

User's Guide

VMG4927-B50A /

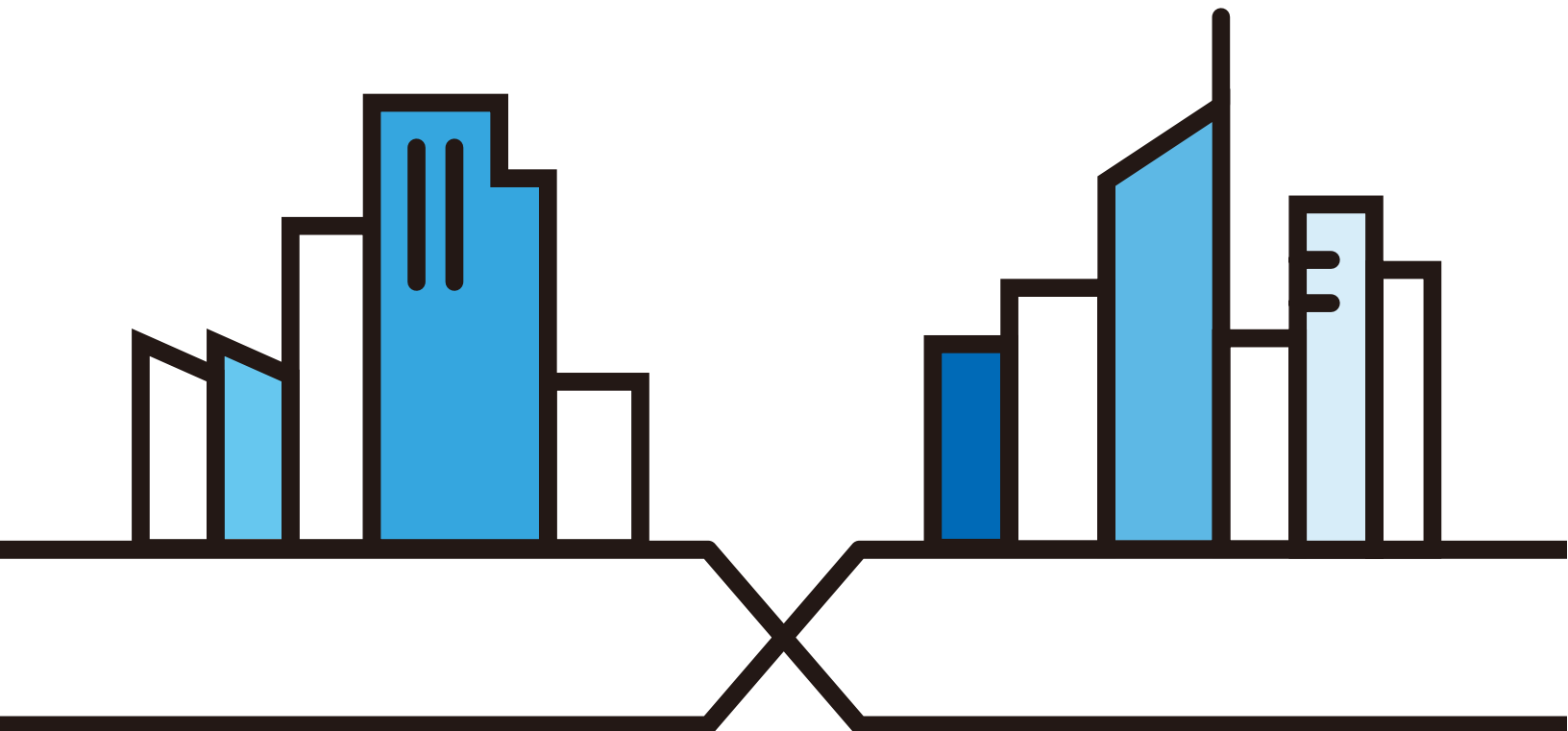
VMG9827-B50A/

VMG3927-B50B

Default Login Details

Version 5.13 Edition 1, 06/2019

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



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the VMG and access the Web Configurator.

- More Information

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



Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your device.











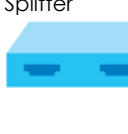

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The VMG4927-B50A / VMG9827-B50A / VMG3927-B50B may be referred to as the “VMG” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Network Setting > Broadband > Advanced** means you first click **Network Setting** in the navigation panel, then the **Broadband** sub menu and finally the **Advanced** tab to get to that screen.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The VMG icon is not an exact representation of your device.

VMG 	Generic Router 	Wireless Router / Access Point 
Switch 	Firewall 	USB Storage Device 
Server 	Cell Tower 	Printer 
Telephone Jack 	Splitter 	Telephone 

Contents Overview

User's Guide	15
VMG Introduction	16
The Web Configurator	32
Quick Start	39
Tutorials	42
Technical Reference	65
Network Map and Status Screens	66
Broadband	71
Wireless	93
Home Networking	116
Routing	133
Quality of Service (QoS)	140
Network Address Translation (NAT)	159
Dynamic DNS Setup	176
IGMP/MLD	180
VLAN Group	183
Interface Grouping	185
Firewall	190
MAC Filter	198
Parental Control	200
Scheduler Rule	204
Certificates	206
Voice	213
Log	240
Traffic Status	243
ARP Table	247
Routing Table	249
Multicast Status	251
xDSL Statistics	253
System	256
User Account	257
Remote Management	260
SNMP	263
Time Settings	265
Email Notification	268
Log Setting	270
Firmware Upgrade	273

Backup/Restore	275
Diagnostic	278
Troubleshooting	285
Appendices	292

Table of Contents

Document Conventions	3
Contents Overview	4
Table of Contents	6
Part I: User's Guide.....	15
Chapter 1	
VMG Introduction	16
1.1 Overview	16
1.1.1 Internet Access	16
1.1.2 Wireless Access	20
1.1.3 VoIP Features	20
1.2 Ways to Manage the VMG	21
1.3 Good Habits for Managing the VMG	21
1.4 Hardware	21
1.4.1 Front Panels	21
1.4.2 WPS Button	24
1.4.3 LEDs (Lights)	25
1.4.4 Rear Panel	28
1.4.5 RESET Button	29
1.4.6 Wall Mounting	29
Chapter 2	
The Web Configurator.....	32
2.1 Overview	32
2.1.1 Access the Web Configurator	32
2.2 Web Configurator Layout	34
2.2.1 Title Bar	34
2.2.2 Navigation Panel	35
Chapter 3	
Quick Start.....	39
3.1 Overview	39
3.2 Quick Start Setup	39
Chapter 4	
Tutorials	42

4.1 Overview	42
4.2 Set Up an ADSL PPPoE Connection	42
4.3 Set Up a Secure WiFi Network	45
4.3.1 Configure the WiFi Network Settings	45
4.3.2 Use WPS	47
4.3.3 Connect to the VMG's WiFi Network Manually (No WPS)	49
4.3.4 Configure Wireless Security on the VMG	49
4.3.5 Configure Your Laptop	51
4.4 Set Up Multiple Wireless Groups	53
4.5 Configure Static Route for Routing to Another Network	56
4.6 Configure QoS Queue and Class Setup	58
4.7 Access the VMG Using DDNS	62
4.7.1 Register a DDNS Account on www.dyndns.org	62
4.7.2 Configure DDNS on Your VMG	63
4.7.3 Test the DDNS Setting	63
4.8 Configure the MAC Address Filter	63

Part II: Technical Reference..... 65

Chapter 5 Network Map and Status Screens66

5.1 Overview	66
5.2 Network Map	66
5.3 Status	68

Chapter 6 Broadband.....71

6.1 Overview	71
6.1.1 What You Can Do in this Chapter	71
6.1.2 What You Need to Know	72
6.1.3 Before You Begin	74
6.2 Broadband	75
6.2.1 Add/Edit Internet Connection	76
6.3 Advanced Settings	84
6.4 Ethernet WAN	87
6.5 Technical Reference	87

Chapter 7 Wireless93

7.1 Overview	93
7.1.1 What You Can Do in this Chapter	93

7.1.2 What You Need to Know	93
7.2 WiFi	94
7.2.1 WiFi Edit	94
7.3 Guest WiFi	96
7.3.1 Edit Guest WiFi	97
7.4 WPS	98
7.5 Advanced Settings	98
7.6 Channel Status	101
7.7 MESH	103
7.8 Technical Reference	105
7.8.1 Wireless Network Overview	105
7.8.2 Additional Wireless Terms	107
7.8.3 Wireless Security Overview	107
7.8.4 Signal Problems	109
7.8.5 BSS	109
7.8.6 MBSSID	110
7.8.7 Preamble Type	110
7.8.8 WiFi Protected Setup (WPS)	110
Chapter 8	
Home Networking.....	116
8.1 Overview	116
8.1.1 What You Can Do in this Chapter	116
8.1.2 What You Need To Know	117
8.1.3 Before You Begin	118
8.2 LAN Setup	118
8.3 Static DHCP	122
8.4 UPnP	123
8.4.1 Turn On UPnP in Windows 7 Example	125
8.5 Additional Subnet	126
8.6 STB Vendor ID	128
8.7 Wake on LAN	128
8.8 TFTP Server Name	129
8.9 Technical Reference	130
8.9.1 LANs, WANs and the VMG	130
8.9.2 DHCP Setup	130
8.9.3 DNS Server Addresses	130
8.9.4 LAN TCP/IP	131
Chapter 9	
Routing.....	133
9.1 Overview	133
9.2 Routing	133

9.2.1 Add/Edit Static Route	134
9.3 DNS Route	135
9.3.1 DNS Route Add	136
9.4 Policy Route	137
9.4.1 Add/Edit Policy Route	138
9.5 RIP Overview	139
9.5.1 RIP	139
Chapter 10	
Quality of Service (QoS).....	140
10.1 Overview	140
10.1.1 What You Can Do in this Chapter	140
10.2 What You Need to Know	141
10.3 Quality of Service General Settings	142
10.4 Queue Setup	143
10.4.1 Adding a QoS Queue	145
10.5 Classification Setup	145
10.5.1 Add/Edit QoS Class	146
10.6 QoS Shaper Setup	150
10.6.1 Add/Edit a QoS Shaper	151
10.7 QoS Policer Setup	151
10.7.1 Add/Edit a QoS Policer	152
10.8 QoS Monitor	153
10.9 Technical Reference	154
Chapter 11	
Network Address Translation (NAT).....	159
11.1 Overview	159
11.1.1 What You Can Do in this Chapter	159
11.1.2 What You Need To Know	159
11.2 Port Forwarding	160
11.2.1 Add/Edit Port Forwarding	162
11.3 Applications Settings	163
11.3.1 Add New Application	164
11.4 Port Triggering	165
11.4.1 Add/Edit Port Triggering Rule	166
11.5 DMZ	167
11.6 ALG	168
11.7 Address Mapping	169
11.7.1 Add/Edit Address Mapping Rule	170
11.8 Sessions	171
11.9 Technical Reference	171
11.9.1 NAT Definitions	172

11.9.2 What NAT Does	172
11.9.3 How NAT Works	173
11.9.4 NAT Application	173
Chapter 12	
Dynamic DNS Setup.....	176
12.1 Overview	176
12.1.1 What You Can Do in this Chapter	176
12.1.2 What You Need To Know	176
12.2 DNS Entry	177
12.2.1 Add/Edit DNS Entry	177
12.3 Dynamic DNS	178
Chapter 13	
IGMP/MLD.....	180
13.1 Overview	180
13.1.1 What You Need To Know	180
13.2 IGMP/MLD	180
Chapter 14	
VLAN Group.....	183
14.1 Overview	183
14.1.1 What You Can Do in this Chapter	183
14.2 VLAN Group	183
14.2.1 Add/Edit a VLAN Group	184
Chapter 15	
Interface Grouping.....	185
15.1 Overview	185
15.1.1 What You Can Do in this Chapter	185
15.2 Interface Grouping Overview	185
15.2.1 Interface Grouping Configuration	186
15.2.2 Interface Grouping Criteria	188
Chapter 16	
Firewall.....	190
16.1 Overview	190
16.1.1 What You Can Do in this Chapter	190
16.1.2 What You Need to Know	191
16.2 Firewall	191
16.3 Protocol	192
16.3.1 Add/Edit a Service	193
16.4 Access Control	194

16.4.1 Add/Edit an ACL Rule	195
16.5 DoS	196
Chapter 17	
MAC Filter	198
17.1 Overview	198
17.2 MAC Filter	198
Chapter 18	
Parental Control	200
18.1 Overview	200
18.2 Parental Control	200
18.2.1 Add/Edit a Parental Control Profile	201
Chapter 19	
Scheduler Rule	204
19.1 Overview	204
19.2 Scheduler Rule	204
19.2.1 Add/Edit a Schedule	204
Chapter 20	
Certificates	206
20.1 Overview	206
20.1.1 What You Can Do in this Chapter	206
20.2 What You Need to Know	206
20.3 Local Certificates	206
20.3.1 Create Certificate Request	207
20.3.2 View Certificate Request	208
20.4 Trusted CA	209
20.4.1 View Trusted CA Certificate	210
20.4.2 Import Trusted CA Certificate	211
Chapter 21	
Voice	213
21.1 Overview	213
21.1.1 What You Can Do in this Chapter	213
21.1.2 What You Need to Know About VoIP	213
21.2 Before You Begin	214
21.3 SIP Account	214
21.3.1 SIP Account Add/Edit	215
21.4 SIP Service Provider	219
21.4.1 SIP Service Provider Add/Edit	220
21.5 Phone Device	224

21.5.1 Phone Device Edit	225
21.6 Region	226
21.7 Call Rule	226
21.8 Technical Reference	227
21.8.1 Quality of Service (QoS)	235
21.8.2 Phone Services Overview	235
Chapter 22	
Log	240
22.1 Overview	240
22.1.1 What You Can Do in this Chapter	240
22.1.2 What You Need To Know	240
22.2 System Log	241
22.3 Security Log	242
Chapter 23	
Traffic Status	243
23.1 Overview	243
23.1.1 What You Can Do in this Chapter	243
23.2 WAN Status	243
23.3 LAN Status	244
23.4 NAT Status	245
Chapter 24	
ARP Table	247
24.1 Overview	247
24.1.1 How ARP Works	247
24.2 ARP Table	248
Chapter 25	
Routing Table	249
25.1 Overview	249
25.2 Routing Table	249
Chapter 26	
Multicast Status	251
26.1 Overview	251
26.2 IGMP Status	251
26.3 MLD Status	251
Chapter 27	
xDSL Statistics	253
27.1 xDSL Statistics	253

Chapter 28	
System	256
28.1 Overview	256
28.2 System	256
Chapter 29	
User Account	257
29.1 Overview	257
29.2 User Account	257
29.2.1 User Account Add/Edit	258
Chapter 30	
Remote Management	260
30.1 Overview	260
30.2 MGMT Services	260
30.3 Trust Domain	261
30.3.1 Add Trust Domain	262
Chapter 31	
SNMP	263
31.1 Overview	263
31.2 SNMP	263
Chapter 32	
Time Settings	265
32.1 Overview	265
32.2 Time	265
Chapter 33	
Email Notification	268
33.1 Overview	268
33.2 Email Notification	268
33.2.1 Email Notification Edit	269
Chapter 34	
Log Setting	270
34.1 Overview	270
34.2 Log Settings	270
34.2.1 Example Email Log	271
Chapter 35	
Firmware Upgrade	273
35.1 Overview	273

35.2 Firmware	273
Chapter 36	
Backup/Restore	275
36.1 Overview	275
36.2 Backup/Restore	275
36.3 Reboot	277
Chapter 37	
Diagnostic.....	278
37.1 Overview	278
37.1.1 What You Can Do in this Chapter	278
37.2 What You Need to Know	278
37.3 Ping & TraceRoute & Nslookup	279
37.4 802.1ag	279
37.5 802.3ah	281
37.6 OAM Ping	282
Chapter 38	
Troubleshooting.....	285
38.1 Power, Hardware Connections, and LEDs	285
38.2 VMG Access and Login	286
38.3 Internet Access	287
38.4 Wireless Internet Access	289
38.5 UPnP	290
38.6 VoIP Call Quality	290
Part III: Appendices	292
Appendix A Customer Support	293
Appendix B Wireless LANs.....	299
Appendix C IPv6.....	309
Appendix D Services.....	317
Appendix E Legal Information	321
Index	331

PART I

User's Guide

CHAPTER 1

VMG Introduction

1.1 Overview

VMG refers to these models as outlined below.

- VMG4927-B50A
- VMG9827-B50A
- VMG3927-B50B

The following table describes the feature difference of the VMG by model.

Table 1 VMG Comparison Table

	VMG4927-B50A	VMG9827-B50A	VMG3927-B50B
DSL Bonding (see Section 1.1.1.1 on page 17 for details)	✓	✓	
MESH (see Section 7.7 on page 100 for details)	✓	✓	
VoIP (see Chapter 21 on page 210 for details)		✓	
DFS Channel (see Table 22 on page 96 for details)	✓		

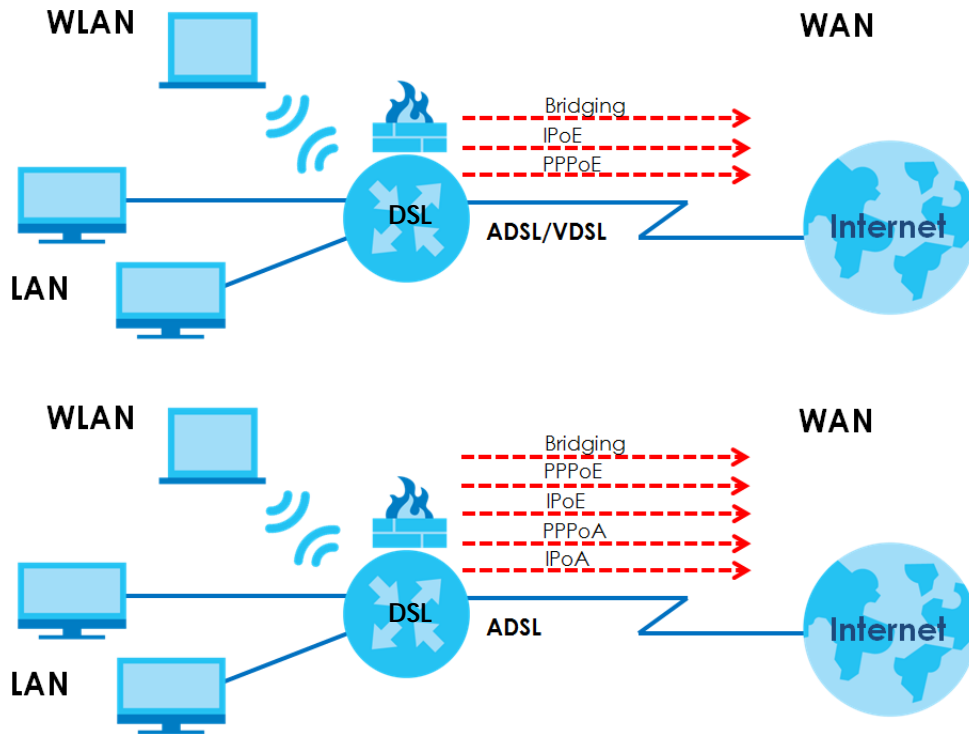
1.1.1 Internet Access

Your VMG has a DSL port and a Gigabit Ethernet port for super-fast Internet access. It 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 75](#) for the **Network Setting > Broadband** screen.

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

Figure 1 VMG's Internet Access Application



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.

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

1.1.1.1 DSL Bonding

DSL bonding allows the VMG to aggregate two DSL lines into a virtual connection. The VMG will have higher bandwidth and faster transmission speed at longer distances. Note that the two DSL lines must come from the same ISP, and they both need to support DSL bonding. Also, only DSL 1 supports telephone service.

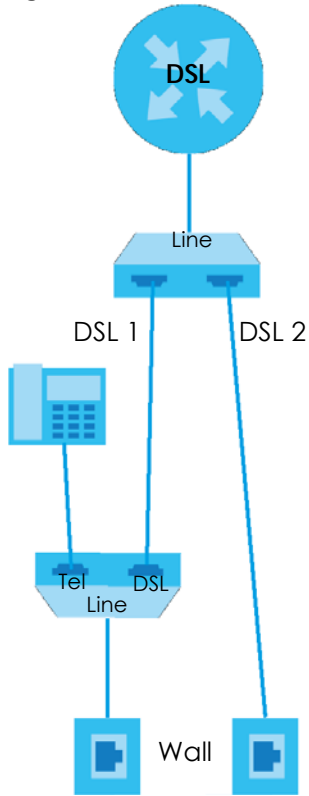
To enable the bonding feature, go to the **Network Setting > Broadband > Advanced** screen.

To set up your network for DSL bonding:

Example 1

- 1 Connect a two-line splitter to the VMG (DSL in the figure).
- 2 Connect two DSL lines to the two-line splitter.
- 3 Connect the two DSL lines to two separate telephone jacks (Wall).

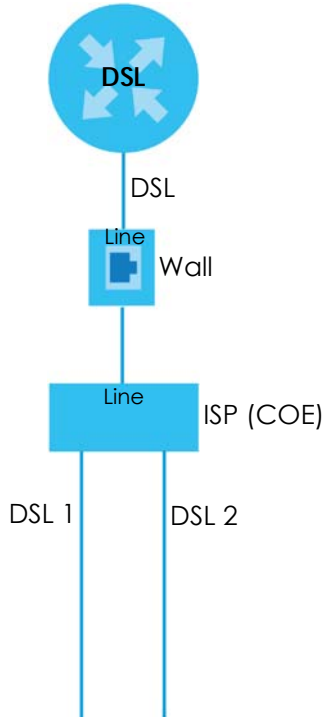
Figure 2 VMG's Internet Access Application: DSL Bonding (Example 1)



Example 2

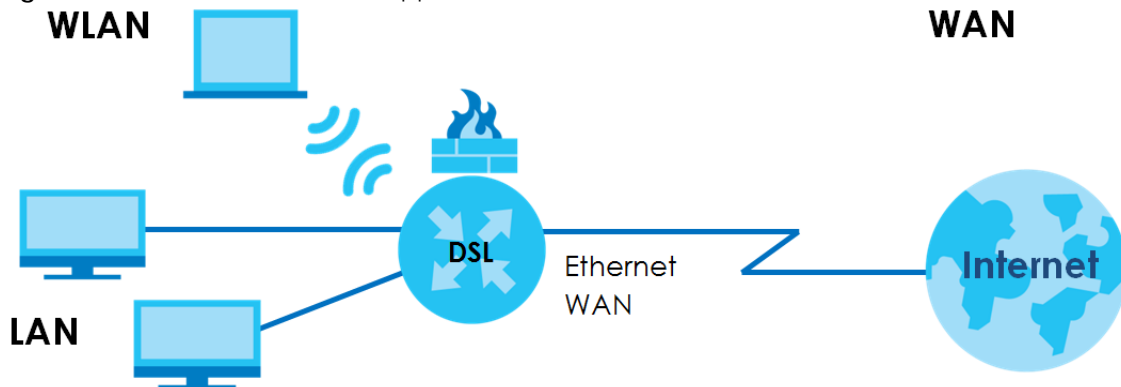
Connect the DSL port on the VMG (**DSL** in the figure) to a telephone jack.

The ISP will split the DSL connection at their end for DSL 1 and DSL 2 bonding.

Figure 3 VMG's Internet Access Application: DSL Bonding (Example 2)

1.1.1.2 Ethernet WAN

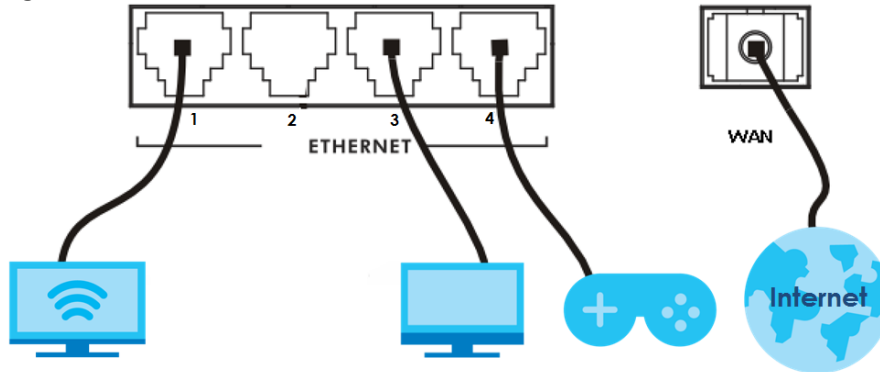
If you prefer not to use a DSL line and you have another broadband modem or router (such as ADSL) available, you can convert LAN port number five as a WAN port using the **Network Setting > Broadband > Ethernet WAN** screen and then connect the LAN port to the broadband modem or router. This way, you can access the Internet via an Ethernet connection and still use the QoS, Firewall and parental control functions on the VMG.

Figure 4 VMG's Internet Access Application: Ethernet WAN

1.1.1.3 Triple Play

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

Figure 5 Triple Play Example



1.1.2 Wireless Access

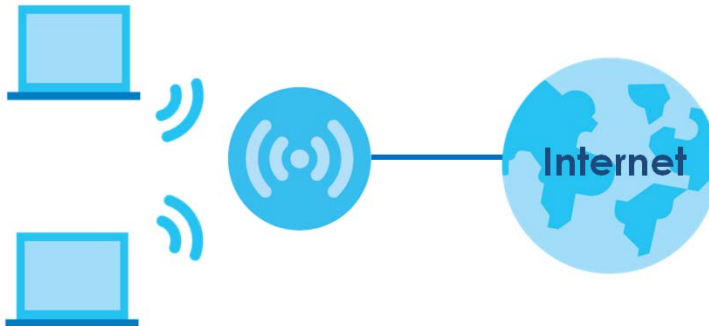
The VMG is a wireless Access Point (AP) for IEEE 802.11b/g/n/a/ac WiFi clients, such as notebook computers, iPads, smartphones, and so on. These devices can connect to the VMG to access network resources and the Internet.

Your VMG supports WiFi Protected Setup (WPS), which allows you to quickly set up a WiFi network with strong security.

You can configure your WiFi network using the built-in Web Configurator.

See [Section 4.3 on page 45](#) for more information about how to set up a WiFi network.

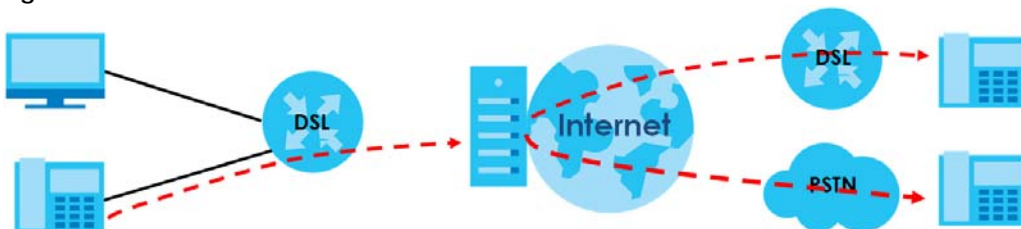
Figure 6 Wireless Access Example



1.1.3 VoIP Features

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

Figure 7 VMG's VoIP Features



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

1.2 Ways to Manage the VMG

Use any of the following methods to manage the VMG.

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

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.

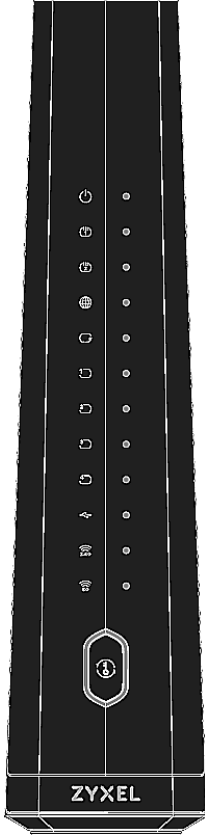
- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration 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 Hardware

1.4.1 Front Panels

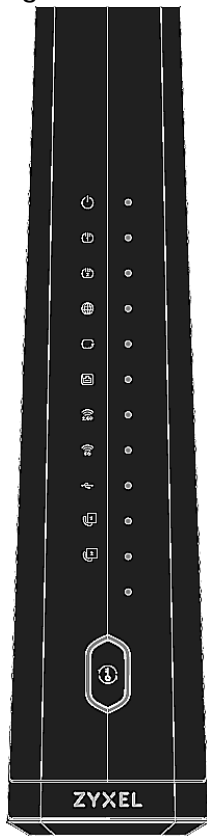
The LED indicators are located on the front panel. The following graphic displays the front panel of the VMG4927-B50A.

Figure 8 LEDs on the VMG4927-B50A

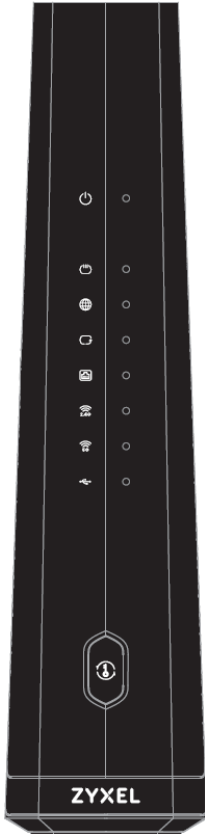


The following graphic displays the front panel of the VMG9827-B50A.

Figure 9 LEDs on the VMG9827-B50A



The following graphic displays the front panel of the VMG3927-B50B.

Figure 10 LEDs on the VMG3927-B50B

1.4.2 WPS Button

Once the **WiFi** LED turns green, WiFi is active. If WiFi is turned off, see [Section 7.2 on page 94](#) for how to enable WiFi on the VMG.

You can also use the **WPS** button to quickly set up a secure WiFi 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 On the VMG, 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 **WiFi 2.4G** and **WiFi 5G** LEDs flash amber while the VMG sets up a WPS connection with the other WiFi device.
- 4 Once the connection is successfully made, the **WPS** LED shines green. Note that it depends on your client's configuration to have a 2.4G or 5G WiFi network.

Note: Your VMG supports both 2.4G and 5G wireless networks, the connection to the 5G wireless network has priority.

The **WPS** LED turns off when WiFi is off.

1.4.3 LEDs (Lights)

The following table describes the LEDs.

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

Table 2 VMG4927-B50A 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.
		Blinking	The VMG is uploading firmware.
		Off	The VMG is not receiving power.
 DSL1 DSL2	Green	On	The ADSL line is up.
		Blinking	The VMG is initializing the ADSL line.
	Amber	On	The VDSL line is up.
		Blinking	The VMG is initializing the VDSL line.
		Off	The DSL line is down.
 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.
 LAN/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	There is no Ethernet connection on the WAN.
 Ethernet 1~4	Green	On	The VMG has a successful 10/100/1000 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 10/100/1000 Mbps.
		Off	The VMG does not have an Ethernet connection with the LAN.
 USB	Note: The USB LED is reserved for future development.		
 WiFi 2.4G WiFi 5G	Green	On	The 2.4G or 5G WiFi network is activated.
		Blinking	The VMG is communicating with 2.4G or 5G WiFi clients.
	Amber	Blinking	The VMG is setting up a WPS connection with a 2.4G or 5G WiFi client.
		Off	The 2.4G or 5G WiFi network is not activated.
 WPS	Amber	On	WPS is enabled.
		Off	WPS is disabled.

Table 3 VMG9827-B50A 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.
		Blinking	The VMG is uploading firmware.
		Off	The VMG is not receiving power.
 DSL1 DSL2	Green	On	The ADSL line is up.
		Blinking	The VMG is initializing the ADSL line.
	Amber	On	The VDSL line is up.
		Blinking	The VMG is initializing the VDSL line.
			Off
 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.
 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
 Ethernet	Green	On	The VMG has a successful 10/100/1000 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 10/100/1000 Mbps.
			Off
 WiFi 2.4G WiFi 5G	Green	On	The 2.4G or 5G WiFi network is activated.
		Blinking	The VMG is communicating with 2.4G or 5G WiFi clients.
	Amber	Blinking	The VMG is setting up a WPS connection with a 2.4G or 5G WiFi client.
			Off
 USB	Note: The USB LED is reserved for future development.		

Table 3 VMG9827-B50A LED Descriptions (continued)



LED	COLOR	STATUS	DESCRIPTION
 Phone1, Phone2	Green	On	A SIP account is registered for the phone port, and there's no voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Amber	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off the hook and there is a voice message in the corresponding SIP account.
		Off	The phone port does not have a SIP account registered.
	Red	On	Registration to the network has failed.
 WPS	Amber	On	WPS is enabled.
		Off	WPS is disabled.

Table 4 VMG3927-B50B 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.
		Blinking	The VMG is uploading firmware.
		Off	The VMG is not receiving power.
 DSL	Green	On	The ADSL line is up.
		Blinking	The VMG is initializing the ADSL line.
	Amber	On	The VDSL line is up.
		Blinking	The VMG is initializing the VDSL line.
		Off	The DSL line is down.
 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.
 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	There is no Ethernet connection on the WAN.
 Ethernet	Green	On	The VMG has a successful 10/100/1000 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 10/100/1000 Mbps.
		Off	The VMG does not have an Ethernet connection with the LAN.

Table 4 VMG3927-B50B LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
 WiFi 2.4G WiFi 5G	Green	On	The 2.4G or 5G WiFi network is activated.
		Blinking	The VMG is communicating with 2.4G or 5G WiFi clients.
	Amber	Blinking	The VMG is setting up a WPS connection with a 2.4G or 5G WiFi client.
		Off	The 2.4G or 5G WiFi network is not activated.
 WPS	Amber	On	WPS is enabled.
		Off	WPS is disabled.
 USB	Note: The USB LED is reserved for future development.		

1.4.4 Rear Panel

The connection ports are located on the rear panel. The following graphics display the rear panels.

Figure 11 VMG4927-B50A Rear Panel

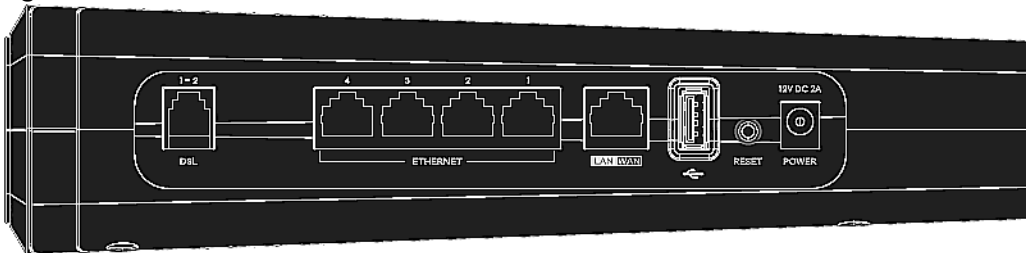


Figure 12 VMG9827-B50A Rear Panel

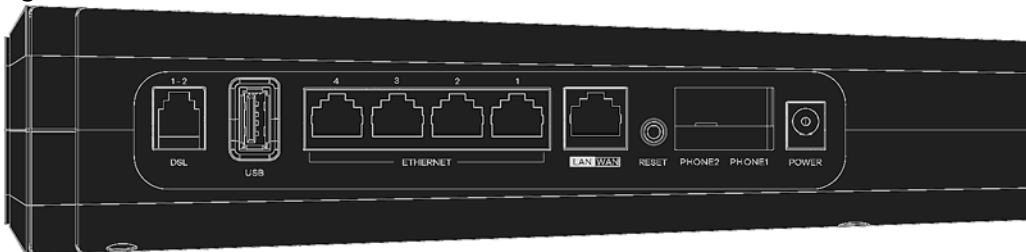
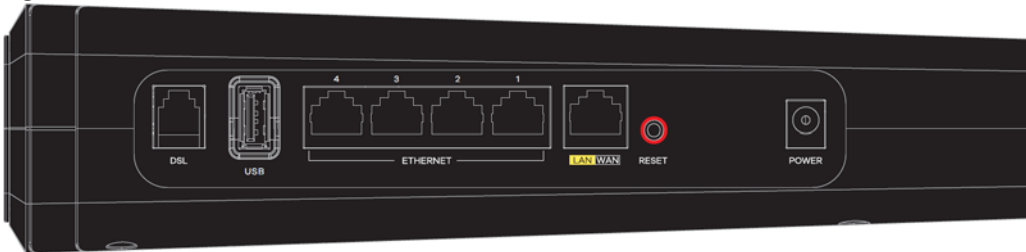


Figure 13 VMG3927-B50B Rear Panel



The following table describes the items on the rear panels.

Rear Panel Ports

LABEL	DESCRIPTION
DSL	Connect a RJ-11 cable to the DSL port for Internet access. See Section 1.1.1.1 on page 17 for more information about DSL bonding.
ETHERNET 1 ~ 4	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
LAN/WAN	Connect an Ethernet cable to the Ethernet WAN port for Internet access. See Section 1.1.1.2 on page 19 for more information about converting the LAN/WAN port as a WAN port.
USB	The USB port is reserved for future development.
PHONE1 ~ PHONE2	Connect analog phones to the phone ports to make phone calls.
Reset	Press the button to return the VMG to the factory defaults.
Power	Connect the power cable to start the VMG.

1.4.5 RESET Button

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

- 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 more than 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.

1.4.6 Wall Mounting

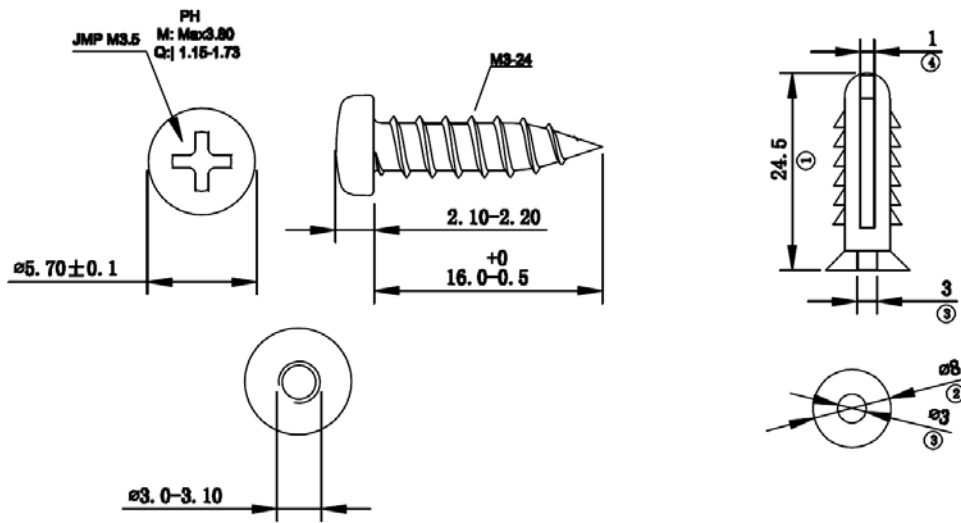
You may need screw anchors if mounting on a concrete or brick wall.

Table 5 Wall Mounting Information

Distance between holes	88 mm
Screws	Two
Screw anchors (optional)	Two
Distance from the ground (maximum)	2 m

The following figure introduces the specifications of the screws and screws anchors for wall mounting.

Figure 14 Screws & Screw Anchors Specifications



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

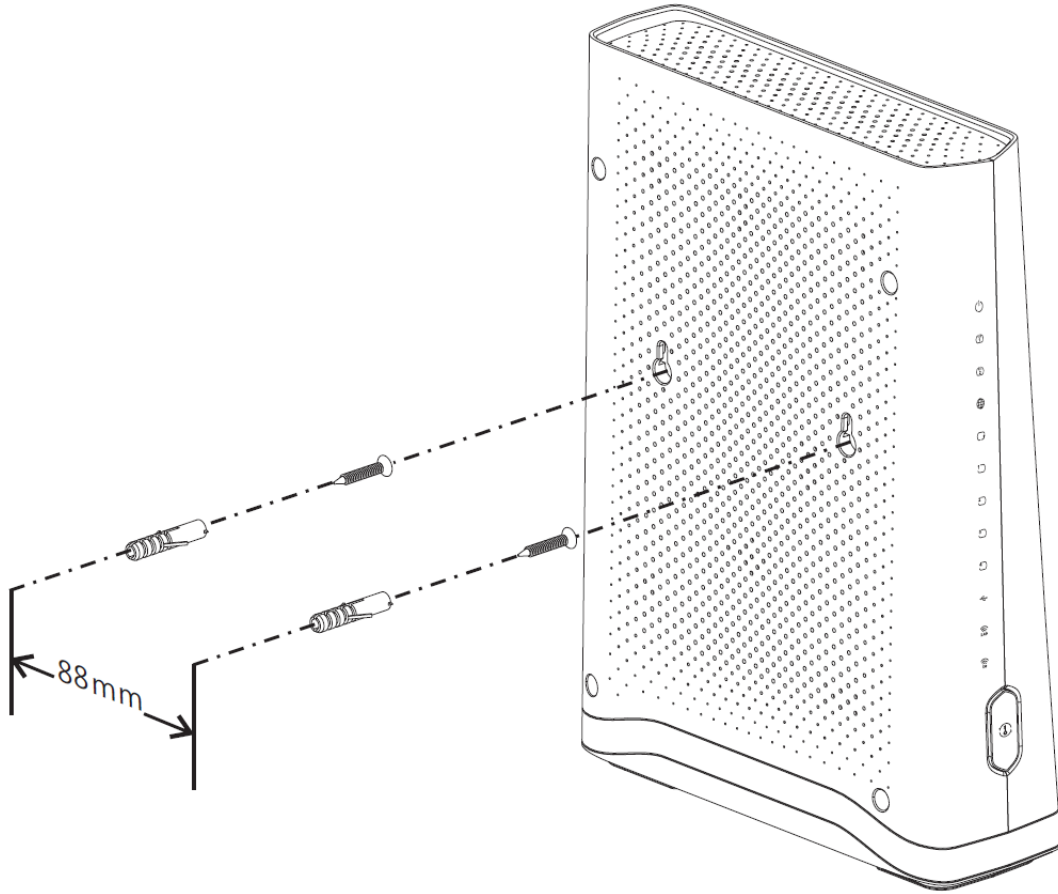
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

- 3 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.

- 4 Make sure the screws are fastened well enough to hold the weight of the VMG with the connection cables.
- 5 Align the holes on the back of the VMG with the screws on the wall. Hang the VMG on the screws.

Figure 15 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 7.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

2.1.1 Access 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 (in the VMG's label) in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 16 Password Screen

The image shows a dark blue login screen for a ZyXEL device. At the top left, the 'ZYXEL' logo is displayed in white. Below the logo, the word 'Welcome' is written in white, followed by the text 'Welcome to VMG3927-B50B configuration interface.' in a smaller font. There are two white input fields: the first is labeled 'Username:' and the second is labeled 'Password:'. A white 'Login' button is located in the bottom right corner of the screen.

- 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 17 Change Password Screen

ZYXEL

Change Password
The password must contain 6 to 64 characters, include 0-9 and a-z.

New Password :

Verify New Password :

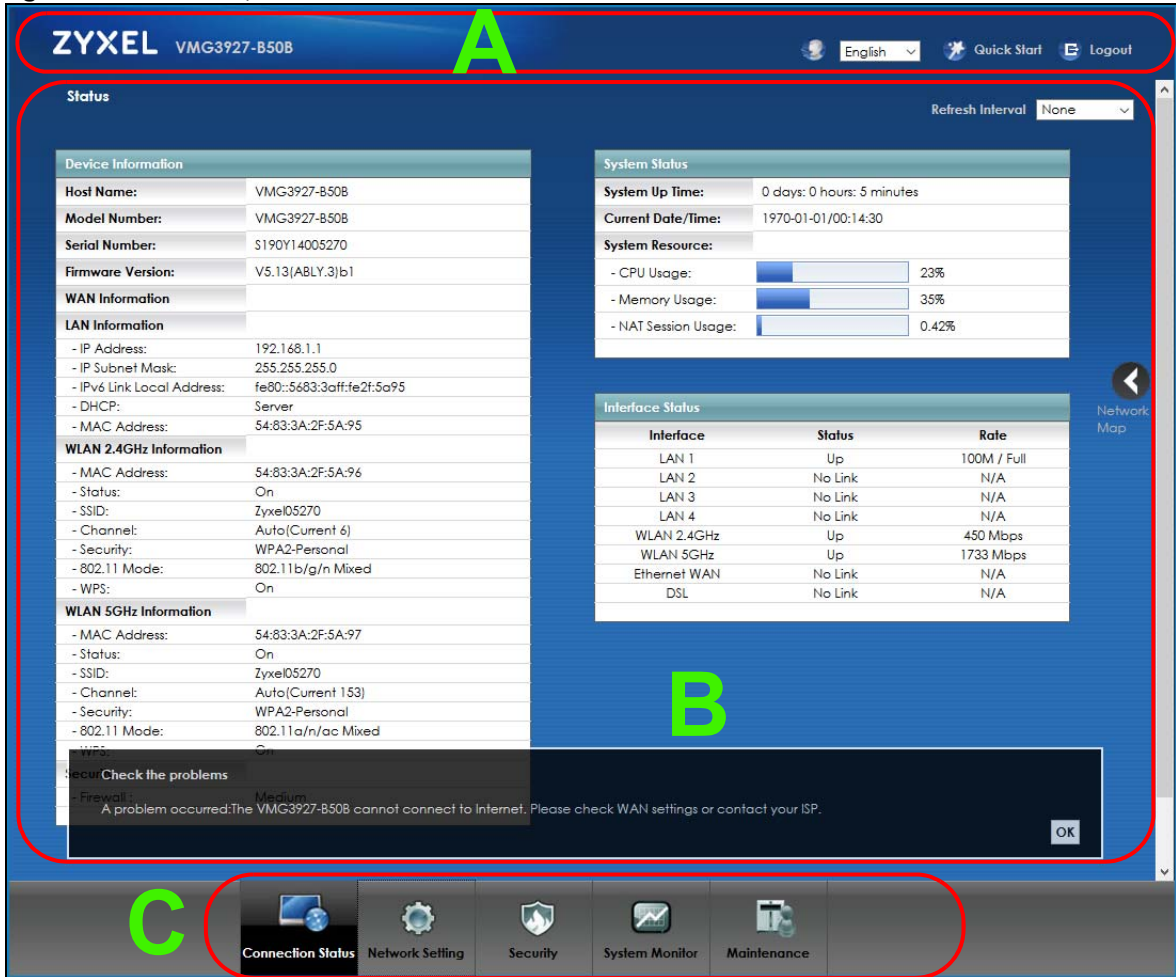
No need to change password. Do not show this page next time.

Apply

- 5 The **Quick Start Wizard** screen appears. You can configure the time zone, basic Internet access, and WiFi settings. See [Chapter 3 on page 39](#) for more information.
- 6 After you finished or closed the **Quick Start Wizard** screen, the **Status** screen appears, where you can view the VMG's interface and system information.

2.2 Web Configurator Layout

Figure 18 Screen Layout

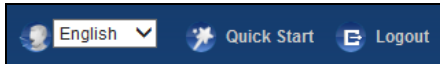


As illustrated above, the main screen is divided into these parts:

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

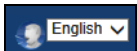
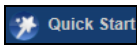

2.2.1 Title Bar

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



The icons provide the following functions.

Table 6 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 WiFi settings.
	Logout: Click this icon to log out of the Web Configurator.

2.2.2 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 7 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.
	Advanced	Use this screen to enable or disable PTM over ADSL, Annex M / Annex J, and DSL PhyR functions.
	Ethernet WAN	Use this screen to enable or disable the Ethernet WAN port.
Wireless	WiFi	Use this screen to configure the WiFi settings and WLAN authentication/security settings.
	Guest WiFi	Use this screen to configure multiple BSSs on the VMG.
	WPS	Use this screen to configure and view your WPS (WiFi Protected Setup) settings.
	Advanced	Use this screen to configure advanced WiFi settings.
	Channel Status	Use this screen to scan WiFi channel noises and view the results.
	MESH	Use this screen to enable MESH which combines the 2.4G and 5G WiFi network name, password, security type together for eliminating configuration hassles.
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.

Table 7 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
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.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Classification Setup	Use this screen to define a classifier.
	Shaper Setup	Use this screen to limit outgoing traffic rate on the selected interface.
	Policer Setup	Use this screen to configure QoS policers.
	Monitor	Use this screen to view QoS packet statistics on WAN/LAN interface and the status of queues.
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.
IGMP/MLD	IGMP/MLD	Use this screen to configure multicast settings (IGMP for IPv4 and MLD for IPv6 multicast groups) on the WAN.
Vlan Group	Vlan Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	Use this screen to map a port to a PVC or bridge group.
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 define time periods and days during which the VMG performs parental control on a specific user.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.

Table 7 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
VoIP		
SIP	SIP Account	Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the VMG.
	SIP Service Provider	Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions, and dialing plan.
Phone	Phone Device	Use this screen to view detailed information of the phone devices.
	Region	Use this screen to select your location and a call service mode.
Call Rule	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the VMG. You can export or email 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.
Multicast Status	IGMP Status	Use this screen to view the status of all IGMP settings on the VMG.
	MLD Status	Use this screen to view the status of all MLD settings on the VMG.
xDSL Statistics	xDSL Statistics	Use this screen to view the VMG's xDSL traffic statistics.
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.

Table 7 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the VMG through the services configured in the Maintenance > Remote Management screen.
SNMP	SNMP	Use this screen to configure SNMP (Simple Network Management Protocol) settings.
Time	Time	Use this screen to change your 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.
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.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	802.3ah	Use this screen to configure link OAM port parameters.
	OAM Ping	Use this screen to view information to help you identify problems with the DSL connection.

CHAPTER 3

Quick Start

3.1 Overview

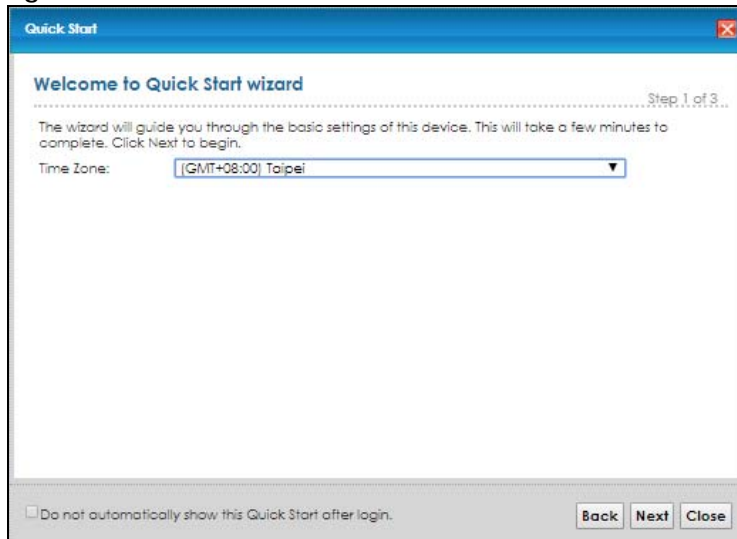
Use the Quick Start screens to configure the VMG's time zone, basic Internet access, and WiFi settings.

Note: See the technical reference chapters (starting on [Chapter 4 on page 42](#)) 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 19 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 20 Quick Start - Internet Connection

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

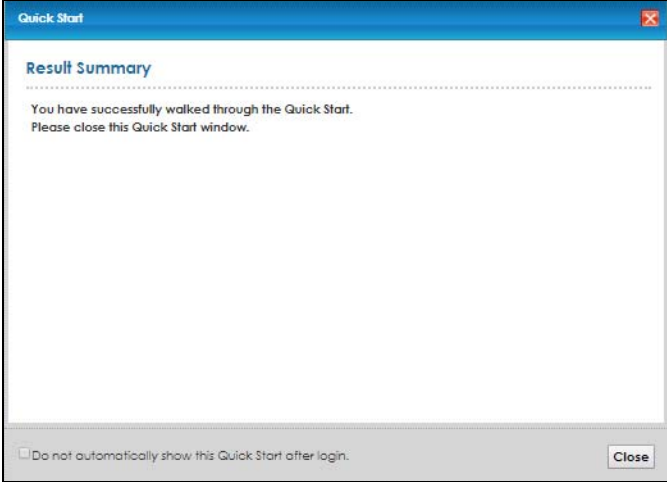
- 3 Turn WiFi on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the VMG. Click **Save**.

Figure 21 Quick Start - Wireless Setting

The screenshot shows a window titled "Quick Start" with a blue header. Below the header, the title "Wireless Setting" is displayed in blue, followed by "Step 3 of 3" in the top right corner. 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, there are four rows of settings: "Wireless Service:" with radio buttons for "Enable" (selected) and "Disable"; "Wireless Network Name (SSID):" with the value "Zyxel07945"; "Security:" with the value "WPA2-Personal"; and "Password:" with a masked password "*****". At the bottom left, there is a checkbox labeled "Do not automatically show this Quick Start after login." At the bottom right, there are 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 22 Quick Start - Result Summary



CHAPTER 4

Tutorials

4.1 Overview

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

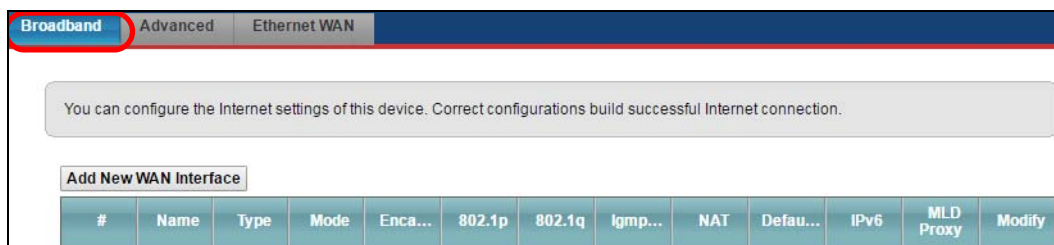
- [Set Up an ADSL PPPoE Connection](#), see page 42
- [Set Up a Secure WiFi Network](#), see page 45
- [Set Up Multiple Wireless Groups](#), see page 53
- [Configure Static Route for Routing to Another Network](#), see page 56
- [Configure QoS Queue and Class Setup](#), see page 58
- [Access the VMG Using DDNS](#), see page 62
- [Configure the MAC Address Filter](#), see page 63

4.2 Set 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**.



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

General	
Name	MyDSLConnection
Type	ADSL
Connection Mode	Routing
Encapsulation	PPPoE
IPv6/IPv4 Mode	IPv4

ATM PVC Configuration	
VPI/VCI	36/48
Encapsulation Mode	LLC/SNAP-Bridging
Service Category	UBR without PCR
Account Information	
PPP User Name	1234@DSL-Ex.com
PPP Password	ABCDEF!
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.

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

OK Cancel

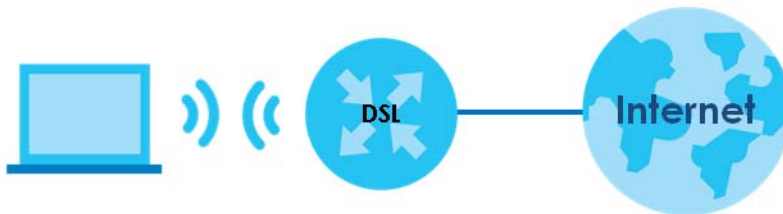
- 8 You should see a summary of your new DSL connection setup in the **Broadband** screen as follows.

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 Set Up a Secure WiFi Network

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



Thomas has to configure the WiFi network settings on the VMG. Then he can set up a WiFi network using WPS (Section 4.3.3 on page 49) or manual configuration (Section 4.3.3 on page 49).

4.3.1 Configure the WiFi Network Settings

This example uses the following parameters to set up a 2.4G WiFi network.

WiFi Network Name	Example
WiFi	Enable
WiFi Security Type	WPA2-PSK
WiFi Password	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n Mixed

- 1 Click **Network Setting > Wireless > WiFi** and click the **Edit** button. Note that you may see one or two network name(s) displayed on this screen depending on whether you have selected **Keep 2.4G and 5G WiFi network name the same**.

WiFi		
<input checked="" type="checkbox"/> Keep 2.4G and 5G WiFi network name the same		
WiFi Network Name	Password	Action
Zyxel06049	YKGGFFGH7F	Edit

OR

WiFi		
<input type="checkbox"/> Keep 2.4G and 5G WiFi network name the same		
WiFi Network Name	Password	Action
<div style="display: flex; align-items: center;"> <div style="margin-right: 5px;"> ▬▬▬ 2.4G </div> <div>Zyxel06049</div> </div> <div style="display: flex; align-items: center; margin-top: 2px;"> <div style="margin-right: 5px;"> ▬▬▬ 5G </div> <div>Zyxel06049_5G</div> </div>	YKGGFFGH7F	Edit

- The **WiFi Edit** screen displays. Select **WPA2-PSK** as the security type. Configure the screen using the provided parameters (see [page 49](#)). Click **Save**.

WiFi Edit	
Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.	
WiFi Network Settings	
WiFi	<input checked="" type="radio"/> Enable <input type="radio"/> Disable (Settings are invalid when disabled)
	<input checked="" type="checkbox"/> Keep 2.4G and 5G WiFi network name the same
WiFi Network Name	<input type="text" value="Zyxel70074"/>
WiFi Password	<input type="text" value="4AJ8FU3P48"/>
WiFi Security Type	<input type="text" value="WPA2-PSK"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- Go to the **Wireless > Advanced** screen and select **802.11b/g/n Mixed** in the **802.11 Mode** field in the **2.4G Advanced Settings** section. Click **Apply**.

The screenshot displays two sections of advanced settings: 2.4G and 5G. Both sections include a 'Hide WiFi Network Name' checkbox (unchecked), 'Channel' (Auto), 'Bandwidth' (40MHz), '802.11 Mode' (802.11b/g/n Mixed), 'RTS/CTS Threshold' (2347), 'Fragmentation Threshold' (2346), 'Output Power' (100%), 'Beacon Interval' (100 ms), 'DTIM Interval' (1 ms), '802.11 Protection' (Off), and 'Preamble' (Long). The 2.4G section has 'WPS' checked, while the 5G section has 'WPS' unchecked. Other options like 'OBSS Coexistence', 'WMM', and 'WMM Automatic Power Save Delivery' are available for both sections with 'Enable' and 'Disable' radio buttons. 'DFS Channel' and 'MU-MIMO' are only present in the 5G section. 'Apply' and 'Cancel' buttons are at the bottom right.

Thomas can now use the WPS feature to establish a WiFi connection between his notebook and the VMG (see [Section 4.3.2 on page 47](#)). He can also use the notebook's WiFi client to search for the VMG (see [Section 4.3.3 on page 49](#)).

4.3.2 Use WPS

This section shows you how to set up a WiFi network using WPS. It uses the VMG as the AP and a WPS-enabled Android smartphone as the WiFi client.

To set up the WiFi client settings:

- 1 Make sure that your VMG is turned on and your Android smartphone is within the cover range of the WiFi signal.
- 2 Make sure WPS is enabled on the VMG. You can check it by logging into the VMG's Web Configurator and see if it is enabled in the **Network Setting > Wireless > Advanced** screen. If not, select the **WPS** check box for the 2.4G or 5G wireless network and then click **Apply**.

Note: When the MESH function is enabled (see [Section 7.7 on page 103](#)), the VMG automatically enables WPS and grays the field out on this **Network Setting > Wireless > Advanced** screen.

2.4G Advanced Settings

Hide WiFi Network Name :

Channel : Auto ▼

802.11 Mode : 802.11b/g/n Mixed ▼

RTS/CTS Threshold : 2347

Fragmentation Threshold : 2346

Output Power : 100% ▼

Beacon Interval : 100 ms

DTIM Interval : 1 ms

802.11 Protection : Off ▼

Preamble : Long ▼

WPS :

OBSS Coexistence : Enable Disable

WMM : Enable Disable

WMM Automatic Power Save Delivery : Enable Disable

5G Advanced Settings

Hide WiFi Network Name :

Channel : Auto ▼

802.11 Mode : 802.11a/n/ac Mixed ▼

RTS/CTS Threshold : 2347

Fragmentation Threshold : 2346

Output Power : 100% ▼

Beacon Interval : 100 ms

DTIM Interval : 1 ms

802.11 Protection : Off ▼

Preamble : Long ▼

WPS :

OBSS Coexistence : Enable Disable

WMM : Enable Disable

WMM Automatic Power Save Delivery : Enable Disable

Apply Cancel

- 3 You can either press the **WPS** button on the VMG's panel or click the **Connect** button for the corresponding 2.4G or 5G wireless band in the **Network Setting > Wireless > WPS** screen.

Connection Type	Wi-Fi Name	WPS
2.4G Wi-Fi	Zyxel06049	<input checked="" type="button" value="Connect"/>
5G Wi-Fi	Zyxel06049	<input checked="" type="button" value="Connect"/>

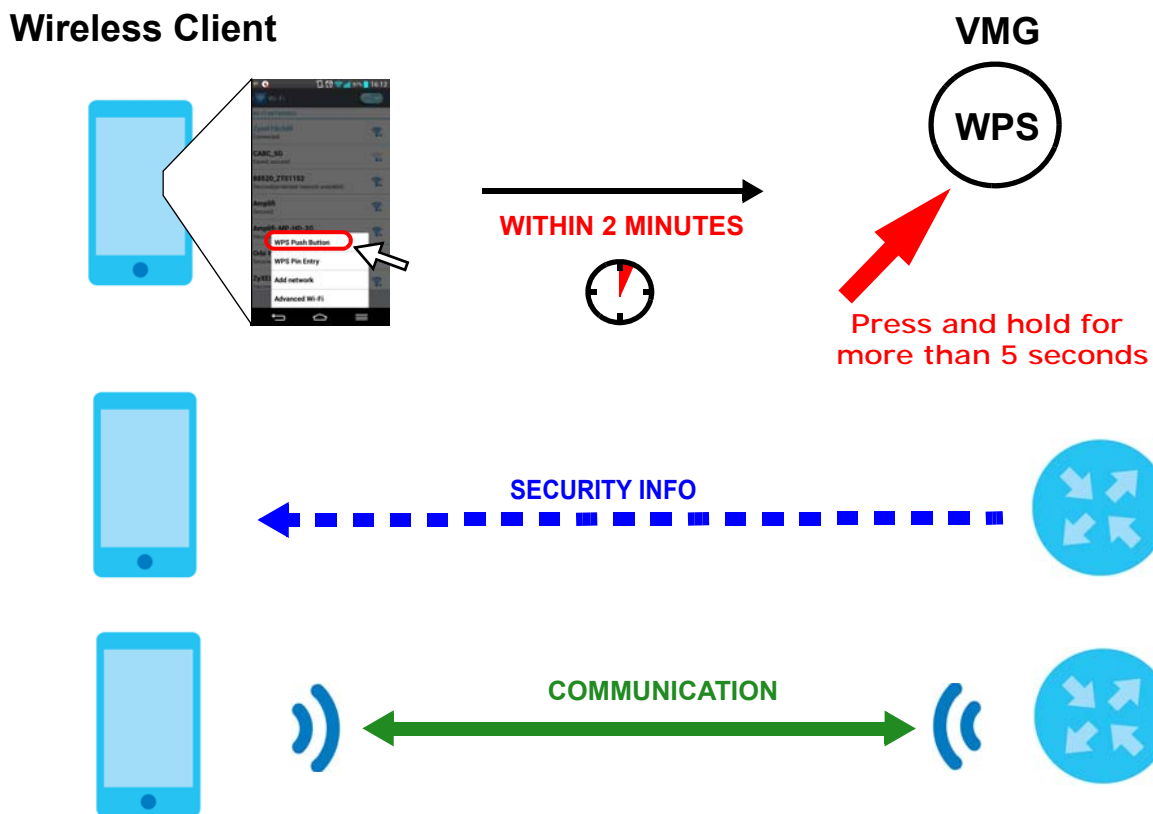
Activate WPS on wireless client within 2 minutes after clicking "Connect".

- 4 Go to your phone settings and turn on WiFi. Open the WiFi networks list and tap **WPS Push Button** or the WPS icon (🌀).

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 (the Android smartphone in this example).



4.3.3 Connect to the VMG’s WiFi Network Manually (No WPS)

In this example, we change the VMG's wireless settings, and then manually select the VMG's new SSID and enter the WiFi key to connect a wireless client to the VMG.

4.3.4 Configure Wireless Security on the VMG

This section shows you how to configure wireless security settings with the following parameters on your VMG.

Frequency Band	2.4G
SSID	SSID_Example
Channel	Auto
Security	WPA2-PSK (Wireless Password: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your VMG.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see [Section 2.2 on page 28](#)).

- 1 Go to the **Network Setting > Wireless > WiFi > Edit** screen to enable the 2.4G wireless network.

- Enter **SSID_Example** as the wireless name. Set WiFi security type to **WPA2-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Save**.

WiFi Network Settings

WiFi Enable Disable (Settings are invalid when disabled)

Keep 2.4G and 5G WiFi network name the same

WiFi Network Name
Zyxel70074

WiFi Password
4AJ8FU3P48

WiFi Security Type
WPA2-PSK

Save Cancel

- Go to the **Network Setting > Wireless > Advanced** screen and select **Auto** in the **Channel** field to have the VMG scan for and select an available channel automatically.
- Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Device Information

Host Name: VMG4927-B50A
 Model Number: VMG4927-B50A
 Serial Number: S170Y43042996
 Firmware Version: V5.13(ABLY.0)b1

WAN1 Information

- Encapsulation: IPoE
 - IP Address: 10.214.80.41 [Release]
 - IP Subnet Mask: 255.255.255.0
 - MAC Address: 5C:E2:8C:46:9D:E1
 - Primary DNS server: 172.21.5.1
 - Secondary DNS server: 172.21.6.1
 - DHCP: Client

LAN Information

- IP Address: 192.168.1.1
 - IP Subnet Mask: 255.255.255.0
 - IPv6 Link Local Address: fe80::5ee2:8cff:fe46:9ddb
 - DHCP: Server
 - MAC Address: 5C:E2:8C:46:9D:DB

WLAN 2.4GHz Information

- MAC Address: 5C:E2:8C:46:9D:DD
 - Status: On
 - SSID: SSID_Example
 - Channel: Auto(Current 11)
 - Security: WPA2-Personal
 - 802.11 Mode: 802.11b/g/n Mixed
 - WPS: On

WLAN 5GHz Information

- MAC Address: 5C:E2:8C:46:9D:DF
 - Status: On
 - SSID: SSID_Example
 - Channel: Auto(Current 36)
 - Security: WPA2-Personal
 - 802.11 Mode: 802.11a/n/ac Mixed
 - WPS: On

Security

- Firewall: Medium

System Status

System Up Time: 0days: 0hours: 14minutes
 Current Date/Time: 2017-12-20/08:36:12
 System Resource:
 - CPU Usage: 4%
 - Memory Usage: 33%
 - NAT Session Usage: 0.078%

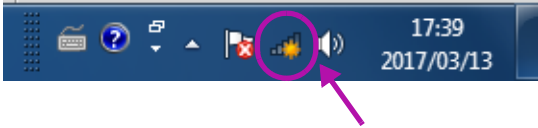
Interface Status

Interface	Status	Rate
LAN 1	Up	1000M / Full
LAN 2	No Link	N/A
LAN 3	No Link	N/A
LAN 4	No Link	N/A
WLAN 2.4GHz	Up	450 Mbps
WLAN 5GHz	Up	1733 Mbps
Ethernet WAN	Up	1000M / Full
DSL	No Link	N/A

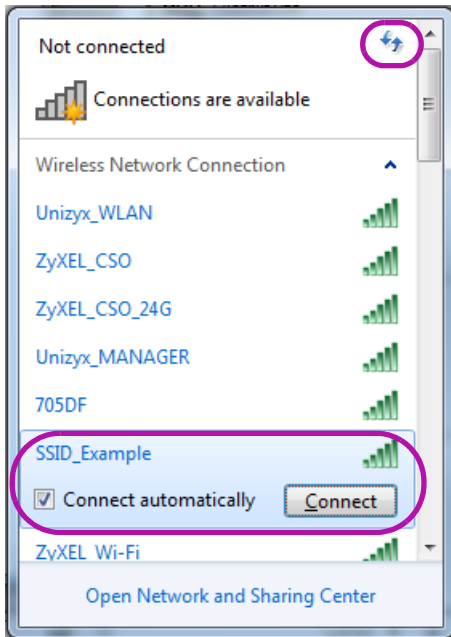
4.3.5 Configure Your Laptop

Note: In this example, we use a Windows 7 laptop that has a built-in wireless adapter as the wireless client.

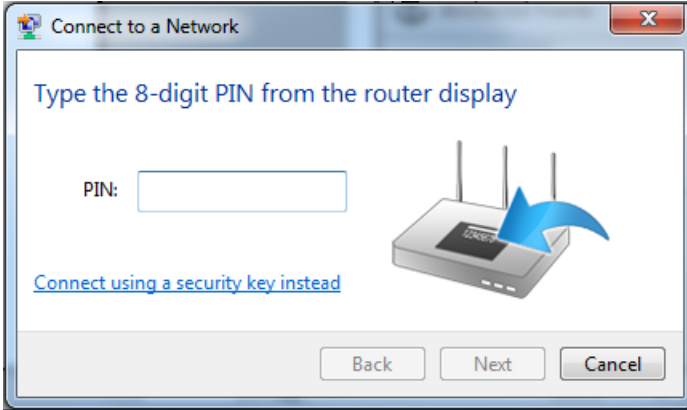
- 1 The VMG supports IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac wireless clients. Make sure that your laptop or computer's wireless adapter supports one of these standards.
- 2 Click the WiFi icon in your computer's system tray.



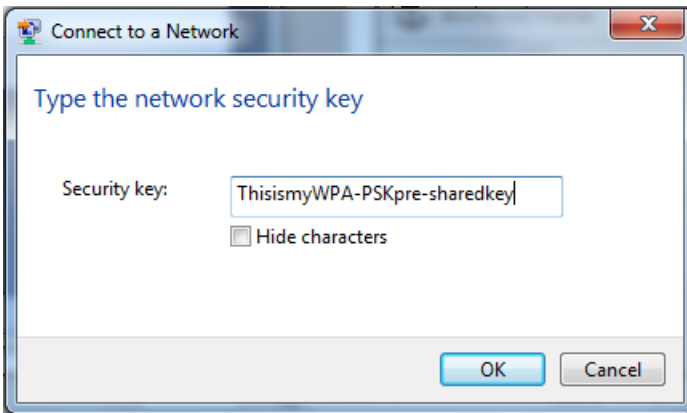
- 3 The **Wireless Network Connection** screen displays. Click the refresh button to update the list of available wireless APs within range.
- 4 Select **SSID_Example** and click **Connect**.



- 5 The following screen displays if WPS is enabled on the VMG but you didn't press the WPS button. Click **Connect using as security key instead**.



- 6 Type the security key in the following screen. Click **OK**.



- 7 Check the status of your wireless connection in the screen below.



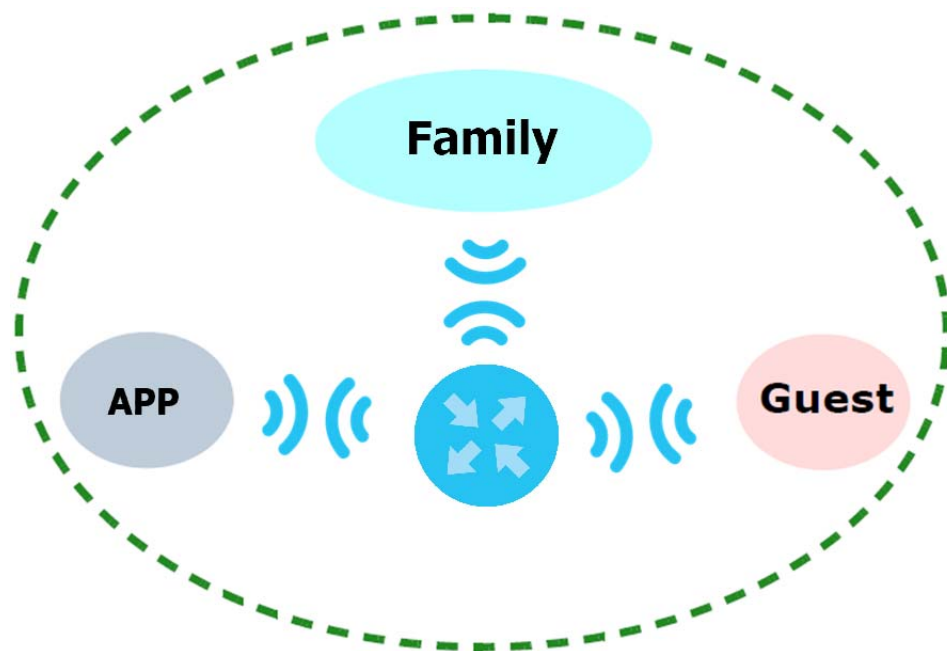
- 8 If the wireless client keeps trying to connect to or acquiring an IP address from the VMG, make sure you entered the correct security key.

If the connection has limited or no connectivity, make sure the VMG is connected to a router with the DHCP server enabled.

If your connection is successful, open your Internet browser and enter <http://www.zyxel.com> or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

4.4 Set Up Multiple Wireless Groups

A family wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own wireless network name (SSID) and security type.



- The family members will use the general **Family** wireless network group.
- Visiting guests will use the **Guest** group with the restriction of the Internet access for the following 48 hours (in this example) after the setting is applied.
- The **APP** group will be dedicated to some home applications that require the Internet or an internal network, such as playing PS4 games.

The family will use the following parameters to set up the wireless network groups.

	FAMILY	GUEST	APP
SSID	Family	Guest	APP
Security Type	WPA2-PSK		
Wireless Password	ForFamilyOnly	guest123	123456789
Available Time	N/A	48 hours	N/A

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

WiFi Network Settings

WiFi Enable Disable (Settings are invalid when disabled)

Keep 2.4G and 5G WiFi network name the same

WiFi Network Name
Family

WiFi Password
ForFamilyOnly

WiFi Security Type
WPA2-PSK

Save Cancel

- 2 Click **Network Setting > Wireless > Guest WiFi** to open the following screen. Click the **Edit** icon in the **Guest WiFi** section to configure the second wireless network group.

Guest WiFi

Enable Guest WiFi

WiFi Network Name	Password	Action
Zyxel06049_guest	YKGGFFGH	Edit

Extra WiFi

Band	WiFi Network Name	Password	Action
2.4G	Zyxel6049_extra2	YKGGFFGH7F	Edit
2.4G	Zyxel6049_extra3	YKGGFFGH7F	Edit
5G	Zyxel6049_extra2_5G	YKGGFFGH7F	Edit

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

Guest WiFi Network Settings

Guest WiFi Enable Disable (Settings are invalid when disabled)

WiFi Network Name

WiFi Password

Time Period Duration (hours) 1 4 8 12 24 48 Always on

- 4 In the **Guest WiFi** screen, click an **Edit** icon next to a 2.4G "extra WiFi" network to configure the third wireless network group. Configure the screen using the provided parameters and click **Save**.

Guest WiFi Network Settings

Guest WiFi Enable Disable (Settings are invalid when disabled)

WiFi Network Name

WiFi Password

- 5 Check the status of **Guest** and **APP** in the **Guest WiFi** screen. The screen also displays the remaining available time for using the **Guest WiFi** network at the upper right corner.

47 hours 54 minutes left

Guest WiFi
 Enable Guest WiFi

WiFi Network Name	Password	Action
Guest	guest123	Edit

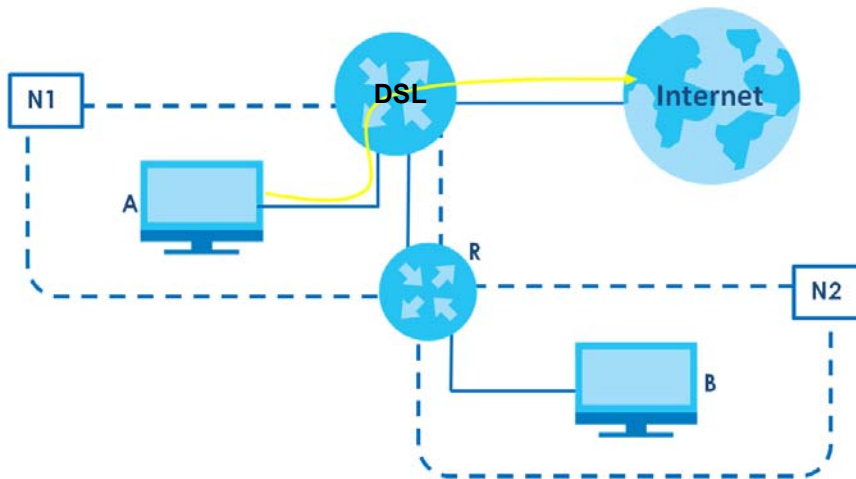
Extra WiFi

Band	WiFi Network Name	Password	Action
2.4G	APP	123456789	Edit
2.4G	Zyxel6049_extra3	YKGGFFGH7F	Edit
5G	Zyxel6049_extra2_5G	YKGGFFGH7F	Edit

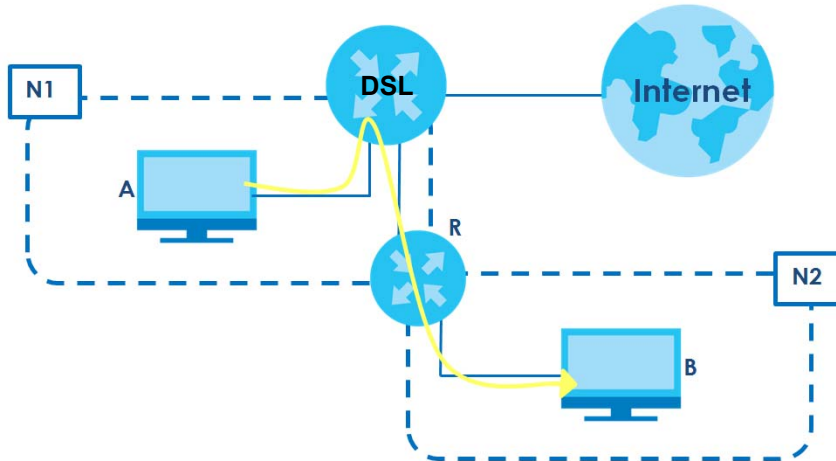
4.5 Configure Static Route for Routing to Another Network

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**.



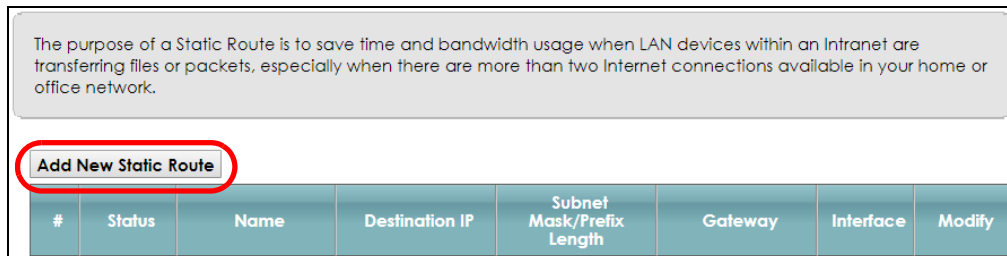
This tutorial uses the following example IP settings:

Table 8 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
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 the **Active** check box. Enter the **Route Name** as **R**.
 - 4b Set **IP Type** to **IPv4**.

- 4c** Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.
- 4d** Select **Enable** in the **Use Gateway IP Address** field. Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.
- 4e** Select **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.

4.6 Configure QoS Queue and Class Setup

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

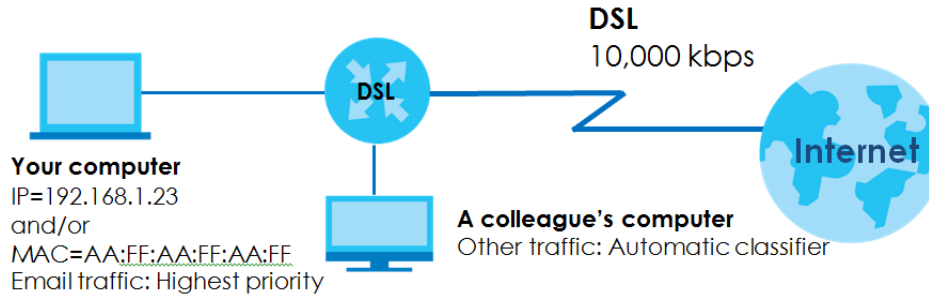
Let's say you are a team leader of a small sales branch office. You want to prioritize email traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and email archives) to the FTP server throughout the day. Your colleagues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

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

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.

Apply **Cancel**

- 2 Click **Queue Setup > Add new Queue** to create a new queue. In the screen that opens, check **Active** and enter or select the following values:
 - **Name:** Email
 - **Interface:** WAN
 - **Priority:** 1 (High)
 - **Weight:** 8
 - **Rate Limit:** 5,000 (kbps)

Add New Queue

Active Enable Disable

Name

Interface

Priority

Weight

Buffer Management

Rate Limit (kbps) (kbps)

OK Cancel

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

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

Step1: Class Configuration

Active 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

Packet Length ~ Exclude

DSCP (0~63) Exclude

802.1P Exclude

VLAN ID (1~4095) 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 (1~4095)

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:

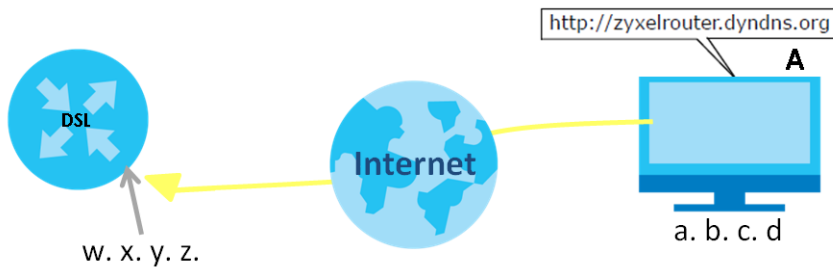
FIELD TO CONFIGURE	HOW TO CONFIGURE
Class Name	Give a class name to this traffic, such as Email in this example.
From Interface	This is the interface from which the traffic will be coming from. Select LAN1 for this example.
Ether Type	Select IP to identify the traffic source by its IP address or MAC 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 Email queue created in this example.

This maps email 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 **Email** queue (see the **Source** fields).

4.7 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 www.dyndns.org.

This tutorial covers:

- [Register a DDNS Account on \[www.dyndns.org\]\(http://www.dyndns.org\)](#)
- [Configure DDNS on Your VMG](#)
- [Test the DDNS Setting](#)

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

4.7.1 Register 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.

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

Dynamic DNS Setup

Dynamic DNS Enable Disable (Settings are invalid when disabled)

Service Provider :

Host/Domain Name :

Username :

Password :

Dynamic DNS Status

User Authentication Result :

Last Updated Time :

Current Dynamic IP :

Click **Apply**.

4.7.3 Test the DDNS Setting

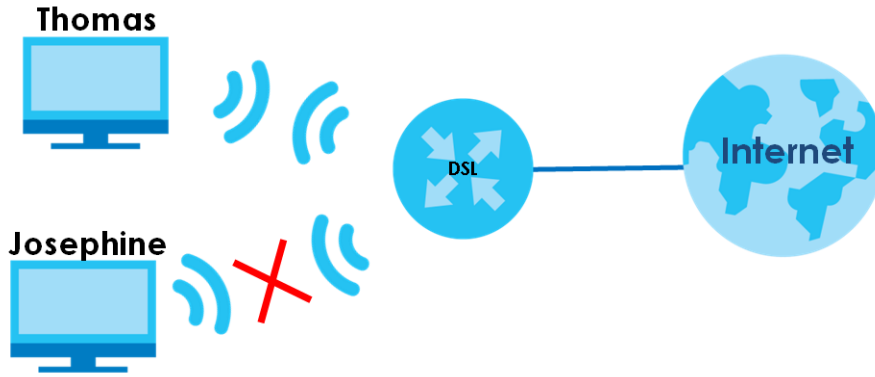
Now you should be able to access the VMG from the Internet. To test this:

- 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.

4.8 Configure 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**.

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

MAC Address Filter Enable Disable (Settings are invalid when disabled)
 MAC Restrict Mode Allow Deny

Set	Active	Host Name	MAC Address
1	<input checked="" type="checkbox"/>	Thomas	00 - 24 - 21 - AB - 1F - 0d
2	<input type="checkbox"/>		- - - - -
3	<input type="checkbox"/>		- - - - -
4	<input type="checkbox"/>		- - - - -
5	<input type="checkbox"/>		- - - - -
6	<input type="checkbox"/>		- - - - -
7	<input type="checkbox"/>		- - - - -
29	<input type="checkbox"/>		- - - - -
30	<input type="checkbox"/>		- - - - -
31	<input type="checkbox"/>		- - - - -
32	<input type="checkbox"/>		- - - - -

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

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.

PART II

Technical Reference

CHAPTER 5

Network Map and Status Screens

5.1 Overview

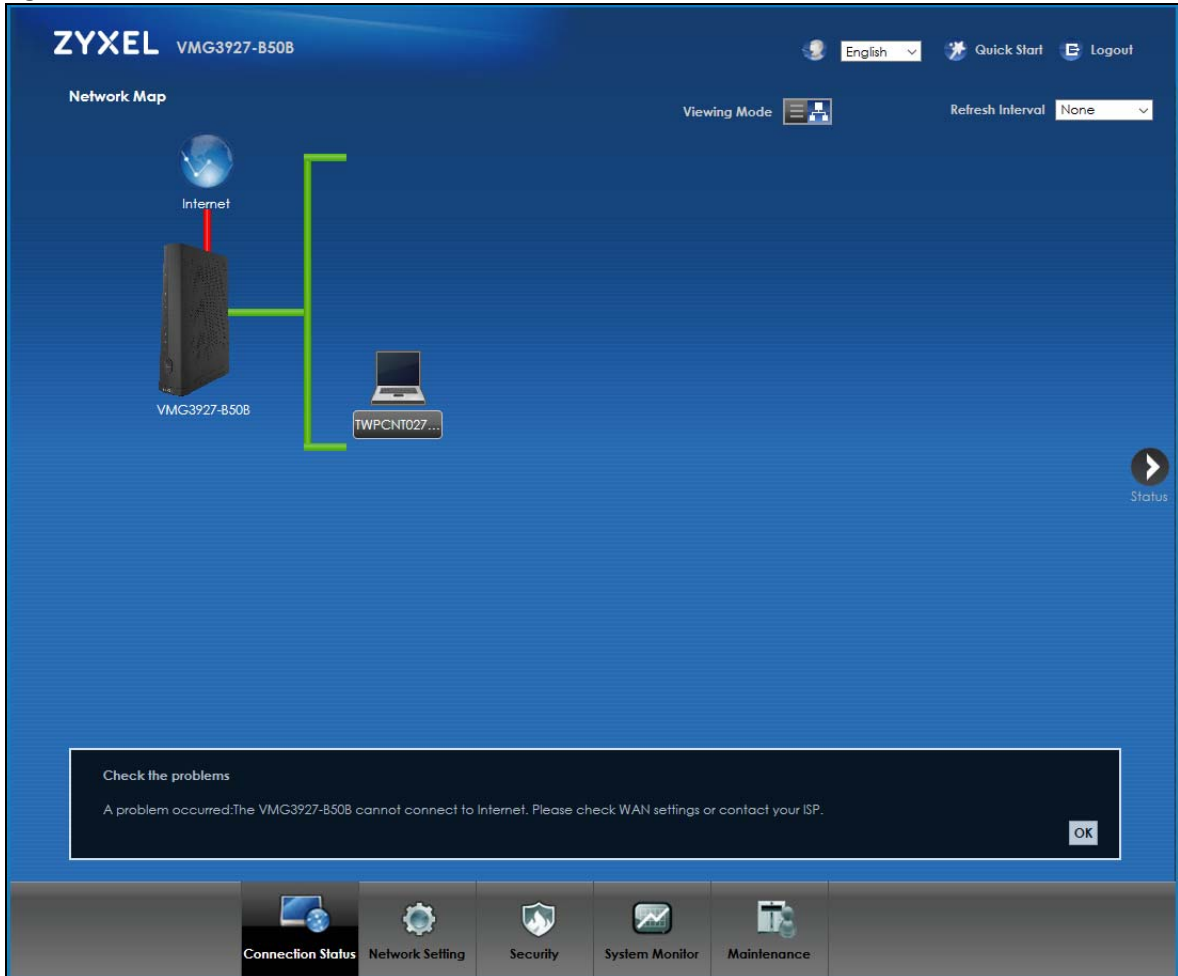
After you log into the Web Configurator, the **Network Map** screen appears. This shows the network connection status of the VMG and clients connected to it.

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

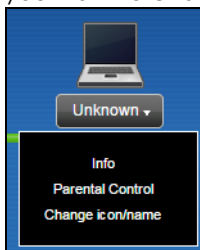
5.2 Network Map

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 23 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 name/icon**.



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 24 Network Map: List View Mode

#	Device Name	IP Address	MAC Address	Address Source	Connect Type
	Unknown	192.168.1.5	c0:3f:d5:ba:9e:b7	Static	Ethernet

5.3 Status

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

Figure 25 Status Screen

The screenshot shows the ZYXEL VMG3927-B50B Status Screen. The interface includes a top navigation bar with 'English', 'Quick Start', and 'Logout' options. A 'Refresh Interval' dropdown is set to 'None'. The main content area is divided into several sections:

- Device Information:** Host Name: VMG3927-B50B, Model Number: VMG3927-B50B, Serial Number: S190Y14005270, Firmware Version: V5.13(ABLY.3)b1.
- System Status:** System Up Time: 0 days: 1 hours: 4 minutes, Current Date/Time: 1970-01-01/09:04:47. Resource usage includes CPU (4%), Memory (35%), and NAT Session (0.063%).
- LAN Information:** IP Address: 192.168.1.1, Subnet Mask: 255.255.255.0, IPv6 Link Local Address: fe80::5683:3aff:fe2f:5a95, DHCP: Server, MAC Address: 54:83:3A:2F:5A:95.
- WLAN 2.4GHz Information:** MAC Address: 54:83:3A:2F:5A:96, Status: On, SSID: ZyxeI05270, Channel: Auto(Current 11), Security: WPA2-Personal, 802.11 Mode: 802.11b/g/n Mixed, WPS: On.
- WLAN 5GHz Information:** MAC Address: 54:83:3A:2F:5A:97, Status: On, SSID: ZyxeI05270, Channel: Auto(Current 153), Security: WPA2-Personal, 802.11 Mode: 802.11a/n/ac Mixed, WPS: On.
- Security:** Firewall: Medium.
- Interface Status Table:**

Interface	Status	Rate
LAN 1	Up	100M / Full
LAN 2	No Link	N/A
LAN 3	No Link	N/A
LAN 4	No Link	N/A
WLAN 2.4GHz	Up	450 Mbps
WLAN 5GHz	Up	1733 Mbps
Ethernet WAN	No Link	N/A
DSL	No Link	N/A

The bottom navigation bar includes icons for Connection Status, Network Setting, Security, System Monitor, and Maintenance.

Each field is described in the following table.

Table 9 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 field displays the serial number of the 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.

Table 9 Status Screen (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This field displays the current subnet mask in the WAN.
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) address of your VMG.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.
DHCP	This field displays whether the WAN interface is using a DHCP IP address or a static IP address. Choices are: Client - The WAN interface can obtain an IP address from a DHCP server. None - 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: Server - The VMG is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay - The VMG acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Disable - 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 2.4GHz/5GHz 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.
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 (Maintenance > Reboot), or when you reset it.
Current Date/Time	This field displays the current date and time in the VMG. You can change this in Maintenance > Time Setting .
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 Chapter 10 on page 140).

Table 9 Status Screen (continued)

LABEL	DESCRIPTION
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 Section 36.2 on page 275 , 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 Up when using the interface and NoLink when not using the interface.</p> <p>For a WLAN interface, this field displays the enabled (Up) or disabled (Disable) state of the interface.</p> <p>For the DSL interface, this field displays Down (line down), Up (line up or connected), Drop (dropping a call) if you're using PPPoE encapsulation, and NoLink when not using the interface.</p>
Rate	<p>For the Ethernet WAN and LAN 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 N/A with WLAN disabled.</p>
Registration Status	
Account	This column displays each SIP account in the VMG.
Action	<p>If the SIP account is already registered with the SIP server, the Account Status field displays Registered.</p> <p>Click Unregister to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name.</p> <p>If the SIP account is not registered with the SIP server, the Account Status field displays Not Registered.</p> <p>Click Register to have the VMG attempt to register the SIP account with the SIP server. The button is grayed out if the SIP account is disabled.</p>
Account Status	<p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p>In-active - The SIP account is not active. You can activate it in VoIP > SIP > SIP Account.</p> <p>Not Registered - The last time the VMG tried to register the SIP account with the SIP server, the attempt failed. Use the Register button to register the account again. The VMG automatically tries to register the SIP account when you turn on the VMG or when you activate it.</p> <p>Registered - The SIP account is already registered with the SIP server. You can use it to make a VoIP call.</p>
Service Provider	This column displays the service provider name and SIP number for each SIP account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the VoIP > SIP screens.

CHAPTER 6

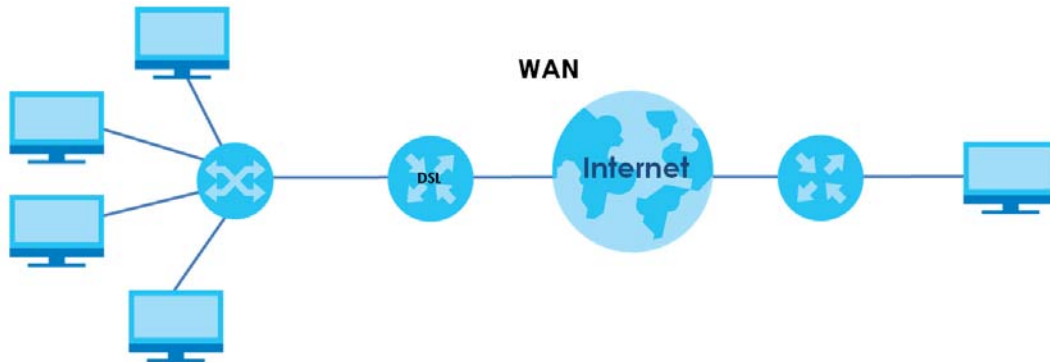
Broadband

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 26 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 75](#)).
- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions ([Section 6.3 on page 84](#)).
- Use the **Ethernet WAN** screen to enable or disable the Ethernet WAN port ([Section 6.4 on page 87](#)).

Table 10 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 10 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).

PTM

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

IPv6 Introduction

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

IPv6 Address

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 Mask

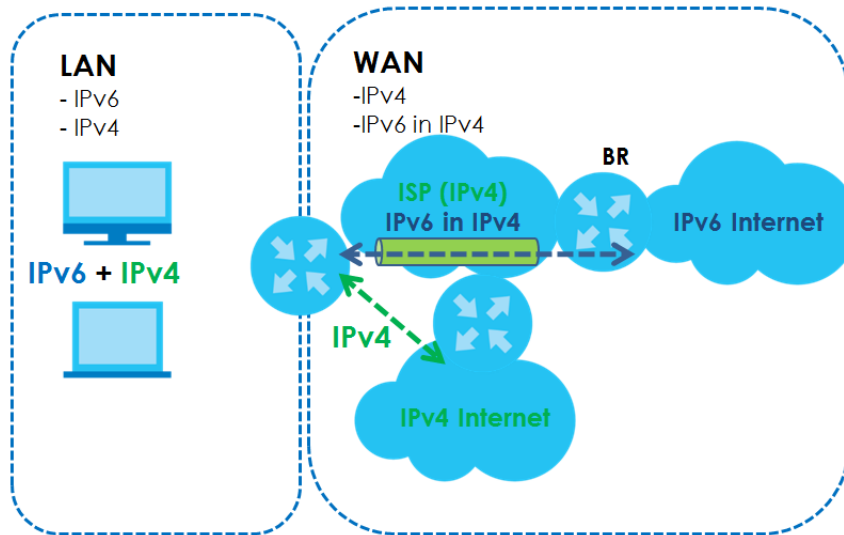
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 0, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, `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 27 IPv6 Rapid Deployment

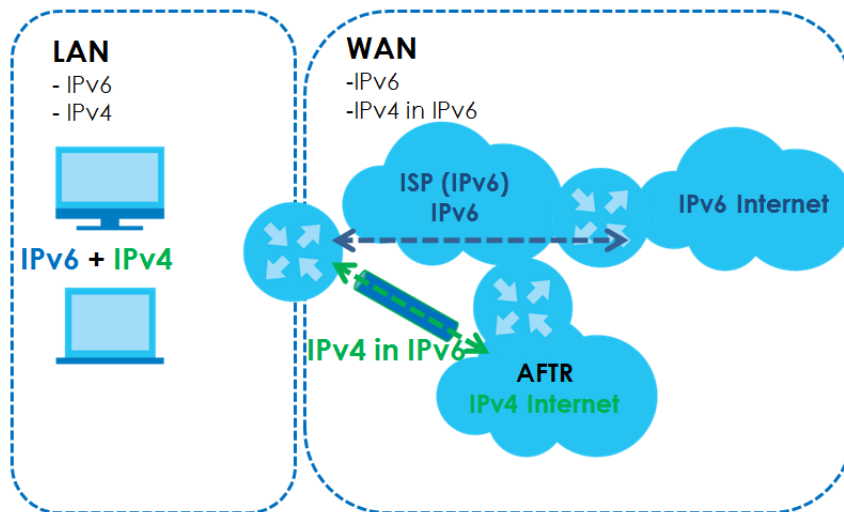


Dual Stack Lite

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 28 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 Broadband

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.

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

Figure 29 Network Setting > Broadband

#	Name	Type	Mode	Encaps...	802.1p	802.1q	IcmpPr...	NAT	Defaul# ...	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
2	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
3	ETHWAN	ETH	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	

The following table describes the labels in this screen.

Table 11 Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows whether it is an ATM, Ethernet or a PTM connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays N/A when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays N/A when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the 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 Edit icon to configure the WAN connection. Click the Delete icon to remove the WAN connection.

6.2.1 Add/Edit Internet Connection

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

6.2.1.1 Routing Mode

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

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

Figure 30 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)

Add New WAN Interface

General

Active: Enable Disable

Name:

Type: ADSL/VDSL over PTM ▼

Mode: Routing Bridge

Encapsulation: PPPoE ▼

IPv4/IPv6 Mode: IPv4 Only ▼

PPP Information

PPP User Name: admin

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

VLAN

Active: Enable Disable

802.1p: 0 ▼

802.1q: (1~4094)

MTU

MTU: 1492

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

6RD

6RD: Enable Disable

OK Cancel

The following table describes the labels in this screen.

Table 12 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)

LABEL	DESCRIPTION
General	
Active	Select Enable or Disable to activate or deactivate the interface.
Name	Specify a descriptive name for this connection.
Type	Select whether it is an ADSL/VDSL over PTM, ADSL over ATM connection or Ethernet.
Mode	Select Routing if your ISP give you one IP address only and you want multiple computers to share an Internet account.

Table 12 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select Routing in the Mode field. The choices depend on the connection type you selected. If your connection type is ADSL/VDSL over PTM , the choices are PPPoE and IPoE . If your connection type is ADSL over ATM , the choices are PPPoE , PPPoA , IPoE and IPoA . If your connection type is Ethernet , the choices are PPPoE and IPoE .
IPv4/IPv6 Mode	Select IPv4 Only if you want the VMG to run IPv4 only. Select IPv4 IPv6 DualStack to allow the VMG to run IPv4 and IPv6 at the same time. Select IPv6 Only if you want the VMG to run IPv6 only.
ATM PVC Configuration (These fields appear when the Type is set to ADSL over ATM .)	
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: <ul style="list-style-type: none"> • LLC/SNAP-BRIDGING: In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select IPoE or PPPoE in the Select DSL Link Type field. • VC/MUX: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the 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. • LLC/ENCAPSULATION: More than one protocol can be carried over the same VC. This is available only when you select PPPoA in the Encapsulation field. • LLC/SNAP-ROUTING: In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LLC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select IPoA in the Encapsulation field.
Service Category	Select UBR Without PCR for applications that are non-time sensitive, such as email. Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
PPP Information (This is available only when you select PPPoE or PPPoA in the Mode field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Select password unmask to show your entered password in plain text.
PPP Connection Trigger	Select when to have the VMG establish the PPP connection. Auto Connect - select this to not let the connection time out. On Demand - select this to automatically bring up the connection when the 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 Auto Connect in the PPP Connection Trigger field.

Table 12 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
PPPoE Passthrough	This field is available when you select PPPoE 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 IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
VLAN (These fields appear when the Type is set to ADSL/VDSL over PTM .)	
Active	Select this to enable VLAN on this WAN interface.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Routing Feature (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode 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	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. 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.
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 IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
	Select Obtain DNS Info Automatically if you want the VMG to use the DNS server addresses assigned by your ISP. Select Use Following Static DNS Address if you want the VMG to use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.

Table 12 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
Tunnel	The DS-Lite (Dual Stack Lite) fields display when you set the IPv4/IPv6 Mode field to IPv6 Only . Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 74 for more information.
Enable DS-Lite	This is available only when you select IPv6 Only in the IPv4/IPv6 Mode field. Select Enable 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 IPv6/IPv4 Mode field to IPv4 Only . See IPv6 Rapid Deployment on page 73 for more information.
6RD	Select Enable to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
	Select Manually Configured if you have the IPv4 address of the relay server. Otherwise, select Automatically configured by DHCP to have the VMG detect it automatically through DHCP. The Automatically configured by DHCP option is configurable only when you set the method of encapsulation to IPoE .
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
Border Relay IPv4 Address	When you select Manually Configured , specify the relay server's IPv4 address in this field.
DHCP Options (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
Request Options	Select Option 43 to have the VMG automatically add vendor specific information in the DHCP packets to request the vendor specific options from the DHCP server. Select Option 121 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 IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field.)	
Obtain an IPv6 Address Automatically	Select Obtain an IPv6 Address Automatically if you want to have the VMG use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Static IPv6 Address	Select Static IPv6 Address 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.
PrefixLength	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.

Table 12 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
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 IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field. You can enable IPv6 routing features in the following section.)	
MLD Proxy Enable	Select this check box to have the 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 IPv4 IPv6 DualStack or IPv6 Only in the IPv4/IPv6 Mode field. Configure the IPv6 DNS server in the following section.	
Obtain IPv6 DNS Info Automatically	Select Obtain IPv6 DNS Info Automatically to have the VMG get the IPv6 DNS server addresses from the ISP automatically.
Use Following Static IPv6 DNS Address	Select Use Following Static IPv6 DNS Address 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.
Apply	Click Apply to save your changes back to the VMG.
Cancel	Click Cancel to exit this screen without saving.

6.2.1.2 Bridge Mode

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

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

Figure 31 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM - Bridge Mode)

The following table describes the fields in this screen.

Table 13 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM - Bridge or Ethernet Mode)

LABEL	DESCRIPTION
General	
Active	Select Enable or Disable to activate or deactivate the interface.
Name	Enter a service name of the connection.
Type	Select ADSL/VDSL over PTM as the interface that you want to configure. The VMG uses the VDSL technology for data transmission over the DSL port.
Mode	Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select Bridge , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	
Active	Select Enable to enable VLAN on this WAN interface.
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 OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

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

Figure 32 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

The following table describes the fields in this screen.

Table 14 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

LABEL	DESCRIPTION
General	
Active	Select Enable or Disable to activate or deactivate the interface.
Name	Enter a service name of the connection.
Type	Select ADSL over ATM as the interface that you want to configure. The VMG uses the ADSL technology for data transmission over the DSL port.
Mode	Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select Bridge , you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
ATM PVC Configuration (These fields appear when the Type is set to ADSL over ATM .)	
VPI	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 14 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

LABEL	DESCRIPTION
Encapsulation	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: <ul style="list-style-type: none"> • LLC/SNAP-BRIDGING: In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select IPoE or PPPoE in the Encapsulation field. • VC/MUX: 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.
Service Category	Select UBR Without PCR for applications that are non-time sensitive, such as email. Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
VLAN	This section is available only when you select ADSL/VDSL over PTM in the Type field.
Active	Select Enable to enable VLAN on this WAN interface.
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 OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

6.3 Advanced Settings

Use the **Advanced** screen to enable or disable ADSL over PTM, 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

Table 15 VDSL Profiles (continued)

PROFILE	BANDWIDTH (MHZ)	NUMBER OF DOWNSTREAM CARRIERS	CARRIER BANDWIDTH (KHZ)	POWER (DBM)	MAX. DOWNSTREAM THROUGHPUT (MBIT/S)
30a	30	3479	8.625	14.5	200
35b	35.328	8192	4.3125	17.0	300

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

Figure 33 Network Setting > Broadband > Advanced

If xDSL setting is changed, the CPE will require a retrain.

DSL Capabilities

PhyR US : Enable Disable

PhyR DS : Enable Disable

Bitswap : Enable Disable

SRA : Enable Disable

DSL Line Mode

State (System will reboot once the config is changed!): Auto Single Bonding

DSL Modulation

PTM over ADSL : Enable Disable

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

35b Enable : Enable Disable

US0 : Enable Disable

Apply Cancel

The following table describes the labels in this screen.

Table 16 Network Setting > Broadband > Advanced

LABEL	DESCRIPTION
DSL Capabilities	
PhyR US	Enable or disable PhyR US (upstream) for upstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
PhyR DS	Enable or disable PhyR DS (downstream) for downstream transmission from the WAN. PhyR DS should be enabled if data being transmitted downstream is sensitive to noise. However, enabling PhyR DS can decrease the DS line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.

Table 16 Network Setting > Broadband > Advanced (continued)

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

Table 16 Network Setting > Broadband > Advanced (continued)

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

6.4 Ethernet WAN

Ethernet WAN is enabled by default. You can disable the Ethernet WAN port and have it act as the fifth Ethernet LAN port in the **Ethernet WAN** screen. Click **Network Setting > Broadband > Ethernet WAN** to display the following screen.

Figure 34 Network Setting > Broadband > Ethernet WAN

You can convert Ethernet WAN port to Ethernet LAN port 5 or restore the LAN port to WAN port.

Active : Enable Disable

Notes:

1. Active Enable, the Ethernet Port is WAN Ethernet.
2. Active Disable, the Ethernet Port is LAN Ethernet.
3. If Ethernet WAN cable and xDSL line are plugged at the same time, only Ethernet WAN will link up.

Apply Cancel

The following table describes the labels in this screen.

Table 17 Network Setting > Broadband > Ethernet WAN

LABEL	DESCRIPTION
Active	Select Enable to convert the fifth Ethernet LAN port to the Ethernet WAN port. Otherwise, select Disable .
Apply	Click Apply to save your changes back to the VMG.
Cancel	Click Cancel 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, and so on) 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.

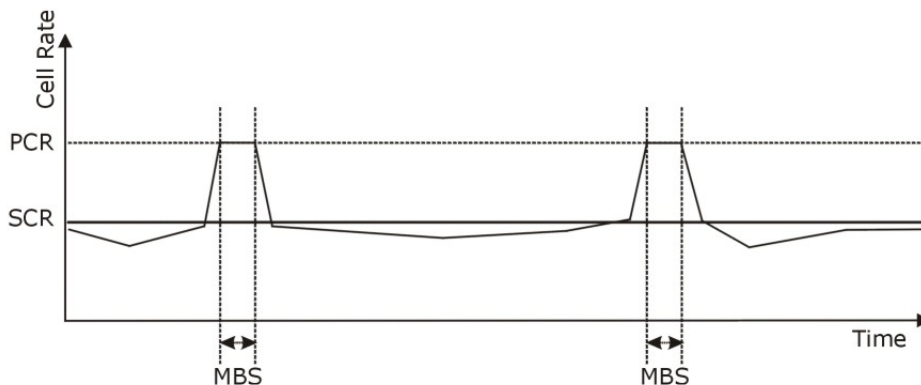
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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 35 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 Address

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 **WiFi** screen to enable WiFi, enter the SSID and select the wireless security mode ([Section 7.2 on page 94](#)).
- Use the **Guest WiFi** screen to set up multiple wireless networks on your VMG ([Section 7.3 on page 96](#)).
- Use the **WPS** screen to enable or disable WPS ([Section 7.4 on page 98](#)).
- Use the **Advanced** screen to configure wireless advanced features, such as the RTS/CTS Threshold ([Section 7.5 on page 98](#)).
- Use the **Channel Status** screen to scan WiFi channel noises and view the results ([Section 7.6 on page 101](#)).
- Use the **MESH** screen to enable or disable wireless roaming between the VMG and a wireless AP ([Section 7.7 on page 103](#)).

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.

Find Out More

See [Section 7.8 on page 105](#) for advanced technical information on wireless networks.

7.2 WiFi

Use this screen to view the wireless network name and password. You can also click the **Edit** icon to configure the settings.

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

Figure 36 Network Setting > Wireless > WiFi

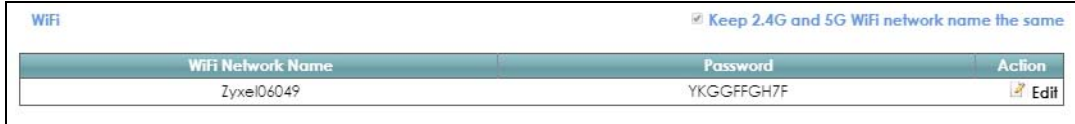
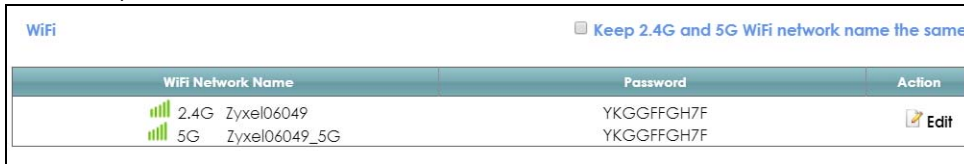


Figure 37 Network Setting > Wireless > WiFi (Without Keeping 2.4G and 5G WiFi Network Name the Same)



The following table describes the general WiFi labels in this screen.

Table 18 Network Setting > Wireless > WiFi

LABEL	DESCRIPTION
Keep 2.4G and 5G WiFi network name the same	Select this if you want the VMG use the same wireless network name, password, and security type for both the 2.4G and 5G band networks. Clear this to have the screen display the corresponding information for the 2.4G and 5G band networks. 2.4G is the frequency used by IEEE 802.11b/g/n wireless clients while 5G is used by IEEE 802.11a/ac wireless clients. Note: This setting is configurable only when the MESH function is disabled in the Network Setting > Wireless > MESH screen.
WiFi Network Name	This is the wireless network name.
Password	This is the password of the wireless network.
Action	Click the Edit icon to configure the wireless network settings.

7.2.1 WiFi Edit

Use this screen to view and configure the wireless network name, password and security type. Click the **Edit** icon on the **Network Setting > Wireless > WiFi** screen to open the **WiFi Edit** screen.

Figure 38 Network Setting > Wireless > WiFi > Edit

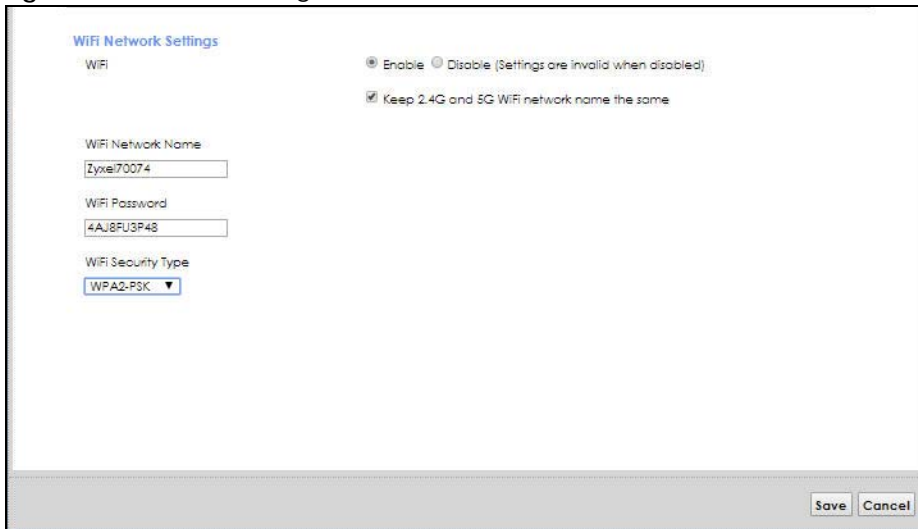
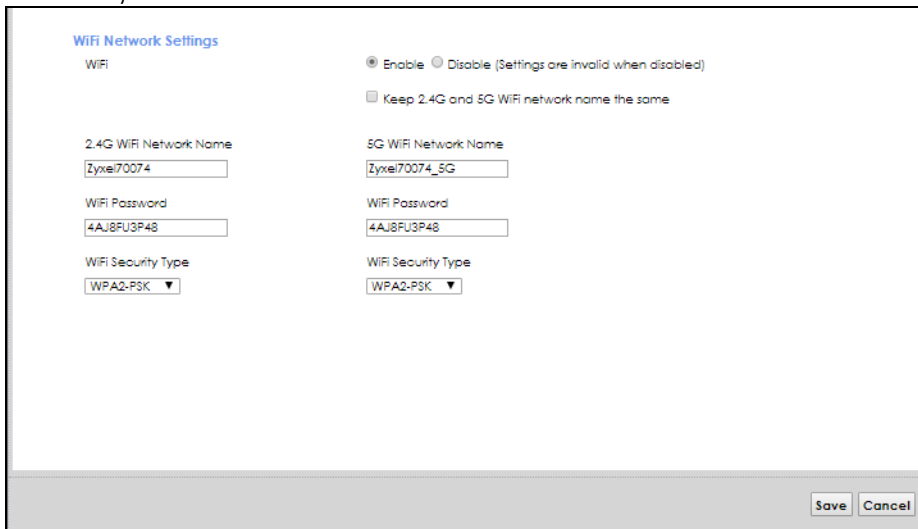


Figure 39 Network Setting > Wireless > WiFi > Edit (Without Keeping 2.4G and 5G WiFi Network Name The Same)



The following table describes the general WiFi labels in this screen.

Table 19 Network Setting > Wireless > WiFi > Edit

LABEL	DESCRIPTION
WiFi	You can Enable or Disable WiFi in this field.
Keep 2.4G and 5G WiFi network name the same	Select this if you want the VMG use the same wireless network name, password, and security type for both the 2.4G and 5G networks. Clear this to have the screen display the corresponding information for the 2.4G and 5G band networks. Note: This setting is configurable only when the MESH function is disabled in the Network Setting > Wireless > MESH screen.
WiFi Network Name	This is the wireless network name.
WiFi Password	This is the password of the wireless network.

Table 19 Network Setting > Wireless > WiFi > Edit (continued)

LABEL	DESCRIPTION
WiFi Security Type	Select WPA2-PSK to add security on this wireless network. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers wireless clients a better and secure connection. The wireless clients which want to associate to this network must have same wireless security settings as the VMG. Or you can select No Security to allow any client to associate this network and the guest wireless network of the same wireless band without any data encryption or authentication.
Save	Click Save to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.3 Guest WiFi

This screen allows you to enable and configure multiple wireless networks for guests on the VMG.

You can view/configure one guest WiFi network and three extra WiFi networks on this screen. The extra WiFi networks include two extra 2.4G WiFi networks and one extra 5G WiFi network. The only difference between guest WiFi and extra WiFi is that you can configure the number of hours to keep the guest WiFi network on before the VMG turns it off.

Click **Network Setting > Wireless > Guest WiFi**. The following screen displays.

Figure 40 Network Setting > Wireless > Guest WiFi

Guest WiFi			
<input type="checkbox"/> Enable Guest WiFi			
WiFi Network Name	Password	Action	
Zyxel06049_guest	YKGGFFGH		
Extra WiFi			
Band	WiFi Network Name	Password	Action
2.4G	Zyxel6049_extra2	YKGGFFGH7F	
2.4G	Zyxel6049_extra3	YKGGFFGH7F	
5G	Zyxel6049_extra2_5G	YKGGFFGH7F	

The following table describes the labels in this screen.

Table 20 Network Setting > Wireless > Guest WiFi

LABEL	DESCRIPTION
Guest WiFi	
Enable Guest WiFi	Select this to enable the guest wireless network.
WiFi Network Name	This field displays the guest WiFi network name.
Password	This field displays the password used to connect to this guest wireless network.
Action	Click the Edit icon to configure the WiFi network profile.
Extra WiFi	
Band	This field indicates whether this extra WiFi network uses 2.4G or 5G band.
WiFi Network Name	This field displays the extra WiFi network name.

Table 20 Network Setting > Wireless > Guest WiFi (continued)

LABEL	DESCRIPTION
Password	This field displays the password used to connect to this extra wireless network.
Action	Click the Edit icon to configure the WiFi network profile.

7.3.1 Edit Guest WiFi

Use this screen to edit a guest WiFi or an extra WiFi settings. Click an **Edit** icon in the **Guest WiFi** screen. The following screen displays.

Note: Guest WiFi and Extra WiFi share the same security type with the main WiFi network setting configured in the **Network Setting > Wireless > WiFi > Edit** screen.

Figure 41 Network Setting > Wireless > Guest WiFi > Edit (For Guest WiFi)

The following table describes the fields in this screen.

Table 21 Network Setting > Wireless > Guest WiFi > Edit

LABEL	DESCRIPTION
Guest WiFi	You can Enable or Disable WiFi in this field.
2.4G/5G WiFi Network Name	Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
WiFi Password	Type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
Time Period Duration (hours)	This field is only available when you are editing for the guest WiFi network, rather than for an extra WiFi network. Select the number of hours that you want to keep this wireless network on right after you apply the setting. The VMG automatically turns it off when time is up. Select Always on to have the VMG never turn the wireless network off.
Save	Click Save to save your changes.
Cancel	Click Cancel to exit this screen without saving.

7.4 WPS

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 7.8.8.2 on page 111](#) for more information about WPS.

Note: The VMG applies the security settings of the main 2.4G or 5G wireless profile (see [Section 7.2.1 on page 94](#)). If you want to use the WPS feature, make sure you have enabled **WPS** in the **Network Setting > Wireless > Advanced** screen.

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

Figure 42 Network Setting > Wireless > WPS

Connection Type	Wi-Fi Name	WPS
2.4G Wi-Fi	Zyxel06049	Connect
5G Wi-Fi	Zyxel06049	Connect

Activate WPS on wireless client within 2 minutes after clicking "Connect".

The following table describes the labels in this screen.

Table 22 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
Connection Type	This field indicates whether you will apply WPS to the 2.4G or 5G wireless network.
Wi-Fi Name	This field displays the wireless network name.
WPS	Click the Connect button to add another WPS-enabled wireless device (within wireless range of the VMG) to the wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the WPS button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.

7.5 Advanced Settings

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

See [Section 7.8.2 on page 107](#) for detailed definitions of the terms listed in this screen.

Figure 43 Network Setting > Wireless > Advanced

The configurations below are the advanced wireless settings.

2.4G Advanced Settings

Hide WiFi Network Name :

Channel :

Bandwidth :

802.11 Mode :

RTS/CTS Threshold :

Fragmentation Threshold :

Output Power :

Beacon Interval : ms

DTIM Interval : ms

802.11 Protection :

Preamble :

WPS :

OBSS Coexistence : Enable Disable

WMM : Enable Disable

WMM Automatic Power Save Delivery : Enable Disable

5G Advanced Settings

Hide WiFi Network Name :

Channel :

802.11 Mode :

RTS/CTS Threshold :

Fragmentation Threshold :

Output Power :

Beacon Interval : ms

DTIM Interval : ms

802.11 Protection :

Preamble :

WPS :

OBSS Coexistence : Enable Disable

WMM : Enable Disable

WMM Automatic Power Save Delivery : Enable Disable

DFS Channel : Enable Disable

MU-MIMO : Enable Disable

The following table describes the labels in this screen.

Table 23 Network Setting > Wireless > Advanced

LABEL	DESCRIPTION
2.4G Advanced Settings / 5G Advanced Settings	
Hide WiFi Network Name	Select this check box to hide the wireless band's network name (SSID) in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool or any wireless clients. Note: This setting only applies to the main 2.4G and 5G wireless networks. It does not apply to the guest and extra wireless networks configured in the Network Setting > Wireless > Guest WiFi screen.
Channel	Select a specific channel the VMG uses for the wireless band. Select Auto to have the VMG automatically determine a channel to use.

Table 23 Network Setting > Wireless > Advanced (continued)

LABEL	DESCRIPTION
802.11 Mode	<p>Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the VMG.</p> <p>Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the VMG.</p> <p>Select 802.11n Only to allow only IEEE 802.11n compliant WLAN devices to associate with the VMG.</p> <p>Select 802.11b/g Mixed 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.</p> <p>Select 802.11b/g/n Mixed 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.</p>
RTS/CTS Threshold	<p>Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake.</p> <p>Enter a value between 0 and 2347.</p>
Fragmentation Threshold	<p>This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.</p>
Output Power	<p>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: 20%, 40%, 60%, 80% or 100%.</p>
Beacon Interval	<p>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.</p> <p>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.</p>
DTIM Interval	<p>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.</p>
802.11 Protection	<p>Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic).</p> <p>Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance.</p> <p>Select Off to disable 802.11 protection. The transmission rate of your VMG might be reduced in a mixed-mode network.</p> <p>This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only.</p>
Preamble	<p>Select a preamble type from the drop-down list box. Choices are Long or Short. See Section 7.8.7 on page 110 for more information.</p> <p>This field is configurable only when you set 802.11 Mode to 802.11b.</p>
WPS	<p>Select this to enable WPS function for the wireless network.</p> <p>Note: This setting only applies to the main 2.4G and 5G wireless networks. It does not apply to the guest and extra wireless networks configured in the Network Setting > Wireless > Guest WiFi screen.</p> <p>Note: This setting is configurable only when the MESH function is disabled in the Network Setting > Wireless > MESH screen.</p>
OBSS Coexistence	<p>Select Enable to allow the coexistence of 20 MHz and 40 MHz Overlapping Basic Service Sets (OBSS) in wireless local area networks. Select Disabled to disable this feature.</p>

Table 23 Network Setting > Wireless > Advanced (continued)

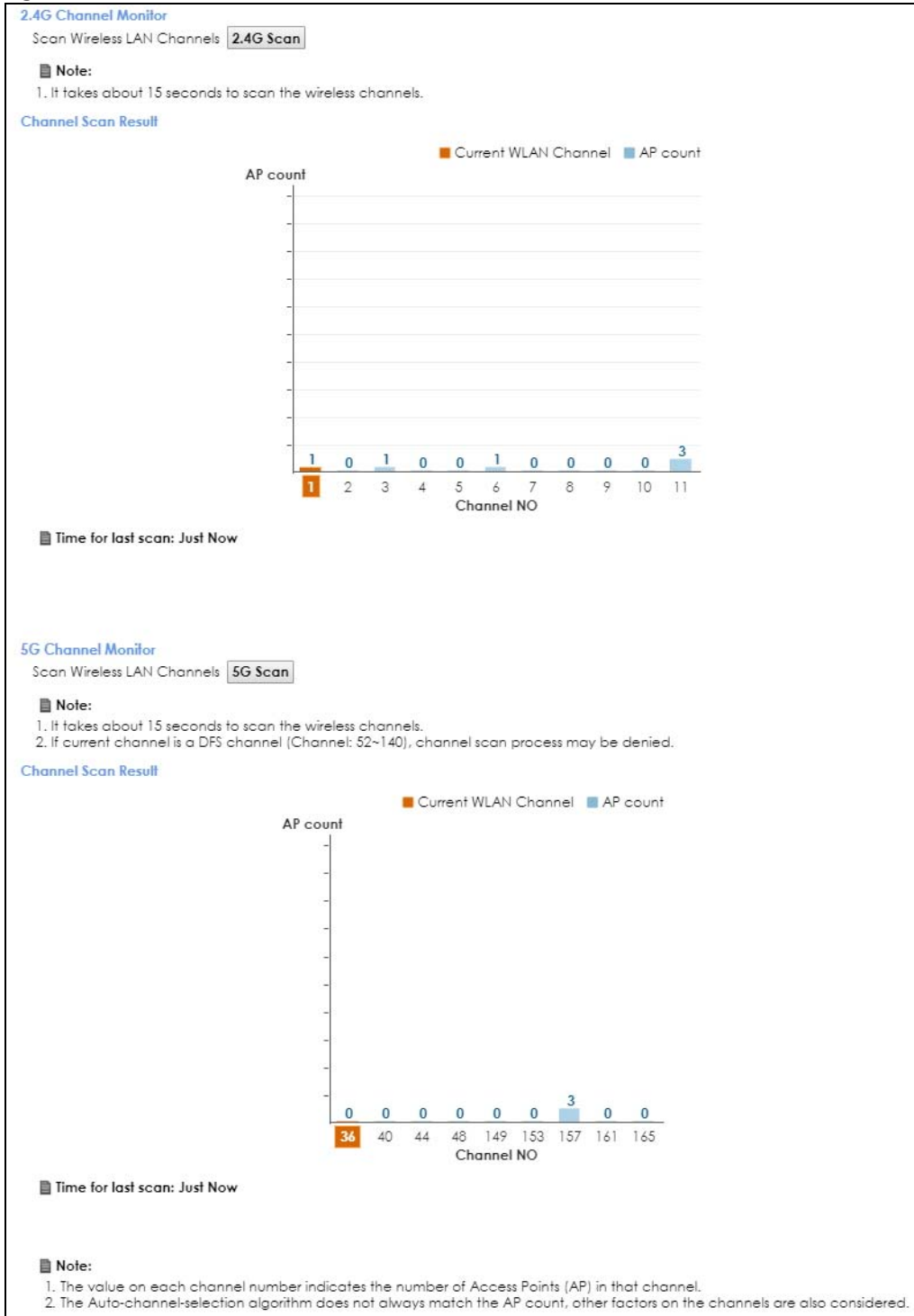
LABEL	DESCRIPTION
WMM	Select Enable to have the VMG automatically give the wireless network a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Note: At the time of writing, WMM is enabled by default and it is not changeable.
WMM Automatic Power Save Delivery	Select Enable 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.
DFS Channel	This option is only available for the 5G band. Disabling it will force Channel in Network Setting > Wireless > General to be set to Auto . Enabling this option allows the use of DFS channel, ranging from 52~144, which may interfere with some RADAR devices. If your device is operating near an area known to have RADAR devices, it is recommended to disable DFS Channel to avoid interfering with their signal. Note: As of this writing, this option is not available for VMG9827-B50A.
MU-MIMO	Select Enable to allow accelerated and simultaneous WiFi service when there are multiple MU-MIMO (Multi User-Multiple input, Multiple Output) ready devices connected to the VMG.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.6 Channel Status

Use the **Channel Status** screen to scan the number of devices which are using 2.4G and/or 5G WiFi channels and view the results. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown. Click **2.4G Scan** and/or **5G Scan** to scan the 2.4G and/or 5G wireless band channels. You can view the results in the corresponding **Channel Scan Result** section.

Note: The **2.4G Scan** or **5G Scan** button only works when the VMG uses 20 MHz for the wireless channel width. You can go to the **Network Setting > Wireless > Advanced** screen, and then change the channel width setting in the **Bandwidth** field.

Figure 44 Network Setting > Wireless > Channel Status



7.7 MESH

Use this screen to enable or disable Zyxel MESH (Multy Pro). It supports AP steering and Band steering. AP steering allows wireless clients to roam seamlessly between Multy-Pro-supported devices in your MESH network by using the same SSID and WiFi password. Also, AP steering helps monitor wireless clients and drop their connections to optimize the VMG bandwidth when the clients are idle or have a low signal.

When a wireless client is dropped, it has the opportunity to steer to a Multy-Pro-supported device with a strong signal. Band steering allows dual band wireless clients to steer from one band to another.

A MESH network consists of a controller, the VMG, and a maximum of three Multy-Pro-supported extenders.

When Multy Pro is enabled:

- One Connect will be enabled and grayed out automatically. It's used for the communication between the VMG and a Multy-Pro-supported extenders for the setup of a MESH network.
- The SSID and WiFi password of the main 2.4G wireless network will be copied to the main 5G wireless network.

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

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

- 1 Prepare a Multy-Pro-supported extender(s) from Zyxel.

The following table lists the Multy-Pro-supported extenders from Zyxel at the time of writing.

Table 24 Multy-Pro-Supported Extenders from Zyxel

MODELS
WAP6804
WAP6906
WAP7205

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

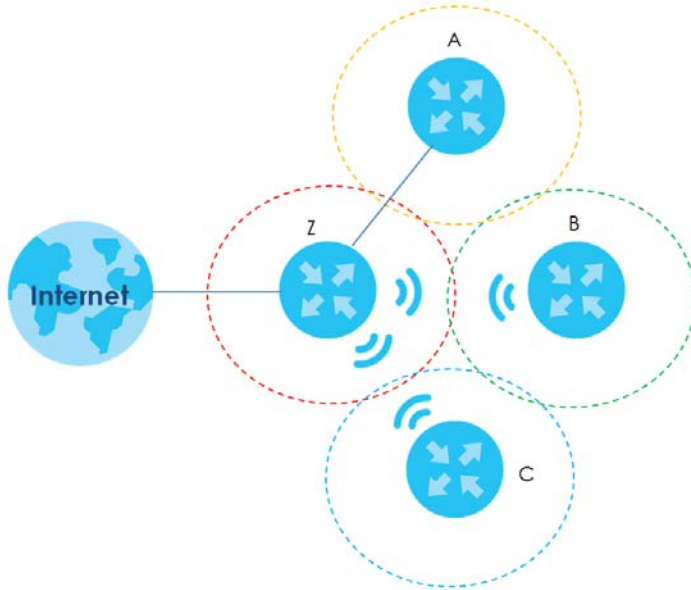
Configurations on the VMG

- 1 If the Multy-Pro-supported extender is in repeater mode, enable WiFi. See [Section 7.2.1 on page 94](#) or [Section 3.2 on page 39](#) for more information on enabling WiFi.
- 2 Enable Zyxel MESH in the **Network > Wireless > MESH** screen.

- 3 Press the **WPS** button for more than five seconds on the VMG.
Or
Click **Add Extender** in the Multy Pro App. Install from Google Play or the Apple App store.

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

Figure 45 MESH Application



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

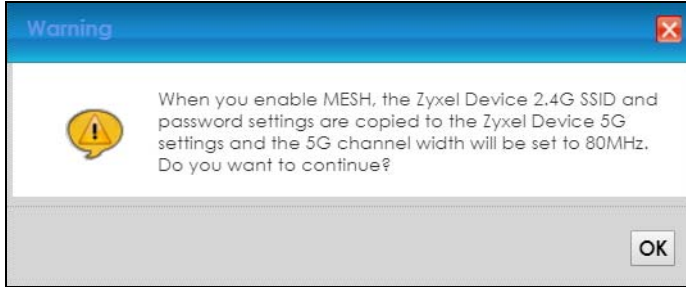
Figure 46 Network Setting > Wireless > MESH

MESH : Enable Disable

The following table describes the labels in this screen.

Table 25 Network Setting > Wireless > MESH

LABEL	DESCRIPTION
MESH	<p>Select Enable to activate MESH and have the VMG apply the wireless name, password, and security type of the main 2.4G wireless network to the main 5G wireless network. A warning displays when you select Enable (see Figure 47 on page 105).</p> <p>Note: When MESH is enabled, the following settings become not configurable:</p> <ul style="list-style-type: none"> • The Keep 2.4G and 5G WiFi network name the same setting in the Network Setting > Wireless > WiFi and Network Setting > Wireless > WiFi > Edit screens. • The WPS setting in the Network Setting > Wireless > Advanced screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

Figure 47 Network Setting > Wireless > MESH > A Warning When You Enable MESH

7.8 Technical Reference

This section discusses WiFi in depth. For more information, see [Appendix B on page 299](#).

7.8.1 Wireless Network Overview

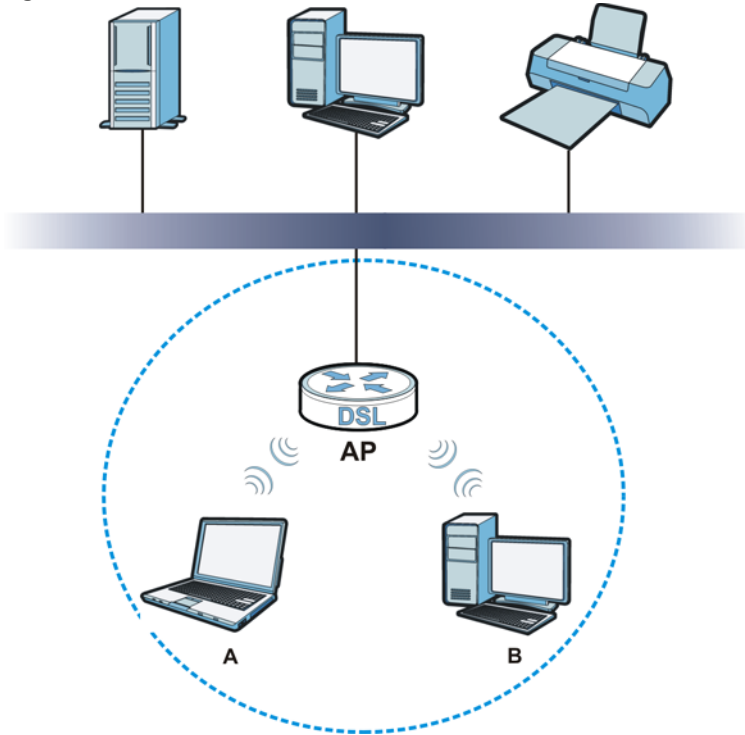
Wireless networks consist of wireless clients, access points and bridges.

- 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 48 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.

7.8.2 Additional Wireless Terms

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

Table 26 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.

7.8.3 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.

Security standards vary in effectiveness. The WPA2-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.

7.8.3.1 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.

7.8.3.2 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.

7.8.3.3 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. 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.

7.8.3.4 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.

Note: It is recommended that wireless networks use **WPA2-PSK** encryption.

-
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.

Encryption uses 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.

7.8.4 Signal Problems

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

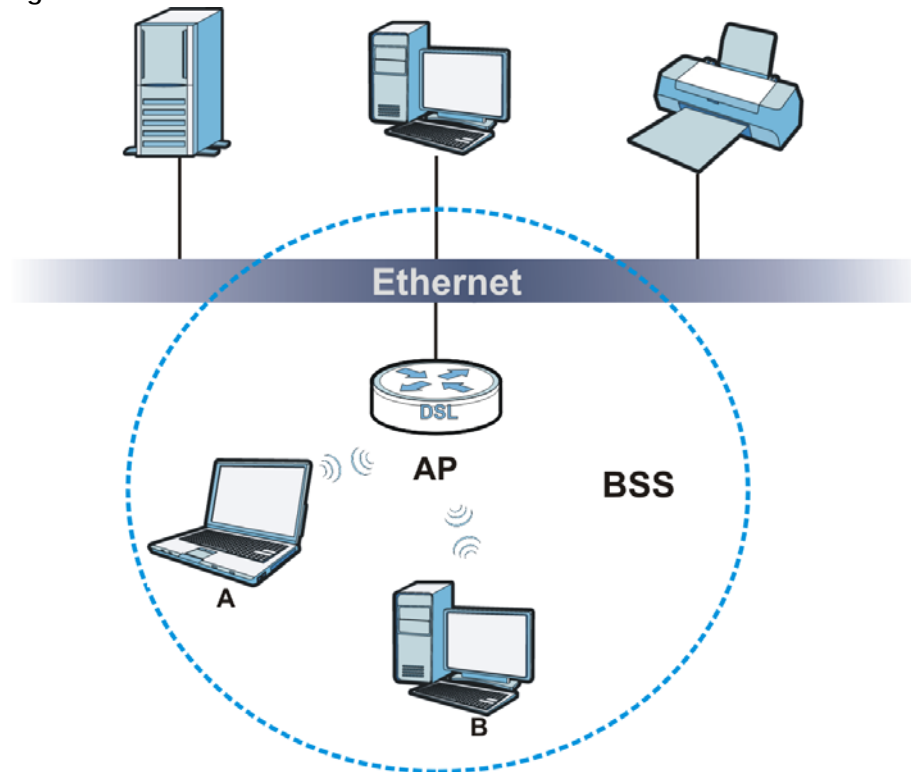
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters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

7.8.5 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 49 Basic Service Set



7.8.6 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.

7.8.6.1 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.

7.8.7 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.

7.8.8 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 press a button (on the device itself, or in its configuration utility) 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.

7.8.8.1 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 [Figure 42 on page 98](#)).
- 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.

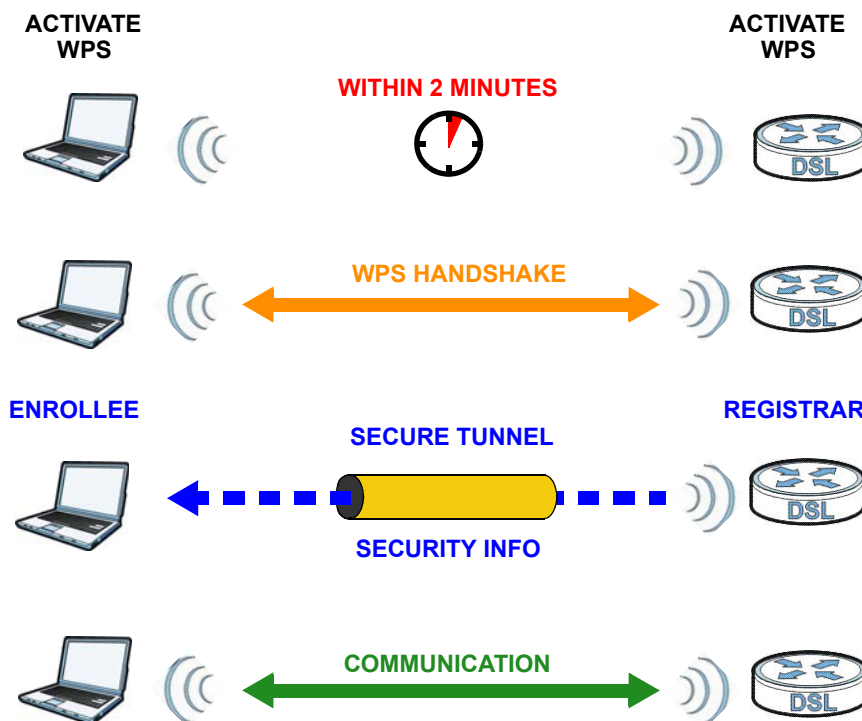
If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

7.8.8.2 How WPS Works

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

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

Figure 50 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.

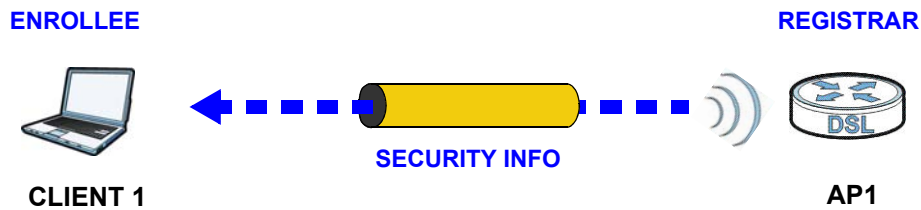
By default, a WPS device is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

7.8.8.3 Example WPS Network Setup

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

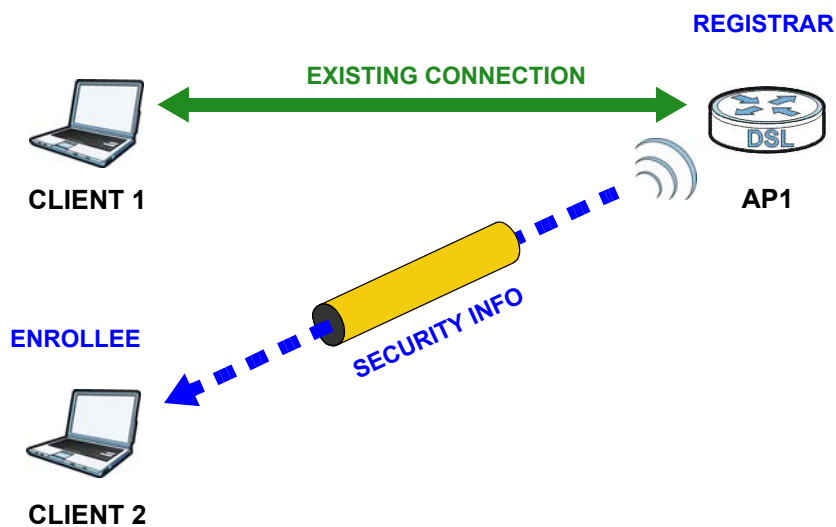
The following figure shows an example network. In step 1, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to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

Figure 51 WPS: Example Network Step 1



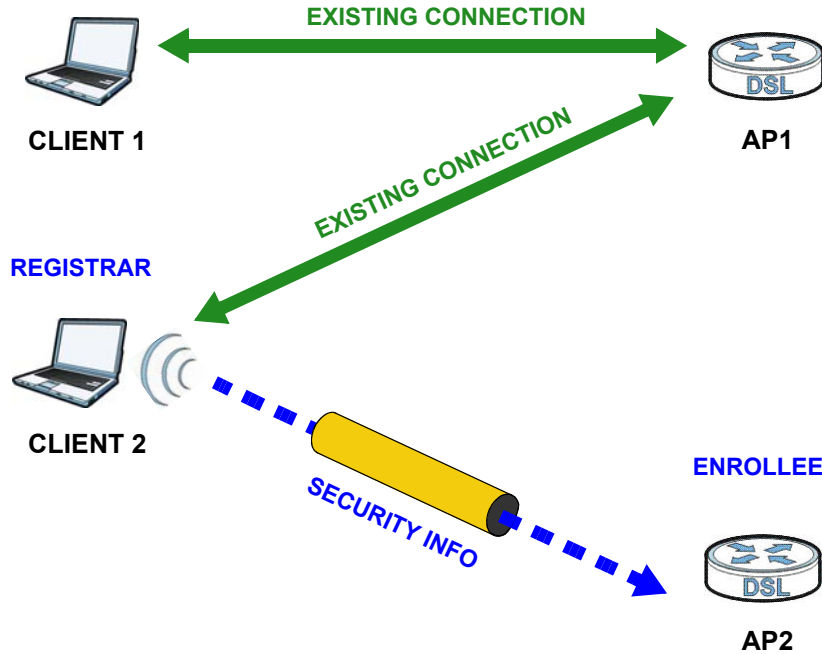
In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar,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

Figure 52 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 53 WPS: Example Network Step 3



7.8.8.4 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access

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

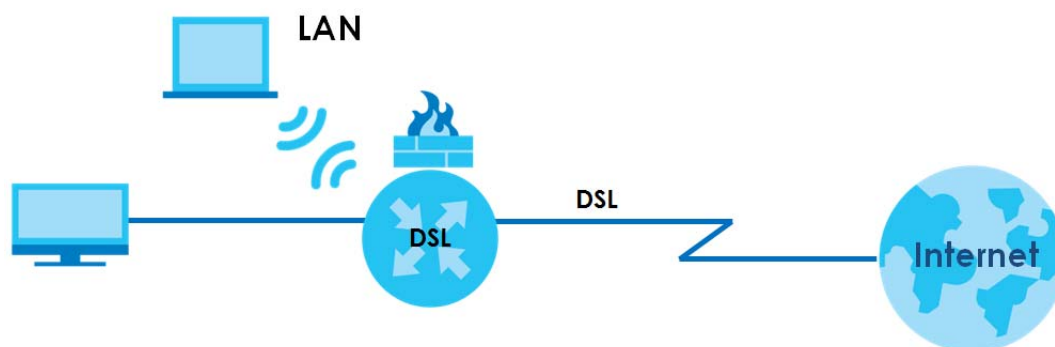
CHAPTER 8

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 118](#)).
- 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 122](#)).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the VMG ([Section 8.4 on page 123](#)).
- Use the **Additional Subnet** screen to configure IP alias and public static IP ([Section 8.5 on page 126](#)).
- 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 128](#)).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. ([Section 8.7 on page 128](#)).
- 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 129](#)).

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, and so forth) 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

Identify UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows 7). 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 159](#) 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 125](#) for examples of installing and using UPnP.

Find Out More

See [Section 8.9 on page 130](#) 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 LAN Setup

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 **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 54 Network Setting > Home Networking > LAN Setup

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

Interface Group
Group Name: Default

LAN IP Setup
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

IGMP Snooping
Active: Enable Disable
IGMP Mode: Standard Mode Blocking Mode

DHCP Server State
DHCP: Enable Disable DHCP Relay

IP Addressing Values
Beginning IP Address: 192.168.1.2
Ending IP Address: 192.168.1.254
Auto reserve IP for the same host: Enable Disable

DHCP Server Lease Time
1 Days 0 Hours 0 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 Prefix Setup
 Delegate prefix from WAN: Default
 Static

MLD Snooping
Active: Enable Disable
MLD Mode: Standard Mode Blocking Mode

LAN IPv6 Address Assign Setup
Stateless

LAN IPv6 DNS Assign Setup
From DHCPv6 Server

DHCPv6 Configuration
DHCPv6 Active: DHCPv6 Server

IPv6 Router Advertisement State
RADVD Active: Enable

IPv6 DNS Values
IPv6 DNS Server 1: From ISP
IPv6 DNS Server 2: From ISP
IPv6 DNS Server 3: From ISP

DNS Query Scenario:
IPv4/IPv6 DNS Server

Apply **Cancel**

The following table describes the fields in this screen.

Table 27 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group name for which you want to configure LAN settings. See Chapter 15 on page 185 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). Your VMG automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IGMP Snooping	
Active	Select Enable to allows the VMG to passively learn multicast group.
IGMP Mode	Select Standard Mode to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select Blocking Mode to block all unknown multicast packets from the WAN.
DHCP Server State	
DHCP	Select Enable to have the VMG act as a DHCP server or DHCP relay agent. Select Disable to stop the DHCP server on the VMG. Select DHCP Relay to have the VMG forward DHCP request to the DHCP server.
DHCP Relay Server Address	This field is only available when you select DHCP Relay in the DHCP field.
IP Address	Enter the IPv4 address of the actual remote DHCP server in this field.
IP Addressing Values	This field is only available when you select Enable in the DHCP field.
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Select Enable 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 Enable in the DHCP field.
Days/Hours/Minutes	Enter the lease time of the DHCP server.
DNS Values	This field is only available when you select Enable in the DHCP field.
DNS	Select From ISP if your ISP dynamically assigns DNS server information. Select DNS Proxy if you have the DNS proxy service. The VMG redirects clients' DNS queries to a DNS server for resolving domain names. Select Static 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.

Table 27 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 Mode Setup	
IPv6 Active	Select Enable 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.
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 Prefix Setup	
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the VMG's LAN IPv6 address.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
Active	Select Enable to activate MLD Snooping on the VMG. This allows the VMG to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.
MLD Mode	Select Standard Mode to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select Blocking Mode to block all unknown multicast packets from the WAN.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: <ul style="list-style-type: none"> • Stateless: The 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. • Stateful: 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.
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"> • From Router Advertisement: The VMG provides DNS information through router advertisements. • From DHCPv6 Server: The VMG provides DNS information through DHCPv6. • From RA & DHCPv6 Server: The VMG provides DNS information through both router advertisements and DHCPv6.
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. DHCPv6 Server 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 From ISP if your ISP dynamically assigns IPv6 DNS server information. Select User-Defined if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the VMG passes to the DHCP clients. Select None if you do not want to configure IPv6 DNS servers.

Table 27 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Query Scenario	<p>Select how the VMG handles clients' DNS information requests.</p> <ul style="list-style-type: none"> IPv4/IPv6 DNS Server: The VMG forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. IPv6 DNS Server Only: The VMG forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives. IPv4 DNS Server Only: The VMG forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. IPv6 DNS Server First: 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. IPv4 DNS Server First: 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.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

8.3 Static DHCP

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 55 Network Setting > Home Networking > Static DHCP

When any of the LAN clients on your network want an assigned fixed IP address, add a static lease for each LAN client. You may need to know the clients' MAC addresses in advance in order to process the setup quickly.

Static DHCP Configuration

#	Status	MAC Address	IP Address	Modify
---	--------	-------------	------------	--------

The following table describes the labels in this screen.

Table 28 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	<p>The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).</p> <p>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.</p>

Table 28 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the Edit icon to have the IP address field editable and change it. Click the Delete icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

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

Figure 56 Static DHCP: Static DHCP Configuration/Edit

The following table describes the labels in this screen.

Table 29 Static DHCP: Static DHCP Configuration/Edit

LABEL	DESCRIPTION
Active	Select this to activate the connection between the client and the VMG.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See Chapter 15 on page 185 for how to create a new interface group.
IP Type	This field displays IPv4 for the type of the DHCP IP address. At the time of writing, it is not allowed to select other type.
Select Device Info	Select a device or computer from the drop-down list or select Manual Input to manually enter a device's MAC address and IP address in the following fields.
MAC Address	If you select Manual Input , enter the MAC address of a computer on your LAN.
IP Address	If you select Manual Input , enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.4 UPnP

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 117](#) 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 57 Network Setting > Home Networking > UPnP

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

UPnP State
UPnP Enable Disable

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

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

#	Description	Destination IP Address	External Port	Internal Port	Protocol

The following table describes the labels in this screen.

Table 30 Network Setting > Home Networking > UPnP

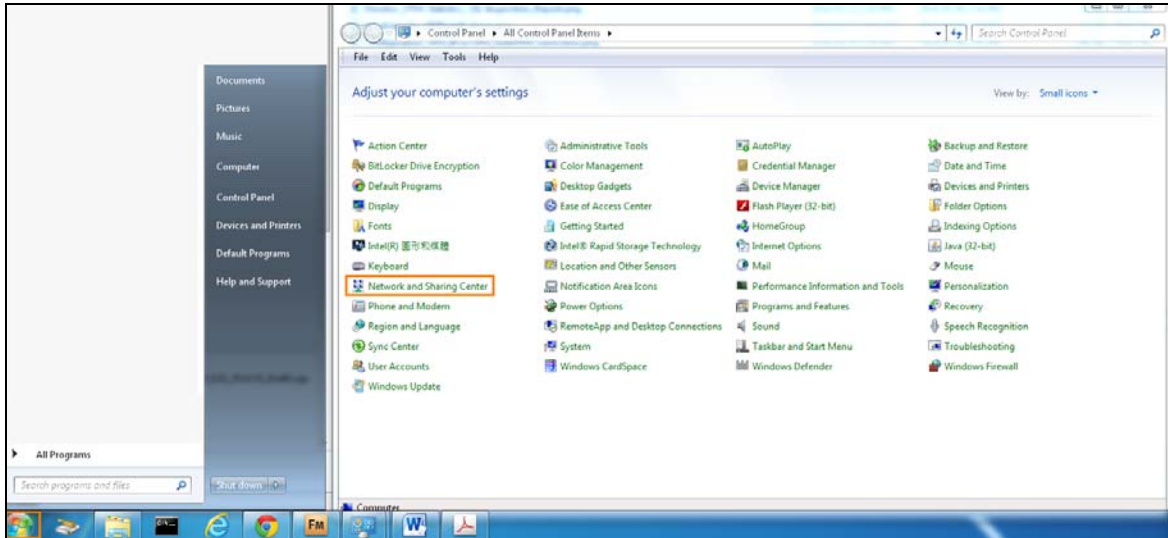
LABEL	DESCRIPTION
UPnP	Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the VMG's IP address (although you must still enter the password to access the Web Configurator).
UPnP NAT-T	Select Enable to allow UPnP-enabled applications to automatically configure the 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 Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.4.1 Turn On UPnP in Windows 7 Example

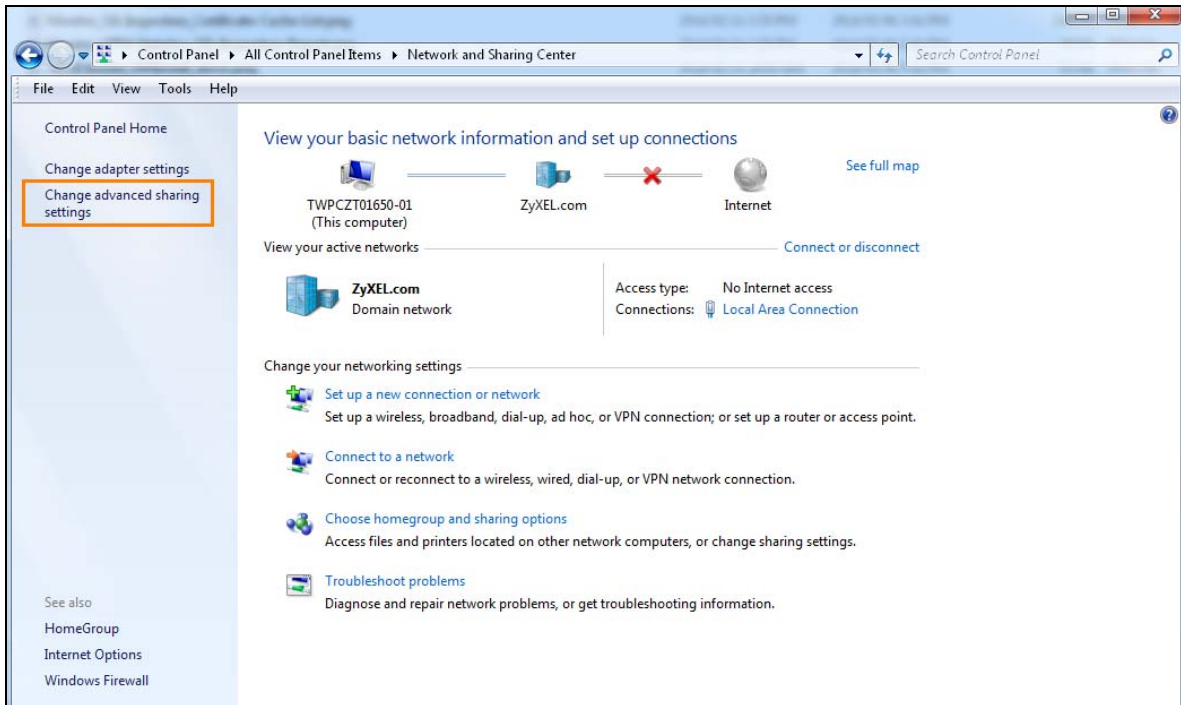
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the VMG.

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

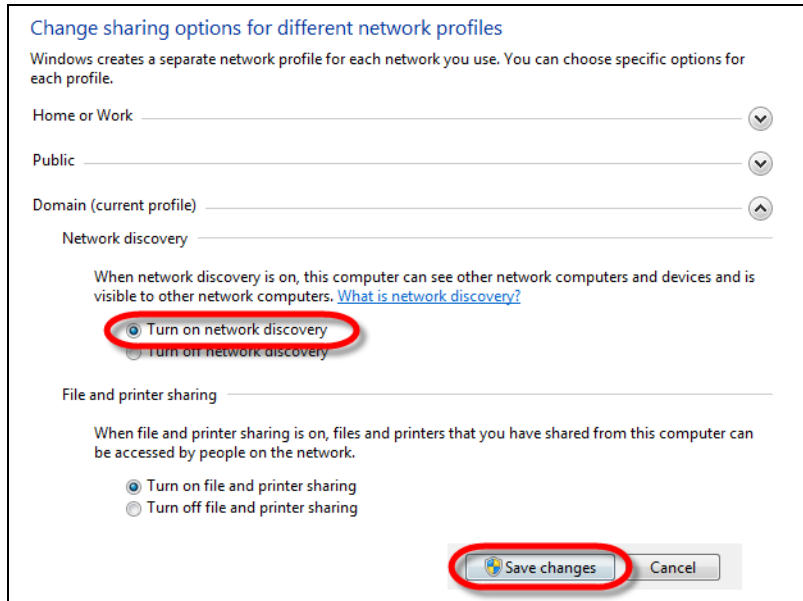
- 1 Click the start icon, **Control Panel** and then the **Network and Sharing Center**.



- 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 Additional Subnet

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 58 Network Setting > Home Networking > Additional Subnet

The following table describes the labels in this screen.

Table 31 Network Setting > Home Networking > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See Chapter 15 on page 185 for how to create a new interface group.
Active	Select Enable 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 Enable to enable 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 IPv4 subnet mask provided by your ISP.
Offer Public IP by DHCP	Select Enable to enable the VMG to provide public IP addresses by DHCP server.
Enable ARP Proxy	Select Enable to enable the ARP (Address Resolution Protocol) proxy.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.6 STB Vendor ID

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 Set-Top Box continues to use an IP address that gets assigned to another device. Use this screen to configure the Vendor IDs of connected Set-Top Boxes, 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 59 Network Setting > Home Networking > STB Vendor ID

The following table describes the labels in this screen.

Table 32 Network Setting > Home Networking > STB Vendor ID

LABEL	DESCRIPTION
Vendor ID 1~5	These are Set-Top Box'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 Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

8.7 Wake on LAN

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 60 Network Setting > Home Networking > Wake on LAN

The following table describes the labels in this screen.

Table 33 Network Setting > Home Networking > Wake on LAN

LABEL	DESCRIPTION
Wake by Address	Select Manual and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the 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 TFTP Server Name

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 that support the TFTP booting mechanism, can then use the TFTP server address or domain name for initial system settings 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 61 Network Setting > Home Networking > TFTP Server Name

The following table describes the labels in this screen.

Table 34 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 Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

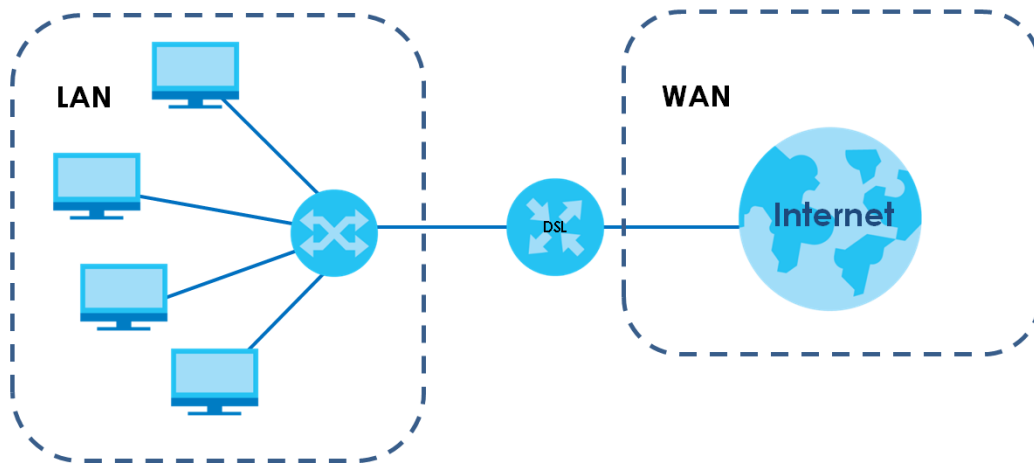
8.9 Technical Reference

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 62 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

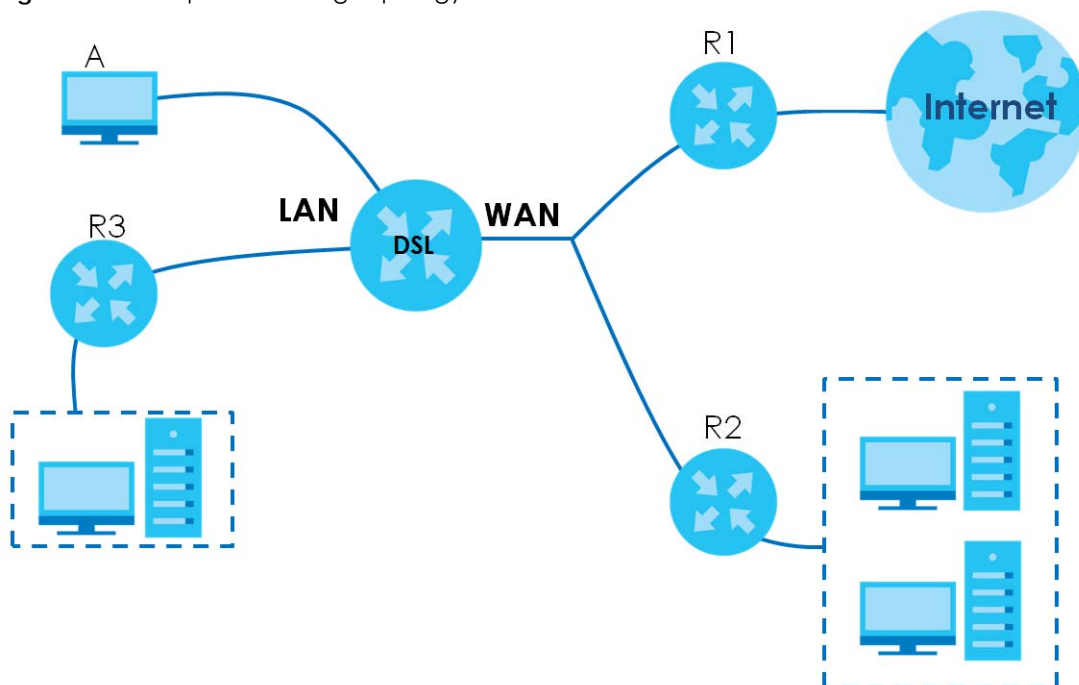
Routing

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 63 Example of Routing Topology



9.2 Routing

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 64 Network Setting > Routing > Static Route

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

Add New Static Route

#	Status	Name	Destination IP	Subnet Mask/Prefix Length	Gateway	Interface	Modify
---	--------	------	----------------	---------------------------	---------	-----------	--------

The following table describes the labels in this screen.

Table 35 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to configure a new static route.
#	This is the index number of the entry.
Status	This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask/Prefix Length	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the WAN interface used for this static route.
Modify	Click the Edit icon to edit the static route on the VMG. Click the Delete 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 65 Routing: Add/Edit

The following table describes the labels in this screen.

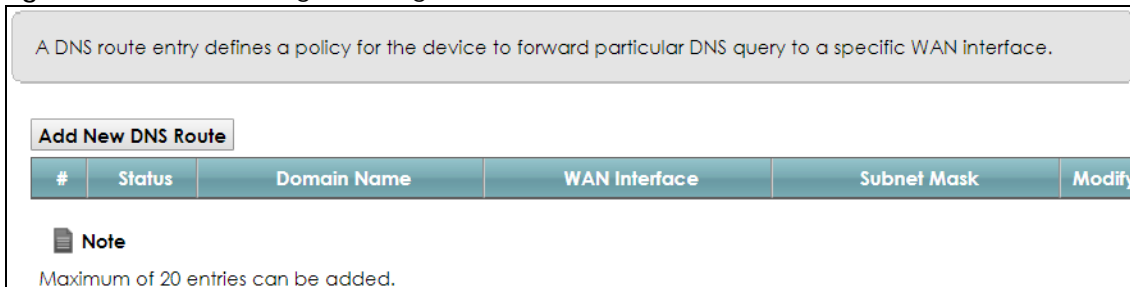
Table 36 Routing: Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route. Select Enable to activate the static route. Select Disable 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 IPv4 or IPv6 .
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 Enable .
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 OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.3 DNS Route

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

Figure 66 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

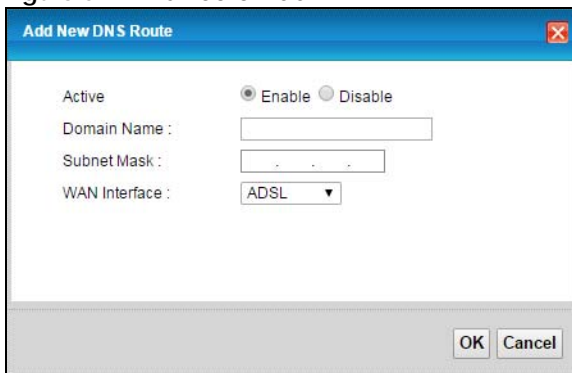
Table 37 Network Setting > Routing > DNS Route

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

9.3.1 DNS Route Add

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 67 DNS Route Add



The following table describes the labels in this screen.

Table 38 DNS Route Add

LABEL	DESCRIPTION
Active	Select to enable or disable this DNS route.
Domain Name	Enter the domain name of the DNS route entry.

Table 38 DNS Route Add (continued)

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

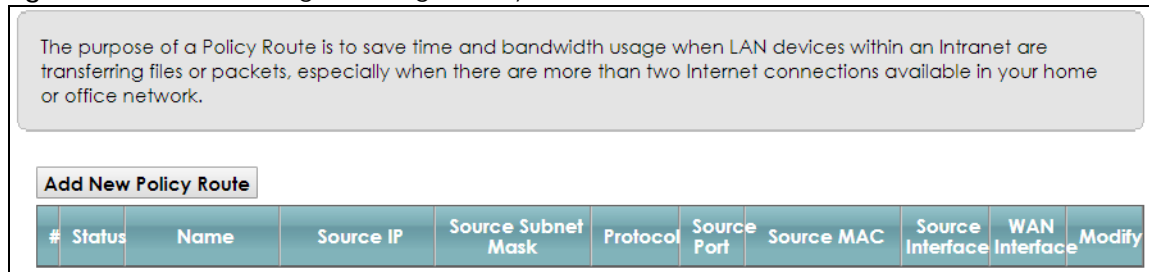
9.4 Policy Route

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 68 Network Setting > Routing > Policy Route



The following table describes the labels in this screen.

Table 39 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.

Table 39 Network Setting > Routing > Policy Route (continued)

LABEL	DESCRIPTION
Source Interface	This is the interface from which the matched traffic is sent.
WAN Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the Edit icon to edit this policy. Click the Delete icon to remove a policy from the 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 69 Policy Route: Add/Edit

The following table describes the labels in this screen.

Table 40 Policy Route: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this 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 (TCP or UDP).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface	Type the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the Broadband screens.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.5 RIP Overview

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

9.5.1 RIP

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

Figure 70 RIP

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

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

The following table describes the labels in this screen.

Table 41 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 Passive 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 Active 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 Apply to save your changes back to the VMG.
Cancel	Click Cancel 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 142](#)).
- Use the **Queue Setup** screen to configure QoS queue assignment ([Section 10.4 on page 143](#)).
- Use the **Classification Setup** screen to add, edit or delete QoS classifiers ([Section 10.5 on page 145](#)).
- Use the **Shaper Setup** screen to limit outgoing traffic transmission rate on the selected interface ([Section 10.6 on page 150](#)).
- Use the **Policer Setup** screen to control incoming traffic transmission rate and bursts ([Section 10.7 on page 151](#)).
- Use the **Monitor** screen to view statistics of QoS on WAN/LAN interface and the status of queues ([Section 10.8 on page 153](#)).

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.

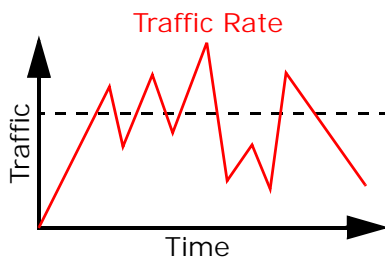
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

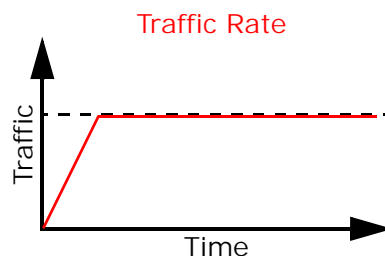
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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



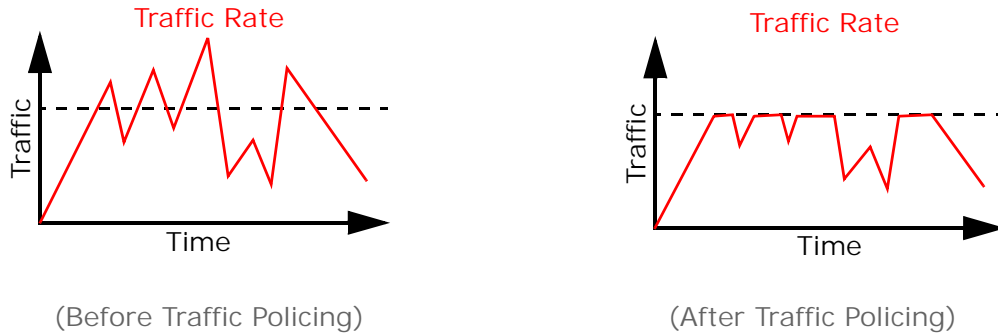
(Before Traffic Shaping)



(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 153](#) for more information on each metering algorithm.

10.3 Quality of Service General Settings

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 140](#) for more information.

Figure 71 Network Settings > QoS > General

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

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 42 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Select the Enable check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	<p>Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS.</p> <p>The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps.</p> <p>You can set this number higher than the interfaces' actual transmission speed. The 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"> • None: 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. • Ethernet Priority: Automatically assign priority based on the IEEE 802.1p priority level. • IP Precedence: Automatically assign priority based on the first three bits of the TOS field in the IP header. • Packet Length: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

10.4 Queue Setup


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

Use this screen to configure QoS queue assignment.

Figure 72 Network Setting > QoS > Queue Setup

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

Add New Queue

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

Note

1. Maximum 7 configurable entries and 1 unconfigurable default queue for WAN port.
2. Priority level 1 is the highest priority for QoS.
3. Rate limit 0 is max bandwidth.
4. If queue is deleted, then related classifiers will be removed too.

The following table describes the labels in this screen.

Table 43 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add New Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the VMG's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
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 Edit icon to edit the queue. Click the Delete icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

10.4.1 Adding a QoS Queue

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

Figure 73 Queue Setup: Add

The following table describes the labels in this screen.

Table 44 Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 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 Drop Tail (DT) . Drop Tail (DT) 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.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

10.5 Classification Setup

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 74 Network Setting > QoS > 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 45 Network Setting > QoS > Classification Setup

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

10.5.1 Add/Edit QoS Class

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

Figure 75 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 type="text"/>	Subnet Mask	<input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	<input type="text" value="~"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	<input type="text" value="- - - - -"/>	MAC Mask	<input type="text"/>	<input type="checkbox"/> Exclude

Destination

<input type="checkbox"/> Address	<input type="text"/>	Subnet Mask	<input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Port Range	<input type="text" value="~"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	<input type="text" value="- - - - -"/>	MAC Mask	<input 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 type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> DHCP	<input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> Packet Length	<input type="text" value="~"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> DSCP	<input type="text" value="(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 type="text" value="(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 ▼

802.1P Mark ▼

VLAN ID Tag ▼

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 46 Classification Setup: Add/Edit

LABEL	DESCRIPTION
Step1: Class Configuration	
Active	Select to enable or disable this 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 Apply . Select Last to put this rule in the back of the classifier list.
Step2: Criteria Configuration	
Basic	
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the From Interface drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select IP , you can configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select 802.1Q , you can configure an 802.1p priority level. You can also select other options, such as ARP , PPPoE_DISC , and so on to make configurations according to your needs.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	Enter the source subnet mask.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the 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 TCP or UDP in the IP Protocol 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.

Table 46 Classification Setup: Add/Edit (continued)

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

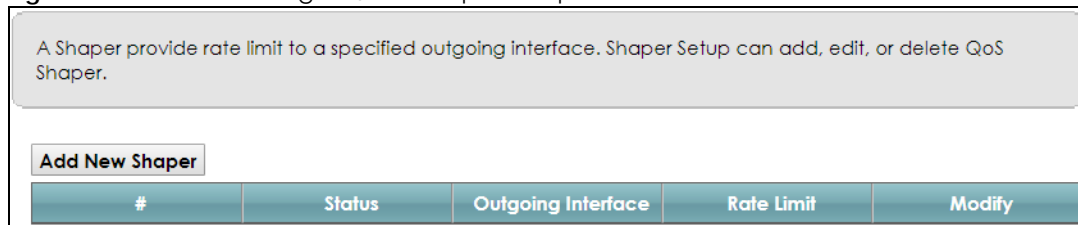
Table 46 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
VLAN ID Tag	<p>If you select Remark, enter a VLAN ID number with which the VMG replaces the VLAN ID of the frames.</p> <p>If you select Remove, the VMG deletes the VLAN ID of the frames before forwarding them out.</p> <p>If you select Add, the VMG treat all matched traffic untagged and add a second VLAN ID.</p> <p>If you select Unchange, the VMG keep the VLAN ID in the packets.</p>
Step4: Class Routing	
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select Unchange , the VMG forward traffic of this class according to the default routing table.
Step5: Outgoing Queue Selection	
To Queue Index	<p>Select a queue that applies to this class.</p> <p>You should have configured a queue in the Queue Setup screen already.</p>
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

10.6 QoS Shaper Setup

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 76 Network Setting > QoS > Shaper Setup



The following table describes the labels in this screen.

Table 47 Network Setting > QoS > Shaper Setup

LABEL	DESCRIPTION
Add New Shaper	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the shaper is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this shaper is not active.
Outgoing Interface	This shows the name of the 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	<p>Click the Edit icon to edit the shaper.</p> <p>Click the Delete icon to delete an existing shaper. Note that subsequent rules move up by one when you take this action.</p>