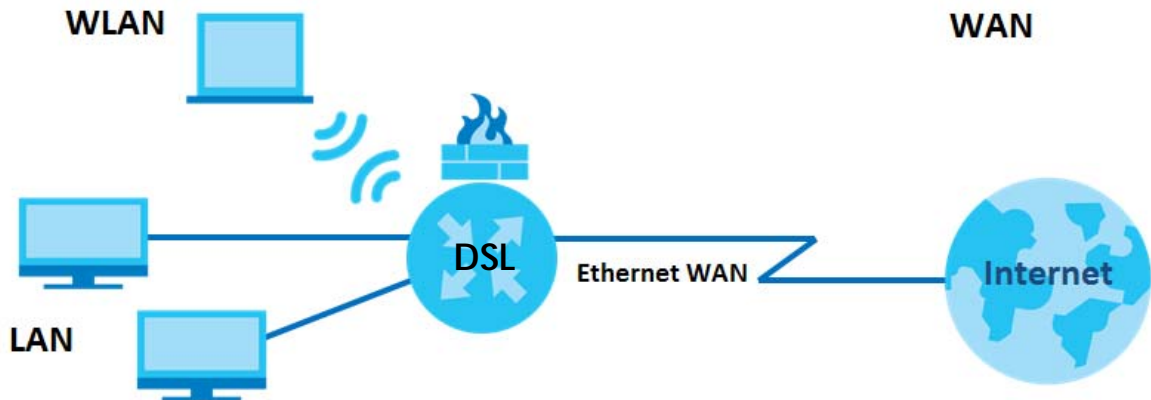
Figure 1 VMG's Internet Access Application: DSL



1.4.1.2 Ethernet WAN

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

Figure 2 VMG's Internet Access Application: Ethernet WAN



1.4.2 VMG's USB Support

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

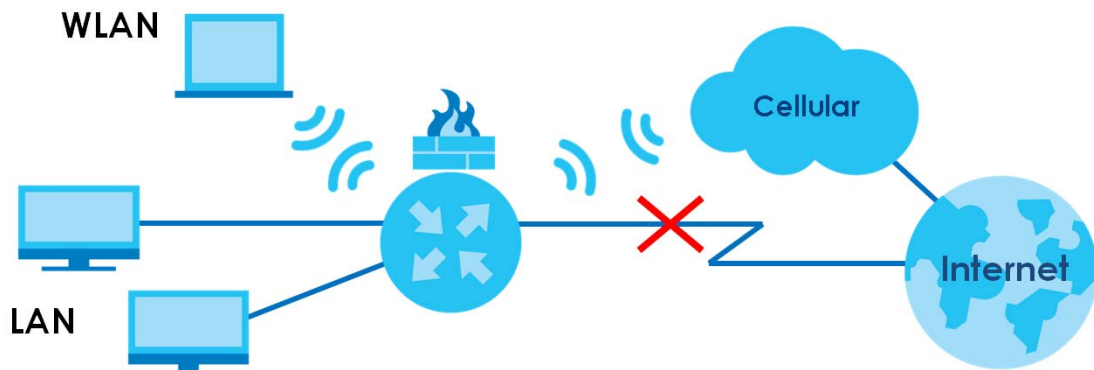
Cellular WAN (3G) Backup

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

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

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

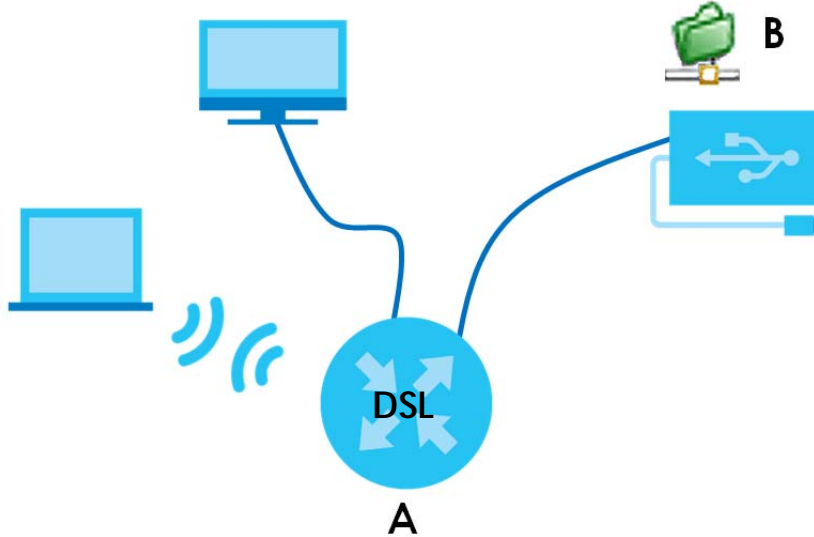
Figure 3 VMG's Internet Access Application: Cellular WAN



File Sharing

Use the built-in USB 2.0 port to share files on a USB memory stick or a USB hard drive (B). Use FTP to access the files on the USB device.

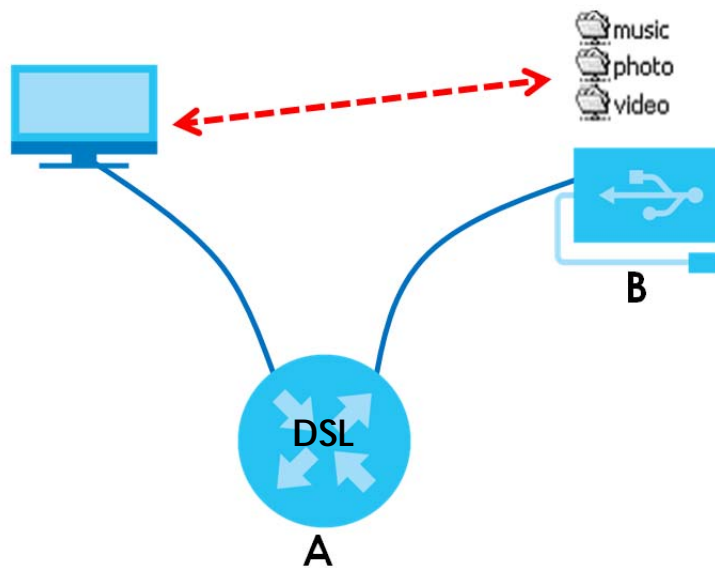
Figure 4 USB File Sharing Application



Media Server

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

Figure 5 USB Media Server Application



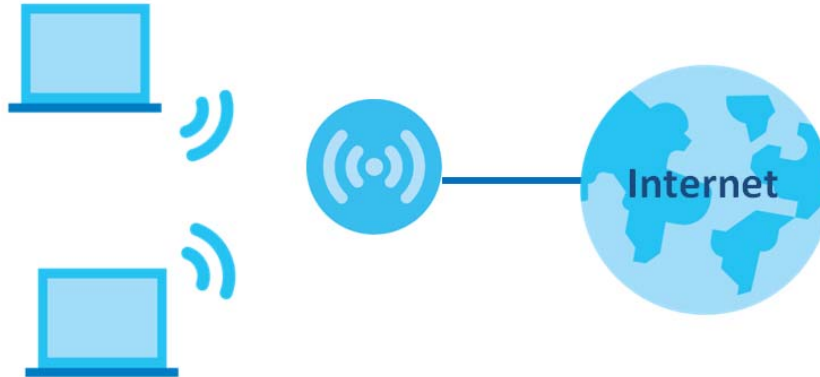
1.5 Wireless Access

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

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

See [Section 1.6.4 on page 23](#) for more information about how to set up a wireless network with WLAN and WPS buttons.

Figure 6 Wireless Access Example



1.6 Hardware

1.6.1 Front Panel

The following graphic displays the front panel of the VMG.

Figure 7 VMG3312-T20A Front Panel



1.6.2 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 8 LEDs on the VMG



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

Table 1 LED Descriptions









LED	COLOR	STATUS	DESCRIPTION
 POWER	Green	On	The VMG is receiving power and ready for use.
		Blinking	The VMG is self-testing.
	Red	On	The VMG detected an error while self-testing, or there is a device malfunction.
		Off	The VMG is not receiving power.
 ETHERNET1~4	Green	On	The VMG has a successful 10/100 Mbps Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The VMG is sending or receiving data to/from the LAN at 10/100 Mbps.
		Off	The VMG does not have an Ethernet connection with the LAN.
 WLAN	Green	On	The wireless network is activated.
		Blinking	The VMG is communicating with wireless clients.
 WPS	Orange	Blinking	The VMG is setting up a WPS connection with a wireless client.
		Off	The wireless network is not activated.

Table 1 LED Descriptions (continued)

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

1.6.3 Side Panels

The following graphics display the side panels of the VMG.

Figure 9 VMG3312-T20A Side Panel



Figure 10 VMG3312-T20A Side Panel



The following table describes the items on the side panels..

Table 2 Side Panel Buttons

LABEL	DESCRIPTION
WLAN	Press the WLAN button for more than two seconds to enable the wireless function.
WPS	Press the WPS button for more than five seconds to quickly set up a secure wireless connection between the device and a WPS-compatible client.

Table 2 Side Panel Buttons (continued)

LABEL	DESCRIPTION
Power Button	Press the power button after the power cable is connected to start the device.
USB	The USB port is used for cellular WAN backup, file-sharing and media server.

1.6.4 Using the WLAN and WPS Buttons

If the wireless network is turned off, press the **WLAN** button for more than two seconds. Once the **WLAN** LED turns green, the wireless network is active.

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

To turn off the wireless network, press the **WLAN** button for more than two seconds. The **WLAN** LED turns off when the wireless network is off.

1.6.5 Rear Panel

The following graphic displays the rear panel of the VMG.

Figure 11 VMG3312-T20A Rear Panel



The following table describes the items on the rear panel..

Table 3 Rear Panel Ports

LABEL	DESCRIPTION
Power	Connect the power cable and press the power button to start the device.
Reset	Press the button to return theVMG to the factory defaults.
LAN1 ~ LAN4	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
WAN	Connect an Ethernet cable to the Ethernet WAN port for Internet access.
DSL	Connect a RJ-11 cable to the DSL port for Internet access.

1.6.6 The RESET Button

If you forget your password or cannot access the Web Configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously. The password will be reset to "1234", and the LAN IP address will be "192.168.1.1".

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button for five 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.

1.6.7 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 4 Wall Mounting Information

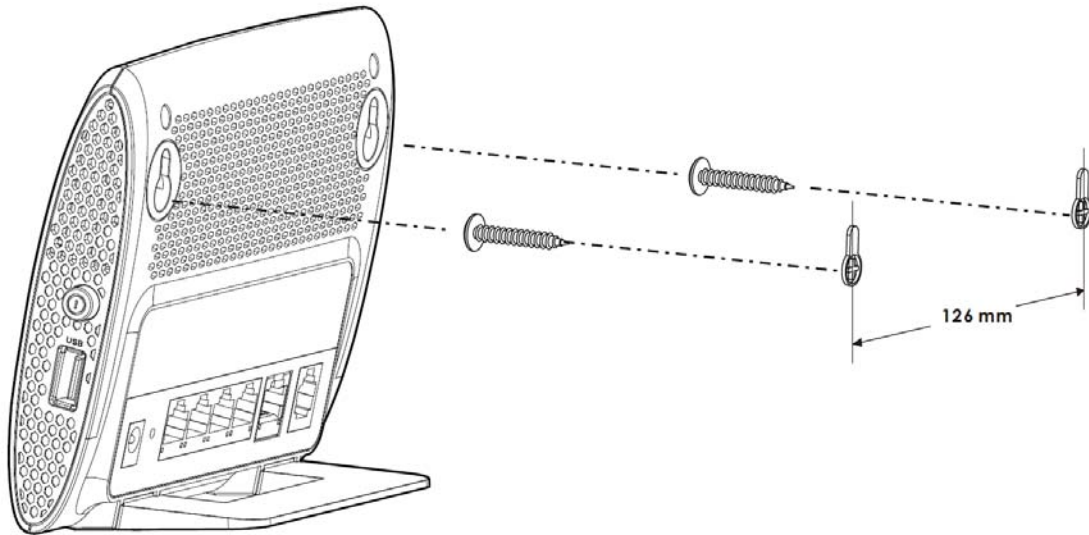
Distance between holes	126 mm
M4 Screws	Two
Screw anchors (optional)	Two

- 3 Select a position free of obstructions on a wall strong enough to hold the weight of the device.
- 4 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 5 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.
If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.
- 6 Make sure the screws are fastened well enough to hold the weight of the VMG with the connection cables.
- 7 Align the holes on the back of the VMG with the screws on the wall. Hang the VMG on the screws.

Figure 12 Wall Mounting Example



CHAPTER 2

The Web Configurator

2.1 Overview

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

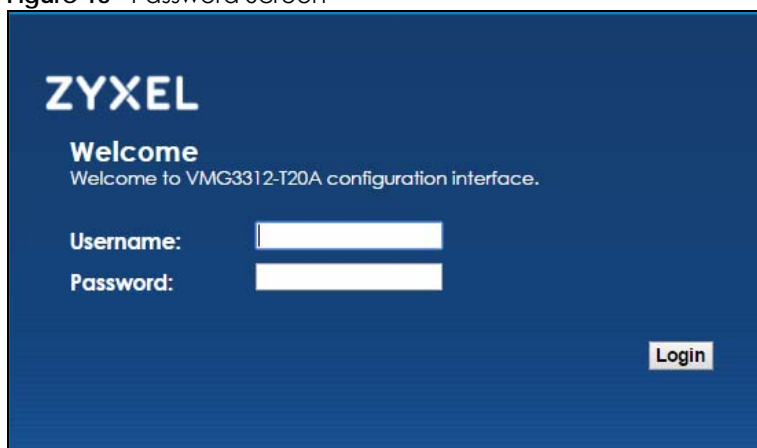
In order to use the web configurator you need to allow:

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

2.1.1 Accessing the Web Configurator

- 1 Make sure your VMG hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser. If the VMG does not automatically re-direct you to the login screen, go to <http://192.168.1.1>.
- 3 A password screen displays. To access the administrative web configurator and manage the VMG, type the default username **admin** and password **1234** in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**.

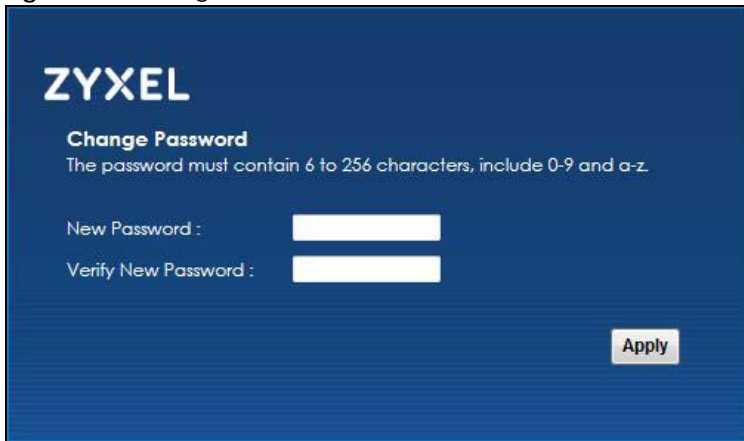
Figure 13 Password Screen



The screenshot shows a dark blue login screen with the ZYXEL logo at the top left. Below the logo, it says "Welcome" and "Welcome to VMG3312-T20A configuration interface." There are two white input fields: one for "Username:" and one for "Password:". A "Login" button is located in the bottom right corner of the form area.

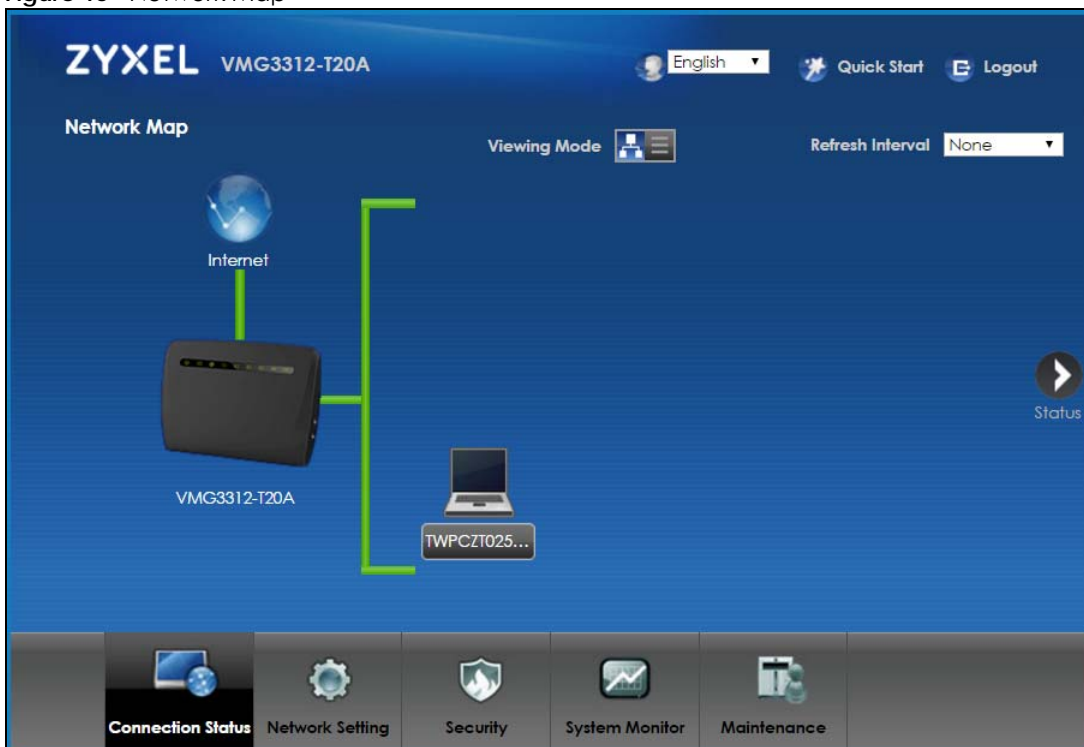
- 4 The following screen displays if you have not yet changed your password. Enter a new password, retype it to confirm and click **Apply**.

Figure 14 Change Password Screen



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

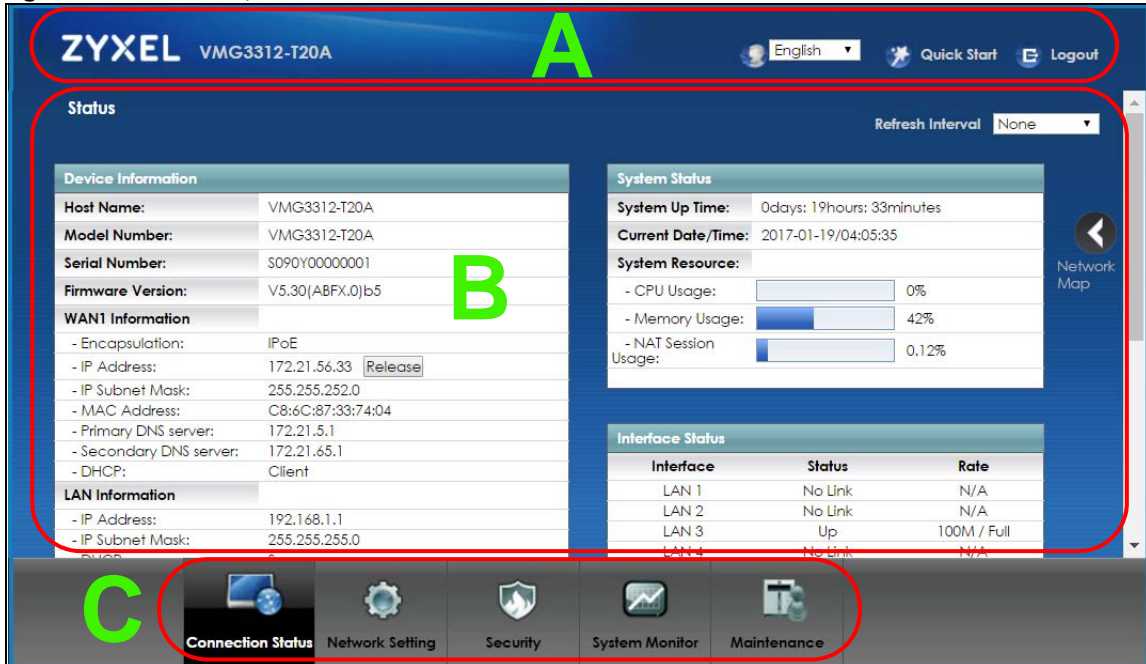
Figure 15 Network Map



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

2.2 Web Configurator Layout

Figure 16 Screen Layout

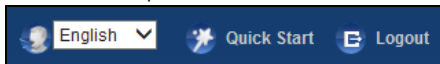


As illustrated above, the main screen is divided into these parts:

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

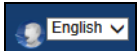
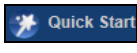

2.2.1 Title Bar

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



The icons provide the following functions.

Table 5 Web Configurator Icons in the Title Bar

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

2.2.2 Main Window

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

After you click the right arrow icon on the **Connection Status (Network Map)** page, the **Status** screen is displayed. See [Chapter 5 on page 67](#) for more information about the **Status** screen.

2.2.3 Navigation Panel

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

Table 6 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the VMG and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.
	Cellular Backup	Use this screen to configure cellular WAN connection.
	Advanced	Use this screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions.
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the VMG.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the VMG.
	WPS	Use this screen to configure and view your WPS (Wi-Fi Protected Setup) settings.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Others	Use this screen to configure advanced wireless settings.
	Channel Status	Use this screen to scan wireless LAN channel noises and view the results.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	STB Vendor ID	Use this screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the VMG automatically create static DHCP entries for the STB devices when they request IP addresses.
	Wake on LAN	Use this screen to remotely turn on a device on the local network.
	TFTP Server Name	Configure a TFTP server name which is sent to clients using DHCP option 66.
Routing	Static Route	Use this screen to view and set up static routes on the VMG.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s).
	Policy Route	Use this screen to configure policy routing on the VMG.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.

Table 6 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Classification Setup	Use this screen to define a classifier.
	Shaper Setup	Use this screen to limit outgoing traffic rate on the selected interface.
	Policer Setup	
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Applications	Use this screen to configure servers behind the VMG.
	Port Triggering	Use this screen to change your VMG's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen.
	ALG	Use this screen to enable or disable SIP ALG.
	Address Mapping	Use this screen to change your VMG's address mapping settings.
	Sessions	Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the VMG.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Interface Grouping	Interface Grouping	Use this screen to map a port to a PVC or bridge group.
USB Service	File Sharing	Use this screen to enable file sharing via the VMG.
	Media Server	Use this screen to use the VMG as a media server.
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the VMG.
Parental Control	Parental Control	Use this screen to block web sites with the specific URL.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		

Table 6 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Log	System Log	Use this screen to view the status of events that occurred to the VMG. You can export or e-mail the logs.
	Security Log	Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window. Levels include: <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Categories include: <ul style="list-style-type: none"> • Account • Attack • Firewall • MAC Filter
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the VMG.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the VMG.
	NAT	Use this screen to view NAT statistics for connected hosts.
ARP table	ARP table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table on the VMG.
xDSL Statistics	xDSL Statistics	Use this screen to view the VMG's xDSL traffic statistics.
Cellular Statistics	Cellular Statistics	Use this screen to look at cellular Internet connection status.
Maintenance		
System	System	Use this screen to set Device name and Domain name.
User Account	User Account	Use this screen to change user password on the VMG.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to configure a list of public IP addresses which are allowed to access the VMG.
SNMP	SNMP	Use this screen to configure SNMP (Simple Network Management Protocol) settings.
Time	Time	Use this screen to change your VMG's time and date.
Email Notification	Email Notification	Use this screen to configure up to two mail servers and sender addresses on the VMG.
Log Setting	Log Setting	Use this screen to change your VMG's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your VMG.
Backup Restore	Backup/Restore	Use this screen to backup and restore your VMG's configuration (settings) or reset the factory default settings.

Table 6 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Reboot	Reboot	Use this screen to reboot the VMG without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the DSL connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems.

CHAPTER 3

Quick Start

3.1 Overview

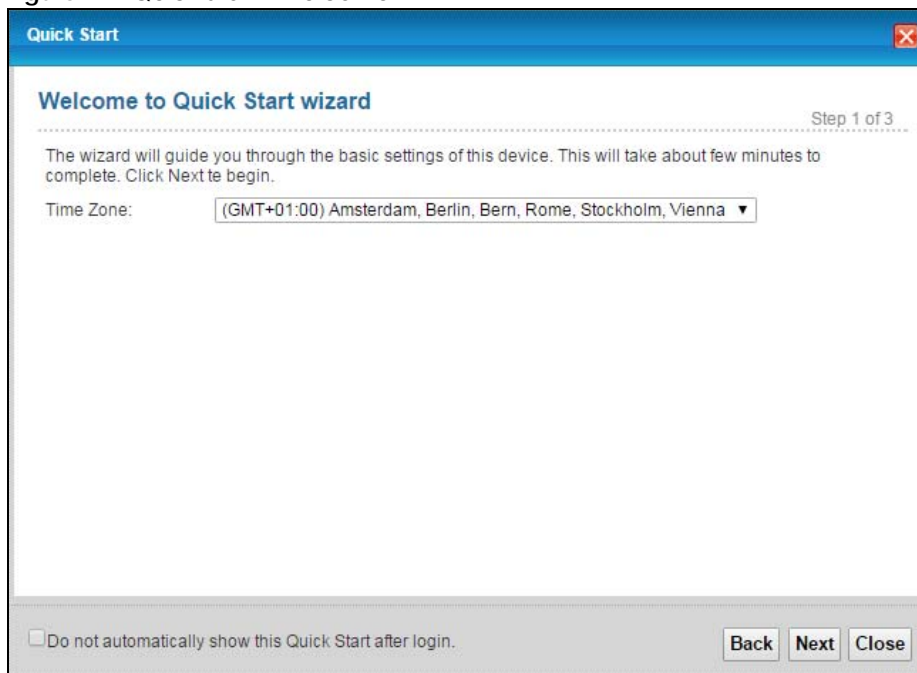
Use the Quick Start screens to configure the VMG's time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on [Chapter 4 on page 36](#)) for background information on the features in this chapter.

3.2 Quick Start Setup

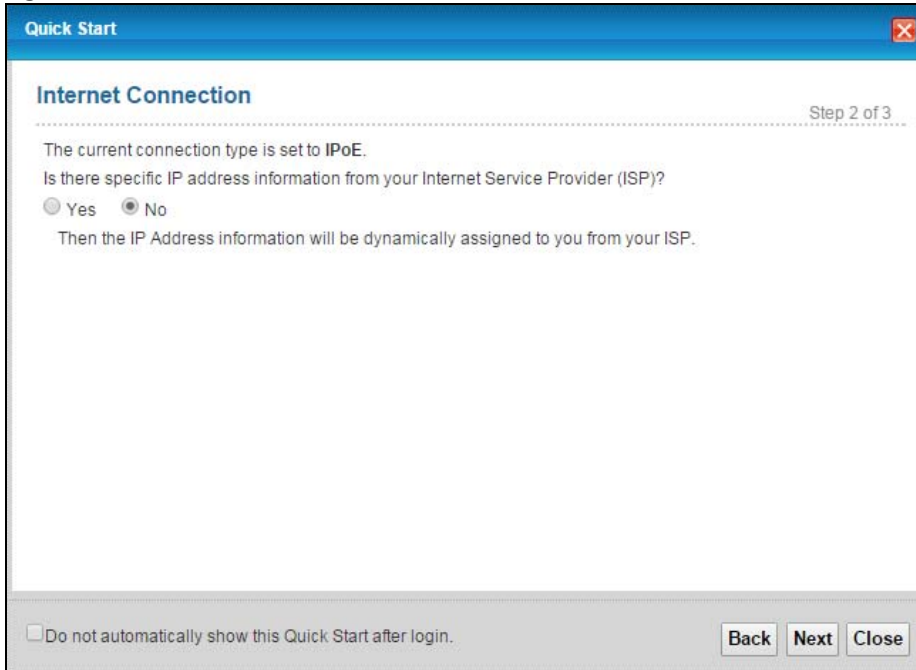
- 1 The Quick Start Wizard appears automatically after login. Or you can click the **Quick Start** icon in the top right corner of the web configurator to open the quick start screens. Select the time zone of your location. Click **Next**.

Figure 17 Quick Start - Welcome



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

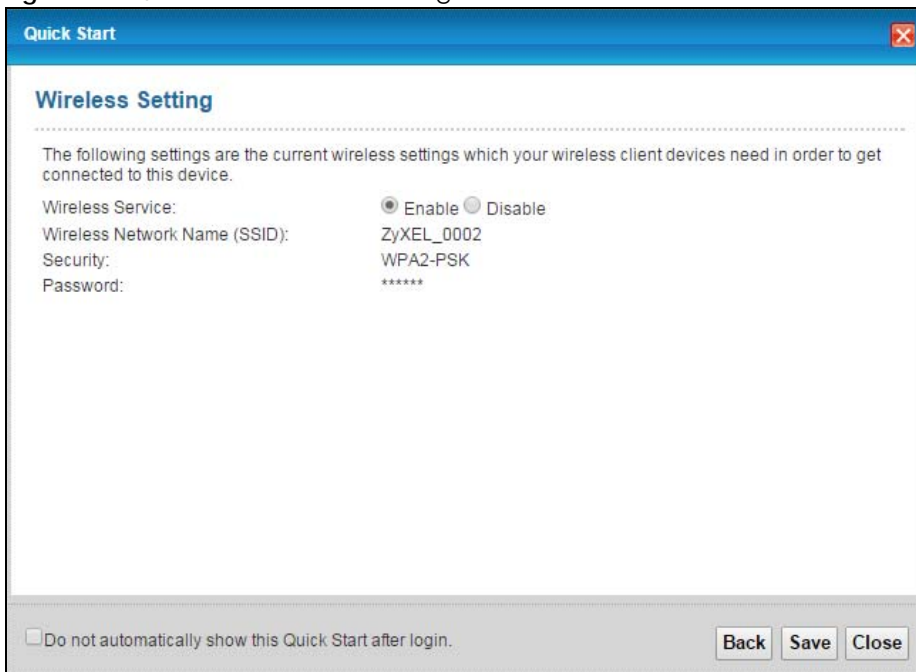
Figure 18 Quick Start - Internet Connection



The screenshot shows a window titled "Quick Start" with a blue header bar. Below the header, the title "Internet Connection" is displayed in blue. In the top right corner, it says "Step 2 of 3". The main content area contains the following text: "The current connection type is set to IPoE." followed by the question "Is there specific IP address information from your Internet Service Provider (ISP)?". Below this question are two radio buttons: "Yes" (unselected) and "No" (selected). Underneath, it states "Then the IP Address information will be dynamically assigned to you from your ISP." At the bottom of the window, there is a checkbox labeled "Do not automatically show this Quick Start after login." and three buttons: "Back", "Next", and "Close".

- 3 Turn the wireless LAN on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the VMG. Click **Save**.

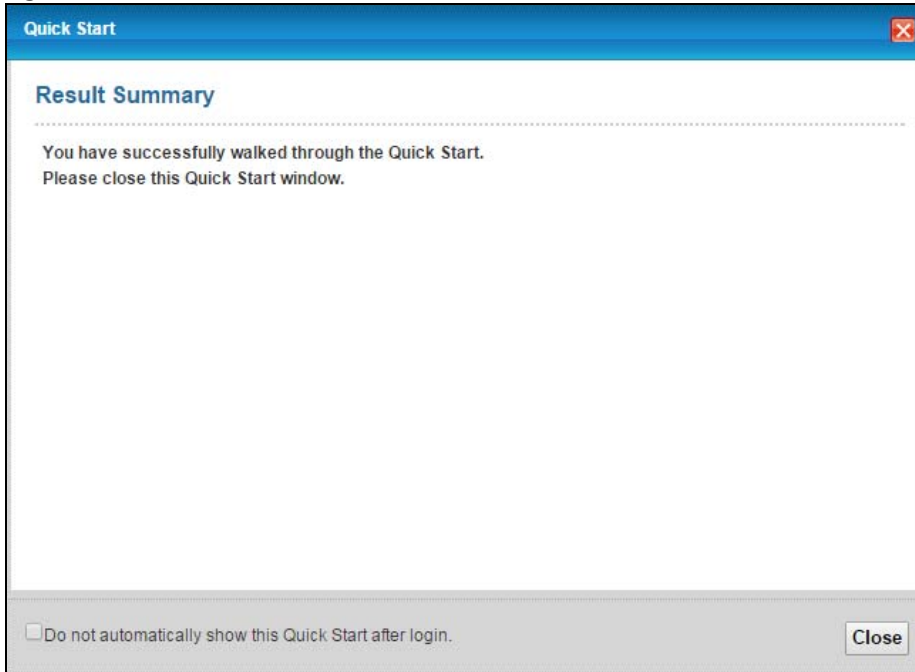
Figure 19 Quick Start - Wireless Setting



The screenshot shows a window titled "Quick Start" with a blue header bar. Below the header, the title "Wireless Setting" is displayed in blue. In the top right corner, it says "Step 2 of 3". The main content area contains the following text: "The following settings are the current wireless settings which your wireless client devices need in order to get connected to this device." Below this text are four settings: "Wireless Service:" with radio buttons for "Enable" (selected) and "Disable" (unselected); "Wireless Network Name (SSID):" with the value "ZyXEL_0002"; "Security:" with the value "WPA2-PSK"; and "Password:" with the value "*****". At the bottom of the window, there is a checkbox labeled "Do not automatically show this Quick Start after login." and three buttons: "Back", "Save", and "Close".

- 4 Your VMG saves your settings and attempts to connect to the Internet. Click **Close** to complete the setup.

Figure 20 Quick Start - Result Summary



CHAPTER 4

Tutorials

4.1 Overview

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

- [Setting Up an ADSL PPPoE Connection](#), see page 36
- [Setting Up a Secure Wireless Network](#), see page 39
- [Setting Up Multiple Wireless Groups](#), see page 44
- [Using the File Sharing Feature](#), see page 48
- [Using the Media Server Feature](#), see page 51
- [Configuring Static Route for Routing to Another Network](#), see page 55
- [Configuring QoS Queue and Class Setup](#), see page 58
- [Access the VMG Using DDNS](#), see page 61
- [Configuring the MAC Address Filter](#), see page 62
- [Access Your Shared Files From a Computer](#), see page 63

4.2 Setting Up an ADSL PPPoE Connection

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

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

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

#	Name	Type	Mode	Enc...	802.1p	802.1q	Igm...	NAT	Defa...	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
2	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	

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

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

- 3 Select **Enable** in the **Active** field. Enter the **General** and **ATM PVC Configuration** settings as provided above.

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

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

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

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

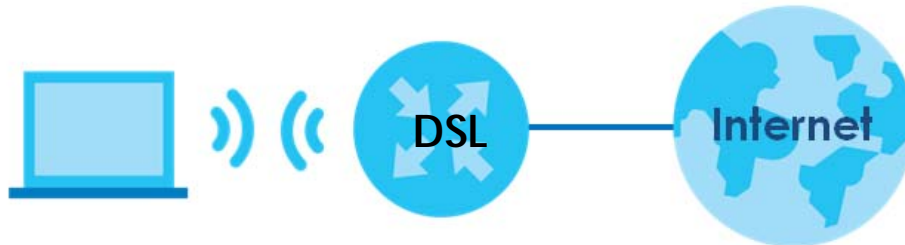
8 You should see a summary of your new DSL connection setup in the **Broadband** screen as follows.

Add New WAN Interface												
#	Name	Type	Mode	Encap...	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	Y	N	
2	MyDS...	ATM	Routing	PPPoE	N/A	N/A	Y	Y	Y	N	N	
3	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	Y	N	

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

4.3 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the VMG 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 VMG. Then he can set up a wireless network using WPS ([Section 4.3.2 on page 41](#)) or manual configuration ([Section 4.3.3 on page 44](#)).

4.3.1 Configuring the Wireless Network Settings

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

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

- 1 Click **Network Setting** > **Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see [page 39](#)). Click **Apply**.

Wireless Network Setup

Band: 2.4GHz ▾

Wireless: Enable Disable (Settings are invalid when disabled)

Channel: Auto ▾ Current : 11

Bandwidth: 20MHz ▾

Control Sideband: None ▾

Wireless Network Settings

Wireless Network Name: Example

Max Clients: 32

Hide SSID

Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Note

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

BSSID: E8:37:7A:9D:1F:A3

Security Level

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

Security Mode: WPA2-PSK ▾

Generate password automatically

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

Password:

password unmask

[more...](#)

Apply **Cancel**

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

RTS/CTS Threshold: 2347

Fragmentation Threshold: 2346

Output Power: 100% ▾

Beacon Interval: 100 ms

DTIM Interval: 1 ms

802.11 Mode: 802.11b/g/n Mixed ▾

802.11 Protection: Off ▾

Preamble: Long ▾

OBSS Coexistence: Enable Disable

Apply **Cancel**

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the VMG (see [Section 4.3.2 on page 41](#)). He can also use the notebook's wireless client to search for the VMG (see [Section 4.3.3 on page 44](#)).

4.3.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the VMG 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 VMG. A wireless client must also use the same PIN in order to download the wireless network settings from the VMG.

Push Button Configuration (PBC)

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

General

WPS Enable Disable (settings are invalid when disabled)

Add a new device with WPS Method

Method 1	Method 2	Method 3
<input checked="" type="radio"/> Enable <input type="radio"/> Disable PBC	<input checked="" type="radio"/> Enable <input type="radio"/> Disable PIN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Step 1. Click WPS button WPS Step 2. Press the WPS button on your new wireless client device within 120 seconds	Step 1. Enter the PIN of your new wireless client device and then click Register <input type="text"/> Enter PIN here <input type="button" value="Register"/> Step 2. Press the WPS button on your new wireless client device within 120 seconds	Enter AP's PIN Number in Wireless Client Current state: Configured 1. Please release configuration if you want to configure the wireless settings <input type="button" value="Release Configuration"/> 2. Enter current PIN number on your wireless client <input type="button" value="Generate New PIN"/>

Note

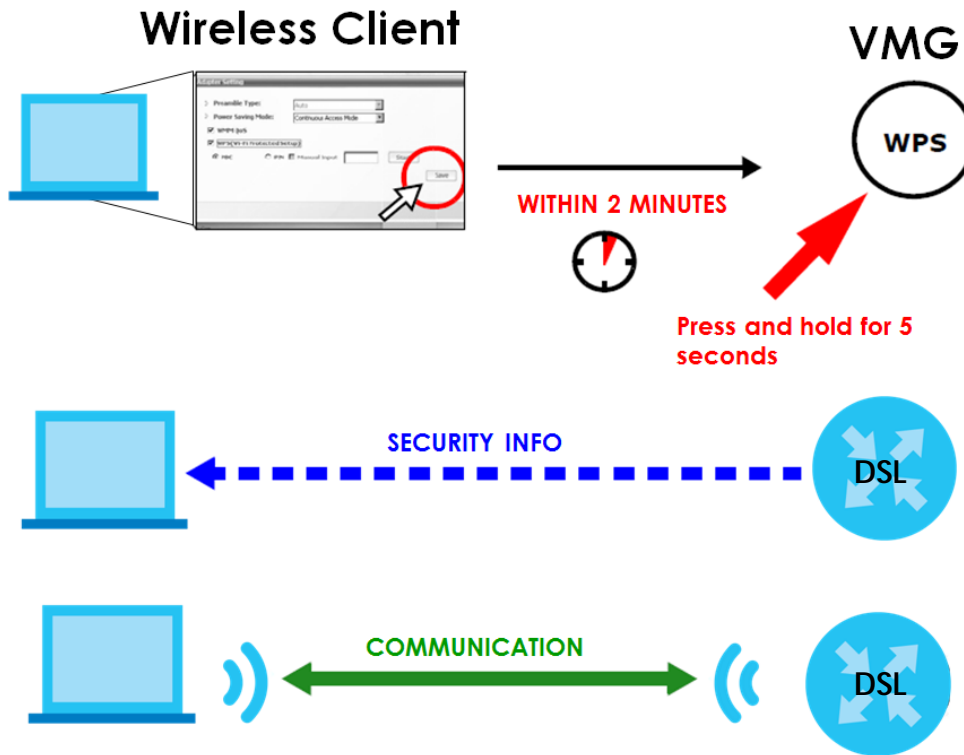
- 1.If WPS is Enabled, UPnP will automatically be turned on.
- 2.This feature is available only when WPA2-PSK or No Security mode is configured.

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

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

The VMG 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 VMG 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 VMG and wireless client.



PIN Configuration

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

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

General

WPS Enable Disable (settings are invalid when disabled)

Add a new device with WPS Method

Method 1	Method 2	Method 3
<input checked="" type="radio"/> Enable <input type="radio"/> Disable PBC	<input checked="" type="radio"/> Enable <input type="radio"/> Disable PIN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<p>Step 1. Click WPS button 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</p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>	<p>Enter AP's PIN Number in Wireless Client</p> <p>Current state: Configured</p> <p>1. Please release configuration if you want to configure the wireless settings</p> <p>Release Configuration</p> <p>2. Enter current PIN number on your wireless client</p> <p>Generate New PIN</p>

Note

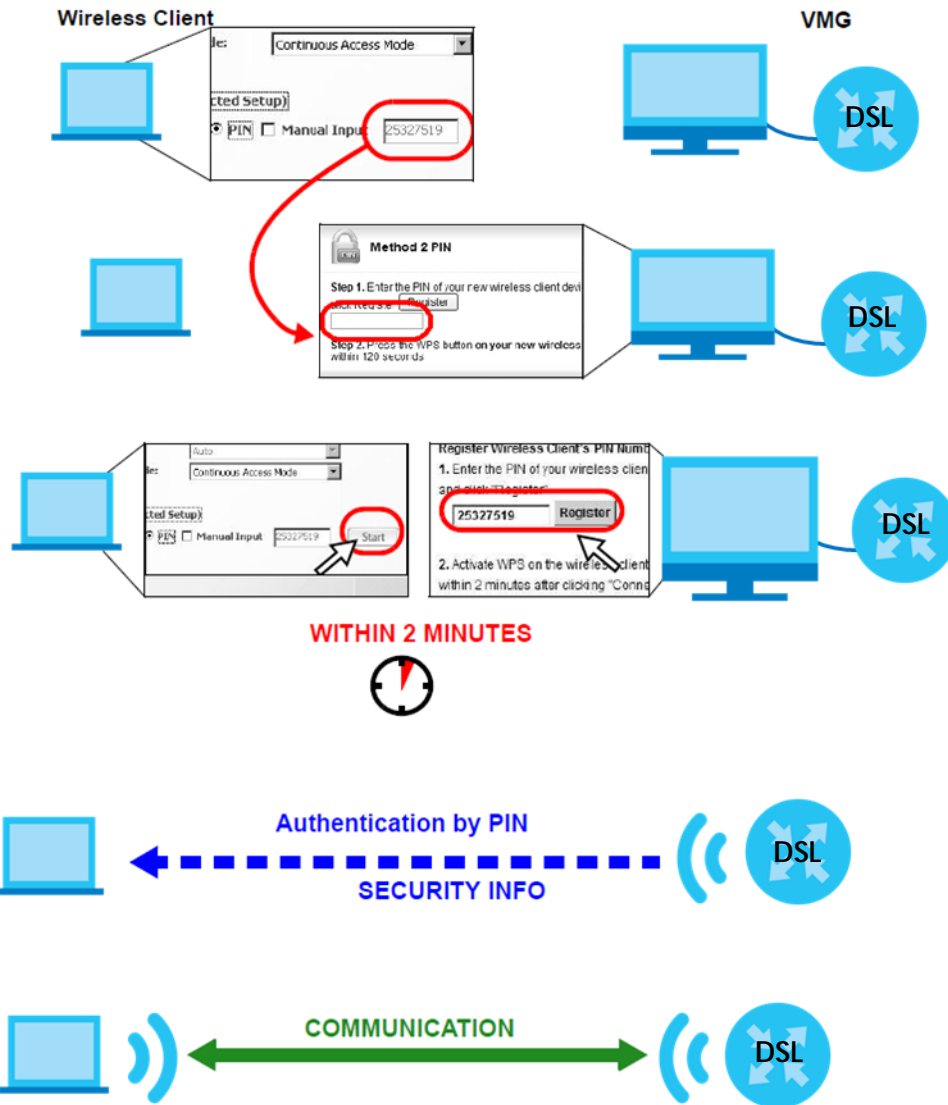
- If WPS is Enabled, UPnP will automatically be turned on.
- This feature is available only when WPA2-PSK or No Security mode is configured.

Apply **Cancel**

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

The VMG 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 VMG securely.

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



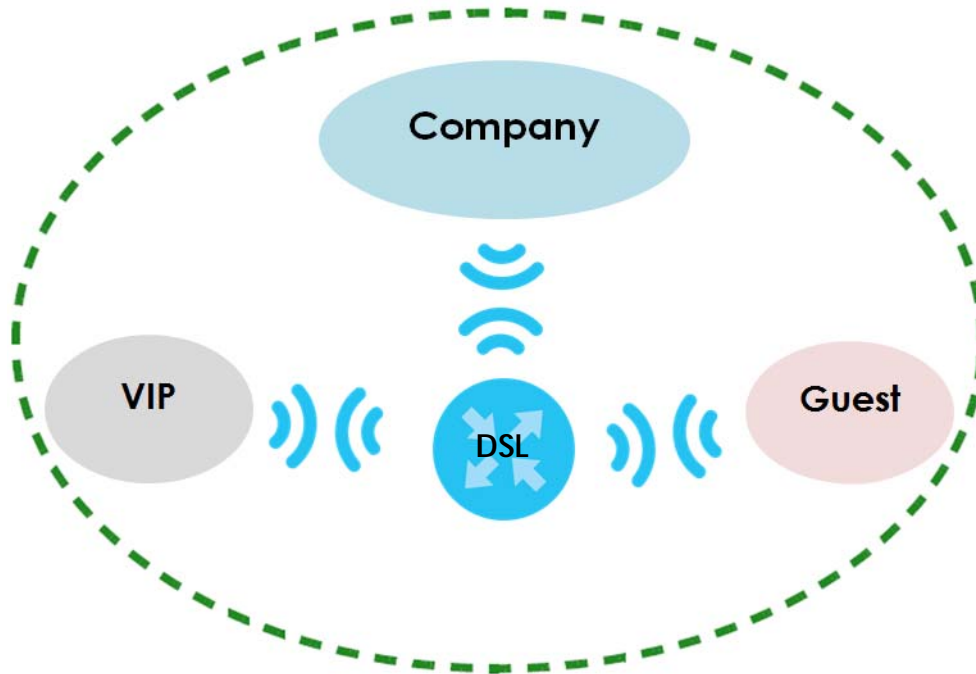
4.3.3 Without WPS

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

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

4.4 Setting Up Multiple Wireless Groups

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



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

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

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

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

Wireless Network Setup

Band: 2.4GHz

Wireless: Enable Disable (Settings are invalid when disabled)

Channel: Auto | Current : 11

Bandwidth: 20MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name:

Max Clients:

Hide SSID

Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Note

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

BSSID: E8:37:7A:9D:1F:A3

Security Level

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

Security Mode: WPA2-PSK

Generate password automatically

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

Password:

password unmask

[more...](#)

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

#	Status	SSID	Security	Guest WLAN	Modify
1		ZyXEL000001_Guest1	Mixed WPA2-PSK/WPA-PSK	External Guest	
2		ZyXEL000001_Guest2	Mixed WPA2-PSK/WPA-PSK	N/A	
3		ZyXEL000001_Guest3	Mixed WPA2-PSK/WPA-PSK	N/A	

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

Wireless Network Setup

Wireless Enable Disable (Settings are invalid when disabled)

Wireless Network Settings

Wireless Network Name

Hide SSID

Guest WLAN

Access Scenario: External Guest ▼

Max. Upstream Bandwidth Kbps

Max. Downstream Bandwidth Kbps

Note:

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

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

SSID Subnet: Enable Disable

Security Level

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

Security Mode WPA2-PSK

Generate password automatically

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

Password

password unmask

[more...](#)

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

Wireless Network Setup

Wireless Enable Disable (Settings are invalid when disabled)

Wireless Network Settings

Wireless Network Name Hide SSID

Guest WLAN

Access Scenario:

Max. Upstream Bandwidth Kbps

Max. Downstream Bandwidth Kbps

Note:

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

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

SSID Subnet: Enable Disable

Security Level

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

Security Mode Generate password automatically

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

Password password unmask

[more...](#)

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

#	Status	SSID	Security	Guest WLAN	Modify
1		ZyXEL000001_Guest1	Mixed WPA2-PSK/WPA-PSK	N/A	
2		VIP	Mixed WPA2-PSK/WPA-PSK	External Guest	
3		Guest	Mixed WPA2-PSK/WPA-PSK	External Guest	

4.5 Using the File Sharing Feature

In this section you can:

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

4.5.1 Set Up File Sharing

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

Before enabling file sharing in the VMG, please set up your shares beforehand in the USB. Also, the following special characters are not allowed for the USB share name: ", ' , ` , < , > , ^ , \$, | , & , ; , \ , / , : , * , and ?.

4.5.1.1 Activate File Sharing

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

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

Information

Volume	Capacity	Used Space
usb2_sda1	30111 MB	2964 MB

Server Configuration

File Sharing Services: Enable Disable

Share Directory List

Add New Share

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

Account Management

Add New User

Status	User Name
	admin
	user

Apply

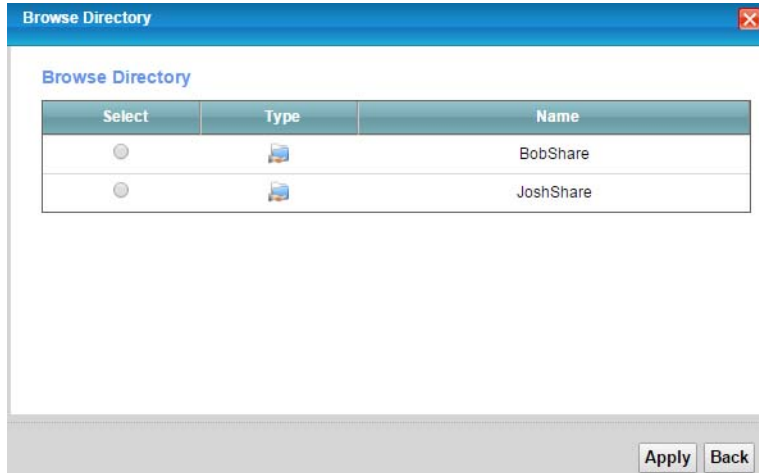
Cancel

4.5.1.2 Set up File Sharing on Your VMG

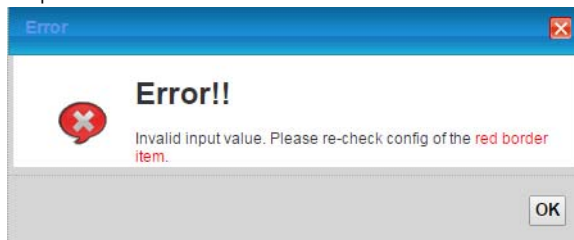
You also need to set up file sharing on your VMG in order to share files.

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

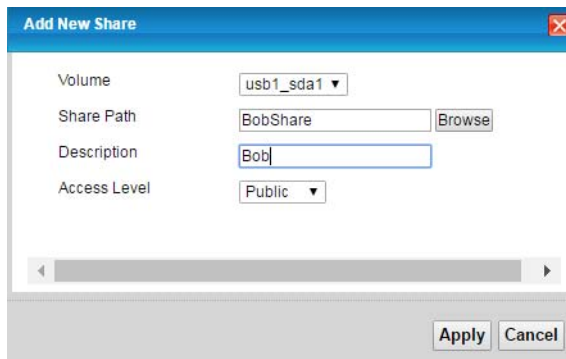
If the share names include the following special characters: ", ' , ` , < , > , ^ , \$, | , & , ; , \ , / , : , * , and ? , the



following screen will appear. To avoid this, please correct your share names in the USB, and repeat the steps above.



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



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

Share Directory List

Active	Status	Share Name	Share Path	Share Description	Modify
<input checked="" type="checkbox"/>		BobShare	/mnt/usb1_sda1/BobShare	Bob	
<input checked="" type="checkbox"/>		JoshShare	/mnt/usb1_sda1/JoshShare	Josh	




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

Please see Chapter 29 on page 225, for detailed information about User Account screen.

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

Account Management

Add New User

Status	User Name
	admin
	Zyxel
	user

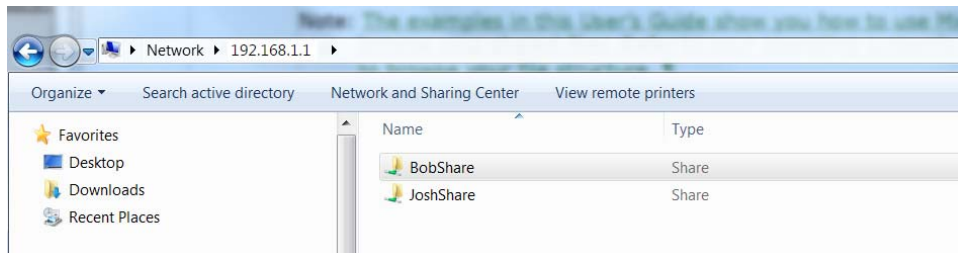
4.5.2 Access Your Shared Files From a Computer

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

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

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

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



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

4.6 Using the Media Server Feature

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

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

- Microsoft (MS) Windows Media Player
Media Server works with Windows 7. Make sure your computer is able to play media files (music, videos and pictures).

- Zyxel DMA-2500, a digital media adapter
You need to set up the DMA-2500 to work with your television (TV). Refer to the DMA-2500 Quick Start Guide for the correct hardware connections.

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

4.6.1 Configuring the VMG

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

Media Server: Enable Disable

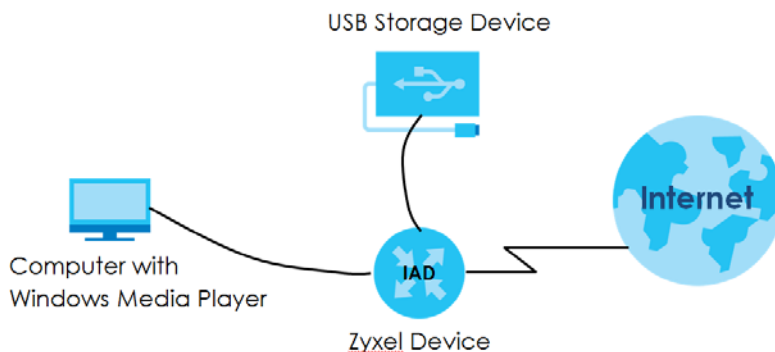
Interface:

Media Library Path:

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

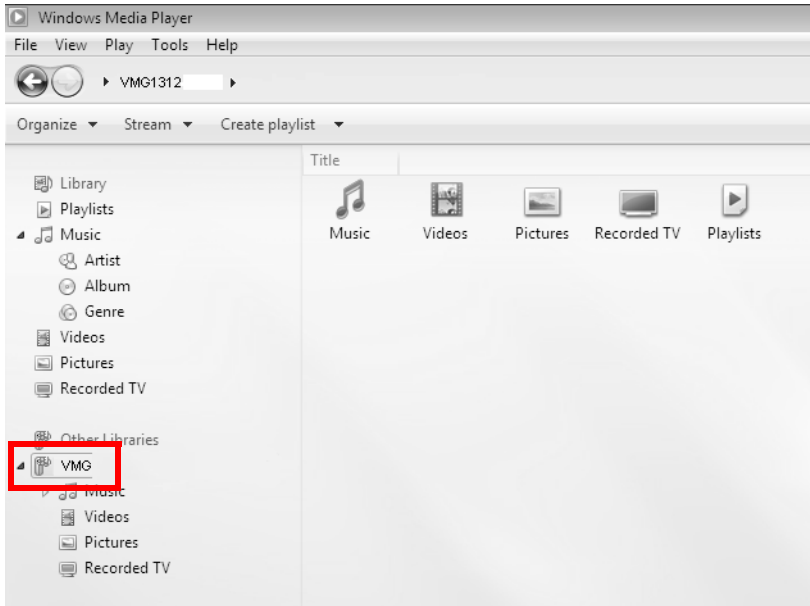
4.6.2 Using Windows Media Player

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

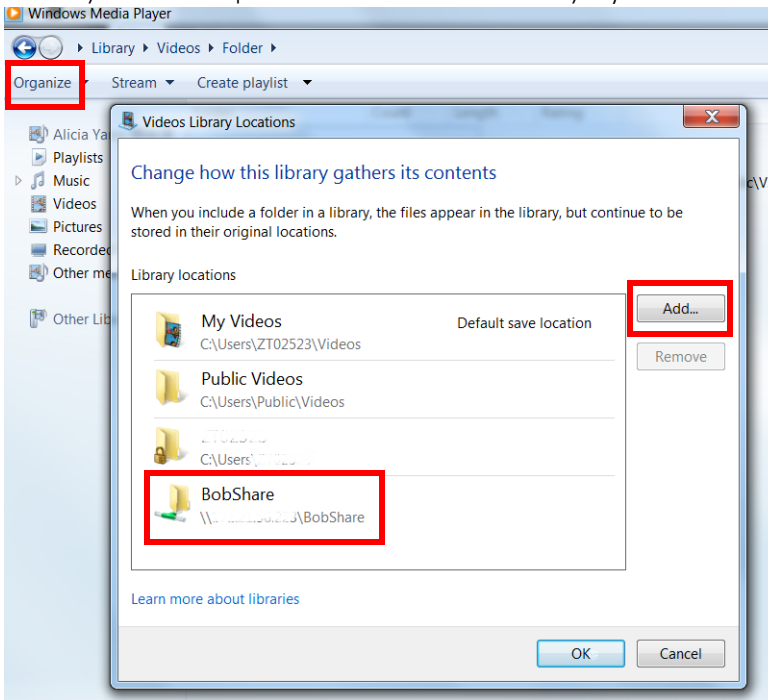


Windows 7

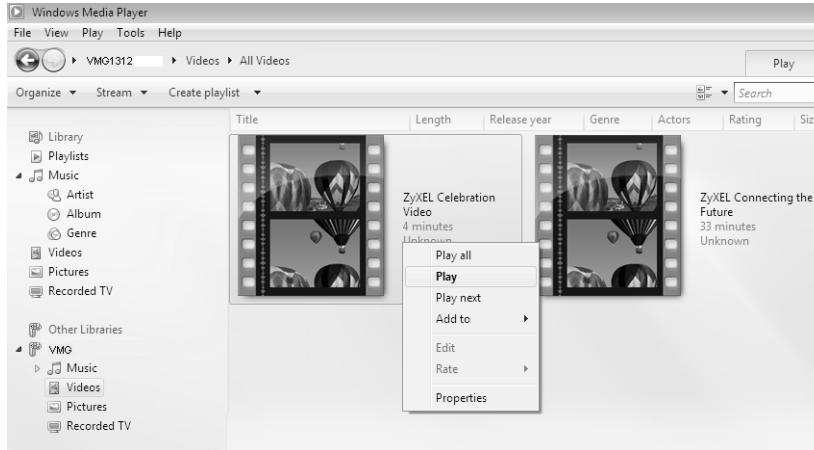
- 1 Open Windows Media Player. It should automatically detect the VMG.



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



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

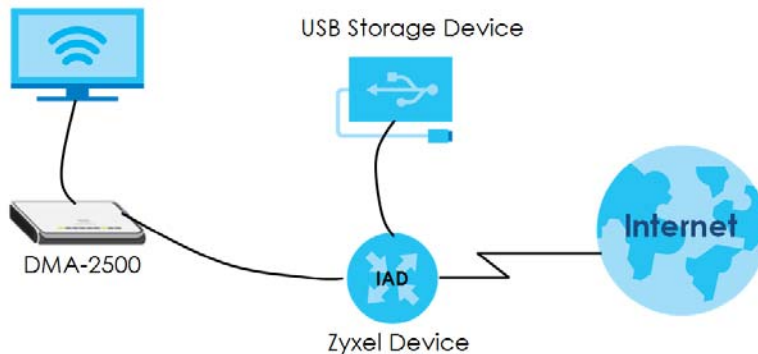


4.6.3 Using a Digital Media Adapter

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

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

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



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



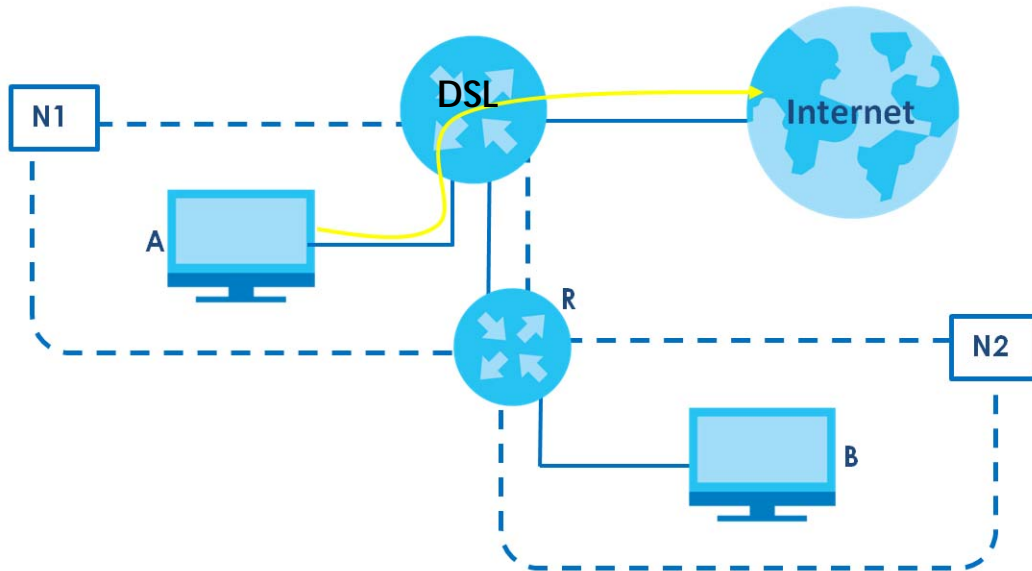
- 3 The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button in the remote control.



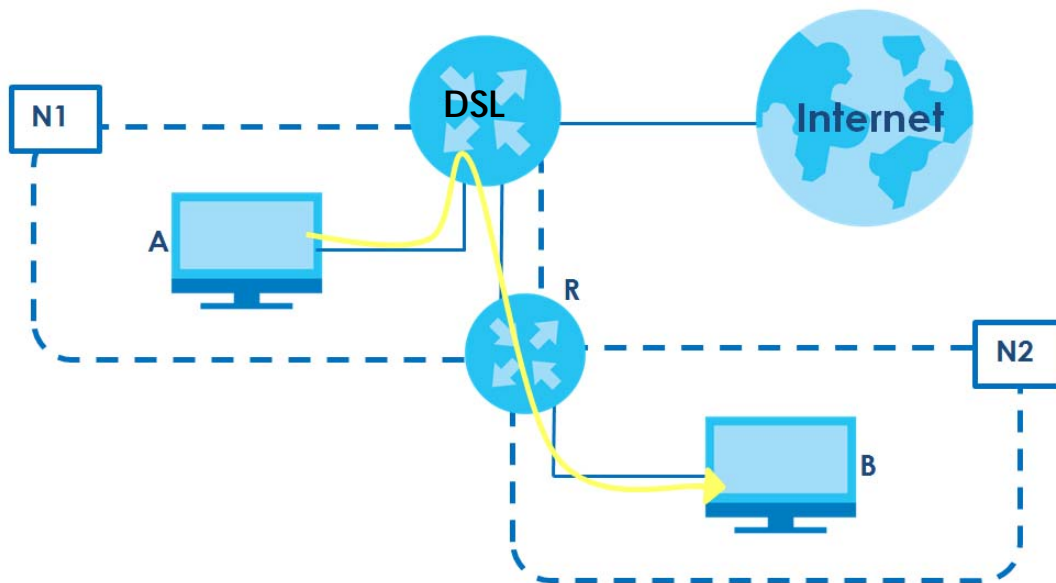
4.7 Configuring Static Route for Routing to Another Network

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



This tutorial uses the following example IP settings:

Table 7 IP Settings in this Tutorial

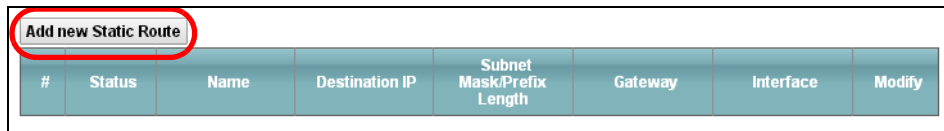
DEVICE / COMPUTER	IP ADDRESS
The VMG's WAN	172.16.1.1
The VMG's LAN	192.168.1.1
IP Type	IPv4
Use Interface	VDSL
A	192.168.1.34

Table 7 IP Settings in this Tutorial

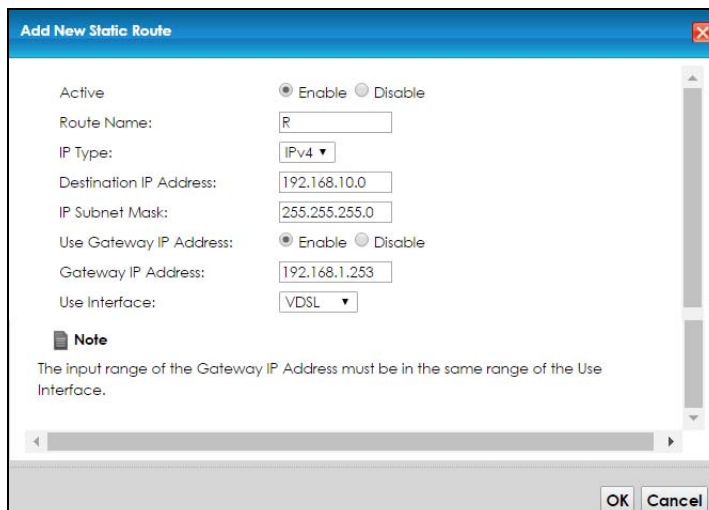
DEVICE / COMPUTER	IP ADDRESS
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

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

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



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



- 4f Click **OK**.

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

4.8 Configuring QoS Queue and Class Setup

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

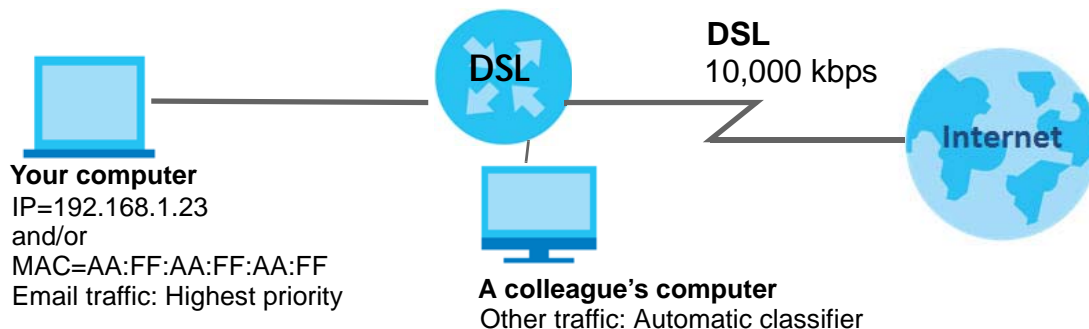
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues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

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

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

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

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



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

QoS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable (Settings are invalid when disabled)
WAN Managed Upstream Bandwidth :	<input type="text" value="10000"/> (kbps)
LAN Managed Downstream Bandwidth :	<input type="text"/> (kbps)
Upstream Traffic Priority Assigned by:	<input type="text" value="None"/>
Note	
1. You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.	
2. If Upstream Traffic Priority is selected, 8 level strict priority QoS will be applied automatically according to the selected criteria. In this mode, user manually defined QoS will not be applied until Auto-Priority Mapping is disabled.	
3. If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- 2 Click **Queue Setup > Edit** to modify a queue. Enter or select the following values:
 - **Name:** E-mail
 - **Interface:** WAN

- **Priority:** 1 (High)
- **Weight:** 8

The screenshot shows a 'Queue Entry Edit' dialog box with the following settings:

Field	Value
Name	Email
Interface	WAN
discipline	SP
Priority	1 (Highest)
Weight	8
Buffer Management	Drop Tail (DT)
Rate Limit	(kbps)

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

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

Step1: Class Configuration

Active Enable Disable

Class Name:

Classification Order:

Step2: Criteria Configuration

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

Basic

From Interface:

Ether Type:

Source

Address: Subnet Mask: Exclude

Port Range: ~ Exclude

MAC: MAC Mask: Exclude

Destination

Address: Subnet Mask: Exclude

Port Range: ~ Exclude

MAC: - - - - - MAC Mask: Exclude

Others

Service: Exclude

IP protocol: Exclude

DHCP: Exclude

IP Packet Length: ~ Exclude

DSCP: (0~63) Exclude

802.1P: Exclude

VLAN ID: (1~4094) Exclude

TCP ACK: Exclude

Step3: Packet Modification

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

DSCP Mark: (0~63)

802.1P Mark:

VLAN ID Tag: (1~4094)

Step4: Class Routing

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

Forward To Interface:

Step5: Outgoing Queue Selection

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

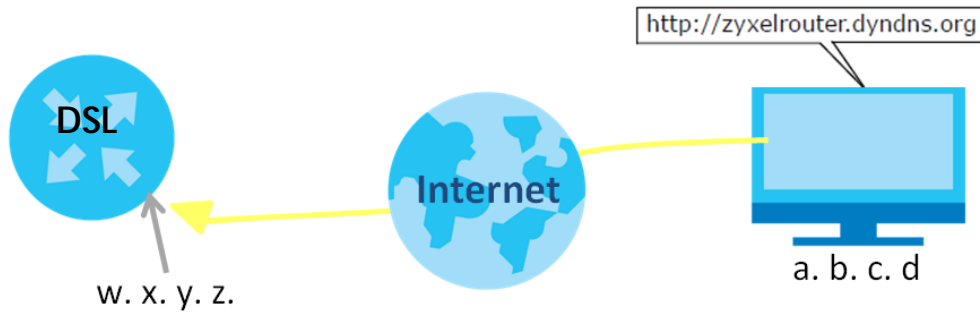
To Queue Index:

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

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

4.9 Access the VMG Using DDNS

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



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

This tutorial covers:

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

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

4.9.1 Registering a DDNS Account on www.dyndns.org

- 1 Open a browser and type <http://www.dyndns.org>.
- 2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
- 3 Log into www.dyndns.org using your account.
- 4 Add a new DDNS host name. This tutorial uses the following settings as an example.
 - Hostname: **zyxelrouter.dyndns.org**
 - Service Type: **Host with IP address**
 - IP Address: Enter the WAN IP address that your VMG is currently using. You can find the IP address on the VMG's Web Configurator **Status** page.

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

4.9.2 Configuring DDNS on Your VMG

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

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.

- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).

Dynamic DNS Setup

Dynamic DNS Enable Disable (Settings are invalid when disabled)

Service Provider :

Host Name :

Username :

Password :

Dynamic DNS Status

User Authentication Result :

Last Updated Time :

Current Dynamic IP :

Click **Apply**.

4.9.3 Testing the DDNS Setting

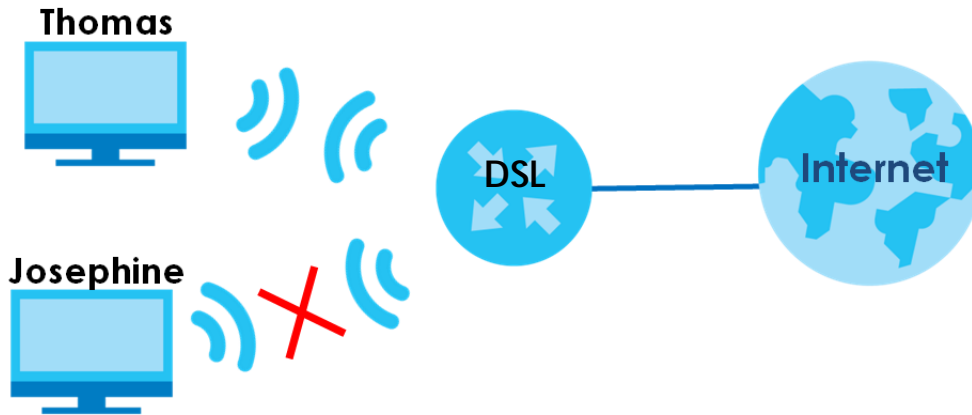
Now you should be able to access the VMG from the Internet. To test this:

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

4.10 Configuring the MAC Address Filter

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

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



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

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

MAC Restrict Mode : Allow Deny

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

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

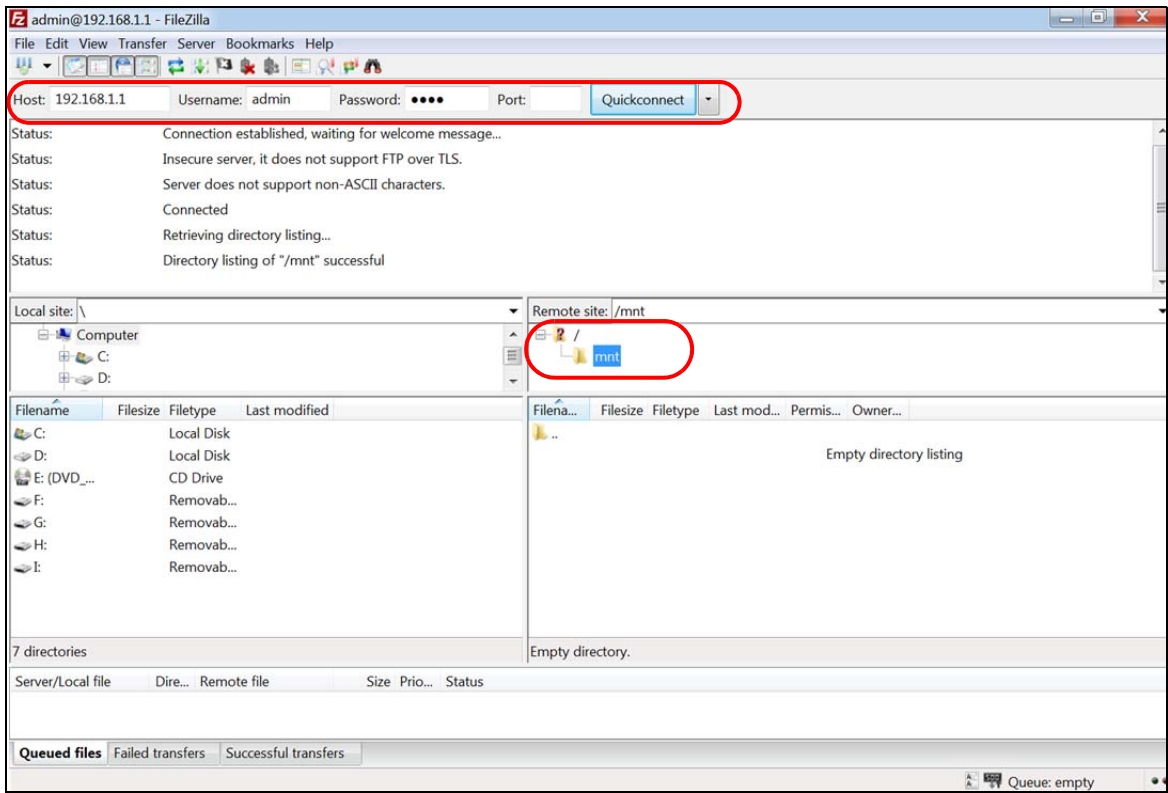
Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the VMG.

## 4.11 Access Your Shared Files From a Computer

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

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

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



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



---

# PART II

## Technical Reference

---

# CHAPTER 5

## Network Map and Status Screens

### 5.1 Overview

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

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

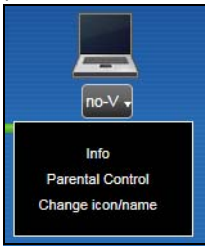
### 5.2 The Network Map Screen

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

**Figure 21** Network Map: Icon View Mode

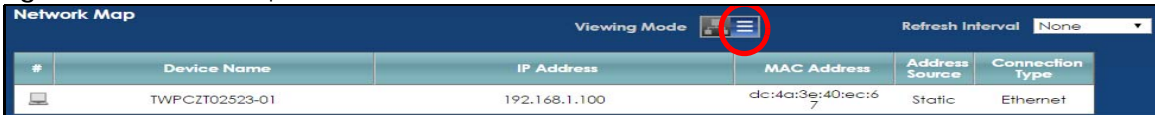


If you want to view information about a client, click the client's name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change icon/name**.



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 VMG to update this screen in **Refresh interval**.

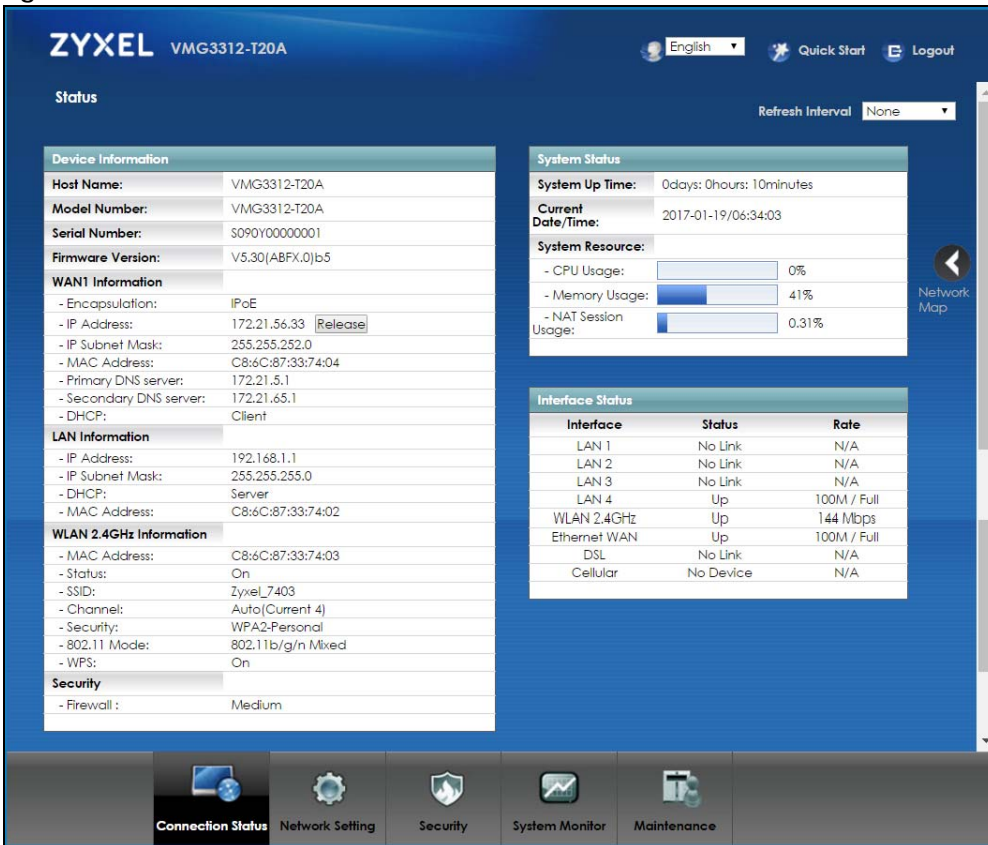
Figure 22 Network Map: List View Mode



## 5.3 The Status Screen

Use this screen to view the status of the VMG. Click the right arrow icon in the **Network Map (Connection Status)** screen to open this screen.

Figure 23 Status Screen



Each field is described in the following table.

Table 8 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen.
Device Information	
Host Name	This field displays the VMG system name. It is used for identification.
Model Number	This shows the model number of your VMG.
Serial Number	This shows the serial number of your VMG.
Firmware Version	This is the current version of the firmware inside the VMG.
WAN Information (These fields display when you have a WAN connection.)	
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IP address of the VMG in the WAN. Click <b>Release</b> to release your IP address to 0.0.0.0. If you want to renew your IP address, click <b>Renew</b> .
IP Subnet Mask	This field displays the current subnet mask in the WAN.
MAC Address	This field displays the WAN Ethernet adapter MAC (Media Access Control) Address of your VMG.
Primary/ Secondary DNS Server	This field displays the first/second DNS server IP address assigned to the VMG.
DHCP	This field displays whether the WAN interface is using a DHCP IP address or a static IP address. Choices are:  <b>Client</b> - The WAN interface can obtain an IP address from a DHCP server.  <b>None</b> - The WAN interface is using a static IP address.
LAN Information	
IP Address	This is the current IP address of the VMG in the LAN.
IP Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Link Local Address	This field displays the current link-local address of the VMG for the LAN interface.
DHCP	This field displays what DHCP services the VMG is providing to the LAN. The possible values are:  <b>Server</b> - The VMG is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.  <b>Relay</b> - The VMG acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.  <b>Disable</b> - The VMG is not providing any DHCP services to the LAN.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your VMG.
WLAN 2.4G Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of the wireless interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the VMG in a wireless LAN.
Channel	This is the channel number used by the wireless interface now.
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.

Table 8 Status Screen (continued)

LABEL	DESCRIPTION
Security	
Firewall	This displays the firewall's current security level.
System Status	
System Up Time	This field displays how long the VMG has been running since it last started up. The VMG starts up when you plug it in, when you restart it ( <b>Maintenance &gt; Reboot</b> ), or when you reset it.
Current Date/Time	This field displays the current date and time in the VMG. You can change this in <b>Maintenance &gt; Time Setting</b> .
System Resource	
CPU Usage	This field displays what percentage of the VMG's processing ability is currently used. When this percentage is close to 100%, the VMG is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see <a href="#">Chapter 10 on page 145</a> ).
Memory Usage	This field displays what percentage of the VMG's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the VMG is probably becoming unstable, and you should restart the device. See <a href="#">Section 34.2 on page 248</a> , or turn off the device (unplug the power) for a few seconds.
NAT Session Usage	This field displays what percentage of the VMG supported NAT sessions are currently being used. This field also displays the number of active NAT sessions and the maximum number of NAT sessions the VMG can support.
Interface Status	
Interface	This column displays each interface the VMG has.
Status	<p>This field indicates the interface's use status.</p> <p>For the LAN and Ethernet WAN interfaces, this field displays <b>Up</b> when using the interface and <b>No Link</b> when not using the interface.</p> <p>For the WLAN interface, this field displays the enabled (<b>Up</b>) or disabled (<b>Disable</b>) state of the interface.</p> <p>For the DSL interface, this field displays <b>Down</b> (line down), <b>Up</b> (line up or connected), <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation, and <b>No Link</b> when not using the interface.</p> <p>For the cellular interface, this field displays <b>Up</b> when using the interface and <b>No Device</b> when no device is detected in any USB slot.</p>
Rate	<p>For the LAN and Ethernet WAN interfaces, this displays the port speed and duplex setting.</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 or <b>N/A</b> with WLAN disabled.</p> <p>For the cellular interface, this field displays signal strength bars when a cellular device is installed in a USB slot and <b>N/A</b> when no device is detected in the USB slot.</p>

# CHAPTER 6

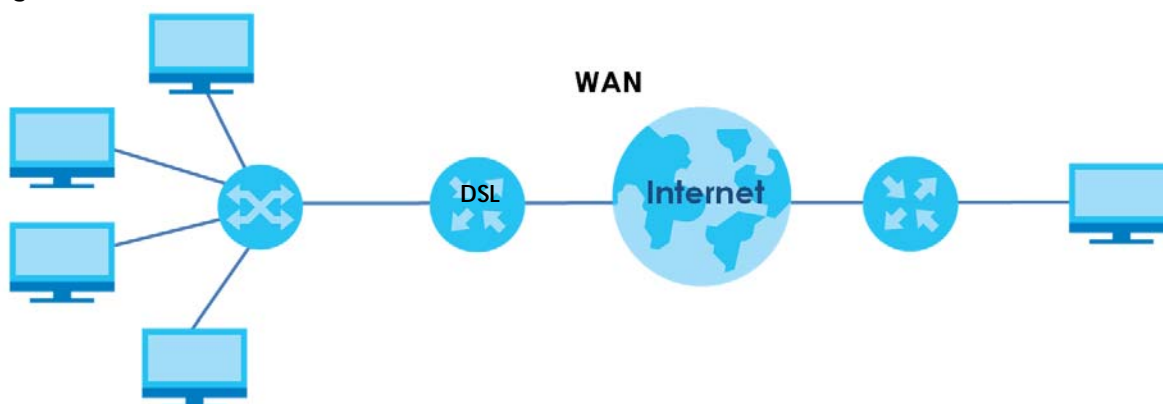
## Broadband

### 6.1 Overview

This chapter discusses the VMG's **Broadband** screens. Use these screens to configure your VMG 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 24 LAN and WAN



#### 6.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the VMG for Internet access ([Section 6.2 on page 74](#)).
- Use the **Cellular Backup** screen to configure cellular WAN connection ([Section 6.3 on page 83](#)).
- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions ([Section 6.4 on page 89](#)).

Table 9 WAN Setup Overview

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

Table 9 WAN Setup Overview

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

## 6.1.2 What You Need to Know

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

### WAN IP Address

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

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

### ATM

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

### PTM

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

### IPv6 Introduction

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

## IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

## IPv6 Prefix and Prefix Length

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

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

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

## IPv6 Subnet Masking

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

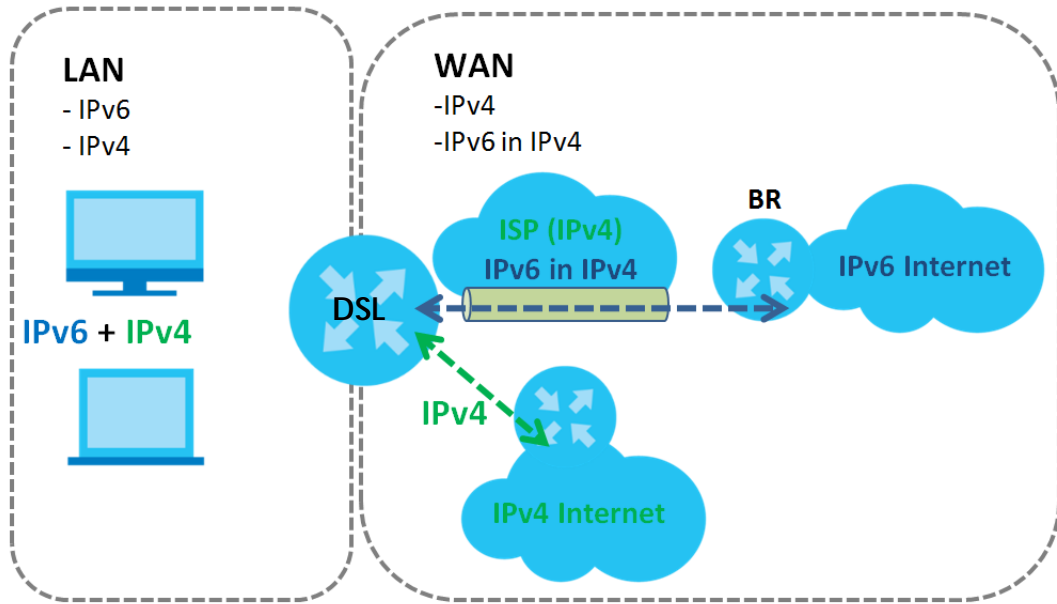
## IPv6 Rapid Deployment

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

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



Figure 25 IPv6 Rapid Deployment

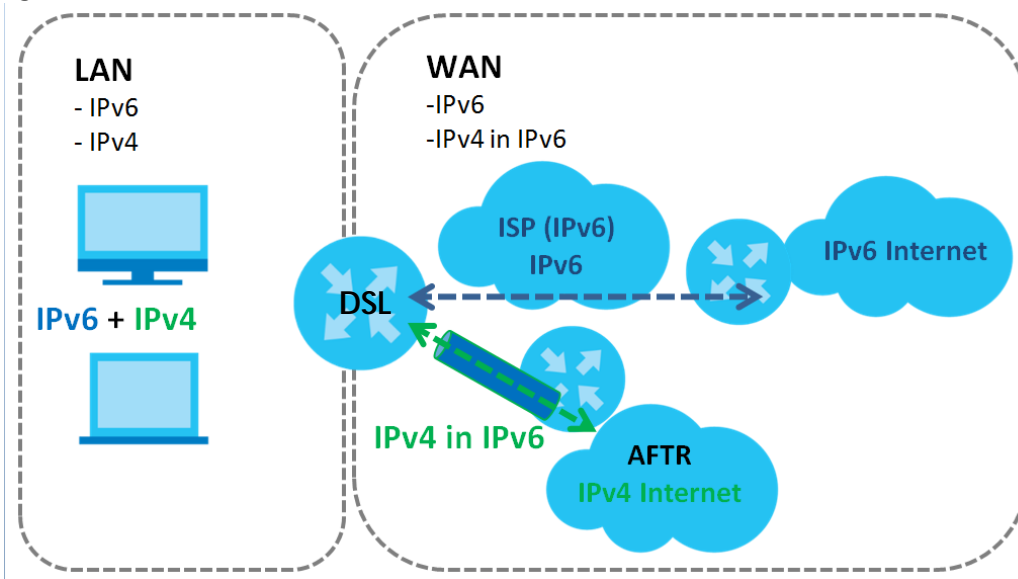


### Dual Stack Lite

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

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

Figure 26 Dual Stack Lite





### 6.1.3 Before You Begin

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

## 6.2 The Broadband Screen

Use this screen to change your VMG's Internet access settings. Click **Network Setting > Broadband** from the menu. The summary table shows you the configured WAN services (connections) on the VMG.

**Figure 27** Network Setting > Broadband

Add New WAN Interface												
#	Name	Type	Mode	Enca...	802.1p	802.1q	Igmp...	NAT	Defa...	IPv6	MLD Proxy	Modify
1	VDSL	PTM	Routin g	PPPo E	N/A	N/A	Y	Y	Y	N	N	 

The following table describes the labels in this screen.

**Table 10** Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows whether it is an ATM, a PTM or an Ethernet connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays <b>N/A</b> when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays <b>N/A</b> when there is no VLAN ID number assigned.
Igmp Proxy	This shows whether the VMG act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the VMG use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.
Modify	Click the <b>Edit</b> icon to configure the WAN connection. Click the <b>Delete</b> icon to remove the WAN connection.

## 6.2.1 Add/Edit Internet Connection

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

### 6.2.1.1 Routing Mode

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

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

Figure 28 Network Setting &gt; Broadband &gt; Add New WAN Interface/Edit (Routing Mode)

**Add New WAN Interface**

**General**

Active:  Enable  Disable

Name:

Type:

Mode:  Routing  Bridge

Encapsulation:

IPv4/IPv6 Mode:

**PPP Information**

PPP User Name:

PPP Password:

password unmask

PPP Connection Trigger:  Auto Connect  On Demand

PPPoE Passthrough:  Enable  Disable

**IP Address**

Obtain an IP Address Automatically

Static IP Address

IP Address:

**ATM PVC Configuration**

VPI [0-255]:

VCI [32-65535]:

Encapsulation:

Service Category:

**VLAN**

Active:  Enable  Disable

802.1p:

802.1q:  (1~4094)

**MTU**

MTU:

**Routing Feature**

NAT Enable:  Enable  Disable

Fullcone NAT Enable:  Enable  Disable

IGMP Proxy Enable:  Enable  Disable

Apply as Default Gateway:  Enable  Disable

**DNS Server**

Obtain DNS Info Automatically

Use Following Static DNS Address

Primary DNS Server:

Secondary DNS Server:

**6RD**

6RD:  Enable  Disable

Automatically configured by DHCP

Manually Configured

Service Provider IPv6 Prefix:

IPv4 Mask Length:

Border Relay IPv4 Address:

OK Cancel

The following table describes the labels in this screen.

Table 11 Network Setting &gt; Broadband &gt; Add New WAN Interface/Edit (Routing Mode)

LABEL	DESCRIPTION
General	
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the interface.
Name	Specify a descriptive name for this connection.
Type	Select whether it is an ADSL/VDSL over PTM or ADSL over ATM connection.

Table 11 Network Setting &gt; Broadband &gt; Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
Mode	Select <b>Routing</b> if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select <b>Routing</b> in the <b>Mode</b> field.  The choices depend on the connection type you selected. If your connection type is <b>ADSL/VDSL over PTM</b> , the choices are <b>PPPoE</b> and <b>IPoE</b> . If your connection type is <b>ADSL over ATM</b> , the choices are <b>PPPoE</b> , <b>PPPoA</b> , <b>IPoE</b> and <b>IPoA</b> . If your connection type is <b>Ethernet</b> , the choices are <b>PPPoE</b> and <b>IPoE</b> .
IPv4/IPv6 Mode	Select <b>IPv4 Only</b> if you want the VMG to run IPv4 only.  Select <b>IPv4 IPv6 DualStack</b> to allow the VMG to run IPv4 and IPv6 at the same time.  Select <b>IPv6 Only</b> if you want the VMG to run IPv6 only.
PPP Information (This is available only when you select <b>PPPoE</b> or <b>PPPoA</b> in the <b>Mode</b> field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Select <b>password unmask</b> to show your entered password in plain text.
PPP Connection Trigger	Select when to have the VMG establish the PPP connection.  <b>Auto Connect</b> - select this to not let the connection time out.  <b>On Demand</b> - select this to automatically bring up the connection when the VMG receives packets destined for the Internet.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.  This field is not available if you select <b>Auto Connect</b> in the <b>PPP Connection Trigger</b> field.
PPPoE Passthrough	This field is available when you select <b>PPPoE</b> encapsulation.  In addition to the VMG's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the VMG. Each host can have a separate account and a public WAN IP address.  PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.  Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
IP Address (This is available only when you select <b>IPv4 Only</b> or <b>IPv4 IPv6 DualStack</b> in the <b>IPv4/IPv6 Mode</b> field.)	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
ATM PVC Configuration (These fields appear when the <b>Type</b> is set to <b>ADSL over ATM</b> .)	
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.

Table 11 Network Setting &gt; Broadband &gt; Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
Encapsulation	<p>Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:</p> <ul style="list-style-type: none"> <li>• <b>LLC/SNAP-BRIDGING:</b> In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select <b>IPoE</b> or <b>PPPoE</b> in the <b>Select DSL Link Type</b> field.</li> <li>• <b>VC/MUX:</b> In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the VMG needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.</li> </ul>
Service Category	<p>Select <b>UBR Without PCR</b> for applications that are non-time sensitive, such as e-mail.</p> <p>Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select <b>Non Realtime VBR</b> (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select <b>Realtime VBR</b> (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
Peak Cell Rate [cells/s]	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size [cells]	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
VLAN (These fields appear when the <b>Type</b> is set to <b>ADSL/VDSL over PTM</b> .)	
Active	Select <b>Enable</b> to activate VLAN on this WAN interface. Otherwise, select <b>Disable</b> to deactivate.
802.1p	<p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.</p> <p>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.</p>
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Routing Feature (This is available only when you select <b>IPv4 Only</b> or <b>IPv4 IPv6 DualStack</b> in the <b>IPv4/IPv6 Mode</b> field.)	
NAT Enable	Select this option to activate NAT on this connection.
Fullcone NAT Enable	Select this option to enable full cone NAT on this connection. This field is available only when you activate NAT. In full cone NAT, the VMG maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The VMG also maps packets coming to that external IP address and port to the internal IP address and port.
IGMP Proxy Enable	<p>Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p> <p>Select this option to have the VMG act as an IGMP proxy on this connection. This allows the VMG to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.</p>
Apply as Default Gateway	Select this option to have the VMG use the WAN interface of this connection as the system default gateway.
DNS Server (This is available only when you select <b>IPv4 Only</b> or <b>IPv4 IPv6 DualStack</b> in the <b>IPv4/IPv6 Mode</b> field.)	
	<p>Select <b>Obtain DNS Info Automatically</b> if you want the VMG to use the DNS server addresses assigned by your ISP.</p> <p>Select <b>Use Following Static DNS Address</b> if you want the VMG to use the DNS server addresses you configure manually.</p>

Table 11 Network Setting &gt; Broadband &gt; Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
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.
Tunnel	The DS-Lite (Dual Stack Lite) fields display when you set the <b>IPv4/IPv6 Mode</b> field to <b>IPv6 Only</b> . Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See <a href="#">Dual Stack Lite on page 73</a> for more information.
Enabled DS-Lite	This is available only when you select <b>IPv6 Only</b> in the <b>IPv4/IPv6 Mode</b> field. Select <b>Enable</b> to let local computers use IPv4 through an ISP's IPv6 network.
DS-Lite Relay Server IP	Specify the transition router's IPv6 address.
6RD	The 6RD (IPv6 rapid deployment) fields display when you set the <b>IPv6/IPv4 Mode</b> field to <b>IPv4 Only</b> . See <a href="#">IPv6 Rapid Deployment on page 72</a> for more information.
6RD	Select <b>Enable</b> to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
	Select <b>Manually Configured</b> if you have the IPv4 address of the relay server. Otherwise, select <b>Automatically configured by DHCP</b> to have the VMG detect it automatically through DHCP.  The <b>Automatically configured by DHCP</b> option is configurable only when you set the method of encapsulation to <b>IPoE</b> .
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
Border Relay IPv4 Address	When you select <b>Manually Configured</b> , specify the relay server's IPv4 address in this field.
DHCP Options (This is available only when you select <b>IPv4 Only</b> or <b>IPv4 IPv6 DualStack</b> in the <b>IPv4/IPv6 Mode</b> field.)	
Request Options	Select <b>Option 42</b> to have the VMG get the NTP server which is available to the client.  Select <b>Option 43</b> to have the VMG automatically add vendor specific information in the DHCP packets to request the vendor specific options from the DHCP server.  Select <b>Option 121</b> to have the VMG push static routes to clients.
Sent Options	
option 60	Select this and enter the device identity you want the VMG to add in the DHCP discovery packets that go to the DHCP server.
Vendor ID	Enter the Vendor Class Identifier, such as the type of the hardware or firmware.
option 61	Select this and enter any string that identifies the device.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID	Enter the hardware type, a time value and the MAC address of the device.
option 125	Select this to have the VMG automatically generate and add vendor specific parameters in the DHCP discovery packets that go to the DHCP server.
IPv6 Address (This is available only when you select <b>IPv4 IPv6 DualStack</b> or <b>IPv6 Only</b> in the <b>IPv4/IPv6 Mode</b> field.)	
Obtain an IPv6 Address Automatically	Select <b>Obtain an IPv6 Address Automatically</b> if you want to have the VMG use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.

Table 11 Network Setting &gt; Broadband &gt; Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
Static IPv6 Address	Select <b>Static IPv6 Address</b> if you have a fixed IPv6 address assigned by your ISP. When you select this, the following fields appear.
IPv6 Address	Enter an IPv6 IP address that your ISP gave to you for this WAN interface.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your VMG's interface(s). The gateway helps forward packets to their destinations.
IPv6 Routing Feature (This is available only when you select <b>IPv4 IPv6 DualStack</b> or <b>IPv6 Only</b> in the <b>IPv4/IPv6 Mode</b> field. You can enable IPv6 routing features in the following section.)	
MLD Proxy Enable	Select this checkbox to have the VMG act as an MLD proxy on this connection. This allows the VMG to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the VMG use the WAN interface of this connection as the system default gateway.
IPv6 DNS Server (This is available only when you select <b>IPv4 IPv6 DualStack</b> or <b>IPv6 Only</b> in the <b>IPv4/IPv6 Mode</b> field. Configure the IPv6 DNS server in the following section.)	
Obtain IPv6 DNS Info Automatically	Select <b>Obtain IPv6 DNS Info Automatically</b> to have the VMG get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select <b>Use Following Static IPv6 DNS Address</b> to have the VMG use the IPv6 DNS server addresses you configure manually.
Primary DNS Server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second IPv6 DNS server address assigned by the ISP.

### 6.2.1.2 Bridge Mode

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

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



**Figure 29** Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM -Bridge Mode)

The following table describes the fields in this screen.

**Table 12** Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM -Bridge or Ethernet Mode)

LABEL	DESCRIPTION
General	
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the interface.
Name	Enter a service name of the connection.
Type	Select <b>ADSL/VDSL over PTM</b> as the interface that you want to configure. The VMG uses the VDSL technology for data transmission over the DSL port.
Mode	Select <b>Bridge</b> 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 <b>Bridge</b> , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	
Active	Select <b>Enable</b> to activate VLAN on this WAN interface. Otherwise, select <b>Disable</b> to deactivate.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.  Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

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

**Figure 30** Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

The following table describes the fields in this screen.

**Table 13** Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

LABEL	DESCRIPTION
General	
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the interface.
Name	Enter a service name of the connection.
Type	Select <b>ADSL over ATM</b> as the interface that you want to configure. The VMG uses the ADSL technology for data transmission over the DSL port.
Mode	Select <b>Bridge</b> 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 <b>Bridge</b> , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
ATM PVC Configuration (These fields appear when the <b>Type</b> is set to <b>ADSL over ATM</b> .)	
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.
Encapsulation	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: <ul style="list-style-type: none"> <li>• <b>LLC/SNAP-BRIDGING</b>: In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select <b>IPoE</b> or <b>PPPoE</b> in the <b>Encapsulation</b> field.</li> <li>• <b>VC/MUX</b>: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the VMG needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.</li> </ul>

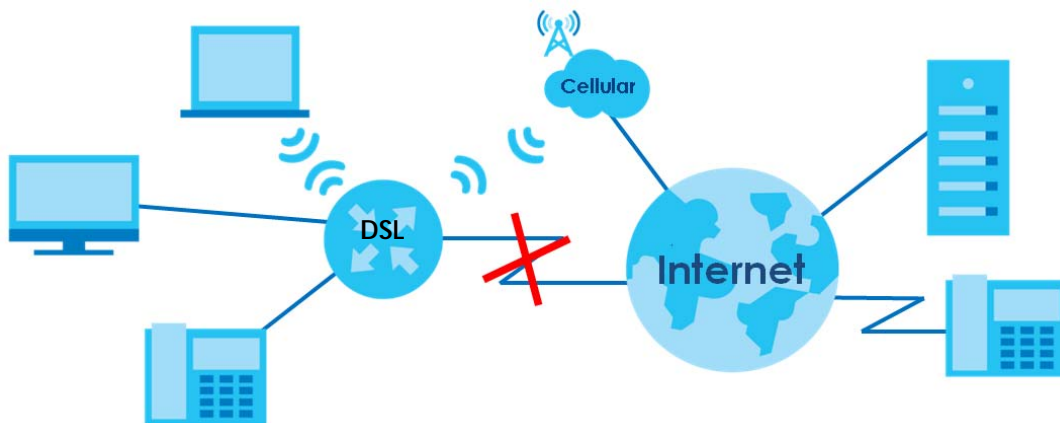
Table 13 Network Setting &gt; Broadband &gt; Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode) (continued)

LABEL	DESCRIPTION
Service Category	Select <b>UBR Without PCR</b> for applications that are non-time sensitive, such as e-mail. Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select <b>Non Realtime VBR</b> (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select <b>Realtime VBR</b> (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate [cells/s]	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size [cells]	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
VLAN	
Active	Select <b>Enable</b> to activate VLAN on this WAN interface. Otherwise, select <b>Disable</b> to deactivate.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.  Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 6.3 The Cellular Backup Screen

The USB port (at the side panel of the VMG) allows you to attach a cellular dongle to wirelessly connect to a cellular network for Internet access. You can have the VMG use the cellular WAN connection as a backup. Disconnect the DSL and Ethernet WAN ports to use the cellular dongle as your primary WAN connection. The VMG automatically uses a wired WAN connection when available.

Figure 31 Internet Access Application: Cellular WAN



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

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

Figure 32 Network Setting > Broadband > Cellular Backup

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

### General

Cellular Backup  Enable  Disable (Settings are invalid when disabled)

Trigger Cellular backup when physical link of primary WAN is down

Ping Check  Enable  Disable

Check Cycle : Every  (20~180 Sec)

Consecutive Fail :  (2~5 times)

Ping Default Gateway

Ping Host  (Host name or IP address)

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

### Cellular Connection Settings

Card Description : N/A

Username :  (Optional)

Password :  (Optional)

Authentication :  ▾

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

Dial String :

APN :

Connection :  ▾

Obtain an IP Address Automatically

Use the Following Static IP Address

Obtain DNS Info Dynamically

Use the Following Static DNS IP Address

Enable E-mail Notification  Enable  Disable

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

### Budget Setup

Enable Budget Control  Enable  Disable

Time Budget:  hours per month

Data Budget:  Mbytes  ▾ per month

Data Budget:  kPackets  ▾ per month

Reset all budget counters on  ▾ day of the month

[Reset time and data budget counters](#)

Actions before over budget:

Enable  % of time budget

Enable  % of data budget (Mbytes)

Enable  % of data budget (Packets)

Actions when over budget:

Current Cellular Connection  ▾

Actions:

Enable E-mail Notification  Enable  Disable

Enable Log: Interval  minutes

**Note:**  
Budget control is an approximate value.

[Basic](#)

The following table describes the labels in this screen.

Table 14 Network Setting > Broadband > cellular Backup

LABEL	DESCRIPTION
General	
Cellular Backup	Select <b>Enable</b> to have the VMG use the cellular connection as your WAN or a backup when the wired WAN connection fails.
Ping Check	Select <b>Enable</b> if you want the VMG to ping check the connection status of your WAN. You can configure the frequency of the ping check and number of consecutive failures before triggering cellular backup.
Check Cycle	Enter the frequency of the ping check in this field.
Consecutive Fail	Enter how many consecutive failures are required before cellular backup is triggered.
Ping Default Gateway	Select this to have the VMG ping the WAN interface's default gateway IP address.
Ping Host	Select this to have the VMG ping the particular host name or IP address you typed in this field.
Cellular Connection Settings	
Card description	This field displays the manufacturer and model name of your cellular card if you inserted one in the VMG. Otherwise, it displays <b>N/A</b> .
Username	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
Authentication	<p>The VMG 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><b>AUTO</b> - Your VMG accepts either CHAP or PAP when requested by this remote node.</p> <p><b>CHAP</b> - Your VMG accepts CHAP only.</p> <p><b>PAP</b> - Your VMG accepts PAP only.</p>
PIN	<p>A PIN (Personal Identification Number) code is a key to a cellular card. Without the PIN code, you cannot use the cellular card.</p> <p>If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the cellular card may be blocked by your ISP and you cannot use the account to access the Internet.</p> <p>If your ISP disabled PIN code authentication, leave this field blank.</p>
Dial string	<p>Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number.</p> <p>For example, *99# is the dial string to establish a GPRS or cellular connection in Taiwan.</p>
APN	<p>Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method.</p> <p>You can enter up to 32 ASCII printable characters. Spaces are allowed.</p>
Connection	<p>Select <b>Nailed UP</b> if you do not want the connection to time out.</p> <p>Select <b>on Demand</b> if you do not want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.</p>

Table 14 Network Setting &gt; Broadband &gt; cellular Backup (continued)

LABEL	DESCRIPTION
Max Idle Timeout	This value specifies the time in minutes that elapses before the VMG automatically disconnects from the ISP.
Obtain an IP Address Automatically	Select this option if your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected <b>Use the following static IP address</b> .
Subnet Mask	Enter the subnet mask of the IP address.
Obtain DNS info Dynamically	Select this to have the VMG get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the VMG 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.
Enable E-mail Notification	Select this to enable the e-mail notification function. The VMG will e-mail you a notification when the cellular connection is up.
Mail Account	Select an e-mail address you have configured in <b>Maintenance &gt; Email Notification</b> . The VMG uses the corresponding mail server to send notifications. You must have configured a mail server already in the <b>Maintenance &gt; Email Notification</b> screen.
Cellular Backup E-mail Title	Type a title that you want to be in the subject line of the e-mail notifications that the VMG sends.
Send Notification to E-mail	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail.
Advanced	Click this to show the advanced cellular backup settings.
Budget Setup	
Enable Budget Control	Select <b>Enable</b> to set a monthly limit for the user account of the installed cellular card. You can set a limit on the total traffic and/or call time. The VMG takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the cellular connection can be used within one month. If you change the value after you configure and enable budget control, the VMG resets the statistics.
Data Budget (Mbytes)	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the cellular connection within one month.  Select <b>Download/Upload</b> to set a limit on the total traffic in both directions.  Select <b>Download</b> to set a limit on the downstream traffic (from the ISP to the VMG).  Select <b>Upload</b> to set a limit on the upstream traffic (from the VMG to the ISP).  If you change the value after you configure and enable budget control, the VMG resets the statistics.

Table 14 Network Setting &gt; Broadband &gt; cellular Backup (continued)

LABEL	DESCRIPTION
Data Budget (kPackets)	<p>Select this and specify how much downstream and/or upstream data (in k Packets) can be transmitted via the cellular connection within one month.</p> <p>Select <b>Download/Upload</b> to set a limit on the total traffic in both directions.</p> <p>Select <b>Download</b> to set a limit on the downstream traffic (from the ISP to the VMG).</p> <p>Select <b>Upload</b> to set a limit on the upstream traffic (from the VMG to the ISP).</p> <p>If you change the value after you configure and enable budget control, the VMG resets the statistics.</p>
Reset all budget counters on	Select the date on which the VMG resets the budget every month. Select <b>last</b> if you want the VMG to reset the budget on the last day of the month. Select <b>specific</b> and enter the number of the date you want the VMG to reset the budget
Reset time and data budget counters	Click this button to reset the time and data budgets immediately. The count starts over with the cellular connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.
Actions before over budget	Specify the actions the VMG takes before the time or data limit exceeds.
Enable % of time budget/data budget (Mbytes)/data budget (kPackets)	Select <b>Enable</b> and enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the VMG resets the statistics.
Actions when over budget	Specify the actions the VMG takes when the time or data limit is exceeded.
Current Cellular connection	Select <b>Keep</b> to maintain an existing cellular connection or <b>Drop</b> to disconnect it.
Actions	
Enable E-mail Notification	Select <b>Enable</b> to enable the e-mail notification function. The VMG will e-mail you a notification when there over budget occurs.
Mail Account	<p>Select an e-mail address you have configured in <b>Maintenance &gt; Email Notification</b>. The VMG uses the corresponding mail server to send notifications.</p> <p>You must have configured a mail server already in the <b>Maintenance &gt; Email Notification</b> screen.</p>
Cellular Backup E-mail Title	Type a title that you want to be in the subject line of the e-mail notifications that the VMG sends.
Send Notification to E-mail	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail.
Enable Log	Select this to activate the logging function at the interval you set in this field.
Interval	Enter the interval of how many minutes you want the VMG to e-mail you.
Basic	Click this to hide the advanced settings of cellular backup.
Apply	Click <b>Apply</b> to save your changes back to the VMG.
Cancel	Click <b>Cancel</b> to return to the previous configuration.



## 6.4 The Advanced Screen

Use the **Advanced** screen to enable or disable Annex M, DSL PhyR, and SRA (Seamless Rate Adaptation) functions. The VMG supports the PhyR retransmission scheme. PhyR is a retransmission scheme designed to provide protection against noise on the DSL line. It improves voice, video and data transmission resilience by utilizing a retransmission buffer.

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

Table 15 VDSL Profiles

PROFILE	BANDWIDTH (MHZ)	NUMBER OF DOWNSTREAM CARRIERS	CARRIER BANDWIDTH (KHZ)	POWER (DBM)	MAX. DOWNSTREAM THROUGHPUT (MBIT/S)
8a	8.832	2048	4.3125	17.5	50
8b	8.832	2048	4.3125	20.5	50
8c	8.5	1972	4.3125	11.5	50
8d	8.832	2048	4.3125	14.5	50
12a	12	2783	4.3125	14.5	68
12b	12	2783	4.3125	14.5	68
17a	17.664	4096	4.3125	14.5	100
30a	30	3479	8.625	14.5	200

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

Figure 33 Network Setting > Broadband > Advanced

The screenshot displays the 'Advanced' settings screen for Broadband. It is organized into three main sections: DSL Capabilities, DSL Modulation, and VDSL Profile. Each setting includes a label and two radio buttons for 'Enable' and 'Disable'. The 'Enable' radio button is selected for all settings shown.

**DSL Capabilities**

- PhyR US/DS :  Enable  Disable
- Bitswap :  Enable  Disable
- SRA :  Enable  Disable

**DSL Modulation**

- G.dmt :  Enable  Disable
- G.lite :  Enable  Disable
- T1.413 :  Enable  Disable
- ADSL2 :  Enable  Disable
- Annex L :  Enable  Disable
- ADSL2+ :  Enable  Disable
- Annex M :  Enable  Disable
- VDSL2 :  Enable  Disable

**VDSL Profile**

- 8a Enable :  Enable  Disable
- 8b Enable :  Enable  Disable
- 8c Enable :  Enable  Disable
- 8d Enable :  Enable  Disable
- 12a Enable :  Enable  Disable
- 12b Enable :  Enable  Disable
- 17a Enable :  Enable  Disable
- 30a Enable :  Enable  Disable

At the bottom right of the screen, there are two buttons: **Apply** and **Cancel**.

The following table describes the labels in this screen.

Table 16 Network Setting > Broadband > Advanced

LABEL	DESCRIPTION
DSL Capabilities	
PhyR US/DS	<p>Enable or disable <b>PhyR US</b> (upstream) for upstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.</p> <p>Enable or disable <b>PhyR DS</b> (downstream) for downstream transmission from the WAN. PhyR DS should be enabled if data being transmitted downstream is sensitive to noise. However, enabling PhyR DS can decrease the DS line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.</p>
Bitswap	<p>Select <b>Enable</b> to allow the VMG to adapt to line changes when you are using G.dmt.</p> <p>Bit-swapping is a way of keeping the line more stable by constantly monitoring and redistributing bits between channels.</p>
SRA	<p>Enable or disable Seamless Rate Adaption (SRA). Select <b>Enable</b> to have the VMG automatically adjust the connection's data rate according to line conditions without interrupting service.</p>
DSL Modulation	
G.Dmt	<p>ITU G.992.1 (better known as G.dmt) is an ITU standard for ADSL using discrete multitone modulation. G.dmt full-rate ADSL expands the usable bandwidth of existing copper telephone lines, delivering high-speed data communications at rates up to 8 Mbit/s downstream and 1.3 Mbit/s upstream.</p>
G.lite	<p>ITU G.992.2 (better known as G.lite) is an ITU standard for ADSL using discrete multitone modulation. G.lite does not strictly require the use of DSL filters, but like all variants of ADSL generally functions better with splitters.</p>
T1.413	<p>ANSI T1.413 is a technical standard that defines the requirements for the single asymmetric digital subscriber line (ADSL) for the interface between the telecommunications network and the customer installation in terms of their interaction and electrical characteristics.</p>
ADSL2	<p>It optionally extends the capability of basic ADSL in data rates to 12 Mbit/s downstream and, depending on Annex version, up to 3.5 Mbit/s upstream (with a mandatory capability of ADSL2 transceivers of 8 Mbit/s downstream and 800 kbit/s upstream).</p>
AnnexL	<p>Annex L is an optional specification in the ITU-T ADSL2 recommendation G.992.3 titled Specific requirements for a Reach Extended ADSL2 (READSL2) system operating in the frequency band above POTS, therefore it is often referred to as Reach Extended ADSL2 or READSL2. The main difference between this specification and commonly deployed Annex A is the maximum distance that can be used. The power of the lower frequencies used for transmitting data is boosted up to increase the reach of this signal up to 7 kilometers (23,000 ft).</p>
ADSL2+	<p>ADSL2+ extends the capability of basic ADSL by doubling the number of downstream channels. The data rates can be as high as 24 Mbit/s downstream and up to 1.4 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises.</p>
Annex M	<p>Annex M is an optional specification in ITU-T recommendations G.992.3 (ADSL2) and G.992.5 (ADSL2+), also referred to as ADSL2 M and ADSL2+ M. This specification extends the capability of commonly deployed Annex A by more than doubling the number of upstream bits. The data rates can be as high as 12 or 24 Mbit/s downstream and 3 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises.</p>
VDSL2	<p>VDSL2 (Very High Speed Digital Subscriber Line 2) is the second generation of the VDSL standard (which is currently denoted VDSL1). VDSL2 allows a frequency band of up to 30MHz and transmission rates of up to 100 Mbps in each direction. VDSL2 is defined in G.993.2.</p>
VDSL Profile	
<p>VDSL2 profiles differ in the width of the frequency band used to transmit the broadband signal. Profiles that use a wider frequency band can deliver higher maximum speeds.</p>	

Table 16 Network Setting &gt; Broadband &gt; Advanced (continued)

LABEL	DESCRIPTION
8a, 8b, 8c, 8d, 12a, 12b, 17a, US0	The G.993.2 VDSL standard defines a wide range of profiles that can be used in different VDSL deployment settings, such as in a central office, a street cabinet or a building.  The VMG must comply with at least one profile specified in G.993.2, but compliance with more than one profile is allowed.
Apply	Click <b>Apply</b> to save your changes back to the VMG.
Cancel	Click <b>Cancel</b> to return to the previous configuration.

## 6.5 Technical Reference

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

### Encapsulation

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

### IP over Ethernet

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

### PPP over ATM (PPPoA)

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

### PPP over Ethernet (PPPoE)

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

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

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

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

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

## RFC 1483

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

## Multiplexing

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

### VC-based Multiplexing

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

### LLC-based Multiplexing

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

## Traffic Shaping

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

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

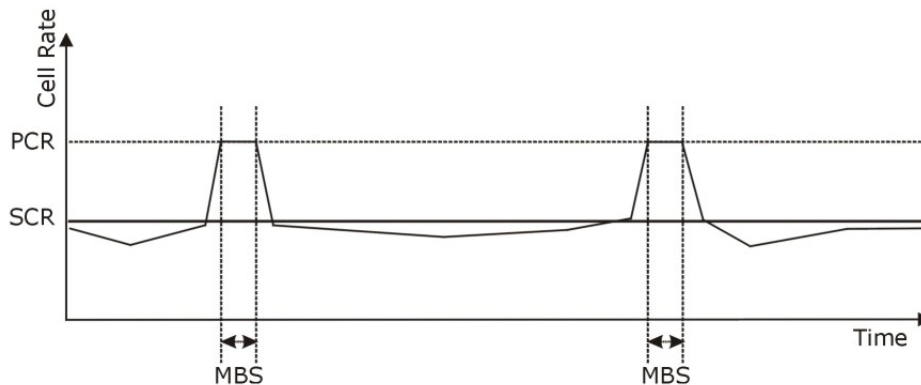
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

**Figure 34** Example of Traffic Shaping



## ATM Traffic Classes

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

### Constant Bit Rate (CBR)

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

### Variable Bit Rate (VBR)

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

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

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

### Unspecified Bit Rate (UBR)

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

## IP Address Assignment

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

## Introduction to VLANs

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

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

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

## Introduction to IEEE 802.1Q Tagged VLAN

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

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

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

## Multicast

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

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

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

## DNS Server Address Assignment

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

The VMG can get the DNS server addresses in the following ways.

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

## IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

## IPv6 Prefix and Prefix Length

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

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

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

# CHAPTER 7

## Wireless

### 7.1 Overview

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

#### 7.1.1 What You Can Do in this Chapter

This section describes the VMG's **Wireless** screens. Use these screens to set up your VMG'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 97](#)).
- Use the **Guest/More AP** screen to set up multiple wireless networks on your VMG ([Section 7.3 on page 101](#)).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the VMG ([Section 7.4 on page 104](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 7.5 on page 105](#)).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications ([Section 7.6 on page 107](#)).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold ([Section 7.7 on page 108](#)).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results ([Section 7.8 on page 109](#)).

#### 7.1.2 What You Need to Know

##### Wireless Basics

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

##### Finding Out More

See [Section 7.9 on page 110](#) for advanced technical information on wireless networks.



## 7.2 The General Screen

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

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

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

**Figure 35** Network Setting > Wireless > General

### Wireless Network Setup

Band: 2.4GHz ▾

Wireless:  Enable  Disable (Settings are invalid when disabled)

Channel: Auto ▾ Current : 9

Bandwidth: 20MHz ▾

Control Sideband: None ▾

### Wireless Network Settings

Wireless Network Name: ZyxeL_1FA3

Max Clients: 32

Hide SSID

Multicast Forwarding

Max. Upstream Bandwidth:  Kbps

Max. Downstream Bandwidth:  Kbps

**Note**

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

BSSID: E8:37:7A:9D:1F:A3

### Security Level

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

Security Mode: WPA2-PSK ▾

Generate password automatically

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

Password:

password unmask

[more...](#)

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

Table 17 Network Setting > Wireless > General

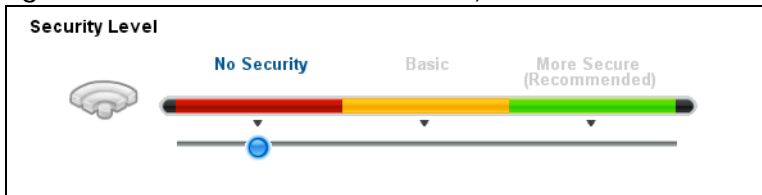
LABEL	DESCRIPTION
Wireless Network Setup	
Band	This shows the wireless band which this radio profile is using. <b>2.4GHz</b> is the frequency used by IEEE 802.11b/g/n wireless clients.
Wireless	You can <b>Enable</b> or <b>Disable</b> the wireless LAN in this field.
Channel	Use <b>Auto</b> to have the VMG automatically determine a channel to use.
Bandwidth	Select whether the VMG uses a wireless channel width of <b>20MHz</b> or <b>40MHz</b> .  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.  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.  Select <b>20MHz</b> if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to <b>40MHz</b> . Set whether the control channel (set in the <b>Channel</b> field) should be in the <b>Lower</b> or <b>Upper</b> range of channel bands.
Wireless Network Settings	
Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.  Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
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.
Multicast Forwarding	Select this check box to allow the VMG to convert wireless multicast traffic into wireless unicast traffic.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the VMG when wireless LAN is enabled.
Security Level	Select <b>Basic (WEP)</b> or <b>More Secure (WPA-PSK, WPA2-PSK, WPA-WPA2-PSK)</b> 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 VMG. When you select to use a security, additional options appears in this screen.  Or you can select <b>No Security</b> 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 <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> 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 VMG, your network is accessible to any wireless networking device that is within range.

Figure 36 Wireless > General: No Security



The following table describes the labels in this screen.

Table 18 Wireless > General: No Security

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

## 7.2.2 Basic (WEP Encryption)

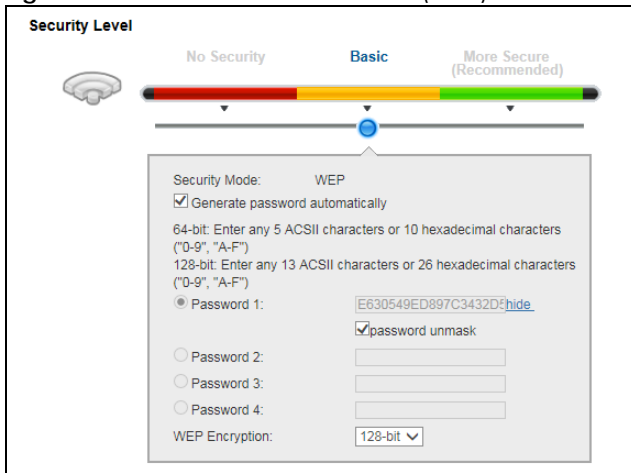
WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

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

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

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

Figure 37 Wireless > General: Basic (WEP)



The following table describes the labels in this screen.

Table 19 Wireless > General: Basic (WEP)

LABEL	DESCRIPTION
Security Level	Select <b>Basic</b> to enable WEP data encryption.
Security Mode	This shows <b>WEP</b> when you set <b>Security Level</b> to <b>Basic</b> .
Generate password automatically	Select this option to have the VMG automatically generate a password. The password field will not be configurable when you select this option.
Password 1~4	The password (WEP keys) are used to encrypt data. Both the VMG and the wireless stations must use the same password (WEP key) for data transmission.  If you chose <b>64-bit</b> WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").  If you chose <b>128-bit</b> WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").  You must configure at least one password, only one password can be activated at any one time.  Select <b>password unmask</b> to display the entered password in plain text. Clear it to hide the password to avoid shoulder surfing.
more.../hide	Click <b>more...</b> to show more fields in this section. Click <b>hide</b> to hide them.
WEP Encryption	Select <b>64-bit</b> or <b>128-bit</b> .  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 VMG 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.

Note: **WPA-PSK** is not available if you enable WPS before you configure them.

Figure 38 Wireless > General: More Secure: WPA2-PSK

**Security Level**

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

Security Mode:

Generate password automatically

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

Password:  [hide](#)

password unmask

Encryption:

Group Key Update Timer:  sec

The following table describes the labels in this screen.

Table 20 Wireless > General: More Secure: WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select <b>More Secure</b> to enable WPA2-PSK data encryption.
Security Mode	Select <b>WPA-PSK</b> , <b>WPA2-PSK</b> or <b>WPA-WPA2-PSK</b> from the drop-down list box.
Generate password automatically	Select this option to have the VMG automatically generate a password. The password field will not be configurable when you select this option.
Password	If you did not select <b>Generate password automatically</b> , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.  Select <b>password unmask</b> to display the entered password in plain text. Clear it to hide the password to avoid shoulder surfing.
more.../hide	Click <b>more...</b> to show more fields in this section. Click <b>hide</b> to hide them.
Encryption	Select the encryption type ( <b>TKIP</b> , <b>AES</b> or <b>TKIP+AES</b> ) for data encryption.  Select <b>TKIP</b> if your wireless clients can all use TKIP.  Select <b>AES</b> if your wireless clients can all use AES.  Select <b>TKIP+AES</b> to allow the wireless clients to use either TKIP or AES.
Group Key Update Timer	The <b>Group Key Update Timer</b> is the rate at which the RADIUS server sends a new group key out to all clients.

### 7.3 The Guest/More AP Screen

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

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

The following table introduces the supported wireless networks..

Table 21 Supported Wireless Networks

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

Figure 39 Network Setting > Wireless > Guest/More AP

#	Status	SSID	Security	Guest WLAN	Modify
2		ZyXEL_Guest	WPA2-Personal	External Guest	
3		ZyXEL_Guest	WPA2-Personal	External Guest	
4		ZyXEL_Guest	WPA2-Personal	External Guest	

The following table describes the labels in this screen.

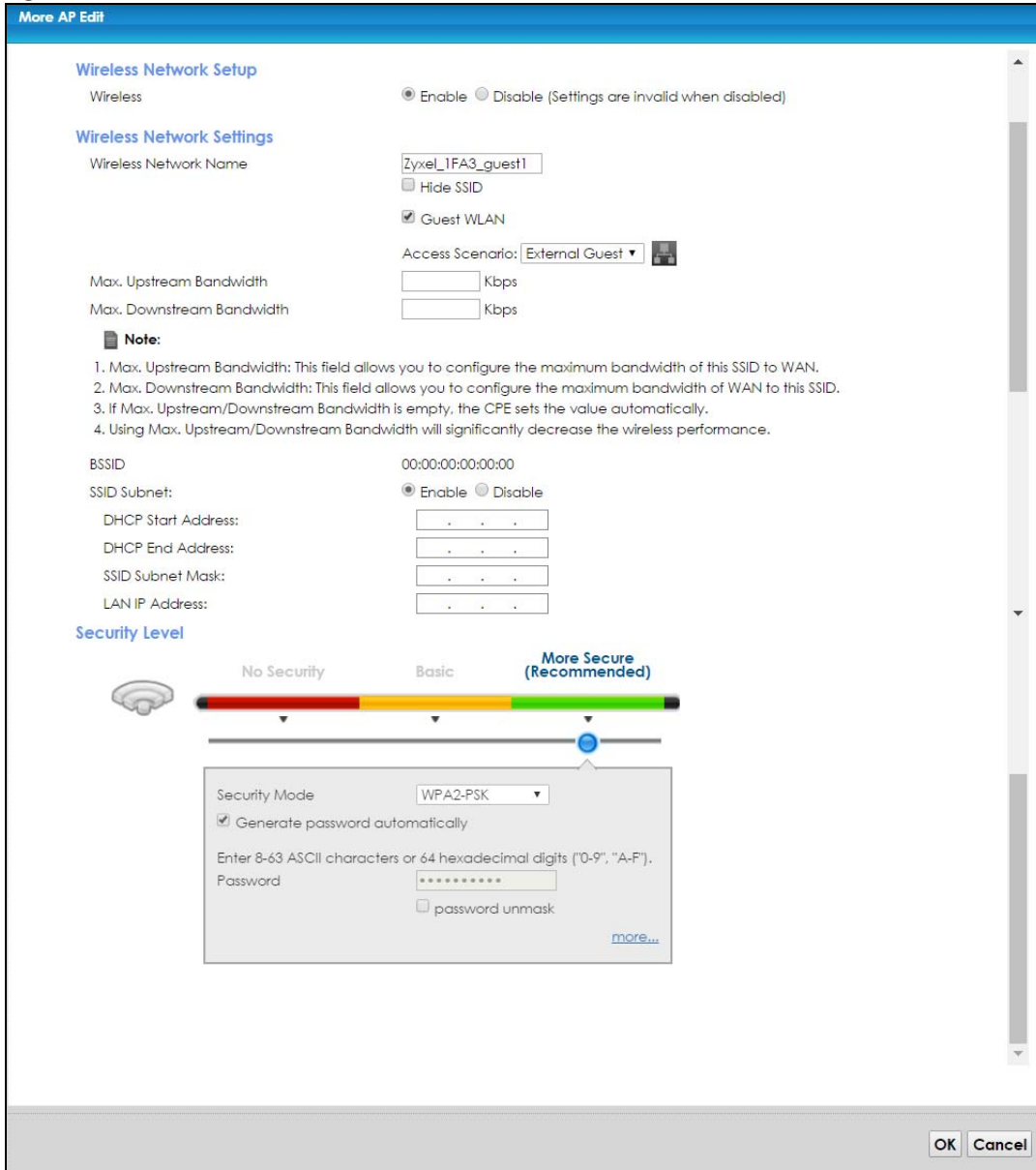
Table 22 Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.
SSID	<p>An SSID profile is the set of parameters relating to one of the VMG's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a wireless device is associated.</p> <p>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.</p>
Security	This field indicates the security mode of the SSID profile.
Guest WLAN	<p>This displays if the guest WLAN function has been enabled for this WLAN.</p> <p>If <b>Home Guest</b> displays, clients connecting to the same SSID can communicate with each other directly.</p> <p>If <b>External Guest</b> displays, clients are blocked from connecting to each other directly.</p> <p><b>N/A</b> displays if guest WLAN is disabled.</p>
Modify	Click the <b>Edit</b> icon to configure the SSID profile.

### 7.3.1 Edit Guest/More AP

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

Figure 40 Network Setting > Wireless > Guest/More AP > Edit



The following table describes the fields in this screen.

Table 23 Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can <b>Enable</b> or <b>Disable</b> the wireless LAN in this field.
Wireless Network Settings	
Wireless Network Name	The SSID (Service Set Identity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.

Table 23 Network Setting &gt; Wireless &gt; Guest/More AP &gt; Edit (continued)

LABEL	DESCRIPTION
Guest WLAN	Select this to create Guest WLANs for home and external clients. Select the WLAN type in the <b>Access Scenario</b> field.
Access Scenario	If you select <b>Home Guest</b> , clients connecting to the same SSID can communicate with each other directly.  If you select <b>External Guest</b> , clients are blocked from connecting to each other directly.  Move your mouse over the network icon next to the drop-down list box to view the corresponding network topology.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
SSID Subnet	Select <b>Enable</b> if you want the wireless network interface to assign DHCP IP addresses to the associated wireless clients.
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool.  The VMG assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the VMG for the SSID subnet.
LAN IP Address	Specify the IP address of the VMG for the SSID subnet.
Security Level	
Security Mode	Select <b>Basic (WEP)</b> or <b>More Secure (WPA-PSK, WPA2-PSK, WPA-WPA2-PSK)</b> 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 VMG. After you select to use a security, additional options appears in this screen.  Or you can select <b>No Security</b> to allow any client to associate this network without any data encryption or authentication.  See <a href="#">Section 7.2.1 on page 98</a> for more details about this field.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 7.4 The MAC Authentication Screen

This screen allows you to configure the VMG to give exclusive access to specific devices (Allow) or exclude specific devices from accessing the VMG (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:C5:01:23:45. You need to know the MAC addresses of the devices to configure this screen.

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



**Figure 41** Network Setting > Wireless > MAC Authentication

**General**

SSID: ZyxeL_1FA3

MAC Restrict Mode: Disable

**MAC address List**

Add new MAC address

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

**Note:**

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

Apply Cancel

The following table describes the labels in this screen.

**Table 24** Network Setting > Wireless > Authentication

LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the MAC address list. Select <b>Disable</b> to turn off MAC filtering. Select <b>Deny</b> to block access to the VMG. MAC addresses not listed will be allowed to access the VMG. Select <b>Allow</b> to permit access to the VMG. MAC addresses not listed will be denied access to the VMG.
MAC address List	
Add new MAC address	Click this if you want to add a new MAC address entry to the MAC filter list below. This button is not configurable when you select <b>Disable</b> in the <b>MAC Restrict Mode</b> field. Enter the MAC addresses of the wireless devices that are allowed or denied access to the VMG. 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 VMG.
Modify	Click the <b>Edit</b> icon to change the MAC address. Click the <b>Delete</b> icon to remove the entry.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 7.5 The WPS Screen

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

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 7.9.8.3 on page 118](#) for more information about WPS.

Note: The VMG applies the security settings of the **SSID1** profile (see [Section 7.2 on page 97](#)). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** 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 42** Network Setting > Wireless > WPS

The following table describes the labels in this screen.

**Table 25** Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
WPS	Select <b>Enable</b> to activate WPS on this VMG.
Add a new device with WPS Method	
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (PBC). Select <b>Enable</b> and click <b>Apply</b> to activate WPS method 1 on the VMG.
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the VMG) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the <b>WPS</b> button on this screen.  Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2	Use this section to set up a WPS wireless network by entering the PIN of the client into the VMG. Select <b>Enable</b> and click <b>Apply</b> to activate WPS method 2 on the VMG.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click <b>Register</b> 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 VMG.
Method 3	Use this section to set up a WPS wireless network by entering the PIN of the VMG into the client. Select <b>Enable</b> and click <b>Apply</b> to activate WPS method 3 on the VMG.

Table 25 Network Setting &gt; Wireless &gt; WPS (continued)

LABEL	DESCRIPTION
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 VMG.
Generate New PIN Number	If this method has been enabled, the PIN (Personal Identification Number) of the VMG 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 <b>Generate New PIN</b> button to have the VMG create a new PIN.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 7.6 The WMM Screen

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

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

Figure 43 Network Setting &gt; Wireless &gt; WMM

WMM of SSID1 :  Enable  Disable  
WMM of SSID2 :  Enable  Disable  
WMM of SSID3 :  Enable  Disable  
WMM of SSID4 :  Enable  Disable  
WMM Automatic Power Save Delivery (APSD) :  Enable  Disable

The following table describes the labels in this screen.

Table 26 Network Setting &gt; Wireless &gt; WMM

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

## 7.7 The Others Screen

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

See [Section 7.9.2 on page 112](#) for detailed definitions of the terms listed in this screen.

**Figure 44** Network Setting > Wireless > Others

RTS/CTS Threshold :	<input type="text" value="2347"/>
Fragmentation Threshold :	<input type="text" value="2346"/>
Output Power :	<input type="text" value="100%"/> ▾
Beacon Interval :	<input type="text" value="100"/> ms
DTIM Interval :	<input type="text" value="1"/> ms
802.11 Mode :	<input type="text" value="802.11b/g/n Mixed"/> ▾
802.11 Protection :	<input type="text" value="Off"/> ▾
Preamble :	<input type="text" value="Long"/> ▾
OBSS Coexistence	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the labels in this screen.

**Table 27** Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the VMG. 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: <b>20%</b> , <b>40%</b> , <b>60%</b> , <b>80%</b> or <b>100%</b> .
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again.  The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50ms to 1000ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
802.11 Mode	Select <b>802.11b Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the VMG.  Select <b>802.11g Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the VMG.  Select <b>802.11n Only</b> to allow only IEEE 802.11n compliant WLAN devices to associate with the VMG.  Select <b>802.11b/g Mixed</b> to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the VMG. The transmission rate of your VMG might be reduced.  Select <b>802.11b/g/n Mixed</b> to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the VMG. The transmission rate of your VMG might be reduced.

Table 27 Network Setting &gt; Wireless &gt; Others (continued)

LABEL	DESCRIPTION
802.11 Protection	<p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select <b>Auto</b> to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select <b>Off</b> to disable 802.11 protection. The transmission rate of your VMG might be reduced in a mixed-mode network.</p> <p>This field displays <b>Off</b> and is not configurable when you set <b>802.11 Mode</b> to <b>802.11b Only</b>.</p>
Preamble	<p>Select a preamble type from the drop-down list box. Choices are <b>Long</b> or <b>Short</b>. See <a href="#">Section 7.9.7 on page 116</a> for more information.</p> <p>This field is configurable only when you set 802.11 Mode to <b>802.11b</b>.</p>
OBSS Coexistence	<p>Select <b>Enable</b> to allow the coexistence of 20 MHz and 40 MHz Overlapping Basic Service Sets (OBSS) in wireless local area networks. Select <b>Disabled</b> to disable this feature.</p>
Apply	<p>Click <b>Apply</b> to save your changes.</p>
Cancel	<p>Click <b>Cancel</b> to restore your previously saved settings.</p>

## 7.8 The Channel Status Screen

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

Note: The **Scan** button only works when the VMG uses 20MHz for the wireless channel width. You can go to the **Network Setting > Wireless > General** screen, click the **more** link, and then change the channel width setting in the **Bandwidth** field.

Figure 45 Network Setting &gt; Wireless &gt; Channel Status



## 7.9 Technical Reference

This section discusses wireless LANs in depth. For more information, see [Appendix B on page 266](#).

### 7.9.1 Wireless Network Overview

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

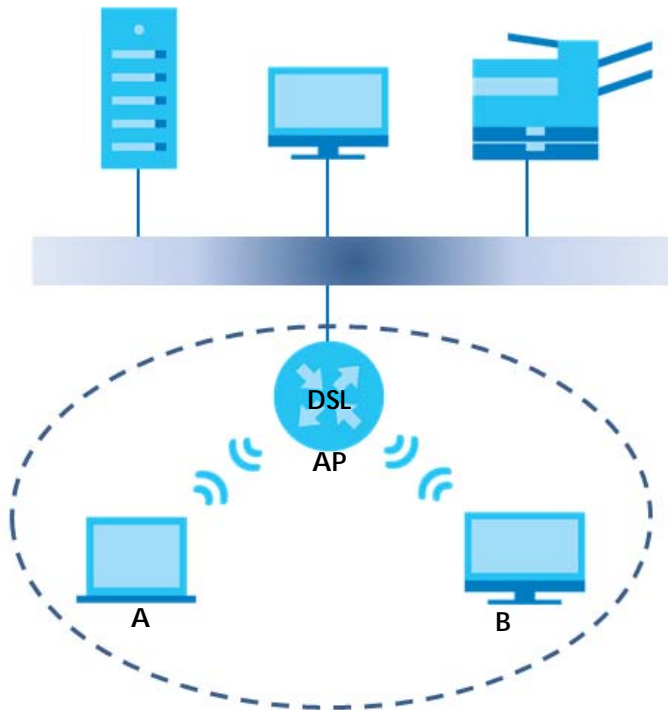
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, 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 46** 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 VMG 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.

## 7.9.2 Additional Wireless Terms

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

Table 28 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	<p>In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.</p> <p>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the VMG. The lower the value, the more often the devices must get permission.</p> <p>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the VMG.</p>
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the VMG does, it cannot communicate with the VMG.
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.

## 7.9.3 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.

### 7.9.3.1 SSID

Normally, the VMG acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the VMG 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.

### 7.9.3.2 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 VMG 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.

### 7.9.3.3 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.

### 7.9.3.4 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 7.9.3.3 on page 113](#) 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 VMG and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

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

When you select **WPA2** or **WPA2-PSK** in your VMG, 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 VMG.

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.

### 7.9.4 Signal Problems

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

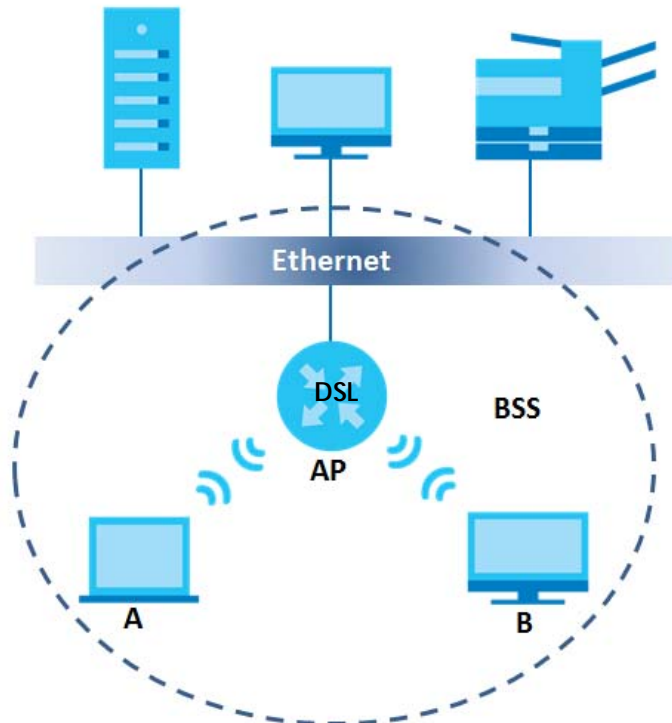
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters 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.

## 7.9.5 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 47** Basic Service Set



## 7.9.6 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 VMG'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.

### 7.9.6.1 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.

## 7.9.7 Preamble Type

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

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

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

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

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

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

## 7.9.8 WiFi Protected Setup (WPS)

Your VMG 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.

### 7.9.8.1 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 VMG, see [Section 7.6 on page 107](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the VMG you must press the WPS button for more than five seconds.

- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

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

### 7.9.8.2 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.

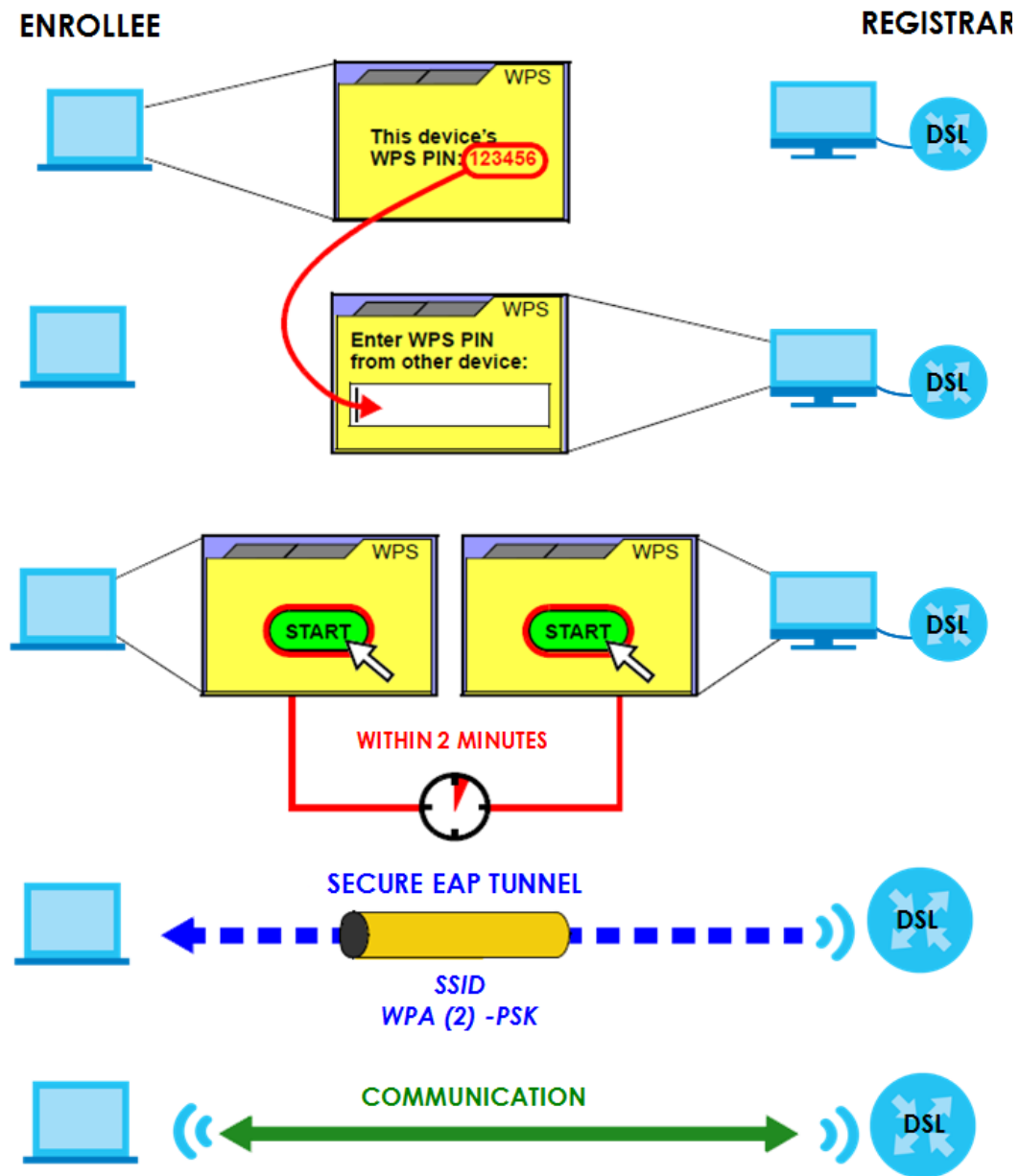
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 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 VMG, see [Section 7.5 on page 105](#)).
- 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 48 Example WPS Process: PIN Method

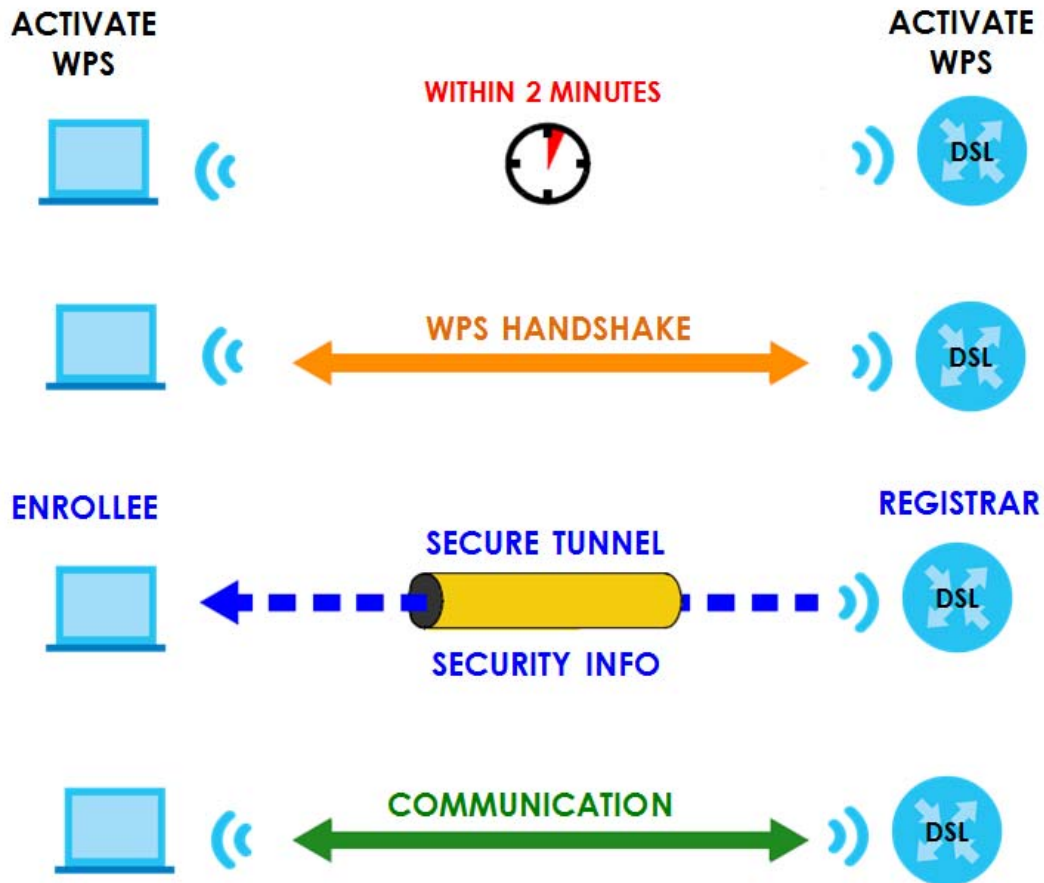


### 7.9.8.3 How WPS Works

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

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

Figure 49 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.

#### 7.9.8.4 Example WPS Network Setup

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

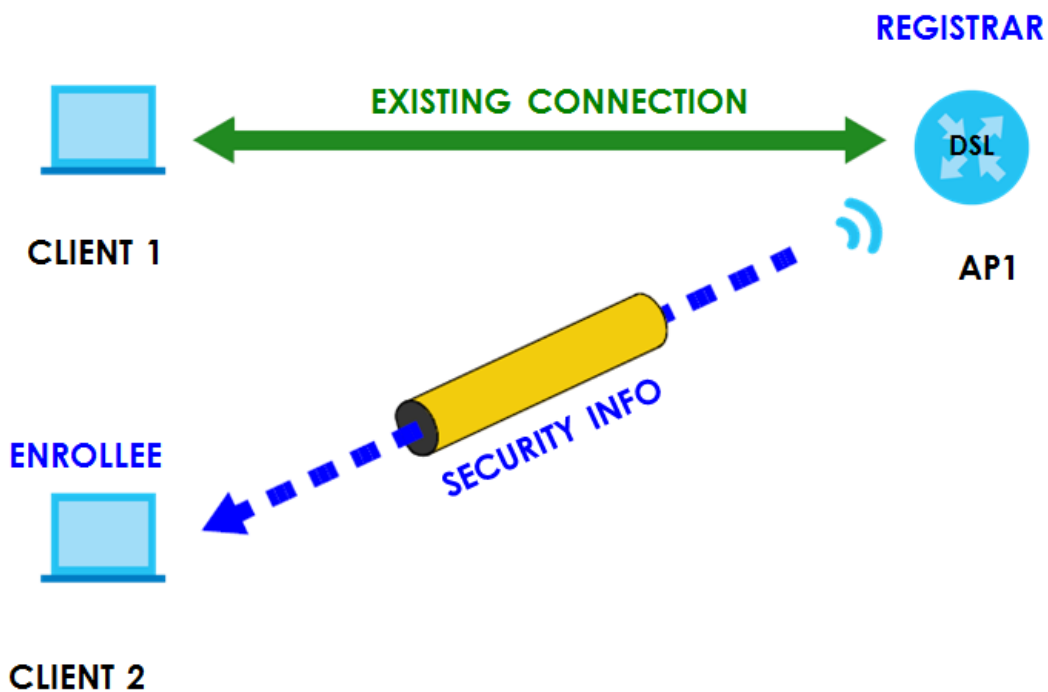
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 50 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**.

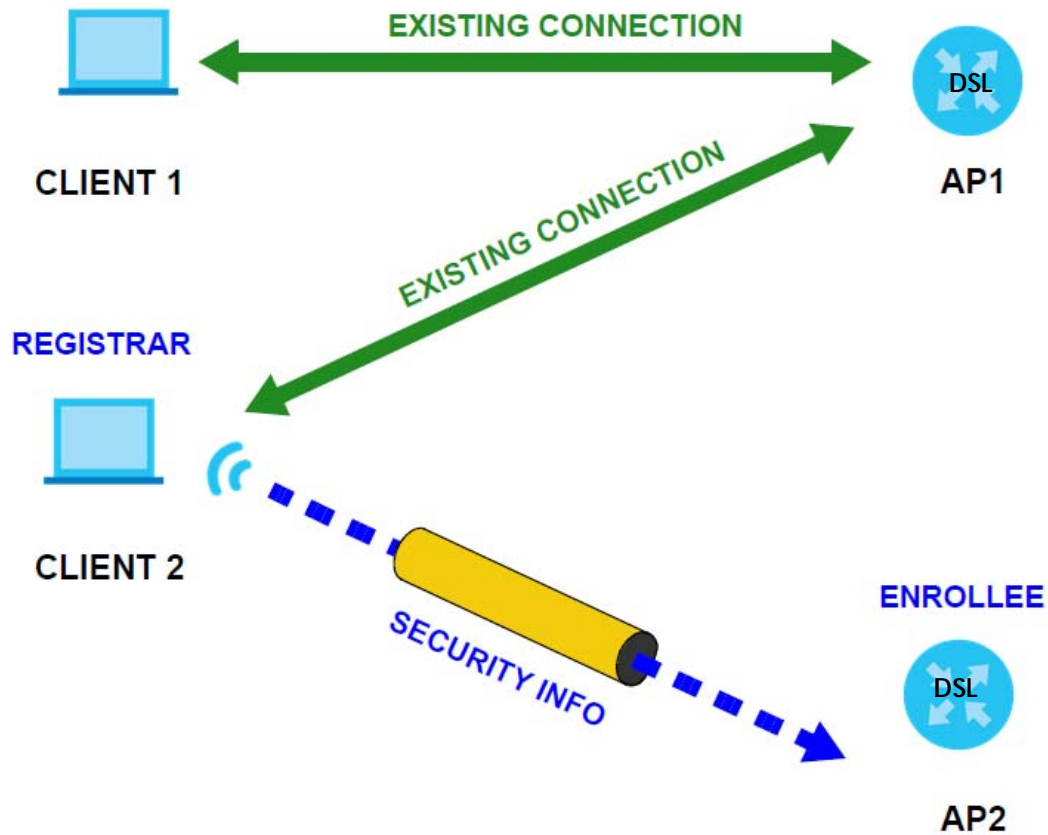
Figure 51 WPS: Example Network Step 2



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 52 WPS: Example Network Step 3



### 7.9.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

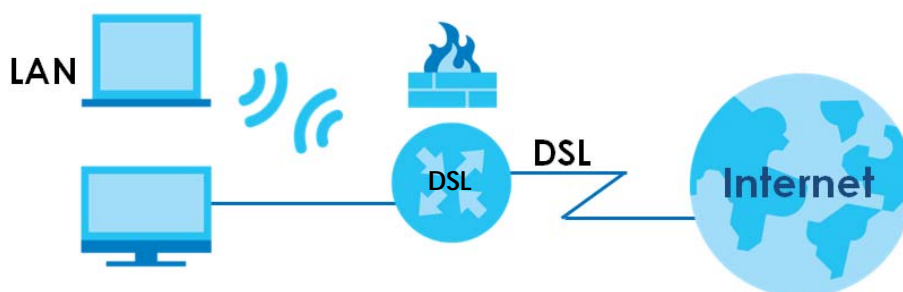
# CHAPTER 8

## Home Networking

### 8.1 Overview

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

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



#### 8.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your VMG ([Section 8.2 on page 125](#)).
- 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 129](#)).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the VMG ([Section 8.4 on page 130](#)).
- Use the **Additional Subnet** screen to configure IP alias and public static IP ([Section 8.5 on page 133](#)).
- Use the **STB Vendor ID** screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the VMG automatically create static DHCP entries for the STB devices when they request IP addresses ([Section 8.6 on page 134](#)).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. ([Section 8.7 on page 134](#)).
- Use the **TFTP Server Name** screen to set a TFTP server address which is passed to the clients using DHCP option 66. ([Section 8.8 on page 135](#)).

## 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 VMG an IP address, subnet mask, DNS and other routing information when it's turned on.

#### DNS

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

#### RADVD (Router Advertisement Daemon)

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

### 8.1.2.2 About UPnP

#### Identifying UPnP Devices

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

#### NAT Traversal

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

- Dynamic port mapping
- Learning public IP addresses

- Assigning lease times to mappings

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

See the [Chapter 11 on page 163](#) 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 VMG allows multicast messages on the LAN only.

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

### UPnP and Zyxel

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

See [Section 8.4.1 on page 131](#) for examples of installing and using UPnP.

### Finding Out More

See [Section 8.9 on page 135](#) for technical background information on LANs.

## 8.1.3 Before You Begin

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

## 8.2 The LAN Setup Screen

Use this screen to set the Local Area Network IP address and subnet mask of your VMG. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

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

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

**Figure 53** Network Setting > Home Networking > LAN Setup

**Interface Group**  
Group Name:

**LAN IP Setup**  
IP Address:   
Subnet Mask:

**DHCP Server State**  
DHCP:  Enable  Disable  DHCP Relay

**IP Addressing Values**  
Beginning IP Address:   
Ending IP Address:   
Auto reserve IP for the same host:  Enable  Disable

**DHCP Server Lease Time**  
 Days  Hours  Minutes

**DNS Values**  
DNS:  DNS Proxy  Static  From ISP

**LAN IPv6 Mode Setup**  
IPv6 Active:  Enable  Disable

**Link Local Address Type**  
 EUI64  
 Manual

**Lan Global Identifier Type**  
 EUI64  
 Manual

**LAN IPv6 Address Setup**  
 Delegate prefix from WAN  Static

**LAN IPv6 Address Assign Setup**

**LAN IPv6 DNS Assign Setup**

**DHCPv6 Configuration**  
DHCPv6 Active:  DHCPv6 Server:

**IPv6 Router Advertisement State**  
RADVD Active:  Enable:

**IPv6 DNS Values**  
IPv6 DNS Server 1:    
IPv6 DNS Server 2:    
IPv6 DNS Server 3:

**DNS Query Scenario:**

The following table describes the fields in this screen.

Table 30 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group name for which you want to configure LAN settings. See <a href="#">Chapter 13 on page 183</a> for how to create a new interface group.
LAN IP Setup	
IP Address	Enter the LAN IPv4 address you want to assign to your VMG 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).
DHCP Server State	
DHCP	Select <b>Enable</b> to have the VMG act as a DHCP server or DHCP relay agent. Select <b>Disable</b> to stop the DHCP server on the VMG. Select <b>DHCP Relay</b> to have the VMG forward DHCP request to the DHCP server.
DHCP Relay Server Address	This field is only available when you select <b>DHCP Relay</b> in the <b>DHCP</b> field.
IP Address	Enter the IPv4 address of the actual remote DHCP server in this field.
IP Addressing Values	This field is only available when you select <b>Enable</b> in the <b>DHCP</b> field.
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Select <b>Enable</b> to have the VMG record DHCP IP addresses with the MAC addresses the IP addresses are assigned to. The VMG assigns the same IP address to the same MAC address when the host requests an IP address again through DHCP.
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.  This field is only available when you select <b>Enable</b> in the <b>DHCP</b> field.
Days/Hours/Minutes	Enter the lease time of the DHCP server.
DNS Values	This field is only available when you select <b>Enable</b> in the <b>DHCP</b> field.
DNS	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information.  Select <b>DNS Proxy</b> if you have the DNS proxy service. The VMG redirects clients' DNS queries to a DNS server for resolving domain names.  Select <b>Static</b> if you have the IP address of a DNS server.
DNS Server 1/2	Enter the first and second DNS (Domain Name System) server IP addresses the VMG passes to the DHCP clients.
LAN IPv6 Mode Setup	
IPv6 Active	Select <b>Enable</b> to activate the IPv6 mode and configure IPv6 settings on the VMG.
Link Local Address Type	
EUI64	Select this to have the VMG generate an interface ID for the LAN interface's link-local address using the EUI-64 format.

Table 30 Network Setting &gt; Home Networking &gt; LAN Setup (continued)

LABEL	DESCRIPTION
Manual	Select this to manually enter an interface ID for the LAN interface's link-local address.
LAN Global Identifier Type	
EUI64	Select this to have the VMG generate an interface ID using the EUI-64 format for its global address.
Manual	Select this to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN IPv6 Address Setup	
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the VMG's LAN IPv6 address.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: <ul style="list-style-type: none"> <li>• <b>Stateless:</b> The VMG uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the VMG send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled.</li> <li>• <b>Stateful:</b> The VMG uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the VMG act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.</li> </ul>
LAN IPv6 DNS Assign Setup	Select how the VMG provide DNS server and domain name information to the clients: <ul style="list-style-type: none"> <li>• <b>From Router Advertisement:</b> The VMG provides DNS information through router advertisements.</li> <li>• <b>From DHCPv6 Server:</b> The VMG provides DNS information through DHCPv6.</li> <li>• <b>From RA &amp; DHCPv6 Server:</b> The VMG provides DNS information through both router advertisements and DHCPv6.</li> </ul>
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. <b>DHCPv6 Server</b> displays if you configured the VMG to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 DNS Values	
IPv6 DNS Server 1-3	Select <b>From ISP</b> if your ISP dynamically assigns IPv6 DNS server information. Select <b>User-Defined</b> if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the VMG passes to the DHCP clients. Select <b>None</b> if you do not want to configure IPv6 DNS servers.
DNS Query Scenario	Select how the VMG handles clients' DNS information requests. <ul style="list-style-type: none"> <li>• <b>IPv4/IPv6 DNS Server:</b> The VMG forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives.</li> <li>• <b>IPv6 DNS Server Only:</b> The VMG forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives.</li> <li>• <b>IPv4 DNS Server Only:</b> The VMG forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives.</li> <li>• <b>IPv6 DNS Server First:</b> The VMG forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives.</li> <li>• <b>IPv4 DNS Server First:</b> The VMG forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives.</li> </ul>
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.



## 8.3 The Static DHCP Screen

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

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

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

**Figure 54** Network Setting > Home Networking > Static DHCP

Static DHCP Configuration				
#	Status	MAC Address	IP Address	Modify

The following table describes the labels in this screen.

**Table 31** Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the VMG.
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 <b>Edit</b> icon to have the IP address field editable and change it.  Click the <b>Delete</b> icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

If you click **Static DHCP Configuration** in the **Static DHCP** screen or the Edit icon next to a static DHCP entry, the following screen displays.

Figure 55 Static DHCP: Static DHCP Configuration/Edit

The following table describes the labels in this screen.

Table 32 Static DHCP: Static DHCP Configuration/Edit

LABEL	DESCRIPTION
Active	Select <b>Enable</b> to activate the connection between the client and the VMG. Otherwise, select <b>Disable</b> to deactivate.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See <a href="#">Chapter 13 on page 183</a> for how to create a new interface group.
IP Type	This field displays <b>IPv4</b> for the type of the DHCP IP address. At the time of writing, it is not allowed to select other type.
Select Device Info	Select a device or computer from the drop-down list or select <b>Manual Input</b> to manually enter a device's MAC address and IP address in the following fields.
MAC Address	If you select <b>Manual Input</b> , enter the MAC address of a computer on your LAN.
IP Address	If you select <b>Manual Input</b> , 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 <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> 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 124](#) for more information on UPnP.

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

**Figure 56** Network Setting > Home Networking > UPnP

The following table describes the labels in this screen.

**Table 33** Network Setting > Home Networking > UPnP

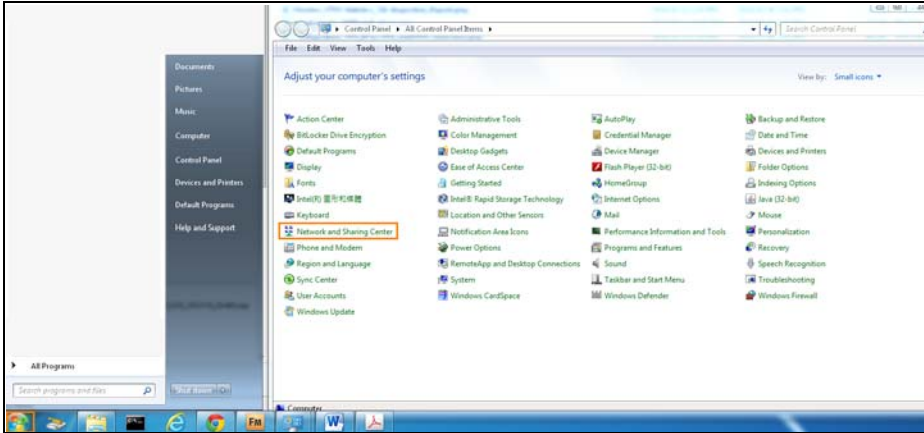
LABEL	DESCRIPTION
UPnP	Select <b>Enable</b> to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the VMG's IP address (although you must still enter the password to access the web configurator).
UPnP NAT-T	Select <b>Enable</b> to allow UPnP-enabled applications to automatically configure the VMG so that they can communicate through the VMG by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.  The table below displays the NAT port forwarding rules added automatically by UPnP NAT-T.
#	This is the index number of the UPnP NAT-T connection.
Description	This is the description of the UPnP NAT-T connection.
Destination IP Address	This is the IP address of the other connected UPnP-enabled device.
External Port	This is the external port number that identifies the service.
Internal Port	This is the internal port number that identifies the service.
Protocol	This is the transport layer protocol used for the service.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

### 8.4.1 Turning On UPnP in Windows 7 Example

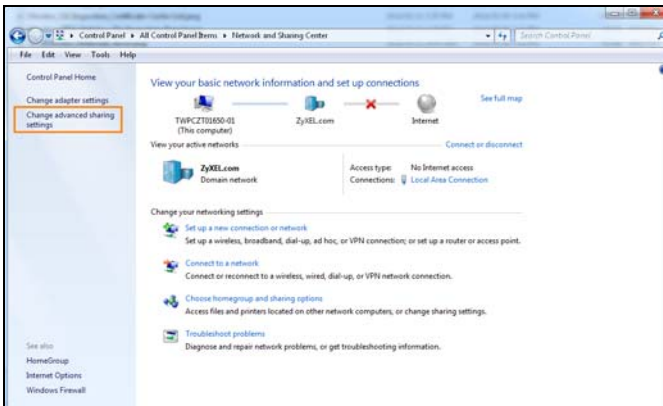
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the VMG.

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

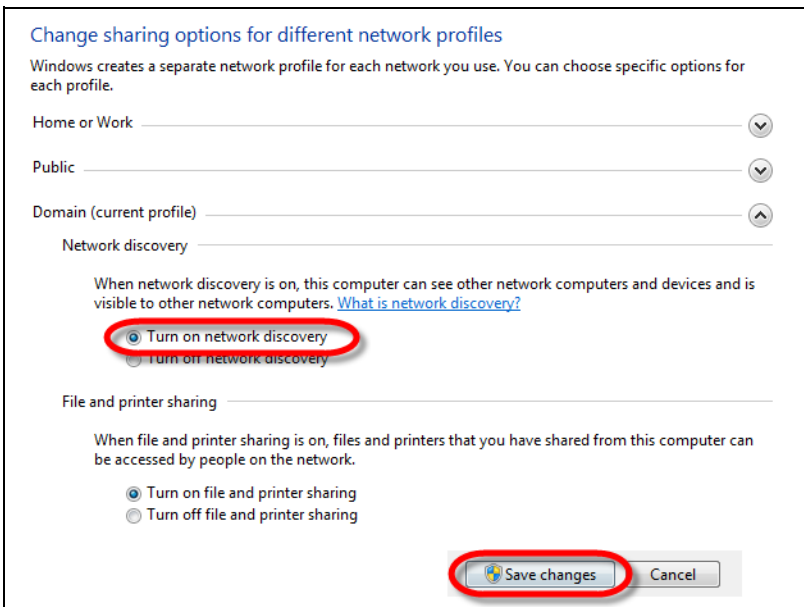
- 1 Click the start icon, **Control Panel** and then the **Network and Sharing Center**.



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



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



## 8.5 The Additional Subnet Screen

Use the **Additional Subnet** screen to configure IP alias and public static IP.

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The VMG supports multiple logical LAN interfaces via its physical Ethernet interface with the VMG itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

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

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

**Figure 57** Network Setting > Home Networking > Additional Subnet

The following table describes the labels in this screen.

**Table 34** Network Setting > Home Networking > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See <a href="#">Chapter 13 on page 183</a> for how to create a new interface group.
Active	Select <b>Enable</b> to configure a LAN network for the VMG.
IPv4 Address	Enter the IP address of your VMG in dotted decimal notation.
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).
Public LAN	
Active	Select <b>Enable</b> to turn on the Public LAN feature. Your ISP must support Public LAN and Static IP.
IPv4 Address	Enter the public IP address provided by your ISP.
Subnet Mask	Enter the public IP subnet mask provided by your ISP.
Offer Public IP by DHCP	Select <b>Enable</b> to allow the VMG to provide public IP addresses by DHCP server.
Enable ARP Proxy	Select <b>Enable</b> to activate the ARP (Address Resolution Protocol) proxy.

Table 34 Network Setting &gt; Home Networking &gt; Additional Subnet (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 8.6 The STB Vendor ID Screen

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

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

Figure 58 Network Setting &gt; Home Networking &gt; STB Vendor ID

The following table describes the labels in this screen.

Table 35 Network Setting &gt; Home Networking &gt; STB Vendor ID

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

## 8.7 The Wake on LAN Screen

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

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

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

Figure 59 Network Setting &gt; Home Networking &gt; Wake on LAN

The following table describes the labels in this screen.

Table 36 Network Setting > Home Networking > Wake on LAN

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

## 8.8 The TFTP Server Name Screen

Use the **TFTP Server Name** screen to set the TFTP server address which is passed to the clients using DHCP option 66. The DHCP clients in the VMG local network, such as STB devices, can then use the TFTP server address or domain name for configuration file download. RFC 2132 defines the option 66 open standard. DHCP option 66 carries the IP address or the domain name of a single TFTP server.

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

Figure 60 Network Setting > Home Networking > TFTP Server Name



The following table describes the labels in this screen.

Table 37 Network Setting > Home Networking > TFTP Server Name

LABEL	DESCRIPTION
TFTP Server Name	Enter the IP address or the domain name of a single TFTP server.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

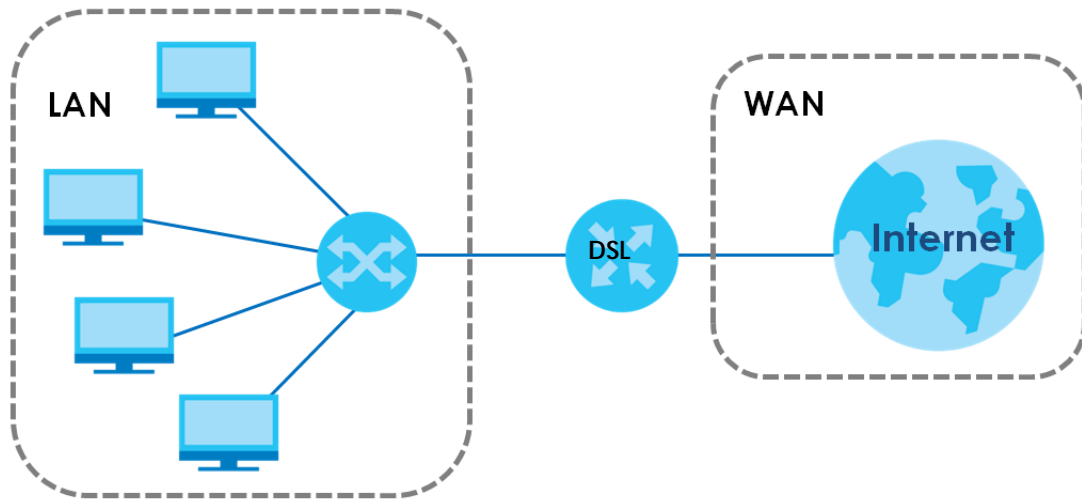
## 8.9 Technical Reference

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

### 8.9.1 LANs, WANs and the VMG

The actual physical connection determines whether the VMG 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 61 LAN and WAN IP Addresses



## 8.9.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the VMG as a DHCP server or disable it. When configured as a server, the VMG 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 VMG is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

## 8.9.3 DNS Server Addresses

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

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

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

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



## 8.9.4 LAN TCP/IP

The VMG 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 VMG. 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 VMG, 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 VMG 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 VMG unless you are instructed to do otherwise.

### Private IP Addresses

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

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

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

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

# CHAPTER 9

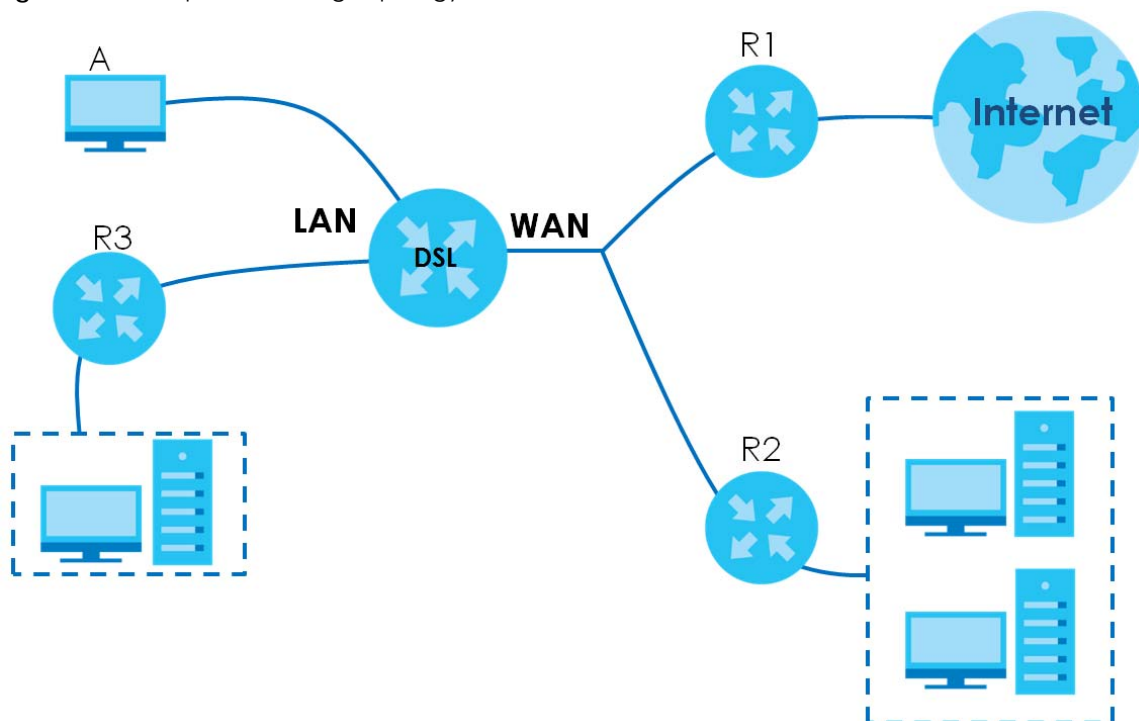
## Routing

### 9.1 Overview

The VMG usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the VMG 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 VMG's LAN interface. The VMG routes most traffic from **A** to the Internet through the VMG'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 62** Example of Routing Topology



### 9.2 The Routing Screen

Use this screen to view and configure the static route rules on the VMG. Click **Network Setting > Routing > Static Route** to open the following screen.

Figure 63 Network Setting &gt; Routing &gt; Static Route

Add new Static Route							
#	Status	Name	Destination IP	Subnet Mask/Prefix Length	Gateway	Interface	Modify

The following table describes the labels in this screen.

Table 38 Network Setting &gt; Routing &gt; Static Route

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

## 9.2.1 Add/Edit Static Route

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

Figure 64 Routing: Add/Edit

The following table describes the labels in this screen.

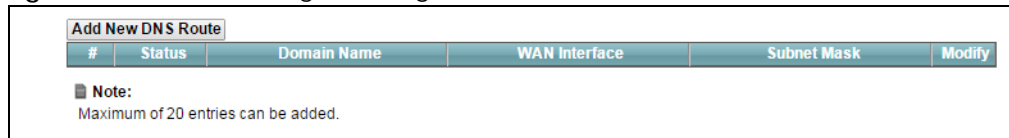
Table 39 Routing: Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.  Select <b>Enable</b> to activate the static route. Select <b>Disable</b> to deactivate this static route without having to delete the entry.
Route Name	Enter a descriptive name for the static route.
IP Type	Select whether your IP type is <b>IPv4</b> or <b>IPv6</b> .
Destination IP Address	Enter the IPv4 or IPv6 network address of the final destination.
IP Subnet Mask	If you are using IPv4 and need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. Enter the IP subnet mask here.
Use Gateway IP Address	The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.  If you want to use the gateway IP address, select <b>Enable</b> .
Gateway IP Address	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 9.3 The DNS Route Screen

Use this screen to view and configure DNS routes on the VMG. Click **Network Setting > Routing > DNS Route** to open the following screen.

Figure 65 Network Setting &gt; Routing &gt; DNS Route



#	Status	Domain Name	WAN Interface	Subnet Mask	Modify
<p><b>Note:</b> Maximum of 20 entries can be added.</p>					

The following table describes the labels in this screen.

Table 40 Network Setting &gt; Routing &gt; DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to add a new DNS route.
#	This is the index number of a DNS route.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.
Domain Name	This is the host name or domain name of the DNS route entry.
WAN Interface	This is the WAN connection through which the VMG forwards DNS requests for this domain name.

Table 40 Network Setting &gt; Routing &gt; DNS Route (continued)

LABEL	DESCRIPTION
Subnet Mask	This is the subnet mask of the DNS route entry.
Modify	Click the <b>Edit</b> icon to modify the DNS route. Click the <b>Delete</b> icon to delete the DNS route.

### 9.3.1 The DNS Route Add Screen

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

Figure 66 DNS Route Add

The following table describes the labels in this screen.

Table 41 DNS Route Add

LABEL	DESCRIPTION
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the DNS route.
Domain Name	Enter the domain name of the DNS route entry.
Subnet Mask	Enter the subnet mask of the DNS route entry.
WAN Interface	Select the WAN connection through which the VMG forwards DNS requests for this domain name. <b>WWAN</b> means the wireless cellular interface.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving any changes.

## 9.4 The Policy Route Screen

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

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

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

**Figure 67** Network Setting > Routing > Policy Route

Add New Policy Route										
#	Status	Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Source Interface	WAN Interface	Modify

The following table describes the labels in this screen.

Table 42 Network Setting > Routing > Policy Route

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

## 9.4.1 Add/Edit Policy Route

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

**Figure 68** Policy Route: Add/Edit

The following table describes the labels in this screen.

**Table 43** Policy Route: Add/Edit

LABEL	DESCRIPTION
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the policy route.
Route Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol ( <b>TCP</b> or <b>UDP</b> ).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (ex: br0 or LAN1~LAN4)	Type the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the <b>Broadband</b> screens. <b>WWAN</b> means the wireless cellular interface.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 9.5 RIP

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

## 9.5.1 The RIP Screen

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

Figure 69 RIP

#	Interface	Version	Operation	Enable	Disable DefaultGateway
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					
<p>RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).</p>					

The following table describes the labels in this screen.

Table 44 RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the VMG sends (it recognizes both formats when receiving). RIP version 1 is universally supported but RIP version 2 carries more information. RIP version 1 is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select <b>Passive</b> to have the VMG update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface.  Select <b>Active</b> to have the VMG advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the check box to activate the settings.
Disable Default Gateway	Select the check box to set the VMG to not send the route information to the default gateway.
Apply	Click <b>Apply</b> to save your changes back to the VMG.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.



# CHAPTER 10

## Quality of Service (QoS)

### 10.1 Overview

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

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

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

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

This chapter contains information about configuring QoS and editing classifiers.

#### 10.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable QoS and set the upstream bandwidth ([Section 10.3 on page 147](#)).
- Use the **Queue Setup** screen to configure QoS queue assignment ([Section 10.4 on page 148](#)).
- Use the **Classification Setup** screen to add, edit or delete QoS classifiers ([Section 10.5 on page 151](#)).
- Use the **Shaper Setup** screen to limit outgoing traffic transmission rate on the selected interface ([Section 10.6 on page 155](#)).
- Use the **Policer Setup** screen to control incoming traffic transmission rate and bursts ([Section 10.6 on page 155](#)).

## 10.2 What You Need to Know

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

### QoS versus Cos

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

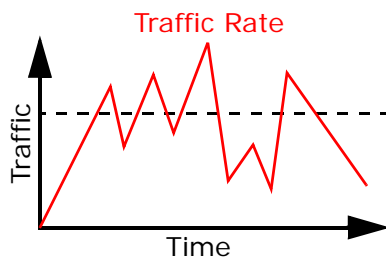
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

### Tagging and Marking

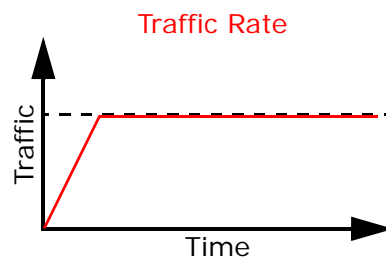
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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

### Traffic Shaping

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



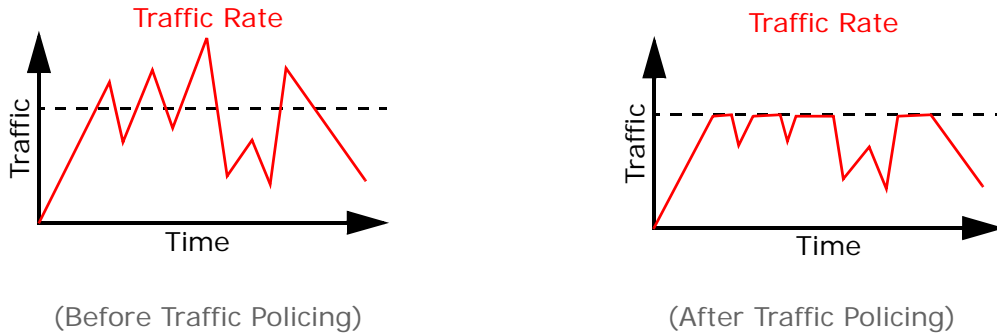
(Before Traffic Shaping)



(After Traffic Shaping)

## Traffic Policing

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



The VMG supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Marker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See [Section 10.8 on page 158](#) for more information on each metering algorithm.

## 10.3 The Quality of Service General Screen

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

Use this screen to enable or disable QoS and set the upstream bandwidth. See [Section 10.1 on page 145](#) for more information.

**Figure 70** Network Settings > QoS > General

QoS  Enable  Disable (Settings are invalid when disabled)

WAN Managed Upstream Bandwidth :  (kbps)

LAN Managed Downstream Bandwidth :  (kbps)

Upstream Traffic Priority Assigned by:

**Note**

1. You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.
2. If Upstream Traffic Priority is selected, 8 level strict priority QoS will be applied automatically according to the selected criteria. In this mode, user manually defined QoS will not be applied until Auto-Priority Mapping is disabled.
3. If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

The following table describes the labels in this screen.

Table 45 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Select the <b>Enable</b> check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	<p>Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.</p> <p>You can set this number higher than the interfaces' actual transmission speed. The VMG uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed.</p> <p>You can also set this number lower than the interfaces' actual transmission speed. This will cause the VMG to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the VMG automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.</p>
LAN Managed Downstream Bandwidth	<p>Enter the amount of downstream bandwidth for the LAN interfaces (including WLAN) that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection.</p> <p>You can also set this number lower than the WAN interfaces' actual transmission speed. This will cause the VMG to not use some of the interfaces' available bandwidth.</p> <p>If you leave this field blank, the VMG automatically sets this to the LAN interfaces' maximum supported connection speed.</p>
Upstream Traffic Priority Assigned by	<p>Select how the VMG assigns priorities to various upstream traffic flows.</p> <ul style="list-style-type: none"> <li>• <b>None:</b> Disables auto priority mapping and has the VMG 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.</li> <li>• <b>Ethernet Priority:</b> Automatically assign priority based on the IEEE 802.1p priority level.</li> <li>• <b>IP Precedence:</b> Automatically assign priority based on the first three bits of the TOS field in the IP header.</li> <li>• <b>Packet Length:</b> 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.</li> </ul>
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 10.4 The Queue Setup Screen

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

Use this screen to configure QoS queue assignment.

Figure 71 Network Setting &gt; QoS &gt; Queue Setup

General Queue Setup Classification Setup Shaper Setup Policer Setup									
Queue Setup decides the priority on WAN/LAN interfaces. Use this page to configure QoS queue assignment.									
#	Status	Name	Interface	Discipline	Priority	Weight	Buffer Management	Rate Limit	Modify
1		Highest	WAN	SP	1	8	DT	N/A	
2		High	WAN	SP	2	5	DT	N/A	
3		Medium	WAN	SP	3	3	DT	N/A	
4		Low	WAN	SP	4	1	DT	N/A	
<p><b>Note</b> Priority level 1 is the highest priority for QoS.</p>									

The following table describes the labels in this screen.

Table 46 Network Setting &gt; QoS &gt; Queue Setup

LABEL	DESCRIPTION
Add New Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the VMG's interface through which traffic in this queue passes.
Discipline	This shows the queuing method of this queue.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the VMG should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the <b>Edit</b> icon to edit the queue. Click the <b>Delete</b> icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

## 10.4.1 Editing a QoS Queue

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

**Figure 72** Queue Setup: Edit

The following table describes the labels in this screen.

**Table 47** Queue Setup: Add

LABEL	DESCRIPTION
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.
Discipline	Select <b>SPQ</b> (Strict Priority Queuing) or <b>WRR</b> (Weighted Round Robin).  Strict Priority Queuing ( <b>SP</b> ) services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q1 has the highest priority and Q4 the lowest.  Weighted Round Robin Scheduling ( <b>WRR</b> ) services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights
Priority	Select the priority level (from 1 to 7) of this queue.  The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue.  If two queues have the same priority level, the VMG divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays <b>Drop Tail (DT)</b> . <b>Drop Tail (DT)</b> is a simple queue management algorithm that allows the VMG buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.

Table 47 Queue Setup: Add (continued)

LABEL	DESCRIPTION
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 10.5 The Classification Setup Screen

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

You can give different priorities to traffic that the VMG 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 > Classification Setup** to open the following screen.

Figure 73 Network Setting &gt; QoS &gt; Classification Setup

Order	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
-------	--------	------------	-------------------------	-----------	-------------	-------------	----------	--------

The following table describes the labels in this screen.

Table 48 Network Setting &gt; QoS &gt; Classification Setup

LABEL	DESCRIPTION
Add New Classification	Click this to create a new classifier.
Order	This is the index number of the entry. The classifiers are applied in order of their numbering.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the <b>Edit</b> icon to edit the classifier.  Click the <b>Delete</b> icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

## 10.5.1 Add/Edit QoS Class

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

**Figure 74** Classification Setup: Add/Edit

**Add New Classification**
✕

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

**Step1: Class Configuration**

Active  Enable  Disable

Class Name

Classification Order:  ▼

**Step2: Criteria Configuration**

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

**Basic**

From Interface  ▼

Ether Type  ▼

**Source**

<input type="checkbox"/> Address	<input style="width: 100%;" type="text"/>	Subnet Mask	<input style="width: 100%;" type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	<input style="width: 50%;" type="text"/> ~ <input style="width: 50%;" type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	<input style="width: 50%;" type="text"/> - <input style="width: 50%;" type="text"/>	MAC Mask	<input style="width: 100%;" type="text"/>	<input type="checkbox"/> Exclude

**Destination**

<input type="checkbox"/> Address	<input style="width: 100%;" type="text"/>	Subnet Mask	<input style="width: 100%;" type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	<input style="width: 50%;" type="text"/> ~ <input style="width: 50%;" type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	<input style="width: 50%;" type="text"/> - <input style="width: 50%;" type="text"/>	MAC Mask	<input style="width: 100%;" type="text"/>	<input type="checkbox"/> Exclude

**Others**

<input type="checkbox"/> Service	<input type="text" value="Age of Empires"/> ▼	<input type="checkbox"/> Exclude
<input type="checkbox"/> IP protocol	<input type="text" value="TCP"/> ▼ <input style="width: 50%;" type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> DHCP	<input style="width: 100%;" type="text"/> ▼	<input type="checkbox"/> Exclude
<input type="checkbox"/> Packet Length	<input style="width: 50%;" type="text"/> ~ <input style="width: 50%;" type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> DSCP	<input style="width: 50%;" type="text"/> (0~63)	<input type="checkbox"/> Exclude
<input type="checkbox"/> 802.1P	<input type="text" value="0 BE"/> ▼	<input type="checkbox"/> Exclude
<input type="checkbox"/> VLAN ID	<input style="width: 50%;" type="text"/> (1~4095)	<input type="checkbox"/> Exclude
<input type="checkbox"/> TCP ACK		<input type="checkbox"/> Exclude

**Step3: Packet Modification**

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

DSCP Mark  ▼  (0~63)

802.1P Mark  ▼

VLAN ID Tag  ▼  (1~4095)

**Step4: Class Routing**

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

Forward To Interface  ▼

**Step5: Outgoing Queue Selection**

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

To Queue Index:  ▼



The following table describes the labels in this screen.

Table 49 Classification Setup: Add/Edit

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

Table 49 Classification Setup: Add/Edit (continued)

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

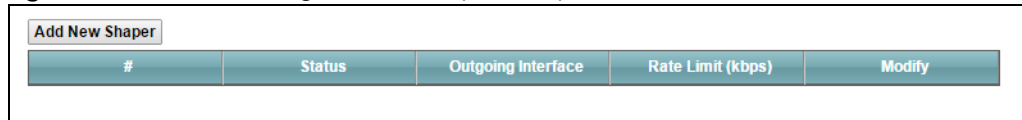
Table 49 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Step4: Class Routing	
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select <b>Unchange</b> , the VMG forward traffic of this class according to the default routing table.
Step5: Outgoing Queue Selection	
To Queue Index	Select a queue that applies to this class.  You should have configured a queue in the <b>Queue Setup</b> screen already.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 10.6 The QoS Shaper Setup Screen

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

Figure 75 Network Setting &gt; QoS &gt; Shaper Setup



The following table describes the labels in this screen.

Table 50 Network Setting &gt; QoS &gt; Shaper Setup

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

## 10.6.1 Add/Edit a QoS Shaper

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

**Figure 76** Shaper Setup: Add/Edit

The following table describes the labels in this screen.

**Table 51** Shaper Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the shaper.
Interface	Select the VMG's interface through which traffic in this shaper applies.
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 10.7 The QoS Policer Setup Screen

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

**Figure 77** Network Setting > QoS > Policer Setup

The following table describes the labels in this screen.

**Table 52** Network Setting > QoS > Policer Setup

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

Table 52 Network Setting &gt; QoS &gt; Policer Setup (continued)

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

## 10.7.1 Add/Edit a QoS Policer

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

Figure 78 Policer Setup: Add/Edit

The following table describes the labels in this screen.

Table 53 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the policer.
Name	Enter the descriptive name of this policer.
Meter Type	This shows the traffic metering algorithm used in this policer.  The <b>Simple Token Bucket</b> algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to $b$ bytes which is also the bucket size.  The <b>Single Rate Three Color Marker</b> (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS).  The <b>Two Rate Three Color Marker</b> (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured.  This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Conforming Action	Specify what the VMG does for packets within the committed rate and burst size (green-marked packets).  <ul style="list-style-type: none"> <li>• <b>Pass:</b> Send the packets without modification.</li> <li>• <b>DSCP Mark:</b> Change the DSCP mark value of the packets. Enter the DSCP mark value to use.</li> </ul>
Non-Conforming Action	Specify what the VMG does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets).  <ul style="list-style-type: none"> <li>• <b>Drop:</b> Discard the packets.</li> <li>• <b>DSCP Mark:</b> Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.</li> </ul>
Available Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier.
Selected Class	Highlight a QoS classifier in the <b>Available Class</b> box and use the > button to move it to the <b>Selected Class</b> box.  To remove a QoS classifier from the <b>Selected Class</b> box, select it and use the < button.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 10.8 Technical Reference

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

### IEEE 802.1Q Tag

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

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

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

Table 54 IEEE 802.1p Priority Level and Traffic Type

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

## DiffServ

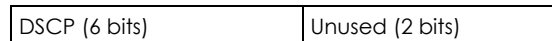
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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

## DSCP and Per-Hop Behavior

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

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



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

## IP Precedence

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

## Automatic Priority Queue Assignment

If you enable QoS on the VMG, the VMG 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 VMG. On the VMG, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested

Table 55 Internal Layer2 and Layer 3 QoS Mapping

PRIORITY	ETHERNET PRIORITY (802.1P)	IP PRECEDENCE	IP PACKET LENGTH (BYTE)
4	001, 010	000XXX, 001XXX	>1100
3	000, 011	010XXX, 011XXX	250-1100
2	100	100XXX	
2	101	101XXX	<250
1 (Highest)	110, 111	110XXX, 111XXX	

## Token Bucket

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

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the VMG stops transmitting until enough tokens are generated.
- If not enough tokens are available, the VMG treats the packet in either one of the following ways:
  - In traffic shaping:
    - Holds it in the queue until enough tokens are available in the bucket.
  - In traffic policing:
    - Drops it.
    - Transmits it but adds a DSCP mark. The VMG may drop these marked packets if the network is overloaded.

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



## Single Rate Three Color Marker

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

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

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

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

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

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

## Two Rate Three Color Marker

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

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

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

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

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.

- If the PBS bucket has enough tokens, the VMG checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

# CHAPTER 11

# Network Address Translation (NAT)

## 11.1 Overview

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

### 11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network ([Section 11.2 on page 164](#)).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network ([Section 11.3 on page 167](#)).
- Use the **Port Triggering** screen to add and configure the VMG's trigger port settings ([Section 11.4 on page 168](#)).
- Use the **DMZ** screen to configure a default server ([Section 11.5 on page 171](#)).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the VMG ([Section 11.6 on page 172](#)).
- Use the **Address Mapping** screen to configure the VMG's address mapping settings ([Section 11.7 on page 172](#)).
- Use the **Sessions** screen to configure the VMG's maximum number of NAT sessions ([Section 11.8 on page 174](#)).

### 11.1.2 What You Need To Know

#### Inside/Outside

Inside/outside denotes where a host is located relative to the VMG, 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 11.9 on page 175](#) for advanced technical information on NAT.

# 11.2 The Port Forwarding Screen

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

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

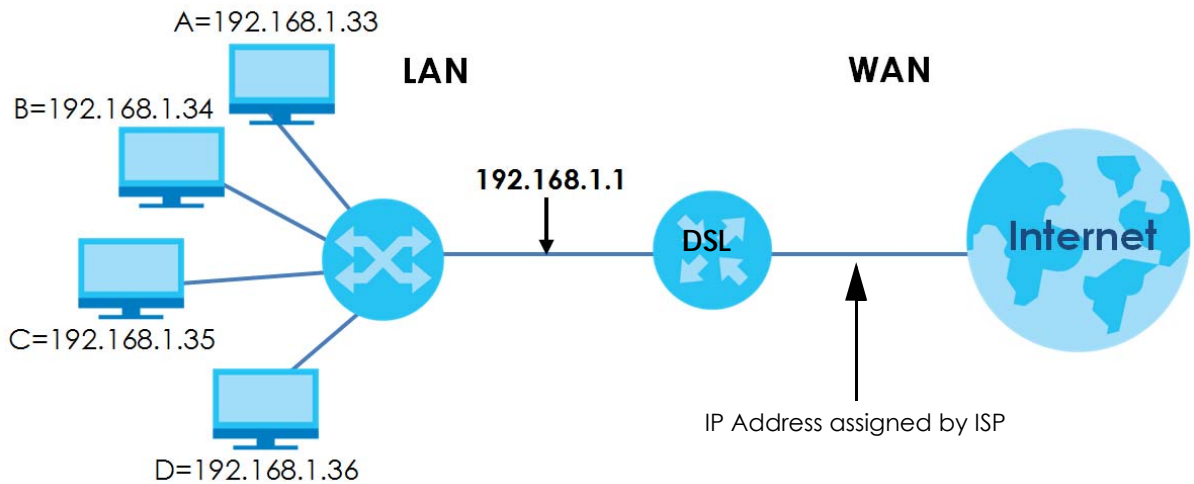
The most often used port numbers and services are shown in [Appendix D on page 287](#). Please refer to RFC 1700 for further information about port numbers.

**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.

## 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.

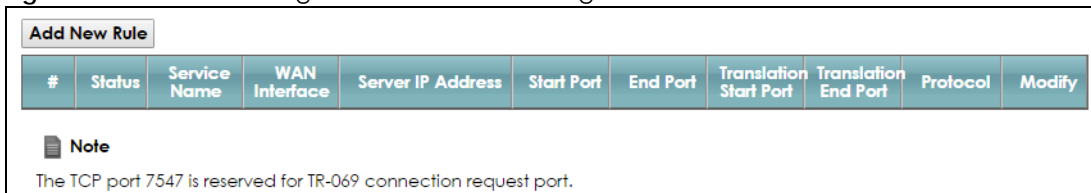
**Figure 79** Multiple Servers Behind NAT Example



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

See [Appendix D on page 287](#) for port numbers commonly used for particular services.

**Figure 80** Network Setting > NAT > Port Forwarding



The following table describes the fields in this screen.

Table 56 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add New Rule	Click this to add a new rule.
#	This is the index number of the entry.
Status	This field displays whether the NAT rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This shows the service's name.
WAN Interface	This shows the WAN interface through which the service is forwarded.
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Protocol	This shows the IP protocol supported by this virtual server, whether it is <b>TCP</b> , <b>UDP</b> , or <b>TCP/UDP</b> .
Modify	Click the <b>Edit</b> icon to edit this rule. Click the <b>Delete</b> icon to delete an existing rule.

## 11.2.1 Add/Edit Port Forwarding

Click **Add New Rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen.

**Figure 81** Port Forwarding: Add/Edit

**Add New Rule**

Active  Enable  Disable

Service Name

WAN Interface

Start Port

End Port

Translation Start Port

Translation End Port

Server IP Address

Protocol

Wake up this target by Wake On Lan(WOL)

MAC address of WOL device

**Note**

- If Start Port and Translation Start Port, End Port and Translation End Port is configured the same, then Port Forwarding is configured.  
If Start Port and Translation Start Port, End Port and Translation End Port are configured differently, then Port Translation is configured (one to one mapping).  
For example: Start Port: 100 End Port: 120; Translation Start Port: 200 Translation End Port: 220
- WAN IP is optional, if Multi-to-Multi NAT is required, enter the WAN IP of the desired device.

OK Cancel

The following table describes the labels in this screen.

**Table 57** Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the <b>End Port</b> field. To forward a series of ports, enter the start port number here and the end port number in the <b>End Port</b> field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the <b>Start Port</b> 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 <b>Start Port</b> field above.

Table 57 Port Forwarding: Add/Edit (continued)

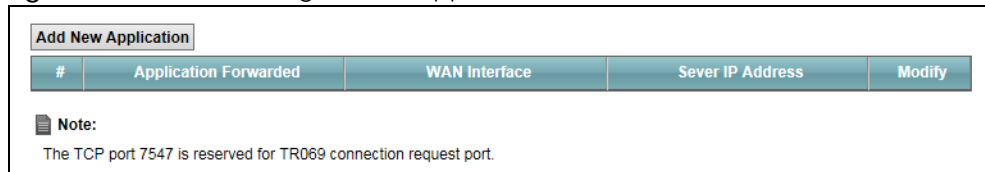
LABEL	DESCRIPTION
Translation Start Port	This shows the port number to which you want the VMG to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are <b>TCP</b> , <b>UDP</b> , or <b>TCP/UDP</b> .
Wake up this target by Wake On Lan(WOL)	Select this to turn on the virtual server remotely.
MAC address of WOL device	Enter the MAC address of the device to turn it on.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 11.3 The Applications Screen

This screen provides a summary of all NAT applications and their configuration. In addition, this screen allows you to create new applications and/or remove existing ones.

To access this screen, click **Network Setting > NAT > Applications**. The following screen appears.

Figure 82 Network Setting &gt; NAT &gt; Applications



The following table describes the labels in this screen.

Table 58 Network Setting &gt; NAT &gt; Applications

LABEL	DESCRIPTION
Add New Application	Click this to add a new NAT application rule.
#	This is the index number of the entry.
Application Forwarded	This field shows the type of application that the service forwards.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Server IP Address	This field displays the destination IP address for the service.
Modify	Click the <b>Delete</b> icon to delete the rule.

## 11.3.1 Add New Application

This screen lets you create new NAT application rules. Click **Add New Application** in the **Applications** screen to open the following screen.

**Figure 83** Applications: Add

The following table describes the labels in this screen.

Table 59 Applications: Add

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface that you want to apply this NAT rule to.
Server IP Address	Enter the inside IP address of the application here.
Application Category	Select the category of the application from the drop-down list box.
Application Forwarded	Select a service from the drop-down list box and the VMG automatically configures the protocol, start, end, and map port number that define the service.
View Rules	Click this to display the configuration of the service that you have chosen in <b>Application Forwarded</b> .
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 11.4 The Port Triggering Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

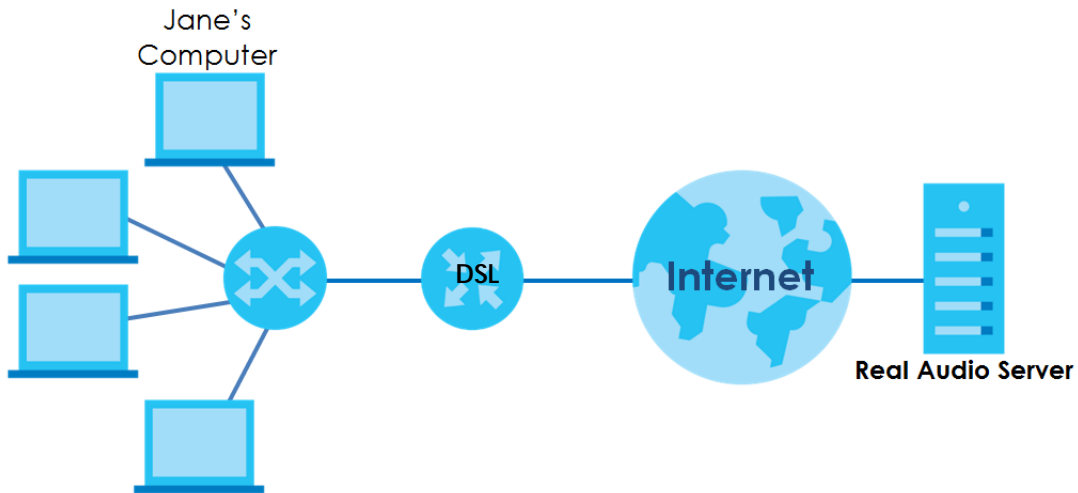
Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The VMG records the IP address of a LAN computer that sends traffic to the WAN to



request a service with a specific port number and protocol (a "trigger" port). When the VMG's WAN port receives a response with a specific port number and protocol ("open" port), the VMG forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

**Figure 84** Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the VMG to record Jane's computer IP address. The VMG associates Jane's computer IP address with the "open" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The VMG forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The VMG times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT > Port Triggering** to open the following screen. Use this screen to view your VMG's trigger port settings.

**Figure 85** Network Setting > NAT > Port Triggering

Add New Rule										
#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Proto.	Modify
<p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice.</li> <li>2. The TCP port 7547 is reserved for TR069 connection request port.</li> </ol>										

The following table describes the labels in this screen.

Table 60 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the VMG to record the IP address of the LAN computer that sent the traffic to a server on the WAN.  This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The VMG forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.  This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Proto.	This is the open transport layer protocol.
Modify	Click the <b>Edit</b> icon to edit this rule.  Click the <b>Delete</b> icon to delete an existing rule.

## 11.4.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen.

Figure 86 Port Triggering: Add/Edit

The following table describes the labels in this screen.

Table 61 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select <b>Enable</b> or <b>Disable</b> to activate or deactivate the rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the VMG to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from <b>TCP</b> or <b>UDP</b> .
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The VMG forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from <b>TCP</b> or <b>UDP</b> .
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 11.5 The DMZ Screen

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 the **NAT Port Forwarding Setup** screen.

Figure 87 Network Setting &gt; NAT &gt; DMZ

Default Server Address :

**Note:**  
Enter IP address and click 'Apply' to activate the DMZ host.  
Clear the IP address field and click 'Apply' to deactivate the DMZ host.

The following table describes the fields in this screen.

Table 62 Network Setting &gt; NAT &gt; DMZ

LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the <b>NAT Port Forwarding</b> screen.  Note: If you do not assign a <b>Default Server Address</b> , the VMG discards all packets received for ports that are not specified in the <b>NAT Port Forwarding</b> screen.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 11.6 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the VMG registers with the SIP register server, the SIP ALG translates the VMG's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your VMG is behind a SIP ALG.

Use this screen to enable and disable the ALGs in the VMG. To access this screen, click **Network Setting > NAT > ALG**.

**Figure 88** Network Setting > NAT > ALG

NAT ALG :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable (settings are invalid when disabled)
SIP ALG :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
RTSP ALG :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
PPTP ALG :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IPSEC ALG :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

The following table describes the fields in this screen.

**Table 63** Network Setting > NAT > ALG

LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
RTSP ALG	Enable this to have the VMG detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
PPTP ALG	Enable this to turn on the PPTP ALG on the VMG to detect PPTP traffic and help build PPTP sessions through the VMG's NAT.
IPSEC ALG	Enable this to turn on the IPsec ALG on the VMG to detect IPsec traffic and help build IPsec sessions through the VMG's NAT.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 11.7 The Address Mapping Screen

Ordering your rules is important because the VMG applies the rules in the order that you specify. When a rule matches the current packet, the VMG takes the corresponding action and the remaining rules are ignored.

Click **Network Setting > NAT > Address Mapping** to display the following screen.

**Figure 89** Network Setting > NAT > Address Mapping

Rule Name	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	WAN Interface	Modify
-----------	----------------	--------------	-----------------	---------------	------	---------------	--------

The following table describes the fields in this screen.

**Table 64** Network Setting > NAT > Address Mapping

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
Rule Name	This is the name of the rule.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for <b>One-to-One</b> mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the <b>Many-to-One</b> mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for <b>One-to-One</b> and <b>Many-to-One</b> mapping types.
Type	<p>This is the address mapping type.</p> <p><b>One-to-One:</b> This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.</p> <p><b>Many-to-One:</b> This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the VMG's Single User Account feature that previous routers supported only.</p> <p><b>Many-to-Many:</b> This mode maps multiple local IP addresses to shared global IP addresses.</p>
Wan Interface	This is the WAN interface to which the address mapping rule applies.
Modify	<p>Click the <b>Edit</b> icon to go to the screen where you can edit the address mapping rule.</p> <p>Click the <b>Delete</b> icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.</p>

### 11.7.1 Add/Edit Address Mapping Rule

To add or edit an address mapping rule, click **Add new rule** or the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 90 Address Mapping: Add/Edit

The following table describes the fields in this screen.

Table 65 Address Mapping: Add/Edit

LABEL	DESCRIPTION
Rule Name	Type up to 20 alphanumeric characters for the name of this rule.
Type	Choose the IP/port mapping type from one of the following.  <b>One-to-One:</b> This mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.  <b>Many-to-One:</b> This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the VMG's Single User Account feature that previous routers supported only.  <b>Many-to-Many:</b> This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is blank for <b>One-to-One</b> mapping types.
Global Start IP	Enter the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for the <b>Many-to-One</b> mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for <b>One-to-One</b> and <b>Many-to-One</b> mapping types.
WAN Interface	Select a WAN interface to which the address mapping rule applies.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 11.8 The Sessions Screen

Use this screen to limit the number of concurrent NAT sessions a client can use. Click **Network Setting > NAT > Sessions** to display the following screen.

**Figure 91** Network Setting > NAT > Sessions

MAX NAT Session Per Host (0 ~ 20480):

**Note**  
 Enter session number and click "Apply" to activate this feature.  
 Clear the session number field and click "Apply" to de-activate this feature.

The following table describes the fields in this screen.

Table 66 Network Setting &gt; NAT &gt; Sessions

LABEL	DESCRIPTION
MAX NAT Session Per Host (0 ~ 20480)	Use this field to set a limit to the number of concurrent NAT sessions each client host can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer-to-peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Apply	Click this to save your changes on this screen.
Cancel	Click this to exit this screen without saving any changes.

## 11.9 Technical Reference

This part contains more information regarding NAT.

### 11.9.1 NAT Definitions

Inside/outside denotes where a host is located relative to the VMG, 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 67 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.

## 11.9.2 What NAT Does

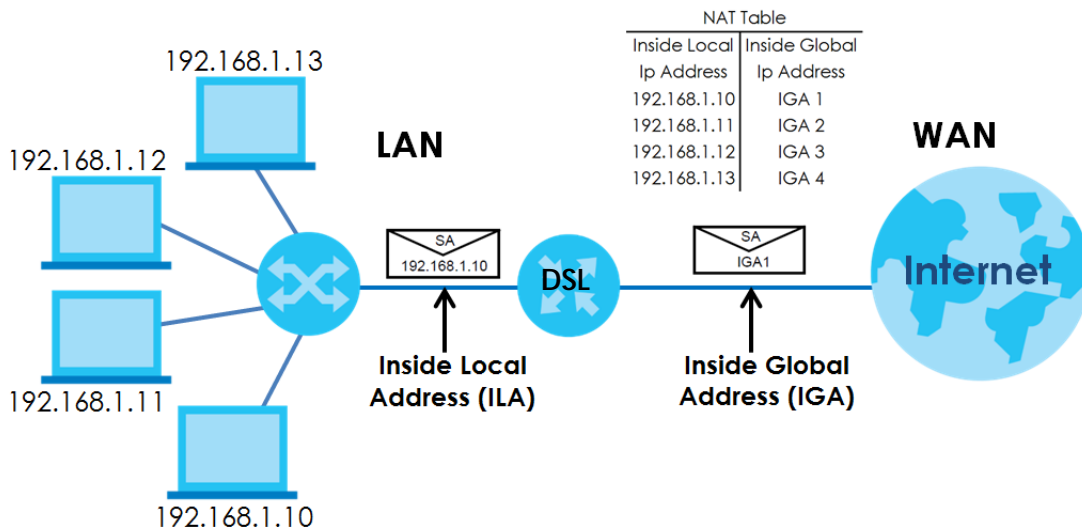
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your VMG 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)*.

## 11.9.3 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 VMG 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 92 How NAT Works

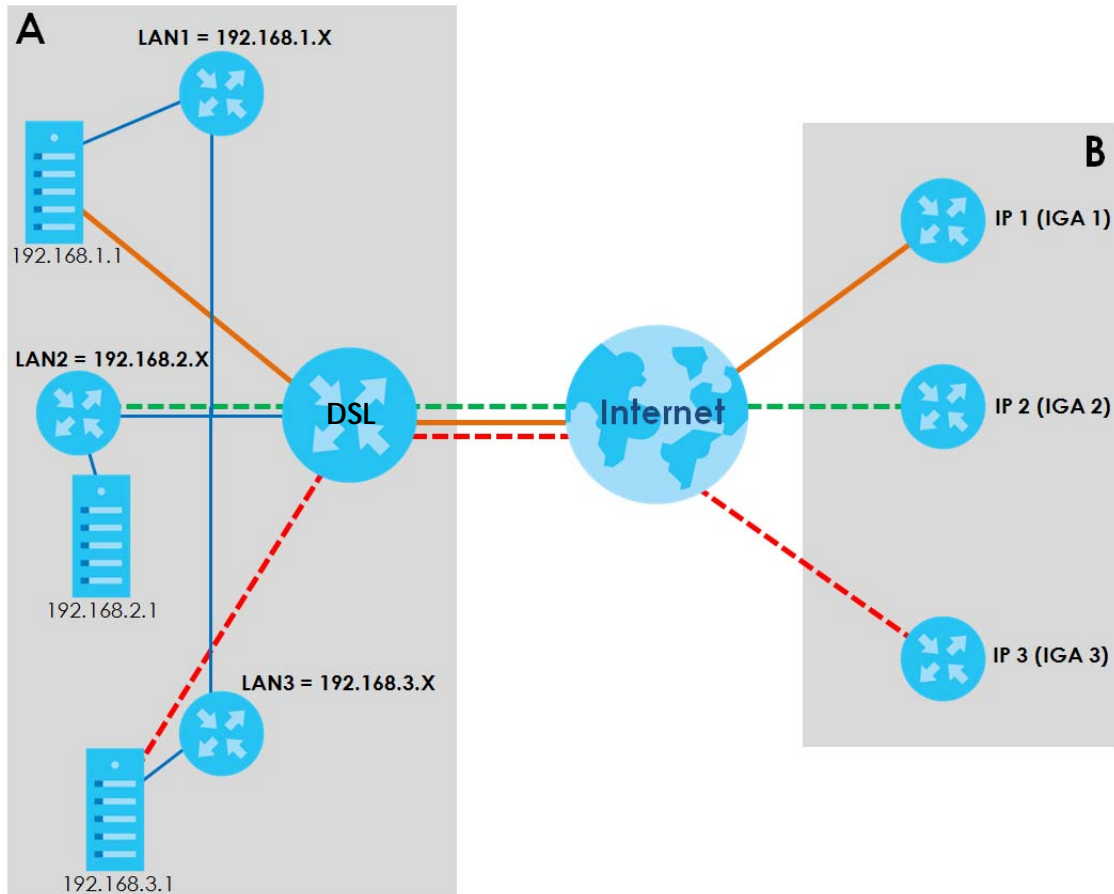


## 11.9.4 NAT Application

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



Figure 93 NAT Application With IP Alias



## Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

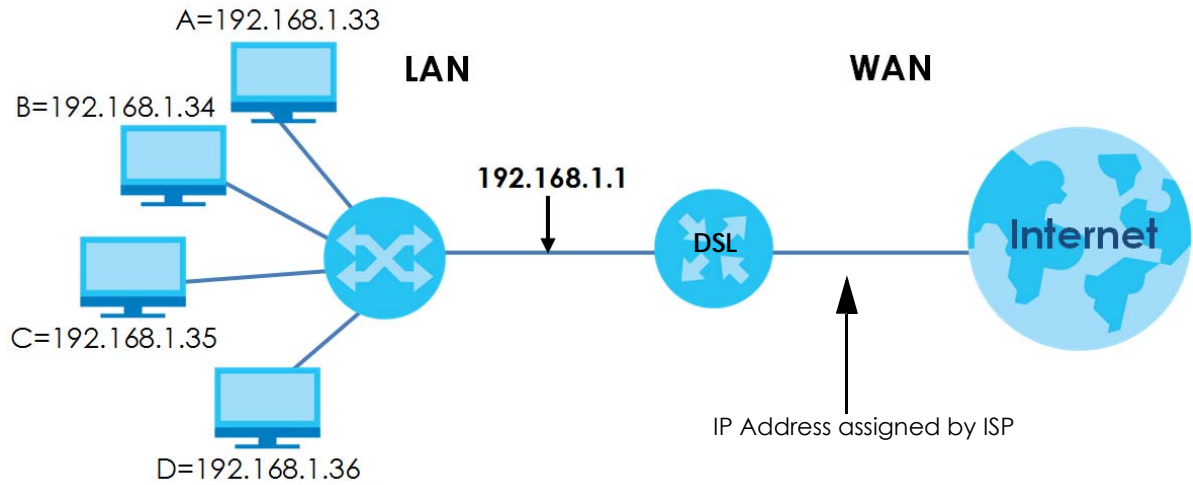
Table 68 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

## Port Forwarding Example

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

**Figure 94** Multiple Servers Behind NAT Example



# CHAPTER 12

## Dynamic DNS Setup

### 12.1 Overview

#### DNS

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

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The VMG uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the VMG receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

#### Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with [www.dyndns.org](http://www.dyndns.org). This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

#### 12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes ([Section 12.2 on page 180](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the VMG ([Section 12.3 on page 181](#)).

#### 12.1.2 What You Need To Know

##### DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

## 12.2 The DNS Entry Screen

Use this screen to view and configure DNS routes on the VMG. Click **Network Setting > DNS** to open the **DNS Entry** screen.

**Figure 95** Network Setting > DNS > DNS Entry

#	HostName	IP Address	Modify
<p><b>Note:</b> The hostnames needs combination of the host's local name with its domain's name. For example, Mycomputer.home consists of a local hostname (Mycomputer) and the domain name (home).</p>			

The following table describes the fields in this screen.

**Table 69** Network Setting > DNS > DNS Entry

LABEL	DESCRIPTION
Add New DNS Entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
Hostname	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the <b>Edit</b> icon to edit the rule. Click the <b>Delete</b> icon to delete an existing rule.

### 12.2.1 Add/Edit DNS Entry

You can manually add or edit the VMG's DNS name and IP address entry. Click **Add New DNS Entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

**Figure 96** DNS Entry: Add/Edit

**DNS Entry Configuration** ✖

Host Name :

IPv4 Address :

OK Cancel

The following table describes the labels in this screen.

Table 70 DNS Entry: Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
IP Address	Enter the IP address of the DNS entry.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 12.3 The Dynamic DNS Screen

Use this screen to change your VMG's DDNS. Click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 97 Network Setting &gt; DNS &gt; Dynamic DNS

The following table describes the fields in this screen.

Table 71 Network Setting &gt; DNS &gt; &gt; Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select <b>Enable</b> to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Type the domain name assigned to your VMG by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Username	Type your user name.
Password	Type the password assigned to you.
Dynamic DNS Status	
User Authentication Result	This shows <b>Success</b> if the account is correctly set up with the Dynamic DNS provider account.
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.

Table 71 Network Setting > DNS >> Dynamic DNS (continued)

LABEL	DESCRIPTION
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

# CHAPTER 13

## Interface Grouping

### 13.1 Overview

By default, all LAN and WAN interfaces on the VMG are in the same group and can communicate with each other. Create interface groups to have the VMG assign the IP addresses in different domains to different groups. Each group acts as an independent network on the VMG. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

#### 13.1.1 What You Can Do in this Chapter

The **Interface Grouping** screens let you create multiple networks on the VMG ([Section 13.2 on page 183](#)).

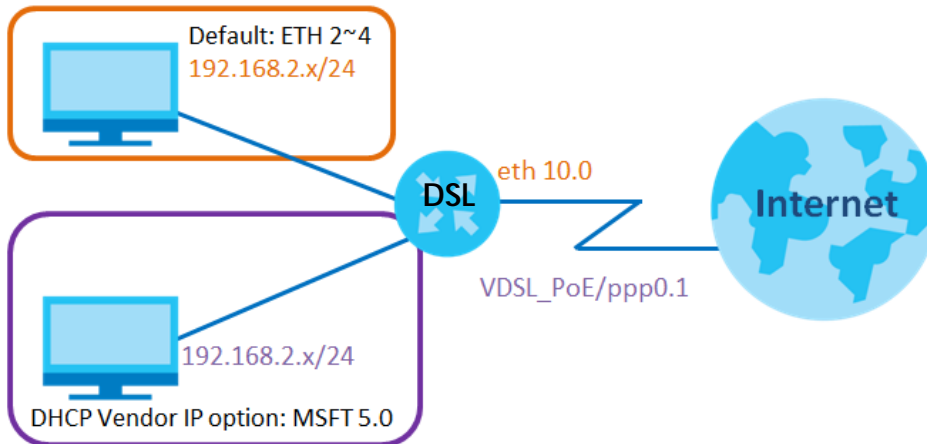
### 13.2 The Interface Group Screen

You can manually add a LAN interface to a new group. Alternatively, you can have the VMG automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the VMG assigns to the clients in the default and/or user-defined groups. If you set the VMG to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See [Chapter 8 on page 123](#) for more information.

In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

Figure 98 Interface Grouping Application



Click **Network Setting > Interface Grouping** to open the following screen.

Figure 99 Network Setting &gt; Interface Grouping

Add New Interface Group				
Group Name	WAN Interface	LAN Interfaces	Criteria	Modify
Default	Any WAN	LAN1, LAN2, LAN3, ZyXEL_0002, ZyXEL_Guest_1, ZyXEL_Guest_2, ZyXEL_Guest_3		

The following table describes the fields in this screen.

Table 72 Network Setting &gt; Interface Grouping

LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.
Modify	Click the <b>Delete</b> icon to remove the group.

### 13.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to only one group at a time.



Figure 100 Interface Group Configuration

1. Enter a unique Group name.  
2. If you like to automatically add LAN clients to a WAN Interface in the new group, add the DHCP vendor ID string. By configuring a DHCP Vendor ID string, any DHCP client request with the specified Vendor ID (DHCP option 60), will be denied an IP address from the local DHCP server.

Group Name

WAN Interfaces used in the grouping

PTM type -

ATM type -

WWAN type -

#	Selected LAN Interfaces

#	Available LAN Interfaces
<input type="checkbox"/>	LAN1
<input type="checkbox"/>	LAN2
<input type="checkbox"/>	LAN3
<input type="checkbox"/>	LAN4
<input type="checkbox"/>	Zyxel_1FA3
<input type="checkbox"/>	Zyxel_1FA3_guest1
<input type="checkbox"/>	Zyxel_1FA3_guest2
<input type="checkbox"/>	Zyxel_1FA3_guest3

Automatically Add Clients With the following DHCP Vendor IDs

#	Filter Criteria	WildCard Support	Modify

**Note**  
If a Vendor ID is configured for a specific client device, please REBOOT the client device attached to the router, to allow the client device to obtain an appropriate IP address.

The following table describes the fields in this screen.

Table 73 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interface used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface, up to one ETH interface, and up to one WWAN interface.
Selected LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the <b>Selected LAN Interfaces</b> list and use the left arrow to move them to the <b>Available LAN Interfaces</b> list to add the interfaces to this group.
Available LAN Interfaces	To remove a LAN or wireless LAN interface from the <b>Available LAN Interfaces</b> , use the right-facing arrow.
Automatically Add Clients With the following DHCP Vendor IDs	Click <b>Add</b> to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See <a href="#">Section 13.2.2 on page 186</a> for more information.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.

Table 73 Interface Group Configuration (continued)

LABEL	DESCRIPTION
Wildcard Support	This shows if wildcard on DHCP option 60 is enabled.
Modify	Click the <b>Edit</b> icon to change the group setting Click the <b>Delete</b> icon to delete this group from the VMG.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 13.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen.

Figure 101 Interface Grouping Criteria

The following table describes the fields in this screen.

Table 74 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Select this option and enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.

Table 74 Interface Grouping Criteria (continued)

LABEL	DESCRIPTION
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

# CHAPTER 14

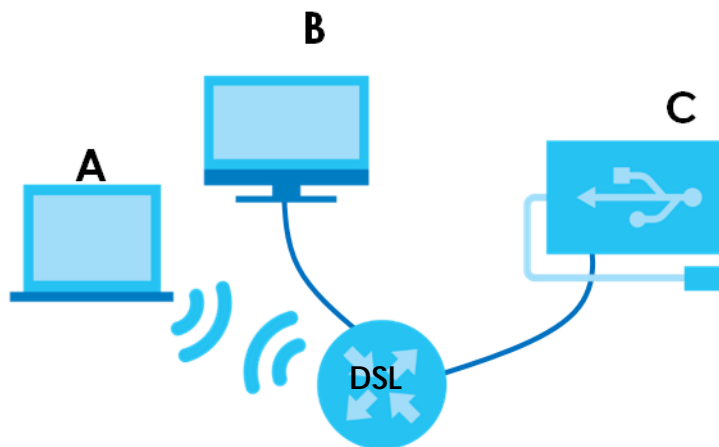
## USB Service

### 14.1 Overview

You can share files on a USB memory stick or hard drive connected to your VMG with users on your network.

The following figure is an overview of the VMG's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the VMG.

**Figure 102** File Sharing Overview



---

The VMG will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

---

#### 14.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to enable file-sharing server ([Section 14.1.3 on page 189](#)).
- Use the **Media Server** screen to enable or disable the sharing of media files ([Section 14.3 on page 192](#)).

#### 14.1.2 What You Need To Know

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

### 14.1.2.1 About File Sharing

#### Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

#### Shares

When settings are set to default, each USB device connected to the VMG is given a folder, called a "share". If a USB hard drive connected to the VMG has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

#### File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your VMG supports File Allocation Table (FAT) and FAT32.

#### Common Internet File System

The VMG uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the VMG. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

### 14.1.3 Before You Begin

Make sure the VMG is connected to your network and turned on.

- 1 Connect the USB device to one of the VMG's USB port. Make sure the VMG is connected to your network.
- 2 The VMG detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the VMG, see the troubleshooting for suggestions.

## 14.2 The File Sharing Screen

Use this screen to set up file sharing through the VMG. The VMG's LAN users can access the shared folder (or share) from the USB device inserted in the VMG. To access this screen, click **Network Setting > USB Service > File Sharing**.

Figure 103 Network Setting &gt; USB Service &gt; File Sharing

**Information**

Volume	Capacity	Used Space
usb2_sda1	30111 MB	2964 MB

**Server Configuration**

File Sharing Services:  Enable  Disable

**Share Directory List**

**Add New Share**

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

**Account Management**

**Add New User**

Status	User Name
	admin
	user

**Apply** **Cancel**



Note: Share Directory List field appears when you connect a USB device to the USB port. Otherwise, it doesn't.

Each field is described in the following table.

Table 75 Network Setting &gt; USB Service &gt; File Sharing

LABEL	DESCRIPTION
Information	
Volume	This is the volume name the VMG gives to an inserted USB device.
Capacity	This is the total available memory size (in megabytes) on the USB device.
Used Space	This is the memory size (in megabytes) already used on the USB device.
Server Configuration	
File Sharing Services	Select <b>Enable</b> to activate file sharing through the VMG.
Share Directory List	
Add New Share	Click this to set up a new share on the VMG.
Active	Select this to allow the share to be accessed.
Status	This field shows the status of the share : The share is not activated. : The share is activated.
Share Name	This field displays the share name on the GPON Device.
Share Path	This field displays the path for the share directories (folders) on the GPON Device. These are the directories (folders) on your USB storage device.
Share Description	This field displays information about the share.
Modify	Click the <b>Edit</b> icon to change the settings of an existing share. Click the <b>Delete</b> icon to delete this share in the list.
Account Management	

Table 75 Network Setting &gt; USB Service &gt; File Sharing

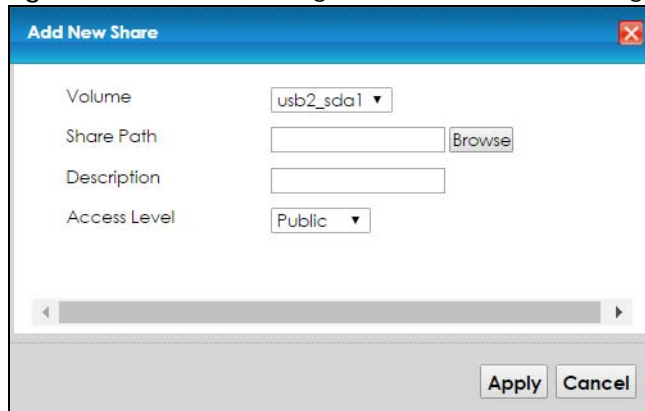
LABEL	DESCRIPTION
Add New User	Click this button to create a user account to access the secured shares.
Status	This field shows the status of the user.  : The user account is not activated for the share.  : The user account is activated for the share.
User Name	This is the name of a user who is allowed to access the secured shares on the USB device.
Apply	Click this to save your changes to the VMG.
Cancel	Click this to restore your previously saved settings.

## 14.2.1 The Add New Share Screen

Use this screen to set up a new share or edit an existing share on the VMG. Click **Add new share** in the **File Sharing** screen or click the **Edit** icon next to an existing share.

Please note that you need to set up your shares in the USB before enabling file sharing in the VMG. Also, the following special characters are not allowed for the USB share name: ", ' , ` , < , > , ^ , \$ , | , & , ; , \ , / , : , * , and ?.

Figure 104 Network Setting &gt; USB Service &gt; File Sharing &gt; Add New Sharer



The following table describes the labels in this menu.

Table 76 Network Setting &gt; USB Service &gt; Media Server

LABEL	DESCRIPTION
Volume	Select the volume in the USB storage device that you want to add as a share in the VMG. This field is read-only when you are editing the share.
Share Path	Manually enter the file path for the share, or click the <b>Browse</b> button and select the folder that you want to add as a share. This field is read-only when you are editing the share.
Description	You can either enter a short description of the share, or leave this field blank.
Access Level	Select <b>Public</b> if you want the share to be accessed by users connecting to the VMG. Otherwise, select <b>Security</b> .
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Back</b> to return to the previous screen.

## 14.2.2 The Add New User Screen

Once you click the **Add New User** button, you'll be directed to the **User Account** screen. To create a user account that can access the secured shares on the USB device, click the **Add New Account** button in the **Network Setting > Maintenance > User Account** screen.

Please see [Chapter 27 on page 231](#), for detailed information about **User Account** screen.

## 14.3 The Media Server Screen

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your VMG (without having to copy them to another computer). The VMG can function as a DLNA-compliant media server. The VMG streams files to DLNA-compliant media clients (like Windows Media Player). The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

The VMG media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the VMG.
- Use hardware-based media clients like the DMA-2500 to play the files.

**Note:** Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

To change your VMG's media server settings, click **Network Setting > USB Service > Media Server**. The screen appears as shown.

**Figure 105** Network Setting > USB Service > Media Server

The following table describes the labels in this menu.

**Table 77** Network Setting > USB Service > Media Server

LABEL	DESCRIPTION
Media Server	Select <b>Enable</b> to have the VMG function as a DLNA-compliant media server. Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares.
Interface	Select an interface on which you want to enable the media server function.
Media Library Path	Enter the path clients use to access the media files on a USB storage device connected to the VMG.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.



# CHAPTER 15

## Firewall

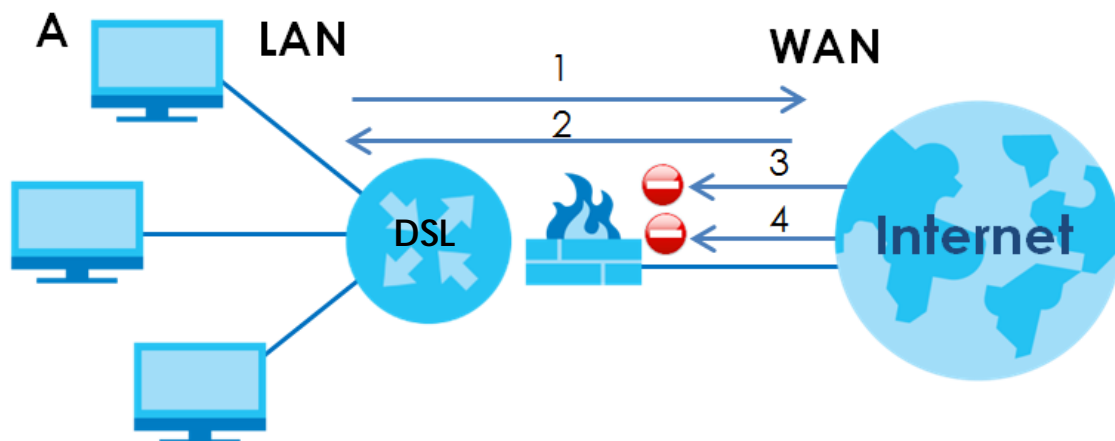
### 15.1 Overview

This chapter shows you how to enable and configure the VMG's security settings. Use the firewall to protect your VMG and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 106 Default Firewall Action



#### 15.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the VMG ([Section 15.2 on page 194](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 15.3 on page 195](#)).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules ([Section 15.4 on page 197](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 15.5 on page 199](#)).

## 15.1.2 What You Need to Know

### SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

### DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The VMG is pre-configured to automatically detect and thwart all known DoS attacks.

### DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

### LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

### Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

### SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

## 15.2 The Firewall Screen

Use this screen to set the security level of the firewall on the VMG. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Security > Firewall** to display the **General** screen.

Figure 107 Security &gt; Firewall &gt; General

IPv4 Firewall :  Enable  Disable  
 IPv6 Firewall :  Enable  Disable

Low Medium (Recommended) High

	Low	Medium (Recommended)	High
LAN to WAN	✓	✓	✗
WAN to LAN	✓	✗	✗

**Note:**  
 (1) LAN to WAN: Allow access to all internet services  
 (2) WAN to LAN: Allow access from other computers on the Internet  
 (3) When the security level is set to 'High', access to the following services is allowed: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP

Apply Cancel

The following table describes the labels in this screen.

Table 78 Security &gt; Firewall &gt; General

LABEL	DESCRIPTION
Firewall	Select <b>Enable</b> to activate the firewall feature on the VMG.
Low	Select <b>Low</b> to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select <b>Medium</b> to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select <b>High</b> to deny LAN to WAN and WAN to LAN packet directions.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 15.3 The Protocol Screen

You can configure customized services and port numbers in the **Protocol** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix D on page 287](#) for some examples.

Click **Security > Firewall > Protocol** to display the following screen.

Figure 108 Security &gt; Firewall &gt; Protocol

Add New Protocol Entry

Name	Description	Ports/Protocol Number	Modify
------	-------------	-----------------------	--------

**Note:**  
 If a protocol rule is removed, related ACL rules will also be removed.

The following table describes the labels in this screen.

Table 79 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to add a new service.
Name	This is the name of your customized service.
Description	This is the description of your customized service.
Ports/Protocol Number	This shows the IP protocol ( <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> , or <b>TCP/UDP</b> ) and the port number or range of ports that defines your customized service. <b>Other</b> and the protocol number displays if the service uses another IP protocol.
Modify	Click the <b>Edit</b> icon to edit the entry. Click the <b>Delete</b> icon to remove this entry.

### 15.3.1 Add/Edit a Service

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add new Protocol entry** or the **Edit** icon next to an existing service rule in the **Protocol** screen to display the following screen.

Figure 109 Security > Firewall > Protocol: Add/Edit

The following table describes the labels in this screen.

Table 80 Security > Firewall > Protocol: Add/Edit

LABEL	DESCRIPTION
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Description	Enter a description for your customized port.
Protocol	Choose the IP protocol ( <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> , or <b>Other</b> ) that defines your customized port from the drop-down list box. Select <b>Other</b> to be able to enter a protocol number.
Protocol Number	This field is displayed if you select <b>Other</b> as the protocol. Enter the protocol number of your customized port.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 15.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

**Figure 110** Security > Firewall > Access Control



The following table describes the labels in this screen.

Table 81 Security > Firewall > Access Control

LABEL	DESCRIPTION
Add New ACL Rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
#	This is the index number of the entry.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to <b>Any</b> .
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to <b>Any</b> .
Service	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.
Action	This field displays whether the rule silently discards packets ( <b>DROP</b> ), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender ( <b>REJECT</b> ) or allows the passage of packets ( <b>ACCEPT</b> ).
Modify	Click the <b>Edit</b> icon to edit the rule.  Click the <b>Delete</b> icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.  Click the <b>Move To</b> icon to change the order of the rule. Enter the number in the # field.

### 15.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 111 Access Control: Add/Edit

The following table describes the labels in this screen.

Table 82 Access Control: Add/Edit

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.  You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Order	Select the order of the ACL rule.
Select Source Device	Select the source device to which the ACL rule applies. If you select <b>Specific IP Address</b> , enter the source IP address in the field below.
Source IP Address	Enter the source IP address.
Select Destination Device	Select the destination device to which the ACL rule applies. If you select <b>Specific IP Address</b> , enter the destination IP address in the field below.
Destination IP Address	Enter the destination IP address.
IP Type	Select whether your IP type is <b>IPv4</b> or <b>IPv6</b> .
Select Service	Select the service rule that defines your customized port from the drop-down list box. The specific service rule you add in the <b>Security &gt; Firewall &gt; Protocol</b> screen display in this list.  If you want to configure a customized service, select <b>Specific Service</b> .

Table 82 Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Protocol	This field is displayed only when you select <b>Specific Service</b> in the <b>Select Service</b> field. Choose the transport layer protocol ( <b>TCP/UDP</b> , <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> , or <b>ICMPv6</b> ) that defines your customized port from the drop-down list box.
Custom Source Port	This field is displayed only when you select <b>Specific Service</b> in the <b>Select Service</b> field. Enter a single port number or the range of port numbers of the source.
Custom Destination Port	This field is displayed only when you select <b>Specific Service</b> in the <b>Select Service</b> field. Enter a single port number or the range of port numbers of the destination.
Policy	Use the drop-down list box to select whether to discard ( <b>DROP</b> ), deny and send an ICMP destination-unreachable message to the sender of ( <b>REJECT</b> ) or allow the passage of ( <b>ACCEPT</b> ) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies.
Enable Rate Limit	Select <b>Enable</b> to set a limit on the upstream/downstream transmission rate for the specified protocol.  Specify how many packets per minute or second the transmission rate is.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click <b>Add New Rule</b> . This will bring you to the <b>Security &gt; Scheduler Rules</b> screen.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 15.5 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 112 Security &gt; Firewall &gt; DoS

DoS Protection Blocking :  Enable  Disable (settings are invalid when disabled)

The following table describes the labels in this screen.

Table 83 Security &gt; Firewall &gt; DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select <b>Enable</b> to enable protection against DoS attacks.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

# CHAPTER 16

## MAC Filter

### 16.1 Overview

You can configure the VMG to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

### 16.2 The MAC Filter Screen

Use this screen to allow wireless and LAN clients access to the VMG. Click **Security > MAC Filter**. The screen appears as shown.

**Figure 113** Security > MAC Filter

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

MAC Restrict Mode  Allow  Deny

Set	Active	Host Name	MAC Address
1	<input type="checkbox"/>		- - - - -
2	<input type="checkbox"/>		- - - - -
3	<input type="checkbox"/>		- - - - -
4	<input type="checkbox"/>		- - - - -
5	<input type="checkbox"/>		- - - - -
6	<input type="checkbox"/>		- - - - -
7	<input type="checkbox"/>		- - - - -
8	<input type="checkbox"/>		- - - - -
9	<input type="checkbox"/>		- - - - -
10	<input type="checkbox"/>		- - - - -
31	<input type="checkbox"/>		- - - - -
32	<input type="checkbox"/>		- - - - -

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

Apply Cancel



The following table describes the labels in this screen.

Table 84 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select <b>Enable</b> to activate the MAC filter function.
MAC Restrict Mode	Select <b>Allow</b> to only permit the listed MAC addresses access to the VMG. Select <b>Deny</b> to permit anyone access to the VMG except the listed MAC addresses.
Set	This is the index number of the MAC address.
Active	Select <b>Active</b> to enable the MAC filter rule. The rule will not be applied if <b>Active</b> is not selected.
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the VMG.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the VMG 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.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

# CHAPTER 17

## Parental Control

### 17.1 Overview

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the VMG performs parental control on a specific user.

### 17.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security > Parental Control** to open the following screen.

**Figure 114** Security > Parental Control

The screenshot shows the 'Security > Parental Control' configuration page. At the top, under 'General', there is a 'Parental Control' section with two radio buttons: 'Enable' and 'Disable (settings are invalid when disabled)'. Below this is the 'Parental Control Profile (PCP)' section, which includes an 'Add New PCP' button. A table with the following columns is displayed: '#', 'Status', 'PCP Name', 'Home Network User MAC', 'Internet Access Schedule', 'Network Service', 'Website Blocked', and 'Modify'. At the bottom right of the table area, there are 'Apply' and 'Cancel' buttons.

The following table describes the fields in this screen.

**Table 85** Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Select <b>Enable</b> to activate parental control.
Add New PCP	Click this if you want to configure a new Parental Control Profile (PCP).
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User MAC	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, <b>None</b> will be shown.
Website Blocked	This shows whether the website block is configured. If not, <b>None</b> will be shown.
Modify	Click the <b>Edit</b> icon to go to the screen where you can edit the rule. Click the <b>Delete</b> icon to delete an existing rule.

Table 85 Security &gt; Parental Control (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 17.2.1 Add/Edit a Parental Control Profile

Click **Add New PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 115 Parental Control Rule: Add/Edit Rule

The following table describes the fields in this screen.

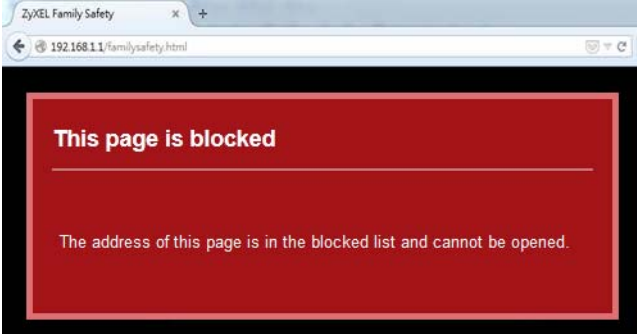
Table 86 Parental Control Rule: Add/Edit

LABEL	DESCRIPTION
General	
Active	Select to enable or disable this parental control rule.

Table 86 Parental Control Rule: Add/Edit (continued)

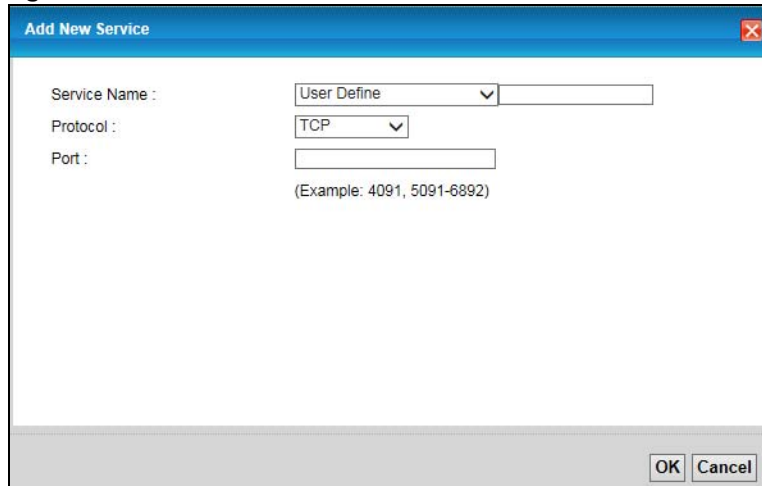
LABEL	DESCRIPTION
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select <b>Custom</b> , enter the LAN user's MAC address. If you select <b>All</b> , the rule applies to all LAN users.
Rule List	In <b>Home Network User</b> , select <b>Custom</b> , enter the LAN user's MAC address, then click the <b>Add</b> icon to enter a computer MAC address for this PCP. Up to five are allowed. Click the <b>Delete</b> icon to remove one.
Internet Access Schedule	
Day	Select check boxes for the days that you want the VMG to perform parental control.
Time (Start - End)	Drag the time bar to define the time that the LAN user is allowed access ( <b>Authorized access</b> ) or denied access ( <b>No access</b> ). Click the <b>Add</b> icon above the time bar to add a new time bar. Up to three are allowed.
Network Service	
Network Service Setting	If you select <b>Block</b> , the VMG prohibits the users from viewing the Web sites with the URLs listed below.  If you select <b>Allow</b> , the VMG blocks access to all URLs except ones listed below.
Add New Service	Click this to show a screen in which you can add a new service rule. You can configure the <b>Service Name</b> , <b>Protocol</b> , and <b>Name</b> of the new rule.
#	This shows the index number of the rule.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.
Modify	Click the <b>Edit</b> icon to go to the screen where you can edit the rule.  Click the <b>Delete</b> icon to delete an existing rule.
Site/URL Keyword	
Block or Allow the Web Site	If you select <b>Block the Web URLs</b> , the VMG prohibits the users from viewing the Web sites with the URLs listed below.  If you select <b>Allow the Web URLs</b> , the VMG blocks access to all URLs except ones listed below.
Add	Click <b>Add</b> to show a screen to enter the URL of web site or URL keyword to which the VMG blocks or allows access.
#	This shows the index number of the rule.
WebSite	This shows the URL of web site or URL keyword to which the VMG blocks or allows access.
Modify	Click the <b>Edit</b> icon to go to the screen where you can edit the rule.  Click the <b>Delete</b> icon to delete an existing rule.

Table 86 Parental Control Rule: Add/Edit (continued)

LABEL	DESCRIPTION
Redirect blocked site to Zyxel Family Safety page	Select this to redirect users who access any blocked websites listed above to the Zyxel Family Safety page as shown next.  <b>Figure 116</b> Zyxel Family Safety Page Example  
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to to exit this screen without saving.

Click **Security > Parental Control > Add New PCP > Add New Service** to open the following screen.

Figure 117 Parental Control Rule: Add/Edit Rule > Add Service



The following table describes the fields in this screen.

Table 87 Parental Control Rule: Add/Edit > Add New Service

LABEL	DESCRIPTION
Service Name	Select the name of the service. Otherwise, select <b>User Define</b> and manually specify the protocol and the port of the service.  If you have chosen a pre-defined service in the <b>Service Name</b> field, this field will not be configurable.
Protocol	Select the transport layer protocol used for the service. Choices are <b>TCP</b> , <b>UDP</b> , or <b>TCP &amp; UDP</b> .
Port	Enter the port of the service.  If you have chosen a pre-defined service in the <b>Service Name</b> field, this field will not be configurable.

**Table 87** Parental Control Rule: Add/Edit > Add New Service (continued)

LABEL	DESCRIPTION
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

Click **Security** > **Parental Control** > **Add New PCP** > **Add** to open the following screen.

**Figure 118** Parental Control Rule: Add/Edit Rule > Add Keyword

The following table describes the fields in this screen.

**Table 88** Parental Control Rule: Add/Edit > Add Keyword

LABEL	DESCRIPTION
Site/URL Keyword	Enter a keyword and click <b>OK</b> to have the VMG block access to the website URLs that contain the keyword.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

# CHAPTER 18

## Scheduler Rule

### 18.1 Overview

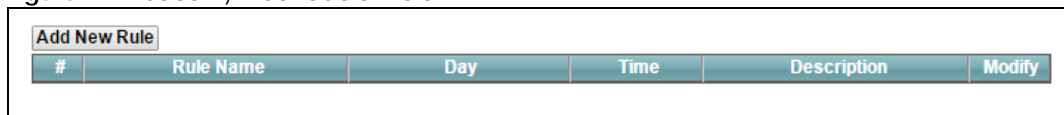
You can define time periods and days during which the VMG performs scheduled rules of certain features (such as Firewall Access Control) in the **Scheduler Rule** screen.

### 18.2 The Scheduler Rule Screen

Use this screen to view, add, or edit time schedule rules.

Click **Security > Scheduler Rule** to open the following screen.

**Figure 119** Security > Scheduler Rule



#	Rule Name	Day	Time	Description	Modify
---	-----------	-----	------	-------------	--------

The following table describes the fields in this screen.

**Table 89** Security > Scheduler Rule

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the day(s) on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the <b>Edit</b> icon to edit the schedule. Click the <b>Delete</b> icon to delete a scheduler rule.  Note: You cannot delete a scheduler rule once it is applied to a certain feature.

#### 18.2.1 Add/Edit a Schedule

Click the **Add New Rule** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

Figure 120 Scheduler Rule: Add/Edit

The following table describes the fields in this screen.

Table 90 Scheduler Rule: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule.
Day	Select check boxes for the days that you want the VMG to perform this scheduler rule.
Time of Day Range	Enter the time period of each day, in 24-hour format, during which the rule will be enforced.
Description	Enter a description for this scheduler rule.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.



# CHAPTER 19

## Certificates

### 19.1 Overview

The VMG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

#### 19.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the VMG's CA-signed certificates ([Section 19.4 on page 213](#)).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the VMG ([Section 19.4 on page 213](#)).

### 19.2 What You Need to Know

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

#### Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the VMG to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

### 19.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the VMG's summary list of certificates and certification requests.

**Figure 121** Security > Certificates > Local Certificates

The screenshot shows the 'Local Certificates' screen. At the top, it says 'Replace PrivateKey/Certificate file in PEM format'. Below this, there is a checkbox labeled 'Private Key is protected by a password.' with an empty text input field to its right. Underneath, there are two buttons: 'Choose File' and 'No file chosen'. To the right of these are two more buttons: 'Import Certificate' and 'Create Certificate Request'. At the bottom, there is a table with a teal header and several columns. The columns are labeled 'Current File', 'Subject', 'Issuer', 'Valid From', 'Valid To', and 'Modify'.

The following table describes the labels in this screen.

Table 91 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Private Key is protected by a password	Select the checkbox and enter the private key into the text box to store it on the VMG. The private key should not exceed 63 ASCII characters (not including spaces).
Choose File	Click this to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the VMG.
Create Certificate Request	Click this button to go to the screen where you can have the VMG generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a <b>Not Yet Valid!</b> message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an <b>Expiring!</b> or <b>Expired!</b> message if the certificate is about to expire or has already expired.
Modify	<p>Click the <b>View</b> icon to open a screen with an in-depth list of information about the certificate (or certification request).</p> <p>For a certification request, click <b>Load Signed</b> to import the signed certificate.</p> <p>Click the <b>Remove</b> icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.</p>

### 19.3.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the VMG generate a certification request.

Figure 122 Create Certificate Request

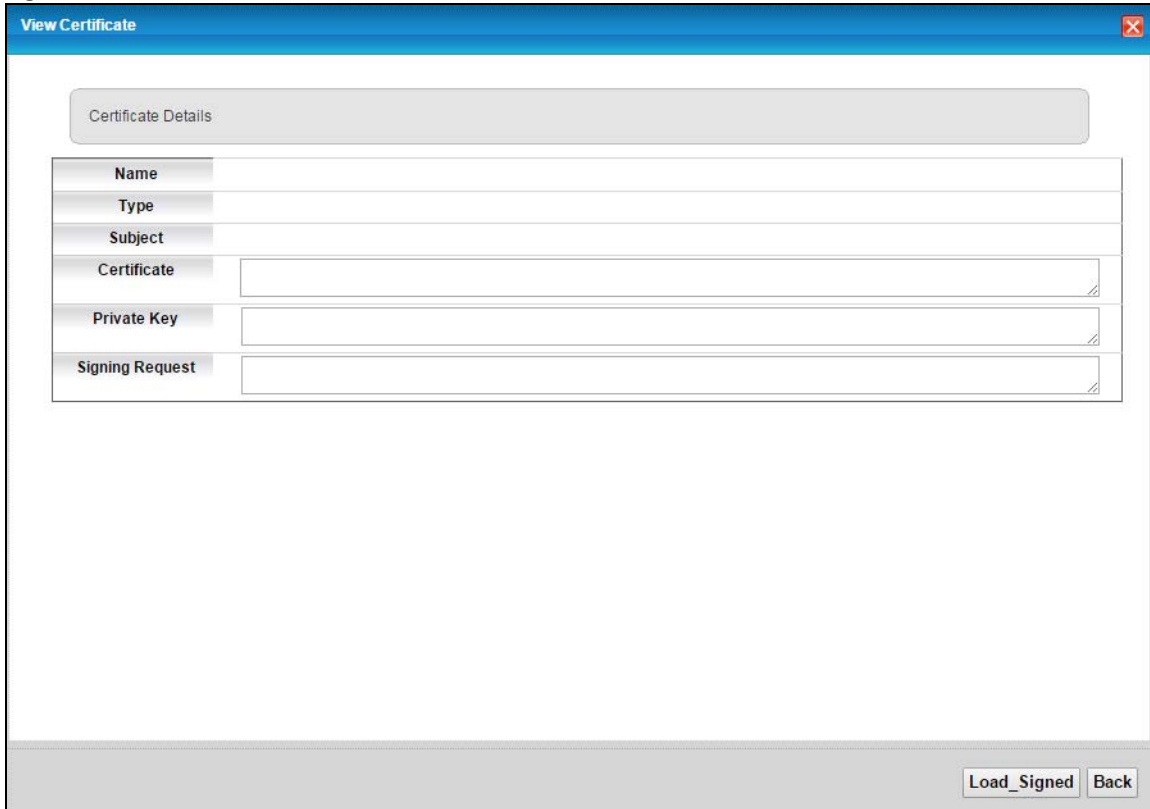
The following table describes the labels in this screen.

Table 92 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select <b>Auto</b> to have the VMG configure this field automatically. Or select <b>Customize</b> to enter it manually.  Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the VMG drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the VMG drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

After you click **Apply** to generate a request, you still need to get the certificate request signed by a Certificate Authority. If you already have, click the request's **Edit** icon and then **Load_Signed** to import the signed certificate into the VMG.

Figure 123 Certificate Request Created



The screenshot shows a window titled "View Certificate" with a blue header bar. Below the header is a grey bar labeled "Certificate Details". The main area contains a form with the following fields:

Name	
Type	
Subject	
Certificate	<input type="text"/>
Private Key	<input type="text"/>
Signing Request	<input type="text"/>

At the bottom right of the window, there are two buttons: "Load_Signed" and "Back".

### 19.3.2 Load Signed Certificate

After you create a certificate request and have it signed by a Certificate Authority, in the **View Certificate** screen click the certificate request's **Load_Signed** button to import the signed certificate into the VMG.

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

Figure 124 Load Signed Certificate

The following table describes the labels in this screen.

Table 93 Load Signed Certificate

LABEL	DESCRIPTION
Certificate Name	This is the name of the signed certificate.
Certificate	Copy and paste the signed certificate into the text box to store it on the VMG.
Load_Signed	Click <b>Load_Signed</b> to import the signed certificate into the VMG.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 19.4 The Trusted CA Screen

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the VMG to accept as trusted. The VMG accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 125 Security &gt; Certificates &gt; Trusted CA

The following table describes the fields in this screen.

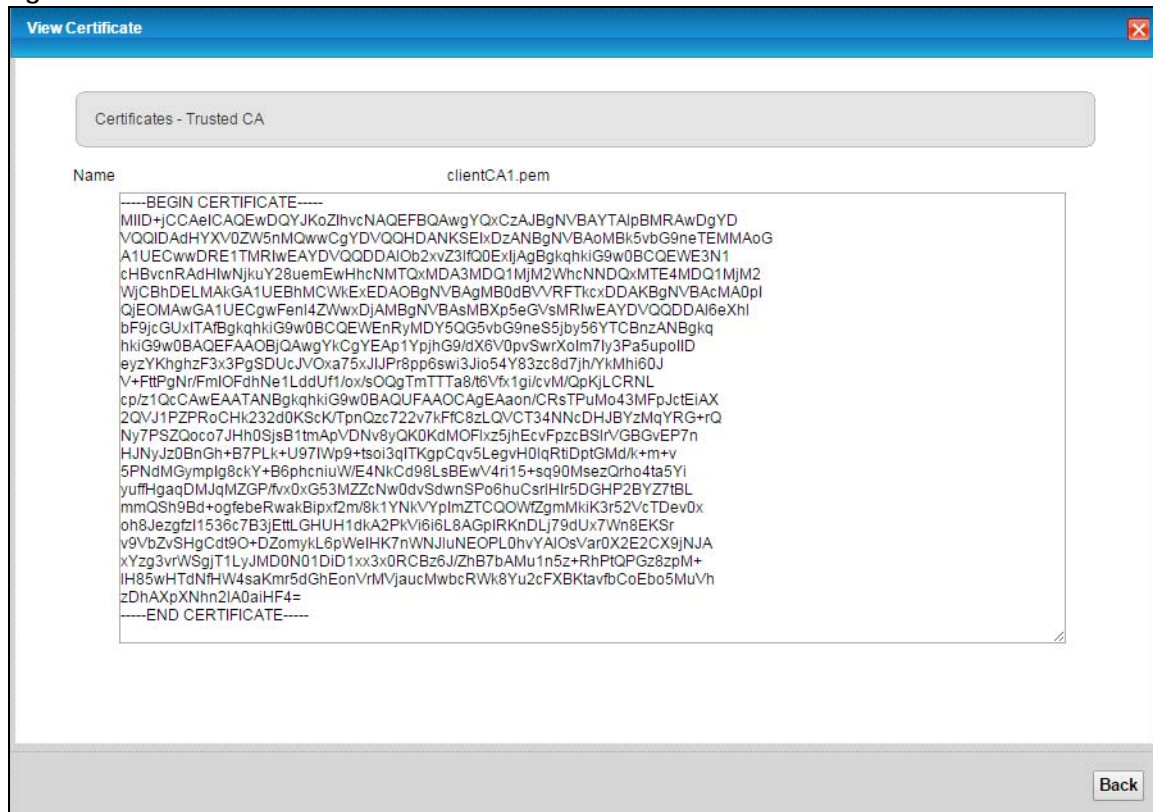
Table 94 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the VMG.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. <b>ca</b> means that a Certification Authority signed the certificate.
Modify	Click the <b>View</b> icon to open a screen with an in-depth list of information about the certificate (or certification request).  Click the <b>Remove</b> button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

## 19.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 126 Trusted CA: View



The following table describes the fields in this screen.

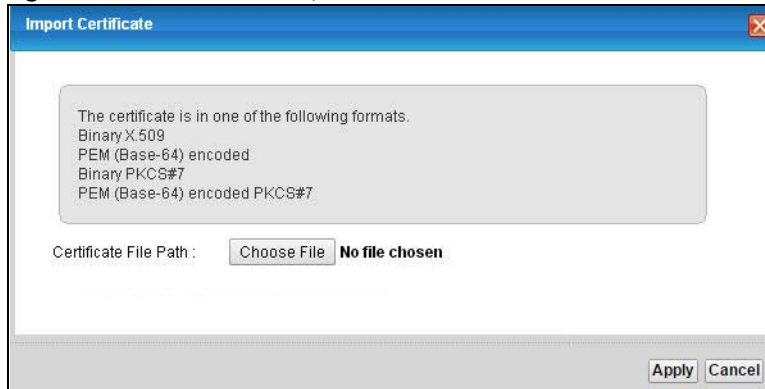
Table 95 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form.  You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click <b>Back</b> to return to the previous screen.

## 19.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The VMG trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 127 Trusted CA: Import Certificate



The following table describes the fields in this screen.

Table 96 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the certificate you want to upload in this field or click Choose File to find it.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

# CHAPTER 20

# Log

## 20.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the VMG log and then display the logs or have the VMG send them to an administrator (as e-mail) or to a syslog server.

### 20.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 20.2 on page 217](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 20.3 on page 217](#)).

### 20.1.2 What You Need To Know

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

#### Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

#### Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 97 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.



Table 97 Syslog Severity Levels

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

## 20.2 The System Log Screen

Use the **System Log** screen to see the system logs. Click **System Monitor > Log** to open the **System Log** screen.

Figure 128 System Monitor &gt; Log &gt; System Log

The screenshot shows the System Log screen interface. At the top, there are two dropdown menus: 'Level: All' and 'Category: All'. Below these are four buttons: 'Clear Log', 'Refresh', 'Export Log', and 'Email Log Now'. At the bottom, there is a table header with the following columns: '#', 'Time', 'Facility', 'Level', 'Category', and 'Messages'.

The following table describes the fields in this screen.

Table 98 System Monitor &gt; Log &gt; System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the VMG searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the <b>Maintenance &gt; Logs Setting</b> screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

## 20.3 The Security Log Screen

Use the **Security Log** screen to see the security-related logs for the categories that you select. Click **System Monitor > Log > Security Log** to open the following screen.

**Figure 129** System Monitor > Log > Security Log

The following table describes the fields in this screen.

**Table 99** System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the VMG searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the <b>Maintenance &gt; Logs Setting</b> screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

# CHAPTER 21

## Traffic Status

### 21.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

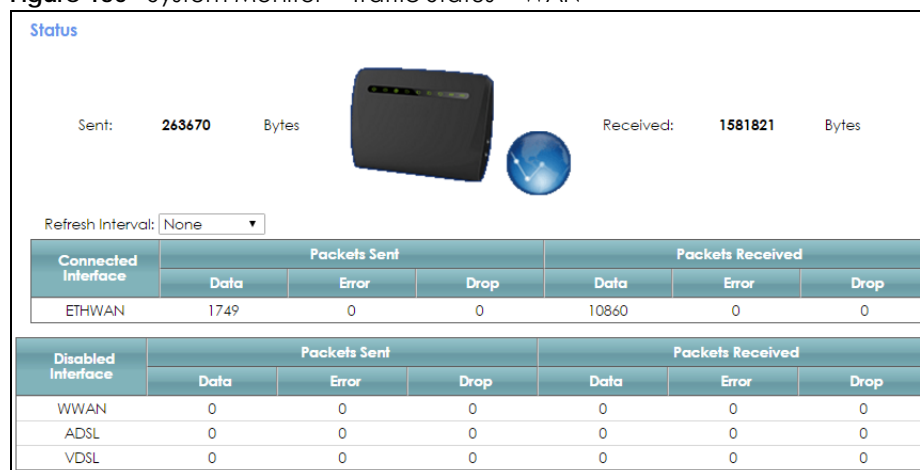
#### 21.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 21.2 on page 219](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 21.3 on page 220](#)).
- Use the **NAT** screen to view the NAT status of the VMG's client(s) ([Section 21.4 on page 221](#))

### 21.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figure in this screen shows the number of bytes received and sent on the VMG.

**Figure 130** System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 100 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	

Table 100 System Monitor &gt; Traffic Status &gt; WAN (continued)

LABEL	DESCRIPTION
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disconnected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

## 21.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figure in this screen shows the interface that is currently connected on the VMG.

Figure 131 System Monitor &gt; Traffic Status &gt; LAN

Refresh Interval:						
None <input type="button" value="v"/>						
Interface	LAN1	LAN2	LAN3	LAN4	2.4G WLAN	
Bytes Sent	0	0	0	2840446	0	
Bytes Received	0	0	0	3331046	0	
Interface	LAN1	LAN2	LAN3	LAN4	2.4G WLAN	
Sent (Packet)	Data	0	0	0	16187	0
	Error	0	0	0	0	0
	Drop	0	0	0	0	0
Received (Packet)	Data	0	0	0	29132	0
	Error	0	0	0	0	0
	Drop	0	0	0	0	0

The following table describes the fields in this screen.

Table 101 System Monitor &gt; Traffic Status &gt; LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen.
Interface	This shows the LAN or WLAN interface.

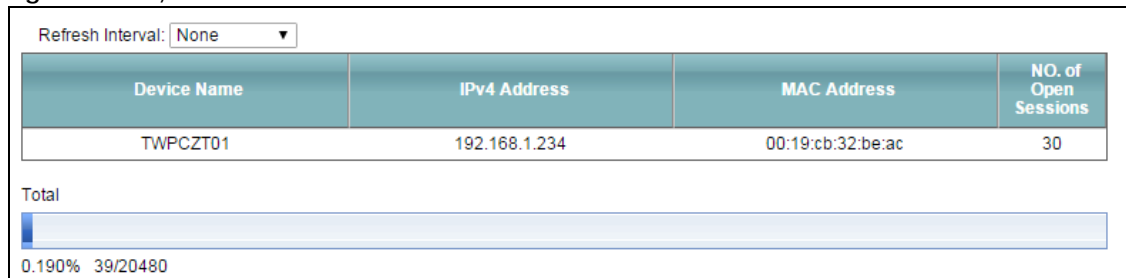
Table 101 System Monitor &gt; Traffic Status &gt; LAN (continued)

LABEL	DESCRIPTION
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interfaces.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

## 21.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. The figure in this screen shows the NAT session statistics for hosts currently connected on the VMG.

Figure 132 System Monitor &gt; Traffic Status &gt; NAT



The following table describes the fields in this screen.

Table 102 System Monitor &gt; Traffic Status &gt; NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen.
Device Name	This displays the name of the connected host.
IP Address	This displays the IP address of the connected host.
MAC Address	This displays the MAC address of the connected host.
No. of Open Sessions	This displays the number of NAT sessions currently opened for the connected host.
Total	This displays what percentage of NAT sessions the VMG can support is currently being used by all connected hosts. You can also see the number of active NAT sessions and the maximum number of NAT sessions the VMG can support.

# CHAPTER 22

## ARP Table

### 22.1 Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

#### 22.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

## 22.2 ARP Table Screen

Use the ARP table to view IP-to-MAC address mapping(s). To open this screen, click **System Monitor > ARP Table**.

**Figure 133** System Monitor > ARP Table

ARP Table displays the IPv4 address and MAC address of each DHCP connection. Neighbour Table displays the IPv6 address and MAC address of each Neighbour.

IPv4 ARP Table

#	IPv4 Address	MAC Address	Device
1	192.168.1.234	00:19:cb:32:be:ac	br0
2	172.16.56.254	50:67:f0:69:0d:2c	eth3.4
3	172.16.56.201	08:00:37:d4:90:33	eth3.4

IPv6 Neighbour Table

#	IPv6 Address	MAC Address	Device
1	fe80::5881:304e:c8c3:d485	00:19:cb:32:be:ac	br0

The following table describes the labels in this screen.

Table 103 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IPv4/IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device.

# CHAPTER 23

## Routing Table

### 23.1 Overview

Routing is based on the destination address only and the VMG takes the shortest path to forward a packet.

### 23.2 The Routing Table Screen

Click **System Monitor > Routing Table** to open the following screen.

**Figure 134** System Monitor > Routing Table

Destination: The destination network or destination host.  
Gateway : The gateway address or *(IPv4)/:::(IPv6) if none set.  
Subnet Mask (IPv4): The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route.  
Flags: U - up, ! - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect).  
Metric: The distance to the target (usually counted in hops).  
Interface: Interface to which packets for this route will be sent.

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flag	Metric	Interface
10.10.100.1	0.0.0.0	255.255.255.255	UH	0	ppp1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0
10.10.100.0	0.0.0.0	255.255.254.0	U	0	nas8_1
127.0.0.0	0.0.0.0	255.255.0.0	U	0	lo
239.0.0.0	0.0.0.0	255.0.0.0	U	0	br0

The following table describes the labels in this screen.

Table 104 System Monitor > Routing Table

LABEL	DESCRIPTION
IPv4/IPv6 Routing Table	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.



Table 104 System Monitor &gt; Routing Table (continued)

LABEL	DESCRIPTION
Flag	<p>This indicates the route status.</p> <p><b>U-Up:</b> The route is up.</p> <p><b>!-Reject:</b> The route is blocked and will force a route lookup to fail.</p> <p><b>G-Gateway:</b> The route uses a gateway to forward traffic.</p> <p><b>H-Host:</b> The target of the route is a host.</p> <p><b>R-Reinstate:</b> The route is reinstated for dynamic routing.</p> <p><b>D-Dynamic (redirect):</b> The route is dynamically installed by a routing daemon or redirect.</p> <p><b>M-Modified (redirect):</b> The route is modified from a routing daemon or redirect.</p>
Metric	<p>The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".</p>
Interface	<p>This indicates the name of the interface through which the route is forwarded.</p> <p><b>brx</b> indicates a LAN interface where x can be 0~3 to represent LAN1 to LAN4 respectively.</p> <p><b>nas8_x</b> indicates a VDSL WAN interface using IPoE or in bridge mode.</p> <p><b>nasx</b> indicates an ADSL WAN interface using IPoE, IPoA or in bridge mode.</p> <p><b>nas10_x</b> indicates an Ethernet WAN interface using IPoE or in bridge mode.</p> <p><b>ppp0</b> indicates a WAN interface using PPPoE or PPPoA.</p>

# CHAPTER 24

## xDSL Statistics

### 24.1 The xDSL Statistics Screen

Use this screen to view detailed DSL statistics. Click **System Monitor > xDSL Statistics** to open the following screen.

**Figure 135** System Monitor > xDSL Statistics

The screenshot shows a web interface for monitoring xDSL statistics. At the top, there is a 'Monitor' section with two dropdown menus: 'Refresh Interval' set to 'No Refresh' and 'Line' set to 'Line 0'. Below this is a 'Status' section. The status information is displayed in a monospaced font, separated by horizontal lines. It shows the following details:

```
=====
xDSLFWVersion:      FwVer:5.9.0.2_A_A60901 HwVer:T14.F7_0.0
Line State:         Down
Modulation:         N/A
Annex Mode:         N/A
=====
                        Downstream
SNR Margin:         N/A
Line Attenuation:   N/A
Data Rate:          0 kbps
ES:                 N/A
SES:                N/A
                        Upstream
SNR Margin:         N/A
Line Attenuation:   N/A
Data Rate:          0 kbps
ES:                 N/A
SES:                N/A
```

The following table describes the labels in this screen.

Table 105 Status > xDSL Statistics

LABEL	DESCRIPTION
Refresh Interval	Select the time interval for refreshing statistics.
Line	Select which DSL line's statistics you want to display.
xDSLFWVersion	This displays the current firmware and hardware versions of the VMG.
Line State	This displays the current state of the DSL connection.
Modulation	This displays the modulation method of the DSL connection.
Annex Mode	This displays the annex mode of the DSL connection.
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
SNR Margin	This is the upstream and downstream Signal-to-Noise Ratio margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the system still being able to meet its transmission targets.

Table 105 Status &gt; xDSL Statistics (continued)

LABEL	DESCRIPTION
Line Attenuation	This is the upstream and downstream line attenuation, measured in decibels (dB). This attenuation is the difference between the power transmitted at the near-end and the power received at the far-end. Attenuation is affected by the channel characteristics (wire gauge, quality, condition and length of the physical line).
Data Rate	These are the data transfer rates at which the port is sending and receiving data.
ES	This is the number of Errored Seconds meaning the number of seconds containing at least one errored block or at least one defect.
SES	This is the number of Severely Errored Seconds meaning the number of seconds containing 30% or more errored blocks or at least one defect. This is a subset of ES.

# CHAPTER 25

## Cellular Statistics

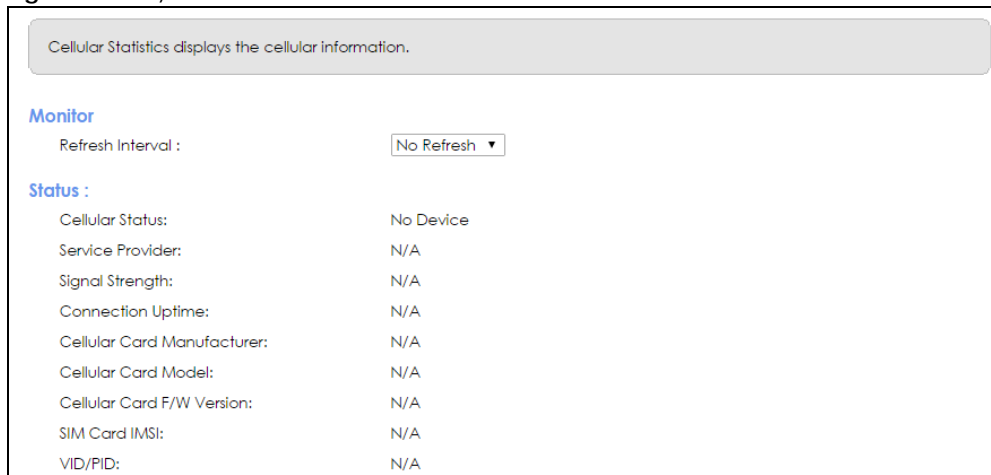
### 25.1 Overview

Use the **Cellular Statistics** screens to look at cellular Internet connection status.

### 25.2 The Cellular Statistics Screen

To open this screen, click **System Monitor > Cellular Statistics**. The Cellular status is available on this screen only when you insert a compatible cellular dongle in a USB port on the VMG.

**Figure 136** System Monitor > Cellular Statistics



The following table describes the labels in this screen.

Table 106 System Monitor > Cellular Statistics

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen. Select <b>No Refresh</b> to stop refreshing.
Cellular Status	This field displays the status of the cellular Internet connection. This field can display: <b>GSM</b> - Global System for Mobile Communications, 2G <b>GPRS</b> - General Packet Radio Service, 2.5G <b>EDGE</b> - Enhanced Data rates for GSM Evolution, 2.75G <b>WCDMA</b> - Wideband Code Division Multiple Access, 3G <b>HSDPA</b> - High-Speed Downlink Packet Access, 3.5G <b>HSUPA</b> - High-Speed Uplink Packet Access, 3.75G <b>HSPA</b> - HSDPA+HSUPA, 3.75G
Service Provider	This field displays the name of the service provider.
Signal Strength	This field displays the strength of the signal in dBm.
Connection Uptime	This field displays the time the connection has been up.
Cellular Card Manufacturer	This field displays the manufacturer of the cellular card.
Cellular Card Model	This field displays the model name of the cellular card.
Cellular Card F/W Version	This field displays the firmware version of the cellular card.
SIM Card IMSI	The International Mobile Subscriber Identity or IMSI is a unique identification number associated with all cellular networks. This number is provisioned in the SIM card.
VID/PID	This field displays the USB Vendor ID and Product ID of the cellular card.

# CHAPTER 26

## System

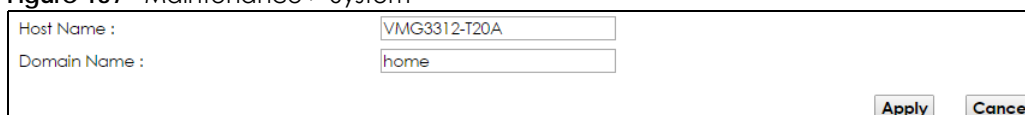
### 26.1 Overview

In the **System** screen, you can name your VMG (Host) and give it an associated domain name for identification purposes.

### 26.2 The System Screen

Click **Maintenance > System** to open the following screen.

**Figure 137** Maintenance > System



The screenshot shows a form with two input fields. The first field is labeled 'Host Name :' and contains the text 'VMG3312-T20A'. The second field is labeled 'Domain Name :' and contains the text 'home'. At the bottom right of the form, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 107 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a hostname for your VMG. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your host VMG.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to abandon this screen without saving.

# CHAPTER 27

## User Account

### 27.1 Overview

In the **User Account** screen, you can view the settings of the “admin” and other user accounts that you used to log in the VMG.

### 27.2 The User Account Screen

Click **Maintenance > User Account** to open the following screen.

**Figure 138** Maintenance > User Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	<input checked="" type="checkbox"/>	admin	3	5	5	Administrator	
2	<input checked="" type="checkbox"/>	Zyxel	3	5	5	Administrator	
3	<input checked="" type="checkbox"/>	user	3	10	5	User	

The following table describes the labels in this screen.

Table 108 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account.
#	This is the index number
Active	This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it.
User Name	This field displays the name of the account used to log into the VMG web configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This field displays the the length of inactive time before the VMG will automatically log the user out of the web configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in <b>Retry Times</b> .
Group	This field displays whether this user has <b>Administrator</b> or <b>User</b> privileges.
Modify	Click the <b>Edit</b> icon to configure the entry. Click the <b>Delete</b> icon to remove the entry.

## 27.2.1 The User Account Add and Edit Screens

Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance > User Account** to open the following screen.

**Figure 139** Maintenance > User Account > Add/Edit

The figure displays two overlapping windows from a web-based user management interface. The background window is titled "User Account Add" and contains the following fields: "Active" with radio buttons for "Enable" (selected) and "Disable"; "User Name" with an empty text box; "Password" with an empty text box; "Verify Password" with an empty text box; "Retry Times" with a spinner box set to "3" and the text "(0~5), 0 : Not limit"; "Idle Timeout" with a spinner box set to "5" and the text "Minute(s) (1~60)"; "Lock Period" with an empty text box; and "Group" with an empty dropdown menu. The foreground window is titled "User Account Edit" and contains the following fields: "Active" with radio buttons for "Enable" (selected) and "Disable"; "User Name" with a text box containing "admin"; "Old Password" with an empty text box; "New Password" with an empty text box; "Verify New Password" with an empty text box; "Retry Times" with a spinner box set to "3" and the text "(0~5), 0 : Not limit"; "Idle Timeout" with a spinner box set to "5" and the text "Minute(s) (1~60)"; "Lock Period" with a spinner box set to "5" and the text "Minute(s) (5~90)"; and "Group" with a dropdown menu showing "Administrator". Both windows have "OK" and "Cancel" buttons at the bottom right.

The following table describes the labels in this screen.

Table 109 Maintenance > User Account > Add/Edit

LABEL	DESCRIPTION
Active	This field indicates whether the user account is active or not. Clear the check box to disable the user account. Select the check box to enable it.
User Name	Enter a new name for the account. This field displays the name of an existing account.
Old Password	Type the default password or the existing password used to access the VMG web configurator.
Password/New Password	Type a new password (up to 256 characters) for this account. Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the VMG.
Verify Password/Verify New Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the VMG will automatically log the user out of the web configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in <b>Retry Times</b> .



Table 109 Maintenance > User Account > Add/Edit (continued) (continued)

LABEL	DESCRIPTION
Group	Specify whether this user will have <b>Administrator</b> or <b>User</b> privileges.
OK	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

# CHAPTER 28

## Remote Management

### 28.1 Overview

Remote management controls through which interface(s), which services can access the VMG.

Note: The VMG is managed using the Web Configurator.

### 28.2 The Remote MGMT Screen

Use this screen to configure through which interface(s), which services can access the VMG. You can also specify the port numbers the services must use to connect to the VMG. Click **Maintenance > Remote MGMT** to open the following screen.

Figure 140 Maintenance > Remote MGMT

**Service Control**

WAN Interface used for services:  Any_WAN  Multi_WAN

WWAN  ADSL  VDSL  ETHWAN

service	LAN/WLAN	WAN	Trust Domain	Port
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	443
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	161
PING	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	

Apply Cancel

The following table describes the fields in this screen.

Table 110 Maintenance > Remote MGMT

LABEL	DESCRIPTION
WAN Interface used for services	Select <b>Any_WAN</b> to have the VMG automatically activate the remote management service when any WAN connection is up. Select <b>Multi_WAN</b> and then select one or more WAN connections to have the VMG activate the remote management service when the selected WAN connections are up.
service	This is the service you may use to access the VMG.
LAN/WLAN	Select the <b>Enable</b> check box for the corresponding services that you want to allow access to the VMG from the LAN/WLAN.

Table 110 Maintenance &gt; Remote MGMT (continued)

LABEL	DESCRIPTION
WAN	Select the <b>Enable</b> check box for the corresponding services that you want to allow access to the VMG from all WAN connections.
Trust Domain	Select the <b>Enable</b> check box for the corresponding services that you want to allow access to the VMG from the trusted hosts configured in the <b>Maintenance &gt; Remote MGMT &gt; Trust Domain</b> screen.  If you only want certain WAN connections to have access to the VMG using the corresponding services, then clear <b>WAN</b> , select <b>Trust Domain</b> and configure the allowed IP address(es) in the <b>Trust Domain</b> screen.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click <b>Apply</b> to save your changes back to the VMG.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

## 28.3 The Trust Domain Screen

Use this screen to view a list of public IP addresses which are allowed to access the VMG through the services configured in the **Maintenance > Remote MGMT** screen. Click **Maintenance > Remote MGMT > Trust Domain** to open the following screen.

Note: If this list is empty, all public IP addresses can access the VMG from the WAN through the specified services.

Figure 141 Maintenance &gt; Remote MGMT &gt; Trust Domain



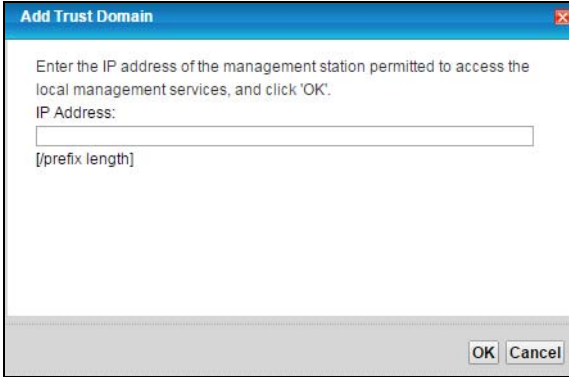
The following table describes the fields in this screen.

Table 111 Maintenance &gt; Remote MGMT &gt; Trust Domain

LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the <b>Delete</b> icon to remove the trust IP address.

### 28.3.1 The Add Trust Domain Screen

Use this screen to configure a public IP address which is allowed to access the VMG. Click the **Add Trust Domain** button in the **Maintenance > Remote MGMT > Trust Domain** screen to open the following screen.

**Figure 142** Maintenance > Remote MGMT > Trust Domain > Add Trust Domain

Enter the IP address of the management station permitted to access the local management services, and click 'OK'.

IP Address:

[/prefix length]

OK Cancel

The following table describes the fields in this screen.

Table 112 Maintenance &gt; Remote MGMT &gt; Trust Domain &gt; Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IPv4 IP address which is allowed to access the service on the VMG from the WAN.
OK	Click <b>OK</b> to save your changes back to the VMG.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

# CHAPTER 29

# SNMP

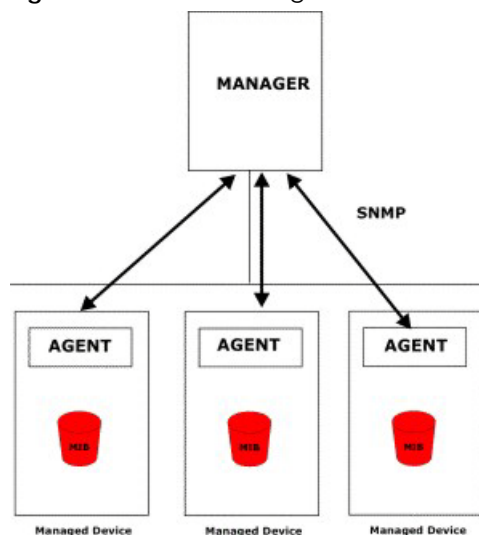
## 29.1 Overview

This chapter explains how to configure the SNMP settings on the VMG.

## 29.2 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your VMG supports SNMP agent functionality, which allows a manager station to manage and monitor the VMG through the network. The VMG supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

**Figure 143** SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the VMG). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Click **Maintenance > SNMP** to open the following screen. Use this screen to configure the VMG SNMP settings.

**Figure 144** Maintenance > SNMP

The following table describes the fields in this screen.

Table 113 Maintenance > SNMP

LABEL	DESCRIPTION
SNMP Agent	Select <b>Enable</b> to let the VMG act as an SNMP agent, which allows a manager station to manage and monitor the VMG through the network. Select <b>Disable</b> to turn this feature off.
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station.
Trap Community	Enter the <b>Trap Community</b> , which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.
System Contact	Enter the SNMP system contact.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click this to save your changes back to the VMG.
Cancel	Click this to restore your previously saved settings.

# CHAPTER 30

## Time Settings

### 30.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

### 30.2 The Time Screen

To change your VMG's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the VMG's time based on your local time zone.

**Figure 145** Maintenance > Time

**Current Date/Time**  
Current Time : 06:22:12  
Current Date : 2016-01-28

**Time and Date Setup**  
Time Protocol : SNTP (RFC-1769)  
First Time Server Address : pool.ntp.org  
Second Time Server Address : None  
Third Time Server Address : None  
Fourth Time Server Address : None  
Fifth Time Server Address : None

**Time Zone**  
Time Zone: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

**Daylight Savings**  
Active  Enable  Disable

**Start Rule**  
Day :  1 in  
 Fifth Sunday in  
Month : March  
Hour : 2 : 0

**End Rule**  
Day :  1 in  
 Fifth Sunday in  
Month : October  
Time : 3 : 0

Apply Cancel

The following table describes the fields in this screen.

Table 114 Maintenance &gt; Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your VMG. Each time you reload this page, the VMG synchronizes the time with the time server.
Current Date	This field displays the date of your VMG. Each time you reload this page, the VMG synchronizes the date with the time server.
Time and Date Setup	
First ~ Fifth Time Server Address	Select an NTP time server from the drop-down list box.  Otherwise, select <b>Other</b> and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.  Select <b>None</b> if you don't want to configure the time server.  Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Active	Select <b>Enable</b> if you use Daylight Saving Time.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The <b>Hour</b> field uses the 24 hour format. Here are a couple of examples:  Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to <b>Second, Sunday</b> , the month to <b>March</b> and the time to <b>2</b> in the <b>Hour</b> field.  Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to <b>Last, Sunday</b> and the month to <b>March</b> . The time you select depends on your time zone. In Germany for instance, you would select <b>2</b> in the <b>Hour</b> field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The <b>Time</b> field uses the 24 hour format. Here are a couple of examples:  Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to <b>First, Sunday</b> , the month to <b>November</b> and the time to <b>2</b> in the <b>Time</b> field.  Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to <b>Last, Sunday</b> , and the month to <b>October</b> . The time you select depends on your time zone. In Germany for instance, you would select <b>2</b> in the <b>Time</b> field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to return to the previous configuration.



# CHAPTER 31

## E-mail Notification

### 31.1 Overview

A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

To have the VMG send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

### 31.2 The E-mail Notification Screen

Click **Maintenance > E-mail Notification** to open the **E-mail Notification** screen. Use this screen to view, remove and add mail server information on the VMG.

**Figure 146** Maintenance > E-mail Notification



The screenshot shows a web interface for managing email notifications. At the top left is a button labeled "Add New E-mail". Below it is a table with six columns: "Mail Server Address", "Username", "Port", "Security", "E-mail Address", and "Remove". Below the table is a "Note" icon followed by the text: "Note: E-mail notification default service port using port 25."

The following table describes the labels in this screen.

Table 115 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New Email	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
Username	This field displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
Email Address	This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the VMG sends.
Remove	Click this button to delete the selected entry(ies).

#### 31.2.1 E-mail Notification Edit

Click the **Add New E-mail** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 147 E-mail Notification &gt; Add New E-mail

The following table describes the labels in this screen.

Table 116 E-mail Notification &gt; Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the <b>Account E-mail Address</b> field.  If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the <b>Account E-mail Address</b> field.
Authentication Password	Enter the password associated with the user name above.
Account E-mail Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the VMG sends.  If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Connection Security	Select <b>SSL</b> to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the VMG.  Select <b>STARTTLS</b> to upgrade a plain text connection to a secure connection using SSL/TLS.
OK	Click this button to save your changes and return to the previous screen.
Cancel	Click this button to exit this screen without saving.

# CHAPTER 32

## Logs Setting

### 32.1 Overview

You can configure where the VMG sends logs and which logs and/or immediate alerts the VMG records in the **Logs Setting** screen.

### 32.2 The Logs Setting Screen

To change your VMG's log settings, click **Maintenance > Logs Setting**. The screen appears as shown.

**Figure 148** Maintenance > Logs Setting

**Syslog Setting**

Syslog Logging :  Enable  Disable (settings are invalid when disabled)

Mode :

Syslog Server :  (Server NAME or IPv4/IPv6 Address)

UDP Port :  (Server Port)

**E-mail Log Settings :**

E-mail Log Settings :  Enable  Disable (settings are invalid when disabled)

Mail Account :

System Log Mail Subject :

Security Log Mail Subject :

Send Log to :  (E-Mail Address)

Send Alarm to :  (E-Mail Address)

Alarm Interval :

**Active Log**

**System Log**

- WAN-DHCP
- DHCP Server
- PPPoE
- TR-069
- HTTP
- UPNP
- System
- xDSL
- ACL
- Wireless

**Security Log**

- Account
- Attack
- Firewall
- MAC Filter

The following table describes the fields in this screen.

Table 117 Maintenance &gt; Logs Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The VMG sends a log to an external syslog server. Select <b>Enable</b> to enable syslog logging.
Mode	Select the syslog destination from the drop-down list box.  If you select <b>Remote</b> , the log(s) will be sent to a remote syslog server. If you select <b>Local File</b> , the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select <b>Local File and Remote</b> .
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
E-mail Log Settings	Select <b>Enable</b> to have the VMG send logs and alarm messages to the configured e-mail addresses.
Mail Account	This section is available only when you select <b>Enable</b> in the <b>E-mail Log Settings</b> field.  Select a mail account from which you want to send logs. You can configure mail accounts in the <b>Maintenance &gt; E-mail Notification</b> screen.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the VMG sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log e-mail message that the VMG sends.
Send Log to	The VMG sends logs to the e-mail address specified in this field. If this field is left blank, the VMG does not send logs via E-mail.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Alarm Interval	Specify how often the alarm should be updated.
Active Log	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Apply	Click <b>Apply</b> to save your changes.
Cancel	Click <b>Cancel</b> to restore your previously saved settings.

### 32.2.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "End of Log" message shows that a complete log has been sent.

Figure 149 E-mail Log Example

```

Subject:
    Firewall Alert From
Date:
    Fri, 07 Apr 2000 10:05:42
From:
    user@zyxel.com
To:
    user@zyxel.com
1|Apr 7 00 |From:192.168.1.1      To:192.168.1.255  |default policy |forward
  |09:54:03 |UDP      src port:00520 dest port:00520  |<1,00>         |
2|Apr 7 00  |From:192.168.1.131   To:192.168.1.255  |default policy |forward
  |09:54:17  |UDP      src port:00520 dest port:00520  |<1,00>         |
3|Apr 7 00  |From:192.168.1.6     To:10.10.10.10   |match          |forward
  |09:54:19  |UDP      src port:03516 dest port:00053  |<1,01>         |
.....{snip}.....
.....{snip}.....
126|Apr 7 00  |From:192.168.1.1     To:192.168.1.255  |match          |forward
   |10:05:00  |UDP      src port:00520 dest port:00520  |<1,02>         |
127|Apr 7 00  |From:192.168.1.131   To:192.168.1.255  |match          |forward
   |10:05:17  |UDP      src port:00520 dest port:00520  |<1,02>         |
128|Apr 7 00  |From:192.168.1.1     To:192.168.1.255  |match          |forward
   |10:05:30  |UDP      src port:00520 dest port:00520  |<1,02>         |

End of Firewall Log

```

# CHAPTER 33

## Firmware Upgrade

### 33.1 Overview

This chapter explains how to upload new firmware to your VMG. You can download new firmware releases from your nearest Zyxel FTP site (or [www.zyxel.com](http://www.zyxel.com)) to use to upgrade your device's performance.

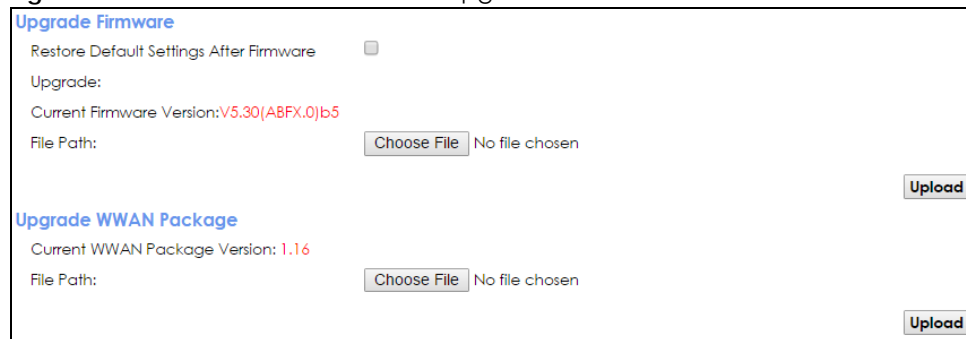
**Only use firmware for your device's specific model. Refer to the label on the bottom of your VMG.**

### 33.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

**Do NOT turn off the VMG while firmware upload is in progress!**

Figure 150 Maintenance > Firmware Upgrade



The screenshot shows the 'Upgrade Firmware' screen. At the top, there is a section for 'Upgrade Firmware' with a checkbox for 'Restore Default Settings After Firmware' which is currently unchecked. Below this, it says 'Upgrade:' and 'Current Firmware Version: V5.30(ABFX.0)b5'. There is a 'File Path:' label followed by a 'Choose File' button and the text 'No file chosen'. To the right of this section is an 'Upload' button. Below this is a section for 'Upgrade WWAN Package' with 'Current WWAN Package Version: 1.16'. It also has a 'File Path:' label, a 'Choose File' button, and 'No file chosen'. To the right of this section is another 'Upload' button.

The following table describes the labels in this screen. After you see the firmware updating screen, wait two minutes before logging into the VMG again.

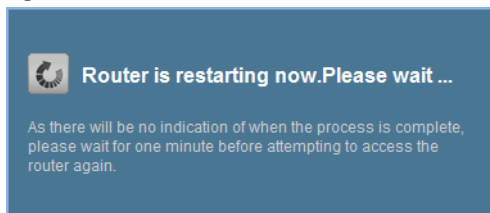
Table 118 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Click the check box to have the VMG automatically reset itself after the new firmware is uploaded.

Table 118 Maintenance &gt; Firmware Upgrade

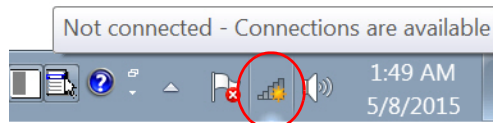
LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click <b>Choose File</b> to find it.
Choose File	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.
Upgrade WWAN Package	
Current WWAN Package Version	This is the present WWAN Package version and the date created.
File Path	Type in the location of the file you want to upload in this field or click <b>Choose File</b> to find it.
Choose File	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

Figure 151 Firmware Uploading



The VMG automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

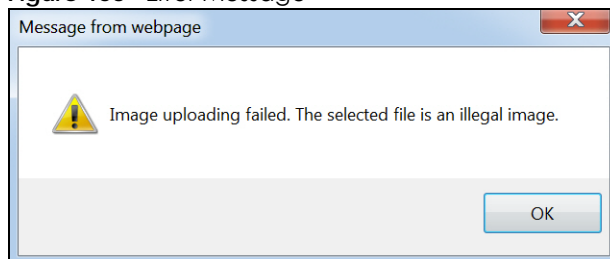
Figure 152 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 153 Error Message



# CHAPTER 34

## Backup/Restore

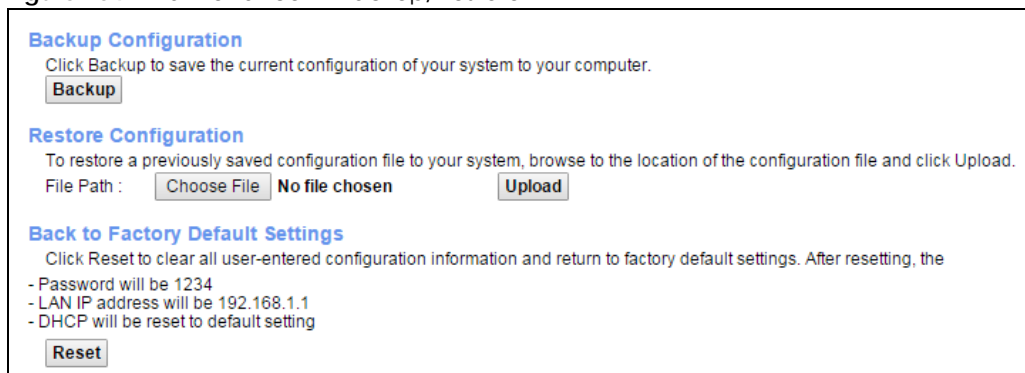
### 34.1 Overview

The **Backup/Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

### 34.2 The Backup/Restore Screen

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

**Figure 154** Maintenance > Backup/Restore



The screenshot displays the 'Maintenance > Backup/Restore' interface. It is divided into three main sections:

- Backup Configuration:** Includes the instruction 'Click Backup to save the current configuration of your system to your computer.' and a 'Backup' button.
- Restore Configuration:** Includes the instruction 'To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.' Below this is a 'File Path' field with a 'Choose File' button, the text 'No file chosen', and an 'Upload' button.
- Back to Factory Default Settings:** Includes the instruction 'Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the' followed by a list of default settings: '- Password will be 1234', '- LAN IP address will be 192.168.1.1', and '- DHCP will be reset to default setting'. A 'Reset' button is located at the bottom of this section.

#### Backup Configuration

Backup Configuration allows you to back up (save) the VMG's current configuration to a file on your computer. Once your VMG is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the VMG's current system configuration to your computer.



## Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your VMG.

Table 119 Restore Configuration

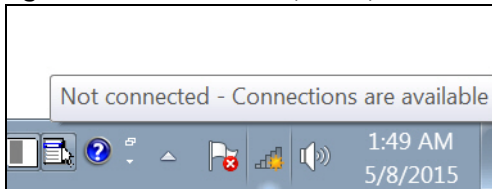
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Choose File</b> to find it.
Choose File	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to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

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

After the VMG configuration has been restored successfully, the login screen appears. Login again to restart the VMG.

The VMG automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

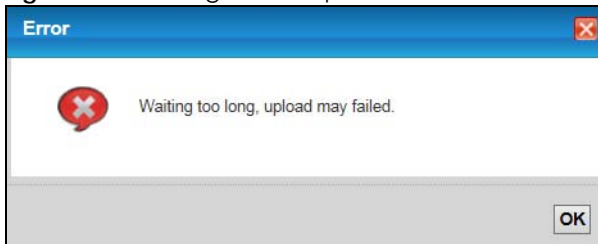
Figure 155 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

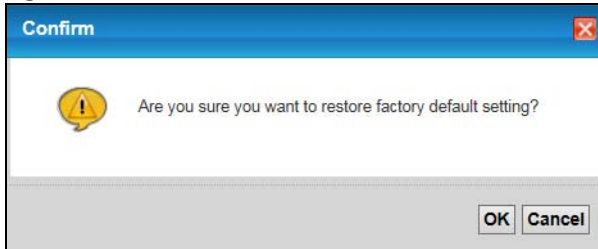
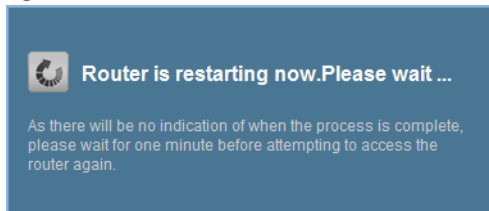
If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 156 Configuration Upload Error



## Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the VMG to its factory defaults. The following warning screen appears.

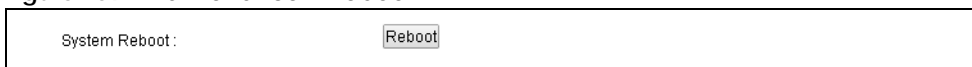
**Figure 157** Reset Warning Message**Figure 158** Reset In Process Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your VMG. Refer to [Section 1.6.6 on page 24](#) for more information on the **RESET** button.

## 34.3 The Reboot Screen

System restart allows you to reboot the VMG remotely without turning the power off. You may need to do this if the VMG hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the VMG reboot. This does not affect the VMG's configuration.

**Figure 159** Maintenance > Reboot

# CHAPTER 35

## Diagnostic

### 35.1 Overview

The **Diagnostic** screens display information to help you identify problems with the VMG.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

#### 35.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & Nslookup** screen lets you ping an IP address or trace the route packets take to a host ([Section 35.3 on page 252](#)).

### 35.2 What You Need to Know

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

#### How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

## 35.3 Ping & TraceRoute & Nslookup

Use this screen to ping, traceroute, or nslookup an IP address. Click **Maintenance > Diagnostic > Ping&TraceRoute&Nslookup** to open the screen shown next.

**Figure 160** Maintenance > Diagnostic > Ping&TraceRoute&Nslookup

The screenshot shows a web interface for network diagnostics. At the top, it says 'Ping/TraceRoute Test' and 'Info-'. Below this is a large, empty rectangular area for displaying test results. At the bottom of the interface, there is a section labeled 'TCP/IP' which contains an input field for 'Address' and five buttons: 'Ping', 'Ping 6', 'Trace Route', 'Trace Route 6', and 'Nslookup'.

The following table describes the fields in this screen.

**Table 120** Maintenance > Diagnostic > Ping & TraceRoute & Nslookup

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IPv4 address that you entered.
Ping 6	Click this to ping the IPv6 address that you entered.
TraceRoute	Click this to display the route path and transmission delays between the VMG to the IPv4 address that you entered.
TraceRoute 6	Click this to display the route path and transmission delays between the VMG to the IPv6 address that you entered.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

# CHAPTER 36

## Troubleshooting

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

- [Power, Hardware Connections, and LEDs](#)
- [VMG Access and Login](#)
- [Internet Access](#)
- [Wireless Internet Access](#)
- [USB Device Connection](#)
- [UPnP](#)

### 36.1 Power, Hardware Connections, and LEDs

---

[The VMG does not turn on. None of the LEDs turn on.](#)

---

- 1 Make sure the VMG is turned on.
- 2 Make sure you are using the power adaptor or cord included with the VMG.
- 3 Make sure the power adaptor or cord is connected to the VMG and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the VMG off and on.
- 5 If the problem continues, contact the vendor.

---

[One of the LEDs does not behave as expected.](#)

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.6.2 on page 20](#).
- 2 Check the hardware connections.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the VMG off and on.

- 5 If the problem continues, contact the vendor.

## 36.2 VMG Access and Login

---

### I forgot the IP address for the VMG.

---

- 1 The default LAN IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the VMG by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the VMG (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6.6 on page 24](#).

### I forgot the password.

---

- 1 See the cover page for the default login names and associated passwords.
- 2 If those do not work, you have to reset the device to its factory defaults. See [Section 1.6.6 on page 24](#).

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

---

- 1 Make sure you are using the correct IP address.
  - The default IP address is [192.168.1.1](#).
  - If you changed the IP address ([Section 8.2 on page 125](#)), use the new IP address.
  - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the VMG](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 1.6.2 on page 20](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).
- 5 Reset the device to its factory defaults, and try to access the VMG with the default IP address. See [Section 1.6.6 on page 24](#).

- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the VMG using another service, such as Telnet. If you can access the VMG, check the remote management settings and firewall rules to find out why the VMG does not respond to HTTP.

---

#### I can see the [Login](#) screen, but I cannot log in to the VMG.

---

- 1 Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the VMG. Log out of the VMG in the other session, or ask the person who is logged in to log out.
- 3 Turn the VMG off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 36.1 on page 253](#).

---

#### I cannot Telnet to the VMG.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

---

#### I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

## 36.3 Internet Access

---

#### I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.6.2 on page 20](#).

- 2 Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure that you enabled the wireless LAN in the VMG and your wireless client and that the wireless settings in the wireless client are the same as the settings in the VMG.
- 4 Disconnect all the cables from your device and reconnect them.
- 5 If the problem continues, contact your ISP.

---

I cannot access the Internet through a DSL connection.

---

- 1 Make sure you have the **DSL WAN** port connected to a telephone jack (or the DSL or modem jack on a splitter if you have one).
- 2 Make sure you configured a proper DSL WAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.
- 3 Check that the LAN interface you are connected to is in the same interface group as the DSL connection (**Network Setting > Interface Grouping**).
- 4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

---

I cannot connect to the Internet using a second DSL connection.

---

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

---

I cannot connect to the Internet using an Ethernet connection.

---

- 1 Make sure you have the Ethernet WAN port connected to a Modem or Router.
- 2 Make sure you configured a proper Ethernet WAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.
- 3 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting > Interface Grouping**).
- 4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.



---

I cannot connect to the Internet using a cellular connection.

---

- 1 The DSL and Ethernet WAN connections have priority in that order. If the DSL or Ethernet WAN connection is up, then the cellular connection will be down.
- 2 Make sure you have connected a compatible cellular dongle to the USB port.
- 3 Make sure you have configured **Network Setting > Broadband > Cellular Backup** correctly.
- 4 Check that the VMG is within range of a cellular base station.

---

I cannot access the VMG anymore. I had access to the VMG, but my connection is not available anymore.

---

- 1 Your session with the VMG may have expired. Try logging into the VMG again.
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.6.2 on page 20](#).
- 3 Turn the VMG off and on.
- 4 If the problem continues, contact your vendor.

## 36.4 Wireless Internet Access

---

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

---

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.

- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

---

### What is a Server Set ID (SSID)?

---

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

## 36.5 USB Device Connection

---

### The VMG fails to detect my USB device.

---

- 1 Disconnect the USB device.
- 2 Reboot the VMG.
- 3 If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
- 4 Re-connect your USB device to the VMG.

## 36.6 UPnP

---

### When using UPnP and the VMG reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

---

- 1 Disconnect the Ethernet cable from the VMG's LAN port or from your computer.
- 2 Re-connect the Ethernet cable.

---

### The **Local Area Connection** icon for UPnP disappears in the screen.

---

Restart your computer.

---

# PART III

# Appendices

---

Appendices contain general information. Some information may not apply to your device.

# APPENDIX A

## Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <http://www.zyxel.com/homepage.shtml> and also [http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml](http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml) for the latest information.

Please have the following information ready when you contact an office.

### Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

### Corporate Headquarters (Worldwide)

#### Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com>

### Asia

#### China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

#### India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

#### Kazakhstan

- Zyxel Kazakhstan
- <http://www.zyxel.kz>

## **Korea**

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

## **Malaysia**

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

## **Pakistan**

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

## **Philippines**

- Zyxel Philippines
- <http://www.zyxel.com.ph>

## **Singapore**

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

## **Taiwan**

- Zyxel Communications Corporation
- <http://www.zyxel.com/tw/zh/>

## **Thailand**

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

## **Vietnam**

- Zyxel Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

## **Europe**

### **Austria**

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

### **Belarus**

- Zyxel BY
- <http://www.zyxel.by>

## **Belgium**

- Zyxel Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

## **Bulgaria**

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

## **Czech Republic**

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

## **Denmark**

- Zyxel Communications A/S
- <http://www.zyxel.dk>

## **Estonia**

- Zyxel Estonia
- <http://www.zyxel.com/ee/et/>

## **Finland**

- Zyxel Communications
- <http://www.zyxel.fi>

## **France**

- Zyxel France
- <http://www.zyxel.fr>

## **Germany**

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

## **Hungary**

- Zyxel Hungary & SEE
- <http://www.zyxel.hu>

## **Italy**

- Zyxel Communications Italy
- <http://www.zyxel.it/>

## **Latvia**

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

## **Lithuania**

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

## **Netherlands**

- Zyxel Benelux
- <http://www.zyxel.nl>

## **Norway**

- Zyxel Communications
- <http://www.zyxel.no>

## **Poland**

- Zyxel Communications Poland
- <http://www.zyxel.pl>

## **Romania**

- Zyxel Romania
- <http://www.zyxel.com/ro/ro>

## **Russia**

- Zyxel Russia
- <http://www.zyxel.ru>

## **Slovakia**

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

## **Spain**

- Zyxel Communications ES Ltd
- <http://www.zyxel.es>

## **Sweden**

- Zyxel Communications
- <http://www.zyxel.se>

## **Switzerland**

- Studerus AG

- <http://www.zyxel.ch/>

### **Turkey**

- Zyxel Turkey A.S.
- <http://www.zyxel.com.tr>

### **UK**

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

### **Ukraine**

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

## **Latin America**

### **Argentina**

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

### **Brazil**

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

### **Ecuador**

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

## **Middle East**

### **Israel**

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

### **Middle East**

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>



## North America

### USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

## Oceania

### Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

## Africa

### South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

# APPENDIX B

## Wireless LANs

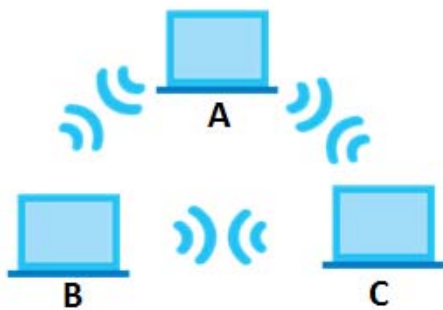
### Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

**Figure 161** Peer-to-Peer Communication in an Ad-hoc Network

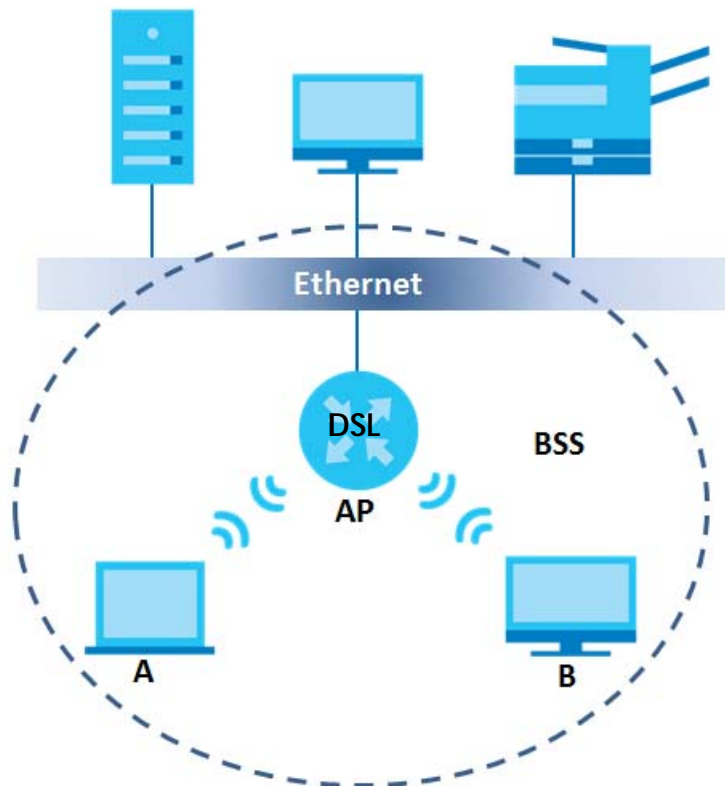


### BSS

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

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

Figure 162 Basic Service Set



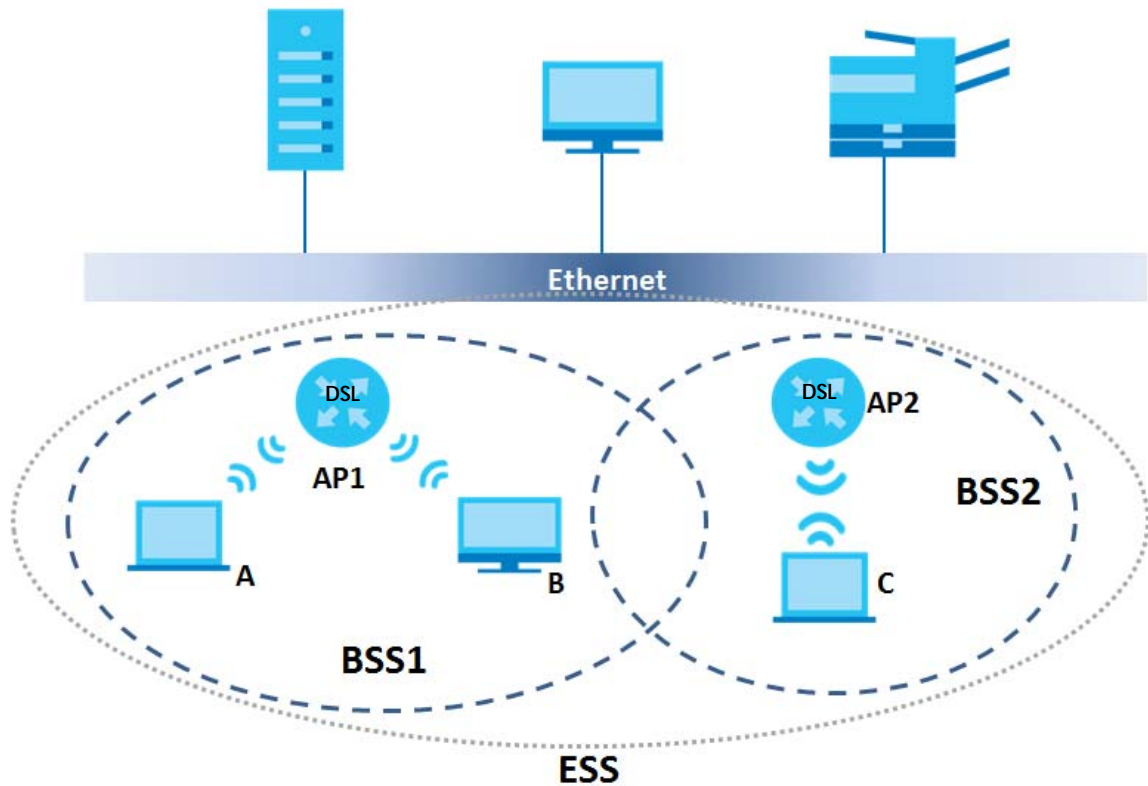
## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 163 Infrastructure WLAN



## Channel

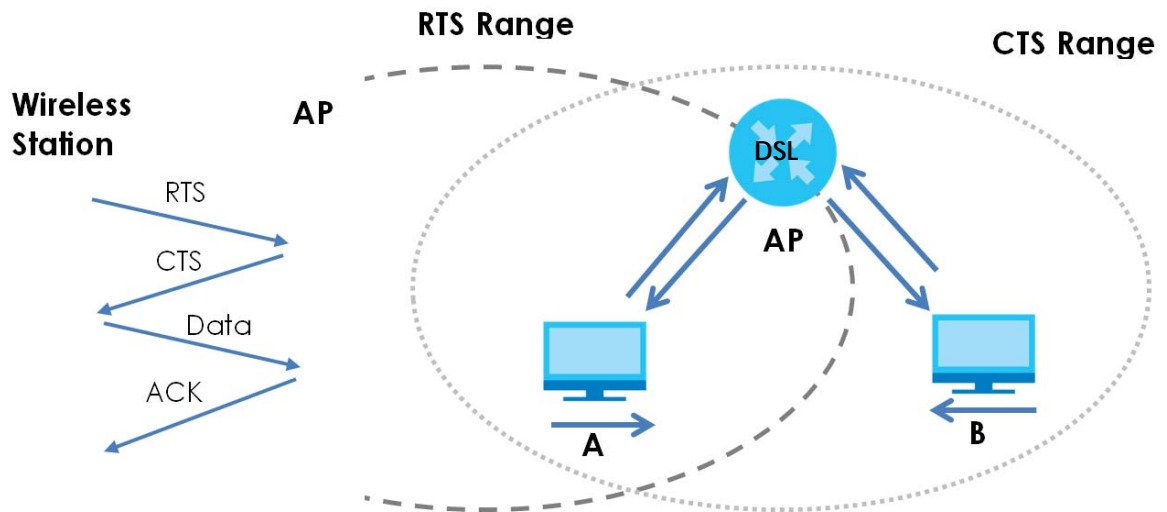
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 164 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 121 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

## Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the VMG are data encryption, wireless client authentication, restricting access by device MAC address and hiding the VMG identity.

The following figure shows the relative effectiveness of these wireless security methods available on your VMG.

Table 122 Wireless Security Levels

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

Note: You must enable the same wireless security settings on the VMG and on all wireless clients that you want to associate with it.

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication  
Determines the identity of the users.
- Authorization  
Determines the network services available to authenticated users once they are connected to the network.
- Accounting  
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

## Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request  
Sent by an access point requesting authentication.
- Access-Reject  
Sent by a RADIUS server rejecting access.
- Access-Accept  
Sent by a RADIUS server allowing access.
- Access-Challenge  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request  
Sent by the access point requesting accounting.
- Accounting-Response  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

## Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

## EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

## EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

## EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.



## PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

## LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

## Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 123 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

## WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point,

wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevents all wireless devices sharing the same encryption keys. (a weakness of WEP)

## User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

## Wireless Client WPA Supplicants

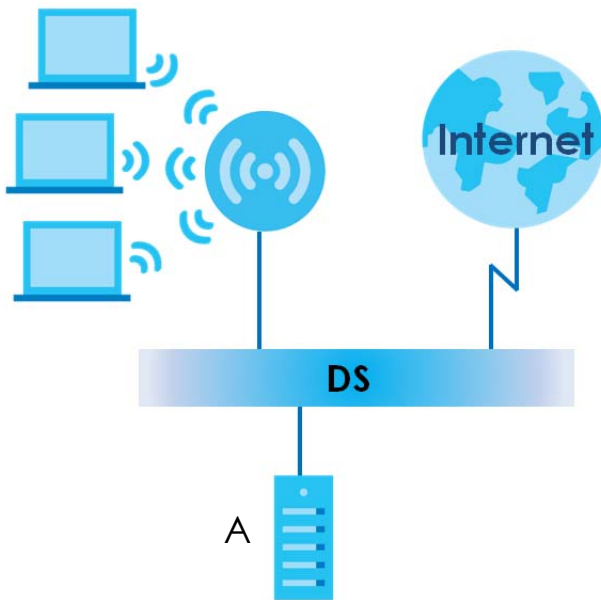
A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

## WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

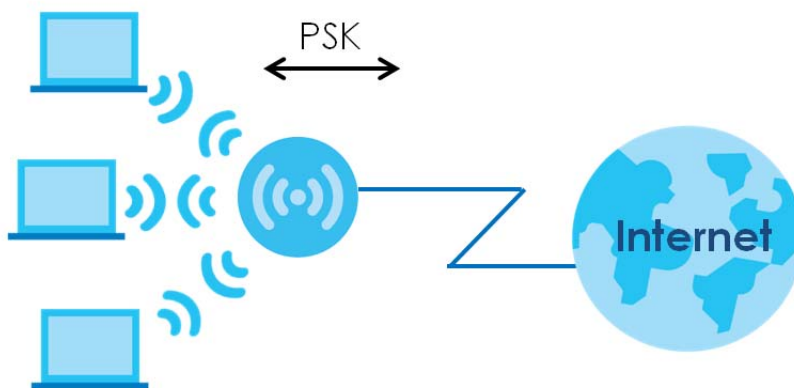
- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 165** WPA(2) with RADIUS Application Example

## WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
- 2 The AP checks each wireless client's password and allows it to join the network only if the password matches.
- 3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
- 4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

**Figure 166** WPA(2)-PSK Authentication

## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 124 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

## Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

## Antenna Characteristics

### Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

### Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

### Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately

5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

## Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

## Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

# APPENDIX C

## IPv6

### Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to  $3.4 \times 10^{38}$  IP addresses.

### IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

### Prefix and Prefix Length

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

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

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

### Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of `fe80::/10`. The link-local unicast address format is as follows.

Table 125 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

### Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

## Unspecified Address

An unspecified address (0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

## Loopback Address

A loopback address (0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

## Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 126 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 127 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0



Table 127 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

## Subnet Masking

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

## Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

## EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits ffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

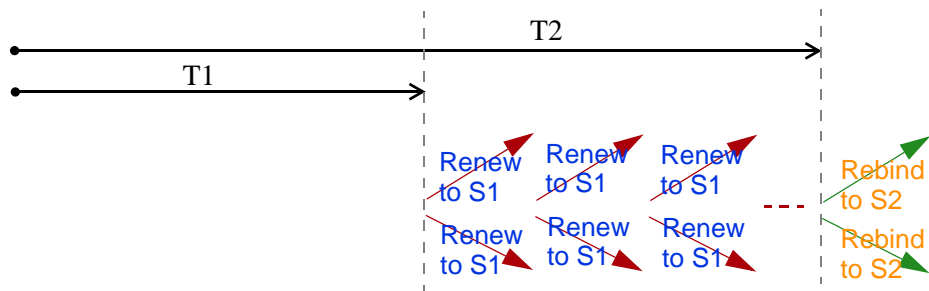
MAC	00 : 13 : 49 : 12 : 34 : 56
EUI-64	02 : 13 : 49 : FF : FE : 12 : 34 : 56

## Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server

does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



## DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

## Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The VMG uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the VMG passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

## ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

## Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.

- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

## IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The VMG maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the VMG configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the VMG also sends out a neighbor solicitation message. When the VMG receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the VMG uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The VMG creates an entry in the default router list cache if the router can be used as a default router.

When the VMG needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the VMG uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlinked, the address is considered as the next hop. Otherwise, the VMG determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the VMG looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the VMG cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

## Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

## MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

## Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 10.1.1.46
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::2d0:59ff:feb8:103c%4
    Default Gateway . . . . . : 10.1.1.254
```

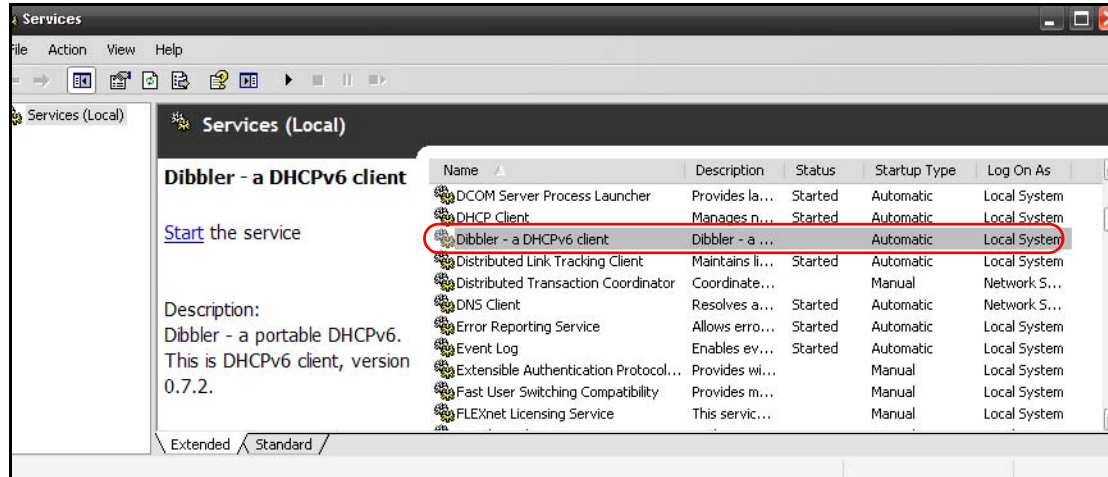
IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

## Example - Enabling DHCPv6 on Windows XP

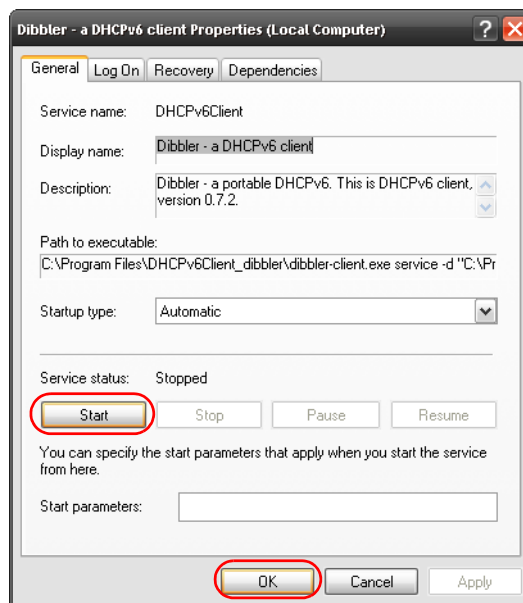
Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

- 1 Install Dibbler and select the DHCPv6 client option on your computer.
- 2 After the installation is complete, select **Start > All Programs > Dibbler-DHCPv6 > Client Install as service**.
- 3 Select **Start > Control Panel > Administrative Tools > Services**.
- 4 Double click **Dibbler - a DHCPv6 client**.



- 5 Click **Start** and then **OK**.



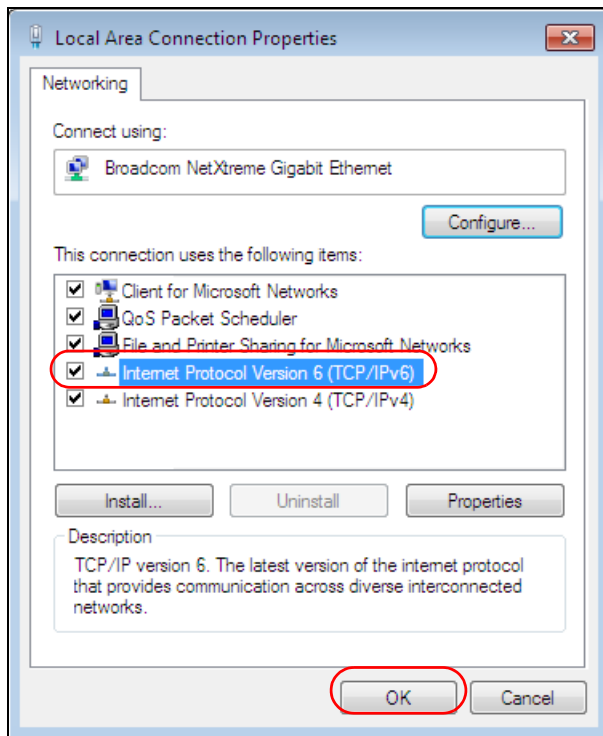
- 6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

## Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
  
```

# APPENDIX D

## Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 128 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.



Table 128 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

Table 128 Examples of Services (continued)

<b>NAME</b>	<b>PROTOCOL</b>	<b>PORT(S)</b>	<b>DESCRIPTION</b>
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user- defined	A videoconferencing solution. The UDP port number is specified in the application.

# APPENDIX E

## Legal Information

### Copyright

Copyright © 2017 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

### Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

### Regulatory Notice and Statement

#### UNITED STATES of AMERICA



The following information applies if you use the product within USA area.

#### FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
  - (1) This device may not cause harmful interference, and
  - (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

#### FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

#### CANADA

The following information applies if you use the product within Canada area.

#### Industry Canada ICES statement

CAN ICES-3 (B)/NMB-3(B)

#### Industry Canada RSS-GEN & RSS-247 statement

- This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

- This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- The worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio de modèle s'il fait partie du matériel de catégorie I a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- Les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élevation, et énoncée à la section 6.2.2 3) du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit, il est nécessaire de porter une attention particulière aux choses suivantes.

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

### Industry Canada radiation exposure statement

This device complies with IC radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

### Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

## EUROPEAN UNION



The following information applies if you use the product within the European Union.

### Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

- Compliance information for 2.4GHz and/or 5GHz wireless products relevant to the EU and other Countries following the EU Directive 1999/5/EC (R&TTE).
- This device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízenj je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EC.

English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 1999/5/EC.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/EC.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/EC.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteen tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 1999/5/EF.

### National Restrictions

- This product may be used in all EU countries (and other countries following the EU Directive 1999/5/EC) without any limitation except for the countries mentioned below:
- Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:
- Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttiva 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:
- Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der Richtlinie 1999/5/CE folgen) mit Ausnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2.4GHz and 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for both the 2.4GHz and 5GHz wireless LANs. The following countries have restrictions and/or requirements in addition to those given in the table labeled "Overview of Regulatory Requirements for Wireless LANs":

#### Belgium

- The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.
- Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.
- Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.

#### Denmark

- In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.
- I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

#### Italy

- This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check <http://www.sviluppoeconomico.gov.it/> for more details.

- Questo prodotto è conforme alle specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <http://www.sviluppoeconomico.gov.it/> per maggiori dettagli.

Latvia

- The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check <http://www.esd.lv> for more details.
- 2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <http://www.esd.lv>.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device.
  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

## Environment Statement

### ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless setting, please refer to "Wireless" chapter for more detail.)

### European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



Environmental Product Declaration

Български (Bulgarian)	Čeština (Czech)	Dansk (Danish)	Deutsch (German)
<p>Екологична продуктова декларация</p> <p>RoHS Директива 2011/65/EC WEEE Директива 2012/19/EC PPW Директива 94/62/EC REACH REGULATION (EC) n° 1907/2006 ECP Директива 2009/125/EC</p> <p>Име/ титла : Richard Hsu / Quality Management Division Senior Manager Подпис : Дата (dd/mm/yyyy): 01/10/2014</p>  	<p>Environmentální prohlášení o produktu</p> <p>RoHS Směrnice 2011/65/EU WEEE Směrnice 2012/19/EU PPW Směrnice 94/62/EC REACH Nařízení (ES) č. 1907/2006 ECP Směrnice 2009/125/ES</p> <p>Jméno/ titul : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy): 01/10/2014</p>  	<p>Miljøerklæring</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EC PPW Direktiv 94/62/EC REACH Forordning (EF) nr. 1907/2006 ECP Direktiv 2009/125/EF</p> <p>Navn/ titel : Richard Hsu / Quality Management Division Senior Manager Underskrift : Dato (dd/mm/åååå): 01/10/2014</p>  	<p>Produkt-Umweltdeklaration</p> <p>RoHS Richtlinie 2011/65/EU WEEE Richtlinie 2012/19/EC PPW Richtlinie 94/62/EG REACH VERORDNUNG (EG) Nr. 1907/2006 ECP Richtlinie 2009/125/EG</p> <p>Name/ titel : Richard Hsu / Quality Management Division Senior Manager Unterschrift : Datum (dd/mm/jj): 2014/10/01</p>  
<p>Tooete keskkonnadeklaratsiooni</p> <p>RoHS Direktiiv 2011/65/EU WEEE Direktiiv 2012/19/EC PPW Direktiiv 94/62/EÜ REACH Määrus (EÜ) nr. 1907/2006 ECP Direktiiv 2009/125/EÜ</p> <p>Nimi/ amet : Richard Hsu / Quality Management Division Senior Manager Allkiri : Kuupäev (pp/kk/aaaa): 01/10/2014</p>  	<p>Environmental product declaration</p> <p>RoHS Directive 2011/65/EU WEEE Directive 2012/19/EC PPW Directive 94/62/EC REACH Regulation (EC) No. 1907/2006 ECP Directive 2009/125/EC</p> <p>Name/ title : Richard Hsu / Quality Management Division Senior Manager Signature : Date (dd/mm/yyyy): 01/10/2014</p>  	<p>Declaraciones Ambientales de Producto</p> <p>RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH Reglamento (CE) n° 1907/2006 ECP Directiva 2009/125/CE</p> <p>Nombre/ título : Richard Hsu / Quality Management Division Senior Manager Firma : Fecha (aaaa/mm/dd): 2014/10/01</p>  	<p>Profil environnemental de produit</p> <p>RoHS Directive 2011/65/UE WEEE Directive 2012/19/UE PPW Directive 94/62/CE REACH REGLEMENTAS (EG) nr 1907/2006 ECP Directive 2009/125/CE</p> <p>Nom/ titre : Richard Hsu / Quality Management Division Senior Manager Signature : Date (aaaa/mm/jj): 2014/10/01</p>  
<p>Deklaraciju o zbrinjavanju proizvoda</p> <p>RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EC PPW Direktiva 94/62/EZ REACH Uredba (EZ) br. 1907/2006 ECP Direktiva 2009/125/EZ</p> <p>Ime/ naslov : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy): 01/10/2014</p>  	<p>Dichiarazione ambientale di prodotto</p> <p>RoHS Diretiva 2011/65/UE WEEE Diretiva 2012/19/UE PPW Diretiva 94/62/CE REACH REGULAMENTUL (CE) n. 1907/2006 ECP Diretiva 2009/125/CE</p> <p>Nume/ titlu : Richard Hsu / Quality Management Division Senior Manager Firma : Data (aaaa/mm/jj): 2014/10/01</p>  	<p>Produkta vides ietekmējuma deklarācija</p> <p>RoHS Direktīva 2011/65/ES WEEE Direktīva 2012/19/ES PPW Direktīva 94/62/EK REACH Regula (EK) Nr. 1907/2006 ECP Direktīva 2009/125/EK</p> <p>Nosaukums/ tituls : Richard Hsu / Quality Management Division Senior Manager Paraksts : Datums (dd/mm/yyyy): 01/10/2014</p>  	<p>Apinkosaušingų gaminių deklaraciją</p> <p>RoHS Direktyva 2011/65/ES WEEE Direktyva 2012/19/ES PPW Direktyva 94/62/EB REACH REGLAMENTAS (EB) nr 1907/2006 ECP Direktyva 2009/125/EB</p> <p>Vardas/ titulė : Richard Hsu / Quality Management Division Senior Manager Parašas : Data (dd/mm/yyyy): 01/10/2014</p>  
<p>Környezetvédelmi terméknyilatkozatot</p> <p>RoHS 2011/65/EU irányelve WEEE 2012/19/EU irányelve PPW 94/62/EK irányelve REACH 1907/2006/EK rendelet ECP 2009/125/EK irányelve</p> <p>Név/ cím : Richard Hsu / Quality Management Division Senior Manager Aláírás : Dátum (dd/mm/yyyy): 2014/10/01</p>  	<p>Dikjarazzjoni Ambientali dwar il-Prodott</p> <p>RoHS Diretiva 2011/65/UE WEEE Diretiva 2012/19/UE PPW Diretiva 94/62/CE REACH REGULAMENTUL (CE) Nr. 1907/2006 ECP Diretiva 2009/125/CE</p> <p>Isim/ titlu : Richard Hsu / Quality Management Division Senior Manager Firma : Data (aaaa/mm/jj): 2014/10/01</p>  	<p>Miljøproductverklaring</p> <p>RoHS Richtlin 2011/65/EU WEEE Richtlin 2012/19/EC PPW Richtlin 94/62/EG REACH Verordning (EG) nr. 1907/2006 ECP Richtlin 2009/125/EG</p> <p>Navn/ titel : Richard Hsu / Quality Management Division Senior Manager Handskrevet : Dato (dd/mm/år): 01/10/2014</p>  	<p>Deklaracja środowiskowa produktu</p> <p>RoHS Dyrektywa 2011/65/UE WEEE Dyrektywa 2012/19/UE PPW Dyrektywa 94/62/WE REACH Rozporządzenie (WE) nr 1907/2006 ECP Dyrektywa 2009/125/WE</p> <p>Nazwisko/ tytuł : Richard Hsu / Quality Management Division Senior Manager Podpis : Data (dd/mm/rrrr): 2014/10/01</p>  
<p>Declaração ambiental do produto</p> <p>RoHS Diretiva 2011/65/UE WEEE Diretiva 2012/19/UE PPW Diretiva 94/62/CE REACH Regulamento (CE) n° 1907/2006 ECP Diretiva 2009/125/CE</p> <p>Nome/ título : Richard Hsu / Quality Management Division Senior Manager Assinatura : Data (dd/mm/aaaa): 01/10/2014</p>  	<p>Declarație de mediu privind produsele</p> <p>RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH REGULAMENTUL (CE) Nr. 1907/2006 ECP Directiva 2009/125/CE</p> <p>Nume/ titlu : Richard Hsu / Quality Management Division Senior Manager Semnatura : Data (dd/mm/aaaa): 01/10/2014</p>  	<p>Vyhľadzenie o environmentálnom výrobku</p> <p>RoHS Smernica 2011/65/EU WEEE Smernica 2012/19/EC PPW Smernica 94/62/ES REACH Nařízení (ES) č. 1907/2006 ECP Smernica 2009/125/ES</p> <p>Menor/ titul : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy): 01/10/2014</p>  	<p>Okoljsko deklaracija izdelka</p> <p>RoHS Direktiva 2011/65/UE WEEE Direktiva 2012/19/UE PPW Direktiva 94/62/ES REACH Uredba (ES) č. 1907/2006 ECP Direktiva 2009/125/ES</p> <p>Ime/ naziv : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/jj): 01/10/2014</p>  
<p>Standardin perustava ympäristötuoteseloste</p> <p>RoHS Direktiiv 2011/65/EU WEEE Direktiiv 2012/19/EC PPW Direktiiv 94/62/EY REACH ASETUS (EY) N:o 1907/2006 ECP Direktiiv 2009/125/EY</p> <p>Nimi/ osasto : Richard Hsu / Quality Management Division Senior Manager Alaenkirja : Päivämäärä (pp/kk/vvvv): 01/10/2014</p>  	<p>Miljöproduktdeklaration</p> <p>RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EC PPW Direktiv 94/62/EG REACH Förordning (EG) nr 1907/2006 ECP Direktiv 2009/125/EG</p> <p>Navn/ titel : Richard Hsu / Quality Management Division Senior Manager Namnteckning : Datum (dd/mm/åååå): 01/10/2014</p>  	<p>Περιβαλλοντική δήλωση προϊόντος</p> <p>RoHS Οδηγία 2011/65/ΕΕ WEEE Οδηγία 2012/19/ΕΕ PPW Οδηγία 94/62/ΕΚ REACH Λειτουργία (ΕΚ) αριθ. 1907/2006 ECP Οδηγία 2009/125/ΕΚ</p> <p>Όνομα/ τμήμα : Richard Hsu / Quality Management Division Senior Manager Υπογραφή : Ημερομηνία (gg/mm/aaaa): 01/10/2014</p>  	<p>Miljødeklarasjon</p> <p>RoHS Direktiv 2011/65/UE WEEE Direktiv 2012/19/UE PPW Direktiv 94/62/EC REACH Forordning (EF) nr. 1907/2006 ECP Direktiv 2009/125/EF</p> <p>Navn/ tittel : Richard Hsu / Quality Management Division Senior Manager Signatur : Dato (dd/mm/åååå): 01/10/2014</p>  



## 台灣



以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中

以下訊息僅適用於產品操作於 5.25-5.35 兆赫頻帶內並銷售至台灣地區

- 在 5.25-5.35 兆赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。





安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不適合的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

## About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

### Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

### Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

### Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

#### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support_warranty_info.php](http://www.zyxel.com/web/support_warranty_info.php).

### Registration

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

### Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at [www.zyxel.com](http://www.zyxel.com). To obtain the source code covered under those Licenses, please contact [support@zyxel.com.tw](mailto:support@zyxel.com.tw) to get it.

**A**

ACL rule [197](#)

activation

- firewalls [194](#)
- media server [192](#)
- SIP ALG [172](#)
- SSID [102](#)

Address Resolution Protocol [222](#)

administrator password [26](#)

antenna

- directional [278](#)
- gain [277](#)
- omni-directional [278](#)

AP (access point) [268](#)

applications

- Internet access [16](#)
- media server [192](#)
  - activation [192](#)
  - iTunes server [192](#)

applications, NAT [176](#)

ARP Table [222](#), [224](#)

authentication [112](#), [113](#)

- RADIUS server [113](#)

**B**

backup

- configuration [248](#)

Basic Service Set, See BSS [266](#)

Basic Service Set, see BSS

blinking LEDs [20](#)

Broadband [70](#)

broadcast [94](#)

BSS [115](#), [266](#)

- example [115](#)

**C**

CA [209](#), [272](#)

Canonical Format Indicator See CFI

CCMs [251](#)

certificate

- factory default [210](#)

Certificate Authority

- See CA.

certificates [209](#)

- authentication [209](#)
- CA
  - creating [210](#)
  - public key [209](#)
  - replacing [210](#)
  - storage space [210](#)

Certification Authority [209](#)

Certification Authority, see CA

certifications [294](#)

- viewing [298](#)

CFI [94](#)

CFM [251](#)

- CCMs [251](#)
- link trace test [251](#)
- loopback test [251](#)
- MA [251](#)
- MD [251](#)
- MEP [251](#)
- MIP [251](#)

channel [268](#)

- interference [268](#)

channel, wireless LAN [111](#)

client list [129](#)

configuration

- backup [248](#)
- firewalls [194](#)
- reset [249](#)
- restoring [249](#)
- static route [139](#), [141](#), [180](#)

Connectivity Check Messages, see CCMs

contact information [260](#)

copyright [291](#)  
CoS [159](#)  
CoS technologies [146](#)  
creating certificates [210](#)  
CTS (Clear to Send) [269](#)  
CTS threshold [108, 112](#)  
customer support [260](#)

## D

data fragment threshold [108, 112](#)  
DDoS [194](#)  
default server address [171](#)  
Denials of Service, see DoS  
DHCP [124, 136](#)  
Differentiated Services, see DiffServ [159](#)  
DiffServ [159](#)  
    marking rule [159](#)  
digital IDs [209](#)  
disclaimer [291](#)  
DLNA [192](#)  
DMZ [171](#)  
DNS [124, 136](#)  
DNS server address assignment [95](#)  
Domain Name [177](#)  
Domain Name System, see DNS  
Domain Name System. See DNS.  
DoS [194](#)  
DS field [159](#)  
DS, see differentiated services  
DSCP [159](#)  
dynamic DNS [179](#)  
    wildcard [179](#)  
Dynamic Host Configuration Protocol, see DHCP  
dynamic WEP key exchange [273](#)  
DYNDNS wildcard [179](#)

## E

EAP Authentication [272](#)  
ECHO [177](#)

e-mail  
    log example [244](#)  
Encapsulation [91](#)  
    MER [91](#)  
    PPP over Ethernet [91](#)  
encapsulation  
    RFC 1483 [92](#)  
encryption [114, 274](#)  
ESS [267](#)  
Extended Service Set IDentification [98, 103](#)  
Extended Service Set, See ESS [267](#)

## F

file sharing [18](#)  
filters  
    MAC address [113](#)  
Finger [177](#)  
firewalls [193](#)  
    add protocols [195](#)  
    configuration [194](#)  
    DDoS [194](#)  
    DoS [194](#)  
    LAND attack [194](#)  
    Ping of Death [194](#)  
    SYN attack [194](#)  
firmware [246](#)  
    version [68](#)  
forwarding ports [164](#)  
fragmentation threshold [108, 112, 269](#)  
FTP [164, 177](#)

## G

General wireless LAN screen [97](#)

## H

hidden node [268](#)  
HTTP [177](#)

**I**

IBSS [266](#)  
 IEEE 802.11g [270](#)  
 IEEE 802.1Q [94](#)  
 IGA [175](#)  
 IGMP [95](#)  
     version [95](#)  
 ILA [175](#)  
 Independent Basic Service Set  
     See IBSS [266](#)  
 initialization vector (IV) [274](#)  
 Inside Global Address, see IGA  
 Inside Local Address, see ILA  
 interface group [183](#)  
 Internet  
     wizard setup [33](#)  
 Internet access [16](#)  
     wizard setup [33](#)  
 Internet Protocol version 6 [71](#)  
 Internet Protocol version 6, see IPv6  
 IP address [124, 137](#)  
     ping [252](#)  
     private [137](#)  
     WAN [71](#)  
 IP Address Assignment [94](#)  
 IP alias  
     NAT applications [177](#)  
 IPv6 [71, 279](#)  
     addressing [72, 95, 279](#)  
     EUI-64 [281](#)  
     global address [279](#)  
     interface ID [281](#)  
     link-local address [279](#)  
     Neighbor Discovery Protocol [279](#)  
     ping [279](#)  
     prefix [72, 95, 279](#)  
     prefix delegation [74](#)  
     prefix length [72, 95, 279](#)  
     unspecified address [280](#)  
 iTunes server [192](#)

**L**

LAN [123](#)

    client list [129](#)  
     DHCP [124, 136](#)  
     DNS [124, 136](#)  
     IP address [124, 125, 137](#)  
     MAC address [129](#)  
     status [68](#)  
     subnet mask [124, 125, 137](#)  
 LAND attack [194](#)  
 LBR [251](#)  
 limitations  
     wireless LAN [114](#)  
     WPS [121](#)  
 link trace [251](#)  
 Link Trace Message, see LTM  
 Link Trace Response, see LTR  
 login [26](#)  
     passwords [26](#)  
 logs [216, 219, 228, 243](#)  
 Loop Back Response, see LBR  
 loopback [251](#)  
 LTM [251](#)  
 LTR [251](#)

**M**

MA [251](#)  
 MAC address [129](#)  
     filter [113](#)  
 Mac filter [200](#)  
 Maintenance Association, see MA  
 Maintenance Domain, see MD  
 Maintenance End Point, see MEP  
 Management Information Base (MIB) [237](#)  
 managing the device  
     good habits [15](#)  
 Maximum Burst Size (MBS) [92](#)  
 MBSSID [115](#)  
 MD [251](#)  
 media server [192](#)  
     activation [192](#)  
     iTunes server [192](#)  
 MEP [251](#)  
 MTU (Multi-Tenant Unit) [94](#)  
 multicast [94](#)

Multiple BSS, see MBSSID  
multiplexing [92](#)  
    LLC-based [92](#)  
    VC-based [92](#)  
multiprotocol encapsulation [92](#)

## N

NAT [163](#), [164](#), [165](#), [175](#), [176](#)  
    applications [176](#)  
        IP alias [177](#)  
    example [176](#)  
    global [175](#)  
    IGA [175](#)  
    ILA [175](#)  
    inside [175](#)  
    local [175](#)  
    outside [175](#)  
    port forwarding [164](#)  
    port number [177](#)  
    services [177](#)  
    SIP ALG [172](#)  
        activation [172](#)  
NAT example [178](#)  
Network Address Translation, see NAT  
Network Map [66](#)  
network map [29](#)  
NNTP [177](#)

## P

Pairwise Master Key (PMK) [274](#), [276](#)  
passwords [26](#)  
PBC [116](#)  
Peak Cell Rate (PCR) [92](#)  
Per-Hop Behavior, see PHB [159](#)  
PHB [159](#)  
PIN, WPS [117](#)  
Ping of Death [194](#)  
Point-to-Point Tunneling Protocol, see PPTP  
POP3 [177](#)  
port forwarding [164](#)  
ports [20](#)

PPPoE [91](#)  
    Benefits [91](#)  
PPTP [177](#)  
preamble [109](#), [112](#)  
preamble mode [116](#)  
prefix delegation [74](#)  
private IP address [137](#)  
PSK [274](#)  
push button [23](#)  
Push Button Configuration, see PBC  
push button, WPS [116](#)

## Q

QoS [145](#), [159](#)  
    marking [146](#)  
    setup [145](#)  
    tagging [146](#)  
    versus CoS [146](#)  
Quality of Service, see QoS

## R

RADIUS [271](#)  
    message types [271](#)  
    messages [271](#)  
    shared secret key [272](#)  
RADIUS server [113](#)  
reset [24](#), [249](#)  
restart [250](#)  
restoring configuration [249](#)  
RFC 1058. See RIP.  
RFC 1389. See RIP.  
RFC 1483 [92](#)  
RFC 3164 [216](#)  
RIP [143](#)  
router features [16](#)  
Routing Information Protocol. See RIP  
RTS (Request To Send) [269](#)  
    threshold [268](#), [269](#)  
RTS threshold [108](#), [112](#)

**S**

security  
 wireless LAN [112](#)

Security Log [217](#)

Security Parameter Index, see SPI

service access control [234, 235](#)

Service Set [98, 103](#)

Services [177](#)

setup  
 firewalls [194](#)  
 static route [139, 141, 180](#)

Simple Network Management Protocol, see SNMP

Single Rate Three Color Marker, see srTCM

SIP ALG [172](#)  
 activation [172](#)

SMTP [177](#)

SNMP [177, 237, 238](#)  
 agents [237](#)  
 Get [238](#)  
 GetNext [238](#)  
 Manager [237](#)  
 managers [237](#)  
 MIB [237](#)  
 network components [237](#)  
 Set [238](#)  
 Trap [238](#)  
 versions [237](#)

SNMP trap [177](#)

SPI [194](#)

srTCM [161](#)

SSID [113](#)  
 activation [102](#)  
 MBSSID [115](#)

static route [138, 143, 241](#)  
 configuration [139, 141, 180](#)  
 example [138](#)

static VLAN

status [66](#)  
 firmware version [68](#)  
 LAN [68](#)  
 WAN [68](#)  
 wireless LAN [68](#)

status indicators [20](#)

subnet mask [124, 137](#)

Sustained Cell Rate (SCR) [92](#)

SYN attack [194](#)

syslog  
 protocol [216](#)  
 severity levels [216](#)

system  
 firmware [246](#)  
 version [68](#)  
 passwords [26](#)  
 reset [24](#)  
 status [66](#)  
 LAN [68](#)  
 WAN [68](#)  
 wireless LAN [68](#)  
 time [239](#)

**T**

Tag Control Information See TCI

Tag Protocol Identifier See TPID

TCI

The [71](#)

thresholds  
 data fragment [108, 112](#)  
 RTS/CTS [108, 112](#)

time [239](#)

TPID [94](#)

traffic shaping [92](#)

trTCM [161](#)

Two Rate Three Color Marker, see trTCM

**U**

unicast [94](#)

Universal Plug and Play, see UPnP

upgrading firmware [246](#)

UPnP [130](#)  
 cautions [125](#)  
 NAT traversal [124](#)

USB features [18](#)

**V**

Vendor ID [134](#)  
 VID  
 Virtual Circuit (VC) [92](#)  
 Virtual Local Area Network See VLAN  
 VLAN [94](#)  
   Introduction [94](#)  
   number of possible VIDs  
   priority frame  
   static  
 VLAN ID [94](#)  
 VLAN Identifier See VID  
 VLAN tag [94](#)

**W**

Wake on LAN [134](#)  
 WAN  
   status [68](#)  
   Wide Area Network, see WAN [70](#)  
 warranty [298](#)  
   note [298](#)  
 web configurator [26](#)  
   login [26](#)  
   passwords [26](#)  
 WEP [114](#)  
 WEP Encryption [100, 101](#)  
 WEP encryption [99](#)  
 WEP key [99](#)  
 Wi-Fi Protected Access [273](#)  
 wireless client WPA supplicants [275](#)  
 wireless LAN [96, 110](#)  
   authentication [112, 113](#)  
   BSS [115](#)  
     example [115](#)  
   channel [111](#)  
   encryption [114](#)  
   example [111](#)  
   fragmentation threshold [108, 112](#)  
   limitations [114](#)  
   MAC address filter [113](#)  
   MBSSID [115](#)  
   preamble [109, 112](#)  
   RADIUS server [113](#)

  RTS/CTS threshold [108, 112](#)  
   security [112](#)  
   SSID [113](#)  
     activation [102](#)  
   status [68](#)  
   WEP [114](#)  
   WPA [114](#)  
   WPA-PSK [114](#)  
   WPS [116, 118](#)  
     example [119](#)  
     limitations [121](#)  
     PIN [117](#)  
     push button [23, 116](#)  
 wireless security [270](#)  
 Wireless tutorial [41](#)  
 wizard setup  
   Internet [33](#)  
 WLAN  
   interference [268](#)  
   security parameters [277](#)  
 WPA [114, 273](#)  
   key caching [275](#)  
   pre-authentication [275](#)  
   user authentication [274](#)  
   vs WPA-PSK [274](#)  
   wireless client supplicant [275](#)  
   with RADIUS application example [275](#)  
 WPA2 [273](#)  
   user authentication [274](#)  
   vs WPA2-PSK [274](#)  
   wireless client supplicant [275](#)  
   with RADIUS application example [275](#)  
 WPA2-Pre-Shared Key [273](#)  
 WPA2-PSK [273, 274](#)  
   application example [276](#)  
 WPA-PSK [114, 274](#)  
   application example [276](#)  
 WPS [116, 118](#)  
   example [119](#)  
   limitations [121](#)  
   PIN [117](#)  
   push button [23, 116](#)

**Z**

ZyXEL Family Safety page [205](#)