



VMG1312-B10D

Wireless N VDSL2 Gateway with USB

Version 5.11
Edition 2, 03/2016

User's Guide

Default Login Details

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

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the VMG and get up and running right away.

- More Information

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



Contents Overview

User's Guide	14
Introducing the VMG	15
The Web Configurator	21
Quick Start	28
Tutorials	31
Technical Reference	53
Network Map and Status Screens	54
Broadband	59
Wireless	87
Home Networking	116
Routing	132
Quality of Service (QoS)	139
Network Address Translation (NAT)	157
Dynamic DNS Setup	173
VLAN Group	177
Interface Grouping	179
USB Service	184
Firewall	189
MAC Filter	196
Parental Control	198
Scheduler Rule	202
Certificates	204
Log	211
Traffic Status	214
ARP Table	217
Routing Table	219
Multicast Status	221
xDSL Statistics	223
3G Statistics	226
System	228
User Account	229
Remote Management	231
SNMP	234
Time Settings	236
E-mail Notification	239
Logs Setting	241
Firmware Upgrade	244

Backup/Restore	246
Diagnostic	249
Troubleshooting	253
Appendices	260

Table of Contents

Contents Overview	3
Table of Contents	5
 Part I: User's Guide	 14
Chapter 1	
Introducing the VMG	15
1.1 Overview	15
1.2 Ways to Manage the VMG	15
1.3 Good Habits for Managing the VMG	15
1.4 Applications for the VMG	16
1.4.1 Internet Access	16
1.4.2 VMG's USB Support	17
1.5 Wireless Access	18
1.5.1 Using the Wi-Fi and WPS Buttons	19
1.6 LEDs (Lights)	19
1.7 The RESET Button	20
 Chapter 2	
The Web Configurator	21
2.1 Overview	21
2.1.1 Accessing the Web Configurator	21
2.2 Web Configurator Layout	23
2.2.1 Title Bar	23
2.2.2 Main Window	24
2.2.3 Navigation Panel	24
 Chapter 3	
Quick Start.....	28
3.1 Overview	28
3.2 Quick Start Setup	28
 Chapter 4	
Tutorials.....	31
4.1 Overview	31
4.2 Setting Up an ADSL PPPoE Connection	31
4.3 Setting Up a Secure Wireless Network	34

4.3.1 Configuring the Wireless Network Settings	34
4.3.2 Using WPS	36
4.3.3 Without WPS	39
4.4 Setting Up Multiple Wireless Groups	40
4.5 Configuring Static Route for Routing to Another Network	43
4.6 Configuring QoS Queue and Class Setup	45
4.7 Access the VMG Using DDNS	49
4.7.1 Registering a DDNS Account on www.dyndns.org	49
4.7.2 Configuring DDNS on Your VMG	50
4.7.3 Testing the DDNS Setting	50
4.8 Configuring the MAC Address Filter	50
4.9 Access Your Shared Files From a Computer	51

Part II: Technical Reference..... 53

Chapter 5 Network Map and Status Screens.....54

5.1 Overview	54
5.2 The Network Map Screen	54
5.3 The Status Screen	55

Chapter 6 Broadband.....59

6.1 Overview	59
6.1.1 What You Can Do in this Chapter	59
6.1.2 What You Need to Know	60
6.1.3 Before You Begin	63
6.2 The Broadband Screen	63
6.2.1 Add/Edit Internet Connection	64
6.3 The 3G Backup Screen	71
6.4 The Advanced Screen	76
6.5 The Ethernet WAN Screen	79
6.6 The 802.1x Screen	80
6.6.1 Modify 802.1X Settings	81
6.7 Technical Reference	81

Chapter 7 Wireless.....87

7.1 Overview	87
7.1.1 What You Can Do in this Chapter	87
7.1.2 What You Need to Know	87

7.2 The General Screen	88
7.2.1 No Security	91
7.2.2 Basic (WEP Encryption)	91
7.2.3 More Secure (WPA(2)-PSK)	92
7.3 The Guest/More AP Screen	93
7.3.1 Edit Guest/More AP	94
7.4 The MAC Authentication Screen	97
7.5 The WPS Screen	98
7.6 The WMM Screen	99
7.7 The Others Screen	100
7.8 The Channel Status Screen	102
7.9 Technical Reference	103
7.9.1 Wireless Network Overview	103
7.9.2 Additional Wireless Terms	105
7.9.3 Wireless Security Overview	105
7.9.4 Signal Problems	107
7.9.5 BSS	108
7.9.6 MBSSID	108
7.9.7 Preamble Type	109
7.9.8 WiFi Protected Setup (WPS)	109
 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 The LAN Setup Screen	118
8.3 The Static DHCP Screen	122
8.4 The UPnP Screen	123
8.4.1 Turning On UPnP in Windows 7 Example	124
8.5 The Additional Subnet Screen	126
8.6 The STB Vendor ID Screen	127
8.7 The Wake on LAN Screen	127
8.8 The TFTP Server Name Screen	128
8.9 Technical Reference	128
8.9.1 LANs, WANs and the VMG	128
8.9.2 DHCP Setup	129
8.9.3 DNS Server Addresses	129
8.9.4 LAN TCP/IP	130
 Chapter 9	
Routing	132

9.1 Overview	132
9.2 The Routing Screen	132
9.2.1 Add/Edit Static Route	133
9.3 The DNS Route Screen	134
9.3.1 The DNS Route Add Screen	135
9.4 The Policy Route Screen	135
9.4.1 Add/Edit Policy Route	137
9.5 RIP	138
9.5.1 The RIP Screen	138

Chapter 10

Quality of Service (QoS)..... 139

10.1 Overview	139
10.1.1 What You Can Do in this Chapter	139
10.2 What You Need to Know	140
10.3 The Quality of Service General Screen	141
10.4 The Queue Setup Screen	142
10.4.1 Adding a QoS Queue	144
10.5 The Classification Setup Screen	145
10.5.1 Add/Edit QoS Class	145
10.6 The QoS Shaper Setup Screen	149
10.6.1 Add/Edit a QoS Shaper	150
10.7 The QoS Policer Setup Screen	150
10.7.1 Add/Edit a QoS Policer	151
10.8 Technical Reference	152

Chapter 11

Network Address Translation (NAT)..... 157

11.1 Overview	157
11.1.1 What You Can Do in this Chapter	157
11.1.2 What You Need To Know	157
11.2 The Port Forwarding Screen	158
11.2.1 Add/Edit Port Forwarding	160
11.3 The Applications Screen	161
11.3.1 Add New Application	162
11.4 The Port Triggering Screen	162
11.4.1 Add/Edit Port Triggering Rule	164
11.5 The DMZ Screen	165
11.6 The ALG Screen	166
11.7 The Address Mapping Screen	166
11.7.1 Add/Edit Address Mapping Rule	167
11.8 The Sessions Screen	168
11.9 Technical Reference	169

11.9.1 NAT Definitions	169
11.9.2 What NAT Does	170
11.9.3 How NAT Works	170
11.9.4 NAT Application	170
Chapter 12	
Dynamic DNS Setup	173
12.1 Overview	173
12.1.1 What You Can Do in this Chapter	173
12.1.2 What You Need To Know	173
12.2 The DNS Entry Screen	174
12.2.1 Add/Edit DNS Entry	174
12.3 The Dynamic DNS Screen	175
Chapter 13	
VLAN Group	177
13.1 Overview	177
13.1.1 What You Can Do in this Chapter	177
13.2 The VLAN Group Screen	177
13.2.1 Add/Edit a VLAN Group	178
Chapter 14	
Interface Grouping	179
14.1 Overview	179
14.1.1 What You Can Do in this Chapter	179
14.2 The Interface Group Screen	179
14.2.1 Interface Group Configuration	180
14.2.2 Interface Grouping Criteria	182
Chapter 15	
USB Service	184
15.1 Overview	184
15.1.1 What You Can Do in this Chapter	184
15.1.2 What You Need To Know	184
15.1.3 Before You Begin	185
15.2 The File Sharing Screen	185
15.2.1 The Add New User Screen	186
15.3 The Media Server Screen	187
Chapter 16	
Firewall	189
16.1 Overview	189
16.1.1 What You Can Do in this Chapter	189

16.1.2 What You Need to Know	190
16.2 The Firewall Screen	190
16.3 The Protocol Screen	191
16.3.1 Add/Edit a Service	192
16.4 The Access Control Screen	193
16.4.1 Add/Edit an ACL Rule	193
16.5 The DoS Screen	195
Chapter 17	
MAC Filter	196
17.1 Overview	196
17.2 The MAC Filter Screen	196
Chapter 18	
Parental Control	198
18.1 Overview	198
18.2 The Parental Control Screen	198
18.2.1 Add/Edit a Parental Control Profile	199
Chapter 19	
Scheduler Rule	202
19.1 Overview	202
19.2 The Scheduler Rule Screen	202
19.2.1 Add/Edit a Schedule	202
Chapter 20	
Certificates	204
20.1 Overview	204
20.1.1 What You Can Do in this Chapter	204
20.2 What You Need to Know	204
20.3 The Local Certificates Screen	204
20.3.1 Create Certificate Request	205
20.3.2 Load Signed Certificate	207
20.4 The Trusted CA Screen	208
20.4.1 View Trusted CA Certificate	209
20.4.2 Import Trusted CA Certificate	210
Chapter 21	
Log	211
21.1 Overview	211
21.1.1 What You Can Do in this Chapter	211
21.1.2 What You Need To Know	211
21.2 The System Log Screen	212

21.3 The Security Log Screen	212
Chapter 22	
Traffic Status	214
22.1 Overview	214
22.1.1 What You Can Do in this Chapter	214
22.2 The WAN Status Screen	214
22.3 The LAN Status Screen	215
22.4 The NAT Status Screen	216
Chapter 23	
ARP Table	217
23.1 Overview	217
23.1.1 How ARP Works	217
23.2 ARP Table Screen	218
Chapter 24	
Routing Table	219
24.1 Overview	219
24.2 The Routing Table Screen	219
Chapter 25	
Multicast Status	221
25.1 Overview	221
25.2 The IGMP Status Screen	221
25.3 The MLD Status Screen	221
Chapter 26	
xDSL Statistics	223
26.1 The xDSL Statistics Screen	223
Chapter 27	
3G Statistics	226
27.1 Overview	226
27.2 The 3G Statistics Screen	226
Chapter 28	
System	228
28.1 Overview	228
28.2 The System Screen	228
Chapter 29	
User Account	229

29.1 Overview	229
29.2 The User Account Screen	229
29.2.1 The User Account Add and Edit Screens	229
Chapter 30	
Remote Management.....	231
30.1 Overview	231
30.2 The Remote MGMT Screen	231
30.3 The Trust Domain Screen	232
30.3.1 The Add Trust Domain Screen	232
Chapter 31	
SNMP	234
31.1 Overview	234
31.2 The SNMP Screen	234
Chapter 32	
Time Settings	236
32.1 Overview	236
32.2 The Time Screen	236
Chapter 33	
E-mail Notification	239
33.1 Overview	239
33.2 The E-mail Notification Screen	239
33.2.1 E-mail Notification Edit	239
Chapter 34	
Logs Setting	241
34.1 Overview	241
34.2 The Logs Setting Screen	241
34.2.1 Example E-mail Log	242
Chapter 35	
Firmware Upgrade	244
35.1 Overview	244
35.2 The Firmware Screen	244
Chapter 36	
Backup/Restore	246
36.1 Overview	246
36.2 The Backup/Restore Screen	246
36.3 The Reboot Screen	248

Chapter 37	
Diagnostic	249
37.1 Overview	249
37.1.1 What You Can Do in this Chapter	249
37.2 What You Need to Know	249
37.3 Ping & TraceRoute & Nslookup	250
37.4 802.1ag	250
37.5 OAM Ping	251
Chapter 38	
Troubleshooting.....	253
38.1 Power, Hardware Connections, and LEDs	253
38.2 VMG Access and Login	254
38.3 Internet Access	256
38.4 Wireless Internet Access	257
38.5 USB Device Connection	258
38.6 UPnP	258
 Part III: Appendices	 260
Appendix A Customer Support	261
Appendix B Wireless LANs.....	267
Appendix C IPv6	280
Appendix D Services	288
Appendix E Legal Information.....	292
Index	300

PART I

User's Guide

Introducing the VMG

1.1 Overview

The VMG is a wireless VDSL router. It has a DSL port for Internet access. The VMG supports both Packet Transfer Mode (PTM) and Asynchronous Transfer Mode (ATM). It is backward compatible with ADSL, ADSL2 and ADSL2+ in case VDSL is not available.

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

The VMG works over the analog telephone system, POTS (Plain Old Telephone Service). The VMG has one USB port for sharing files via a USB storage device or connecting a 3G dongle for a WAN backup connection.

1.2 Ways to Manage the VMG

Use any of the following methods to manage the VMG.

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

1.3 Good Habits for Managing the VMG

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

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

1.4 Applications for the VMG

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

1.4.1 Internet Access

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

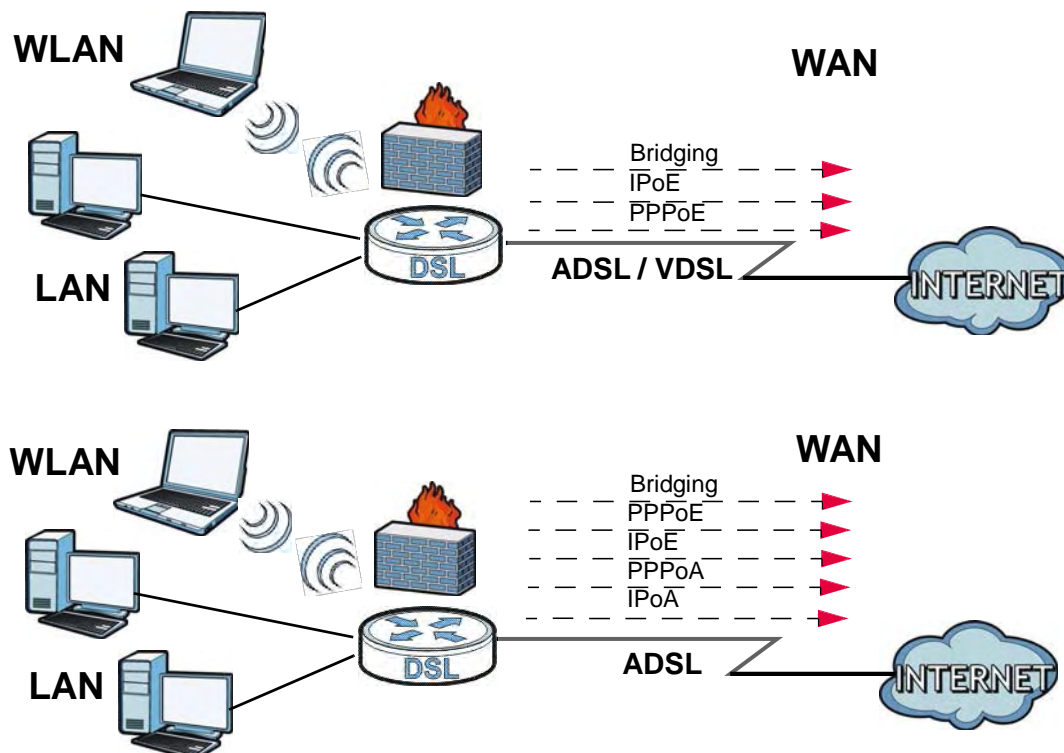
You can also configure IP filtering on the VMG for secure Internet access. When the IP filter is on, all incoming traffic from the Internet to your network is blocked by default unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you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

1.4.1.1 DSL

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

Note: The ADSL and VDSL lines share the same WAN (layer-2) interfaces that you configure in the VMG. Refer to [Section 6.2 on page 63](#) for the **Network Setting > Broadband** screen.

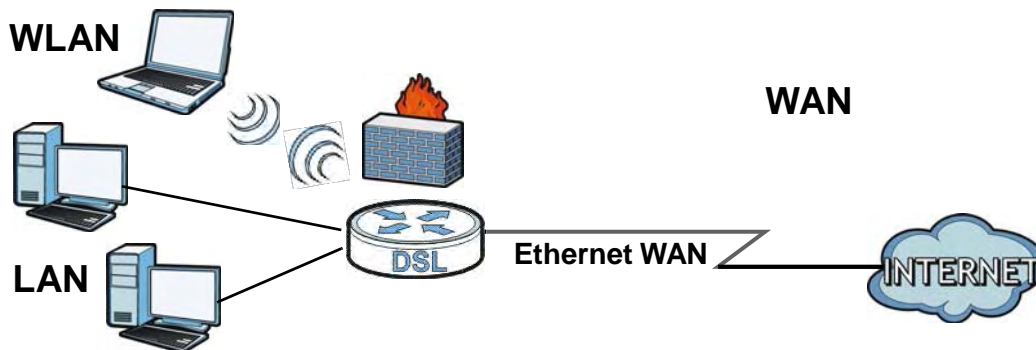
Figure 1 VMG's Internet Access Application: DSL



1.4.1.2 Ethernet WAN

If you prefer not to use a DSL line and you have another broadband modem or router (such as ADSL) available, you can convert LAN port number four 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 2 VMG's Internet Access Application: Ethernet WAN



1.4.2 VMG's USB Support

The USB port of the VMG is used for 3G WAN backup, file-sharing and media server.

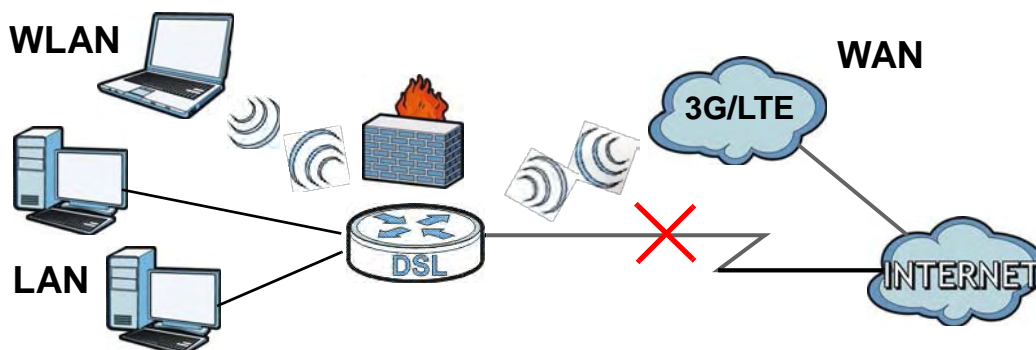
3G WAN Backup

Connect a 3G/LTE USB dongle with an active SIM card to the USB port. This adds a second WAN interface and allows the VMG to wirelessly access the Internet via a 3G/LTE network. The 3G/LTE WAN connection is the failover or a backup in case the DSL or Ethernet WAN connection fails.

To set up a 3G/LTE connection, click **Network Setting > Broadband > 3G Backup**.

To update the supported 3G/LTE USB dongle list, download the latest WWAN package from the ZyXEL website and upload it to the VMG using the **Maintenance > Firmware Upgrade** screen. See the product page on ZyXEL's website for the list of 3G/LTE USB dongles that are compatible.

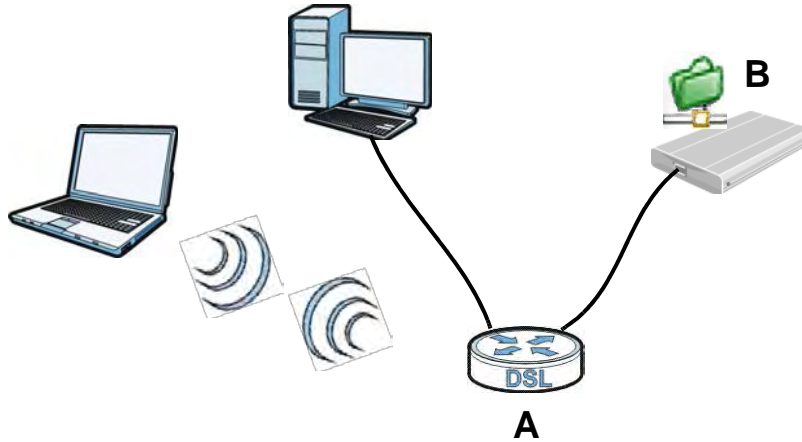
Figure 3 VMG's Internet Access Application: 3G WAN



File Sharing

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

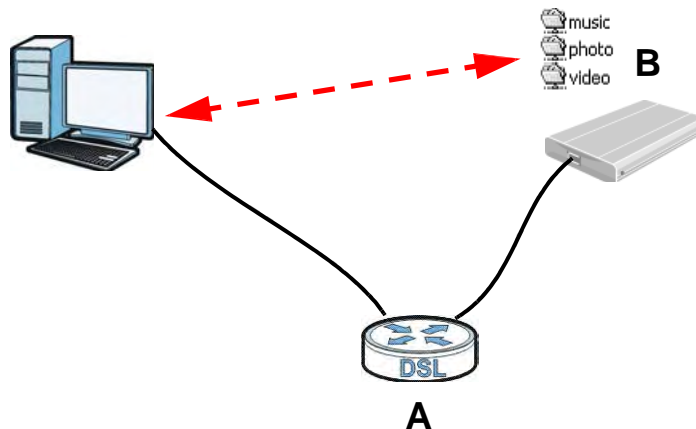
Figure 4 USB File Sharing Application



Media Server

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

Figure 5 USB Media Server Application

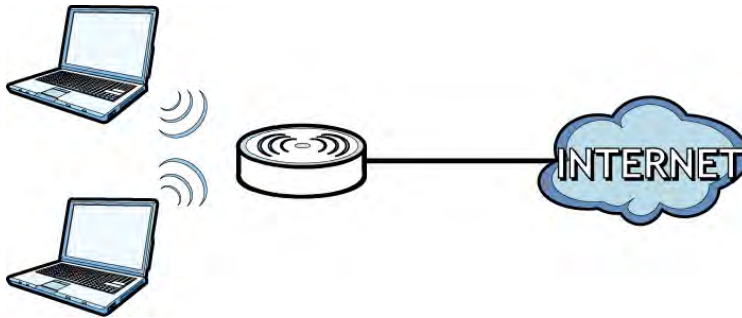


1.5 Wireless Access

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

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

Figure 6 Wireless Access Example



1.5.1 Using the Wi-Fi and WPS Buttons

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

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

To activate WPS:

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

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

1.6 LEDs (Lights)







The following graphic displays the labels of the LEDs.

Figure 7 LEDs on the VMG



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

Table 1 LED Descriptions

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

1.7 The RESET Button

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

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

The Web Configurator

2.1 Overview

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

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

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

2.1.1 Accessing the Web Configurator

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

Figure 8 Password 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 9 Change Password Screen

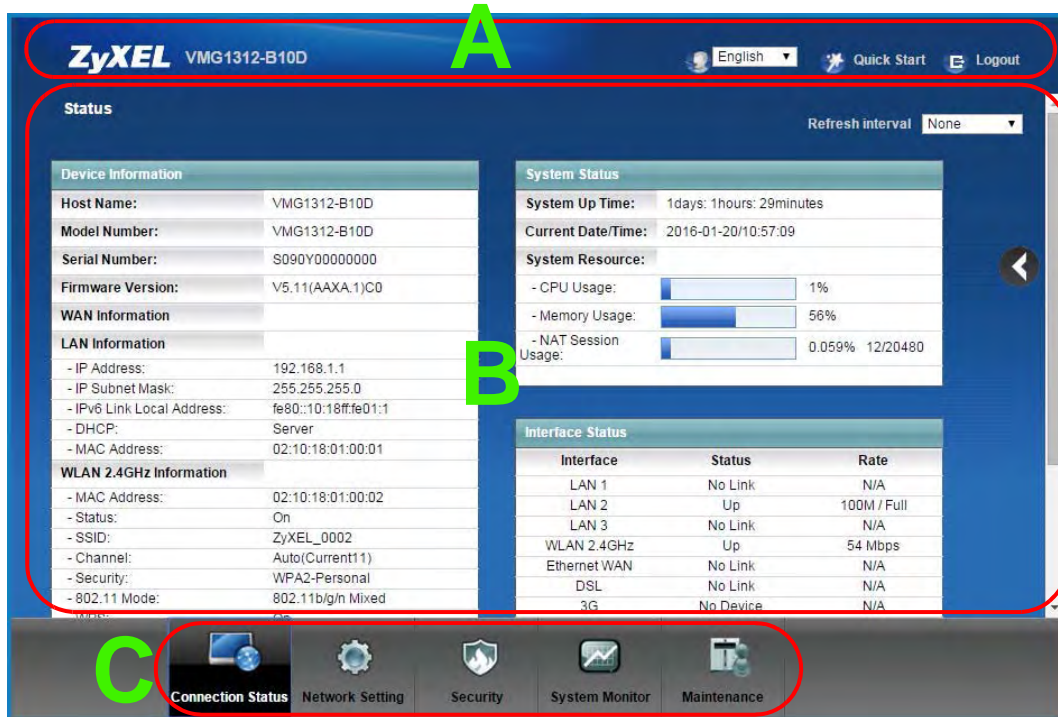
- 5 The **Quick Start Wizard** screen appears. You can configure basic Internet access, and wireless settings. See [Chapter 3 on page 28](#) for more information.
- 6 After you finished or closed the **Quick Start Wizard** screen, the **Network Map** page appears.

Figure 10 Network Map

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

2.2 Web Configurator Layout

Figure 11 Screen Layout

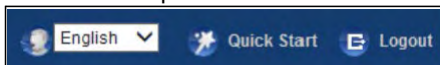


As illustrated above, the main screen is divided into these parts:

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

2.2.1 Title Bar

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



The icons provide the following functions.

Table 2 Web Configurator Icons in the Title Bar

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

2.2.2 Main Window

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

After you click the right arrow icon on the **Connection Status (Network Map)** page, the **Status** screen is displayed. See [Chapter 5 on page 55](#) for more information about the **Status** screen.

2.2.3 Navigation Panel

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

Table 3 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.
	3G Backup	Use this screen to configure 3G/LTE WAN connection.
	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 convert Ethernet LAN 4 port as WAN port, or restore the WAN port to LAN port.
	802.1x	Use this screen to view and configure the IEEE 802.1x settings on the VMG.
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	Guest/More AP	Use this screen to configure multiple BSSs on the VMG.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the VMG.
	WPS	Use this screen to configure and view your WPS (Wi-Fi Protected Setup) settings.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	WDS	Use this screen to set up Wireless Distribution System (WDS) links to other access points.
	Others	Use this screen to configure advanced wireless settings.
	Channel Status	Use this screen to scan wireless LAN channel noises and view the results.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	STB Vendor ID	Use this screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the VMG automatically create static DHCP entries for the STB devices when they request IP addresses.
	Wake on LAN	Use this screen to remotely turn on a device on the local network.
	TFTP Server Name	Configure a TFTP server name which is sent to clients using DHCP option 66.
Routing	Static Route	Use this screen to view and set up static routes on the VMG.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s).
	Policy Route	Use this screen to configure policy routing on the VMG.
	RIP	Use this screen to configure Routing Information Protocol to exchange routing information with other routers.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Classification Setup	Use this screen to define a classifier.
	Shaper Setup	Use this screen to limit outgoing traffic rate on the selected interface.
	Policer Setup	
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Applications	Use this screen to configure servers behind the VMG.
	Port Triggering	Use this screen to change your VMG's port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the Port Forwarding screen.
	ALG	Use this screen to enable or disable SIP ALG.
	Address Mapping	Use this screen to change your VMG's address mapping settings.
	Sessions	Use this screen to configure the maximum number of NAT sessions each client host is allowed to have through the VMG.
DNS	DNS Entry	Use this screen to view and configure DNS routes.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
IGMP/MLD	IGMP/MLD	Use this screen to configure multicast settings (IGMP for IPv4 and MLD for IPv6 multicast groups) on the WAN.
Vlan Group	Vlan Group	Use this screen to group and tag VLAN IDs to outgoing traffic from the specified interface.
Interface Grouping	Interface Grouping	Use this screen to map a port to a PVC or bridge group.
USB Service	File Sharing	Use this screen to enable file sharing via the VMG.
	Media Server	Use this screen to use the VMG as a media server.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Security		
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the VMG.
Parental Control	Parental Control	Use this screen to block web sites with the specific URL.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the VMG. You can export or e-mail the logs.
	Security Log	<p>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.</p> <p>Levels include:</p> <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging <p>Categories include:</p> <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.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
3G Statistics	3G Statistics	Use this screen to look at 3G Internet connection status.
Maintenance		
System	System	Use this screen to set Device name and Domain name.
User Account	User Account	Use this screen to change user password on the VMG.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to configure a list of public IP addresses which are allowed to access the VMG.
SNMP	SNMP	Use this screen to configure SNMP (Simple Network Management Protocol) settings.
Time	Time	Use this screen to change your VMG's time and date.
Email Notification	Email Notification	Use this screen to configure up to two mail servers and sender addresses on the VMG.
Log Setting	Log Setting	Use this screen to change your VMG's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your VMG.
Backup Restore	Backup/Restore	Use this screen to backup and restore your VMG's configuration (settings) or reset the factory default settings.
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.
	OAM Ping	Use this screen to view information to help you identify problems with the DSL connection.

Quick Start

3.1 Overview

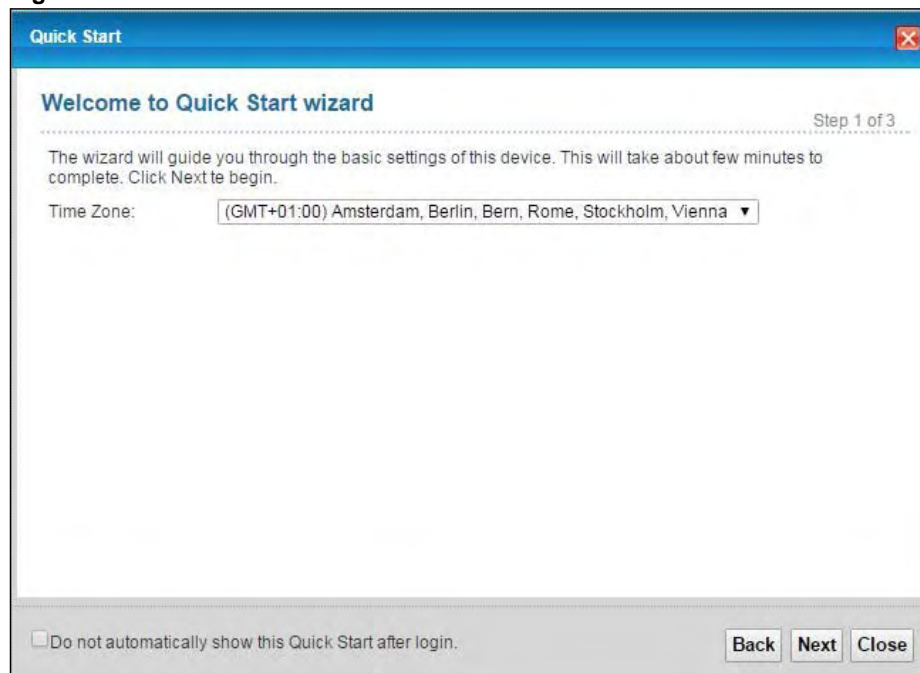
Use the Quick Start screens to configure the VMG's time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on [Chapter 4 on page 31](#)) 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 12 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 13 Quick Start - Internet Connection

Quick Start

Internet Connection Step 2 of 3

The current connection type is set to IPoE.
Is there specific IP address information from your Internet Service Provider (ISP)?

☐ Yes ☒ No

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

☐ Do not automatically show this Quick Start after login.

Back Next Close

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

Figure 14 Quick Start - Wireless Setting

Quick Start

Wireless Setting

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

Wireless Service: ☒ Enable ☐ Disable

Wireless Network Name (SSID): ZyXEL_0002

Security: WPA2-PSK

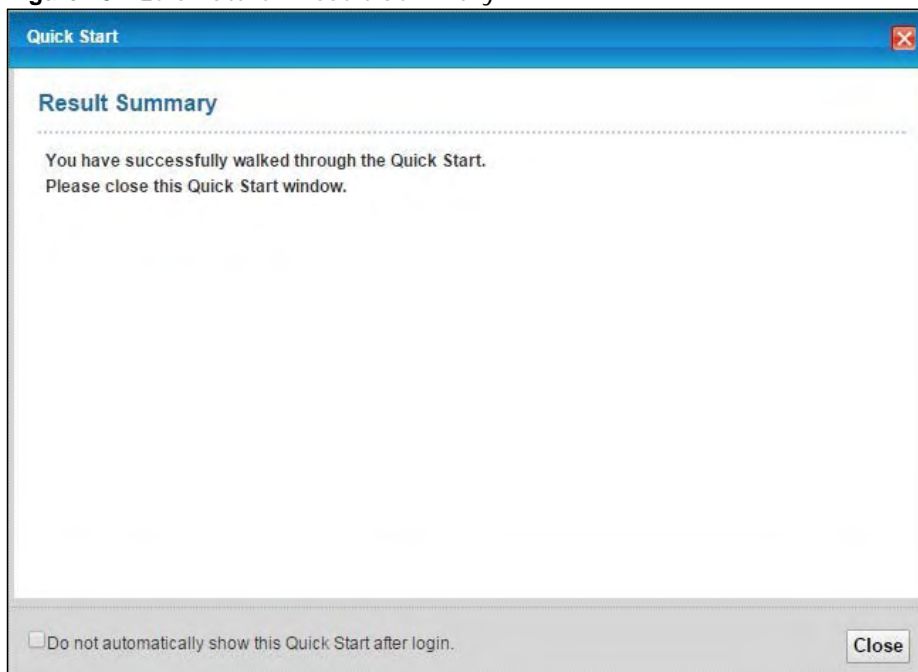
Password: *****

☐ Do not automatically show this Quick Start after login.

Back Save Close

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

Figure 15 Quick Start - Result Summary



4.1 Overview

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

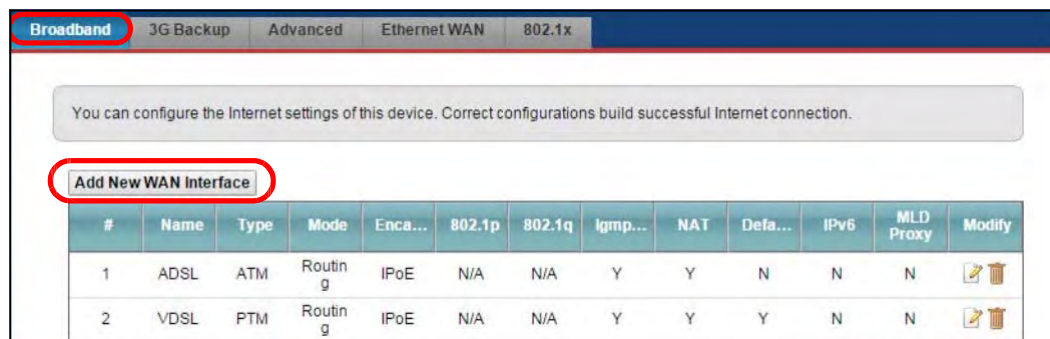
- [Setting Up an ADSL PPPoE Connection](#), see [page 31](#)
- [Setting Up a Secure Wireless Network](#), see [page 34](#)
- [Setting Up Multiple Wireless Groups](#), see [page 40](#)
- [Configuring Static Route for Routing to Another Network](#), see [page 43](#)
- [Configuring QoS Queue and Class Setup](#), see [page 45](#)
- [Access the VMG Using DDNS](#), see [page 49](#)
- [Configuring the MAC Address Filter](#), see [page 50](#)
- [Access Your Shared Files From a Computer](#), see [page 51](#)

4.2 Setting Up an ADSL PPPoE Connection

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

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

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



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

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

- 3 Select the **Active** check box. Enter the **General** and **ATM PVC Configuration** settings as provided above.

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

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

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

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

Add New WAN Interface

General

Name: MyDSLConnection
 Type: ADSL over ATM
 Mode: ☒ Routing ☐ Bridge
 Encapsulation: PPPoE
 IPv4/IPv6 Mode: IPv4 Only

PPP Information

PPP User Name: 1234@DSL-Ex.com
 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: 192.168.1.32

ATM PVC Configuration

VPI [0-255]: 36
 VCI [32-65535]: 48
 Encapsulation: LLC/SNAP-BRIDGING
 Service Category: UBR Without PCR

VLAN

Active: ☐ Enable ☒ Disable
 802.1p: 0
 802.1q: (0~4094)

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
 Primary DNS Server: 192.168.5.2
 Secondary DNS Server: 192.168.5.1

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 Setting Up a Secure Wireless Network

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



Thomas has to configure the wireless network settings on the VMG. Then he can set up a wireless network using WPS ([Section 4.3.2 on page 36](#)) or manual configuration ([Section 4.3.3 on page 39](#)).

4.3.1 Configuring the Wireless Network Settings

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

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

- 1 Click **Network Setting** > **Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see [page 34](#)). Click **Apply**.

Wireless Network Setup

Bandwidth: 2.4GHz ▾

Wireless: ☒ Enable ☐ Disable (settings are invalid when disabled)

Channel: Auto ▾ | Current: 6

Bandwidth: 40MHz ▾

Control Sideband: Lower ▾

Passphrase Type: None ▾

Wireless Network Settings

Wireless Network Name: Example

Max Clients: 32

☐ Hide SSID

☒ Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Note

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

BSSID: 02:10:18:01:00:02

Security Level

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

Security Mode: WPA2-PSK ▾

☐ Generate password automatically

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

Password: DoNotStealMyWirelessNet [more...](#)

☒ password unmask

Apply Cancel

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

RTS/CTS Threshold : 2347

Fragmentation Threshold : 2346

Auto Channel Timer : 0 min

Output Power : 100% ▾

Beacon Interval : 100 ms

DTIM Interval : 1 ms

802.11 Mode : 802.11b/g/n Mixed ▾

802.11 Protection : Off ▾

RIFS Advertisement : Auto ▾

Preamble : Long ▾

RX Chain Power Save: ☒ Enable ☐ Disable

OBSS Coexistence: ☒ Enable ☐ Disable

XPress™ Technology: ☒ Enable ☐ Disable

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the VMG (see [Section 4.3.2 on page 36](#)). He can also use the notebook's wireless client to search for the VMG (see [Section 4.3.3 on page 39](#)).

4.3.2 Using WPS

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

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

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

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

Push Button Configuration (PBC)

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

General

WPS ☒ Enable ☐ Disable (settings are invalid when disabled)

Add a new device with WPS Method

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

Note

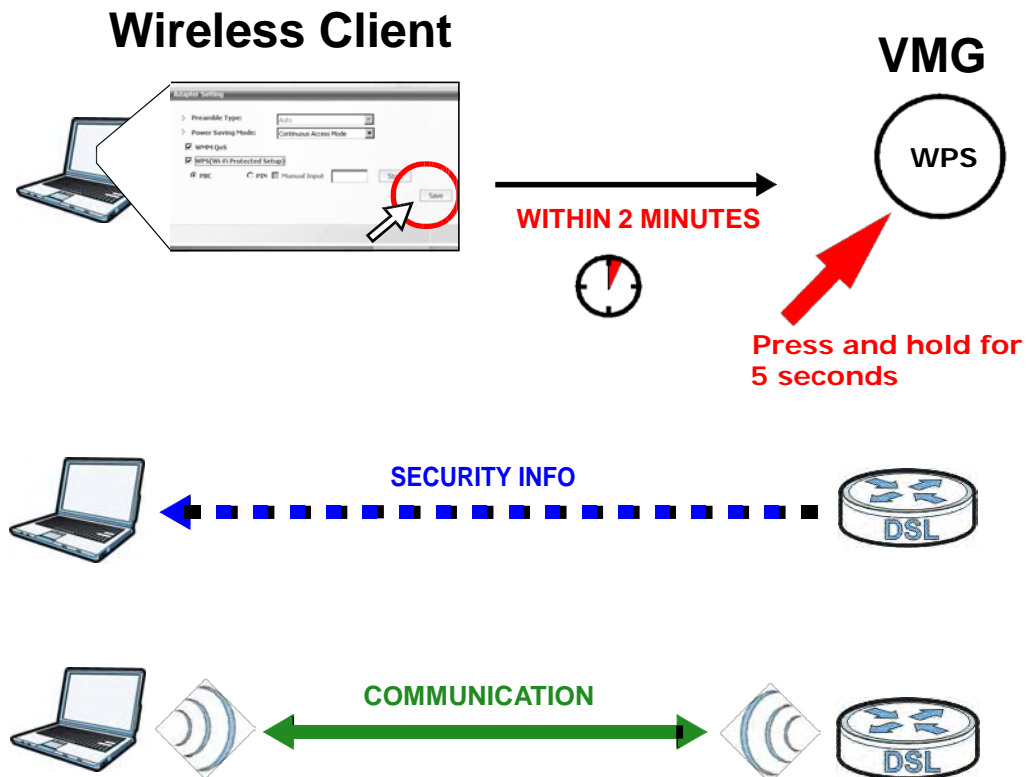
1. If WPS is Enabled, UPnP will automatically be turned on.
2. This feature is available only when WPA2-PSK or No Security mode is configured.

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

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

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

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



PIN Configuration

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

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

General

WPS ☒ Enable ☐ Disable (settings are invalid when disabled)

Add a new device with WPS Method

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

Note

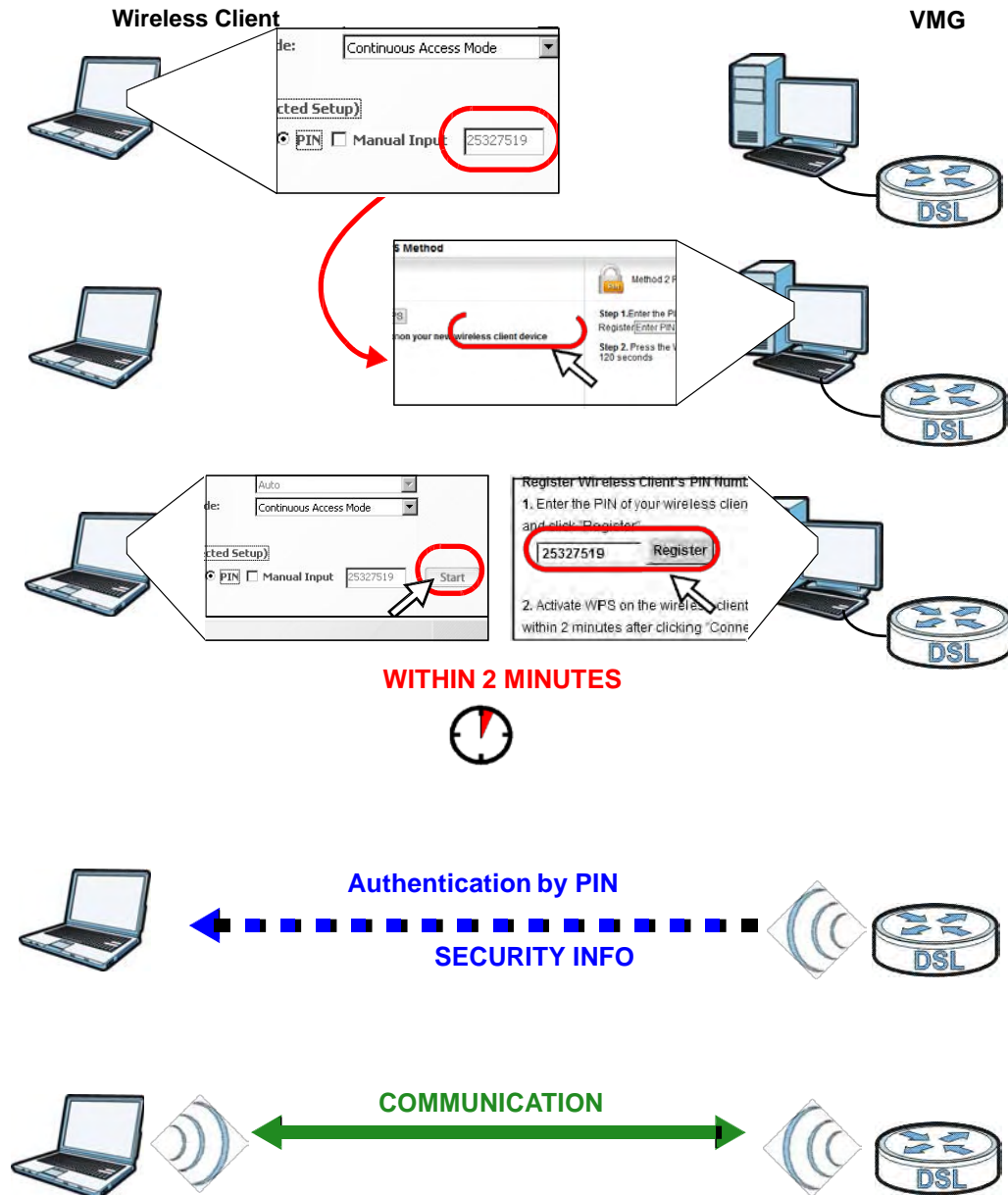
1.If WPS is Enabled, UPnP will automatically be turned on.
2.This feature is available only when WPA2-PSK or No Security mode is configured.

Apply **Cancel**

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

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

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



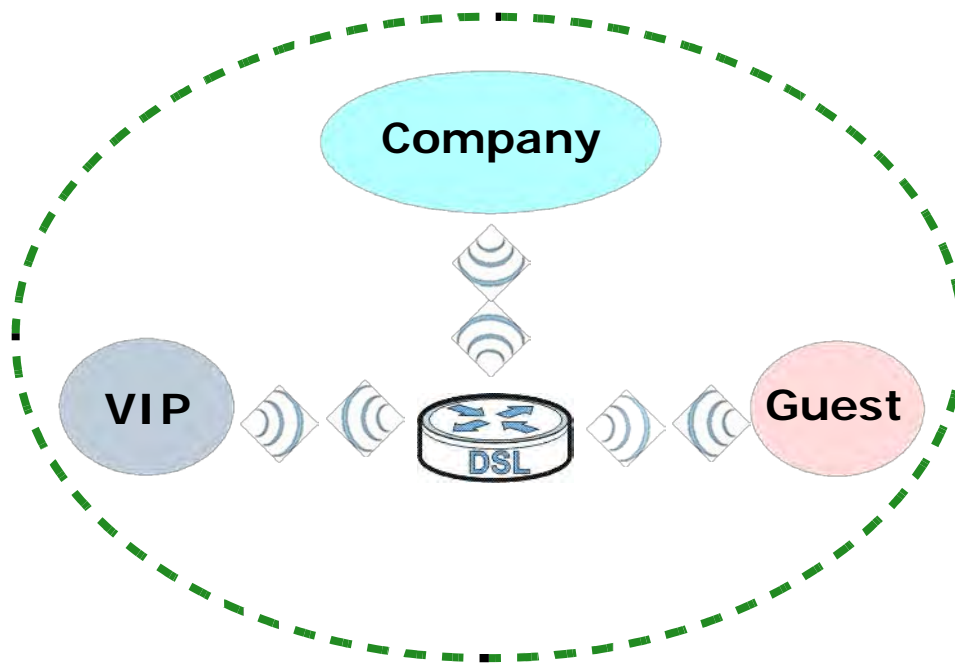
4.3.3 Without WPS

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

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

4.4 Setting Up Multiple Wireless Groups

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



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

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

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

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

Wireless Network Setup

Band: 2.4GHz

Wireless: ☒ Enable ☐ Disabled (settings are invalid when disabled)

Channel: Auto Current: 13 [more...](#)

Wireless Network Settings

Wireless Network Name (SSID): Company

Max clients: 16

☐ Hide SSID

☒ Enhanced Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Notes:

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

BSSID: CC:5D:4E:00:00:02

E-mail notification when the wireless guest visit

☐ Enable Email Notification

Security Level

More Secure (Recommended)

Security Mode: WPA2-PSK

☐ Generate password automatically

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

Password: ForCompanyOnly [more...](#)

☐ password unmask

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

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

This device can enable up to 4 wireless networks to work at the same time. Assign a name and a security level (if needed) to start the 2nd, 3rd, and 4th wireless network services.

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

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

Wireless Network Setup

Wireless : ☒ **Enable** ☐ Disabled (The settings in this screen are invalid if you select this.)

Passphrase Type :

Wireless Network Settings

Wireless Network Name(SSID):

Max clients:

☐ Hide SSID

☐ Enhanced Multicast Forwarding

☒ Guest WLAN

Access Scenario:

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Notes:


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

E-mail notification when the wireless guest visit

☐ Enable Email Notification

SSID Subnet: ☐ Enable ☒ Disabled

Security Level



Security Mode:

☐ Generate password automatically

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

Password: [more...](#)

☒ password unmask

OK Cancel

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

Wireless Network Setup

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

Passphrase Type :

Wireless Network Settings

Wireless Network Name(SSID):

Max clients:

☐ Hide SSID

☐ Enhanced Multicast Forwarding

☒ Guest WLAN

Access Scenario:

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Notes:

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

E-mail notification when the wireless guest visit

☐ Enable Email Notification

SSID Subnet: ☐ Enable ☒ Disabled

Security Level

☐ Not Secure ☐ Secure ☒ More Secure (Recommended)

Security Mode:

☐ Generate password automatically







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

Password: [more...](#)

☒ password unmask

OK Cancel

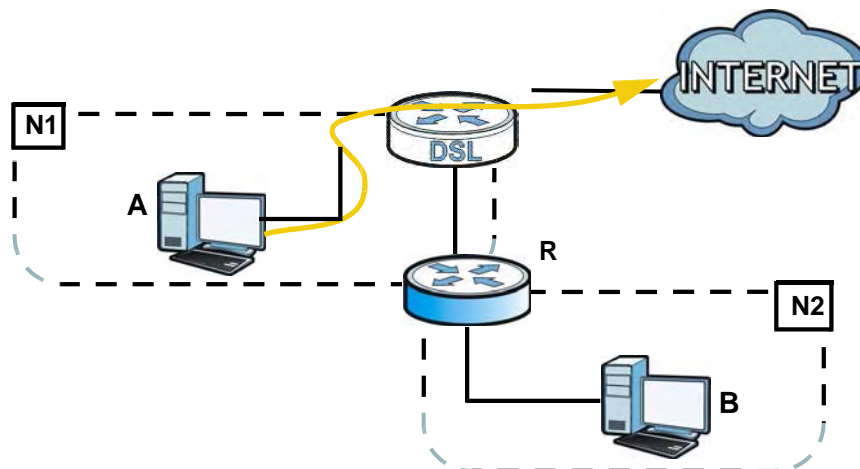
- 5 Check the status of **VIP** and **Guest** in the **Guest/More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.

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

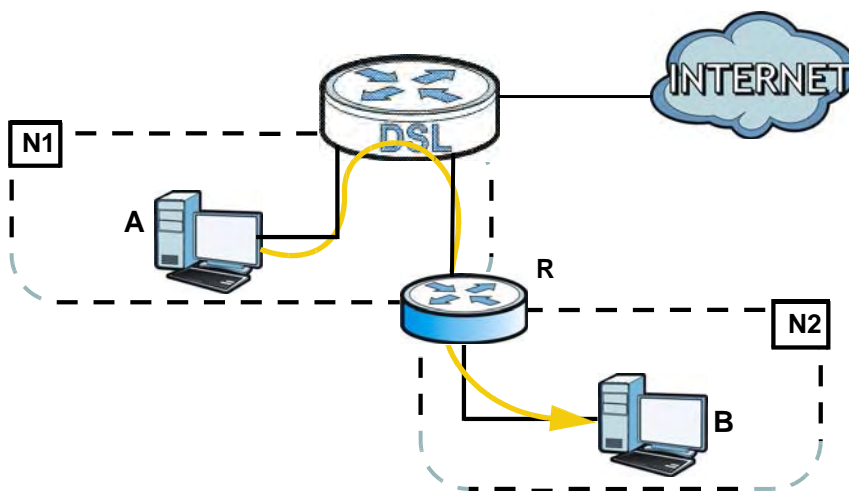
4.5 Configuring Static Route for Routing to Another Network

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

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



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



This tutorial uses the following example IP settings:

Table 4 IP Settings in this Tutorial

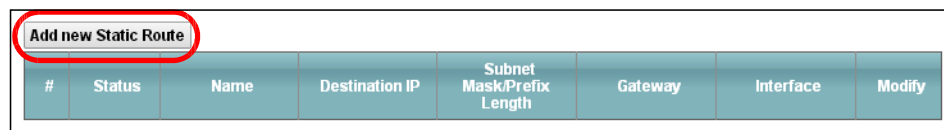
DEVICE / COMPUTER	IP ADDRESS
The VMG's WAN	172.16.1.1
The VMG's LAN	192.168.1.1
IP Type	IPv4
Use Interface	VDSL/ppp1.1
A	192.168.1.34

Table 4 IP Settings in this Tutorial

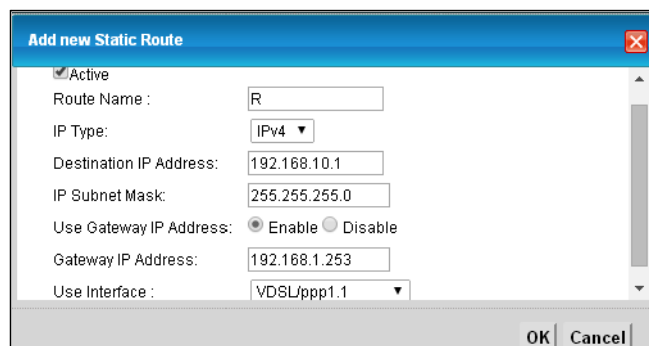
DEVICE / COMPUTER	IP ADDRESS
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

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

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



- 4 Configure the **Static Route Setup** screen using the following settings:
 - 4a Select 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/ppp1.1** 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 Configuring QoS Queue and Class Setup

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

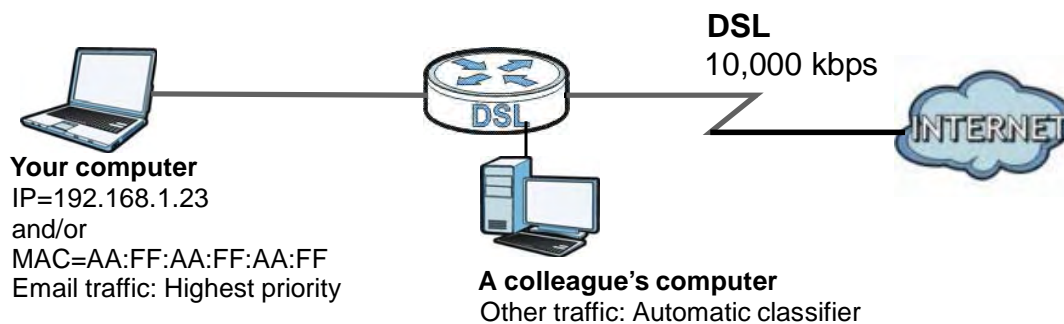
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues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

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

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

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

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



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

QoS

☒ Enable
 ☐ Disable (settings are invalid when disabled)

WAN Managed Upstream Bandwidth : (kbps)

LAN Managed Downstream Bandwidth : (kbps)

Upstream traffic priority Assigned by:

Note:

You can assign the upstream bandwidth manually. If the field is empty, the CPE sets the value automatically.

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.

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

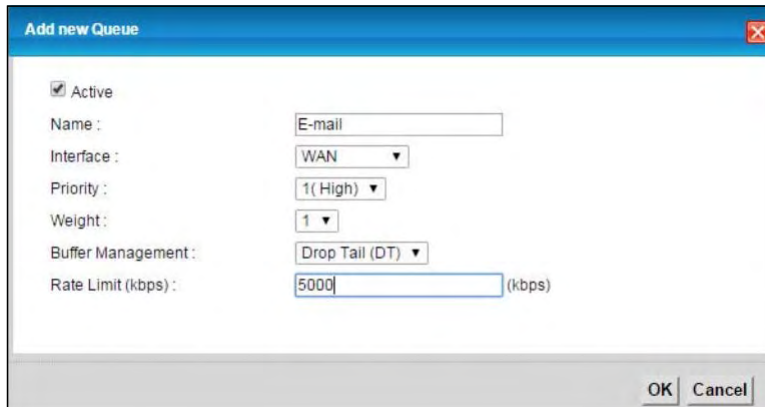
Apply

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:** E-mail

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



Add new Queue

☒ Active

Name : E-mail

Interface : WAN

Priority : 1 (High)

Weight : 1

Buffer Management : Drop Tail (DT)

Rate Limit (kbps) : 5000 (kbps)

OK Cancel

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

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

Step1: Class Configuration

☒ Active

Class Name :

Classification Order :

Step2: Criteria configuration

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

▪ **Basic**

From Interface :

Ether Type :

▪ **Source**

☒ Address Subnet Netmask ☐ Exclude

☐ Port Range ~ ☐ Exclude

☒ MAC MAC Mask ☐ Exclude

▪ **Destination**

☐ Address Subnet Netmask ☐ Exclude

☐ Port Range ~ ☐ Exclude

☐ MAC MAC Mask ☐ Exclude

▪ **Others**

☐ Service ☐ Exclude

☒ IP protocol ☐ Exclude

☐ DHCP ☐ Exclude

☐ Packet Length ~ ☐ Exclude

☐ DSCP (0~63) ☐ Exclude

☐ 802.1P ☐ Exclude

☐ VLAN ID (0~4094) ☐ Exclude

☐ TCP ACK ☐ Exclude

Step3: Packet modification

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

DSCP Mark : (0~63)

802.1P Mark :

VLAN ID : (0~4094)

Step4: Policy Forwarding

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

Forward To Interface :

Step5: Outgoing queue selection

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

To Queue Index :

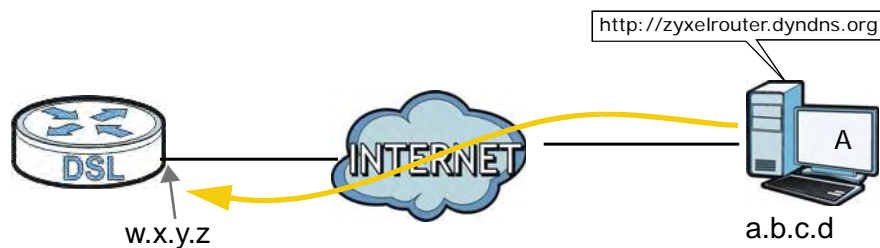
Class Name	Give a class name to this traffic, such as E-mail in this example.
From Interface	This is the interface from which the traffic will be coming from. Select LAN1 for this example.
Ether Type	Select IP to identify the traffic source by its IP address or MAC address.
IP Address	Type the IP address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

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

- 4 Verify that the queue setup works by checking **Network Setting > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.

4.7 Access the VMG Using DDNS

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



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

This tutorial covers:

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

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

4.7.1 Registering a DDNS Account on www.dyndns.org

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

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

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

Dynamic DNS Setup

Dynamic DNS: ☐ Enable ☒ Disable

Service Provider:

Hostname:

Username:

Password:

Dynamic DNS Status

User Authentication Result:

Last Updated Time:

Current Dynamic IP:

Apply **Cancel**

Click **Apply**.

4.7.3 Testing the DDNS Setting

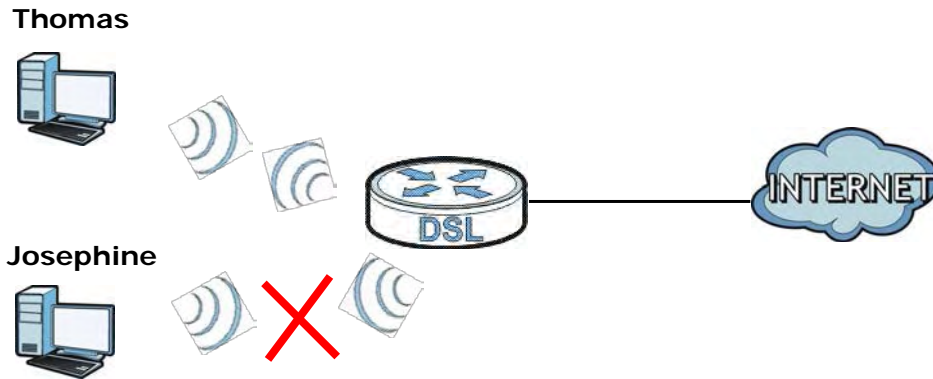
Now you should be able to access the VMG from the Internet. To test this:

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

4.8 Configuring the MAC Address Filter

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

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



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

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

MAC Restrict Mode : ☒ Allow ☐ Deny

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

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

Apply **Cancel**

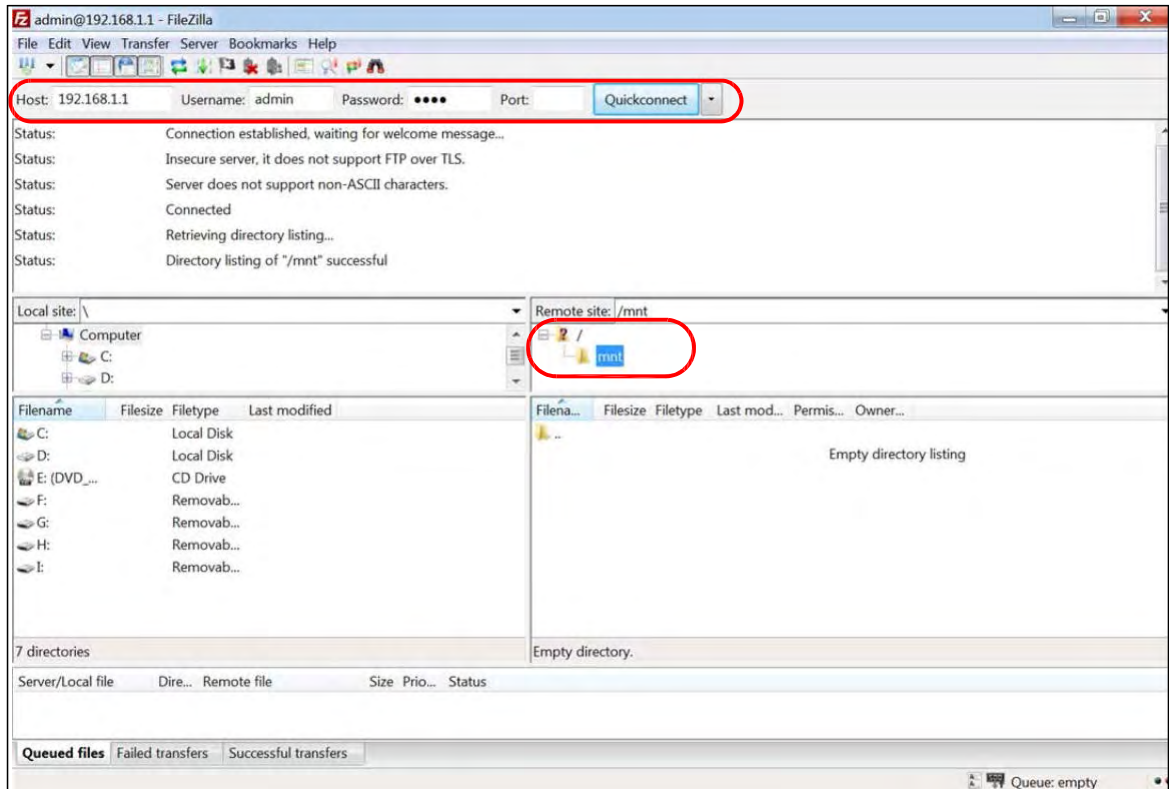
Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the VMG.

4.9 Access Your Shared Files From a Computer

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

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

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



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

PART II

Technical Reference

Network Map and Status Screens

5.1 Overview

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

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

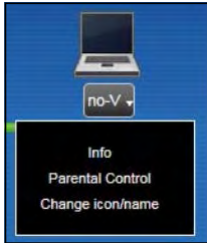
5.2 The Network Map Screen

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

Figure 16 Network Map: Icon View Mode



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



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

Figure 17 Network Map: List View Mode



5.3 The Status Screen

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

Figure 18 Status Screen



Each field is described in the following table.

Table 5 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen.
Device Information	
Host Name	This field displays the VMG system name. It is used for identification.
Model Number	This shows the model number of your VMG.
Serial Number	This shows the serial number of your VMG.
Firmware Version	This is the current version of the firmware inside the VMG.
WAN Information (These fields display when you have a WAN connection.)	
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IP address of the VMG in the WAN. Click Release to release your IP address to 0.0.0.0. If you want to renew your IP address, click Renew .
IP Subnet Mask	This field displays the current subnet mask in the WAN.

Table 5 Status Screen (continued)

LABEL	DESCRIPTION
MAC Address	This field displays the WAN Ethernet adapter MAC (Media Access Control) Address of your VMG.
Primary/ Secondary DNS Server	This field displays the first/second DNS server IP address assigned to the VMG.
DHCP	<p>This field displays whether the WAN interface is using a DHCP IP address or a static IP address. Choices are:</p> <p>Client - The WAN interface can obtain an IP address from a DHCP server.</p> <p>None - The WAN interface is using a static IP address.</p>
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 is the current IPv6 link local address of the VMG in the LAN.
DHCP	<p>This field displays what DHCP services the VMG is providing to the LAN. The possible values are:</p> <p>Server - The VMG is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN.</p> <p>Relay - The VMG acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.</p> <p>Disable - The VMG is not providing any DHCP services to the LAN.</p>
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your VMG.
WLAN 2.4G Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of the wireless interface.
Status	This displays whether the WLAN is activated.
SSID	This is the descriptive name used to identify the VMG in a wireless LAN.
Channel	This is the channel number used by the wireless interface now.
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.
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	<p>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 139).</p>

Table 5 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 246 , 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 No Link when not using the interface.</p> <p>For the 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 No Link when not using the interface.</p> <p>For the 3G interface, this field displays Up when using the interface and No Device when no device is detected in any USB slot.</p>
Rate	<p>For the LAN and Ethernet WAN interfaces, this displays the port speed and duplex setting.</p> <p>For the DSL interface, it displays the downstream and upstream transmission rate.</p> <p>For the WLAN interface, it displays the maximum transmission rate or N/A with WLAN disabled.</p> <p>For the 3G interface, this field displays signal strength bars when a 3G device is installed in a USB slot and N/A when no device is detected in the USB slot.</p>

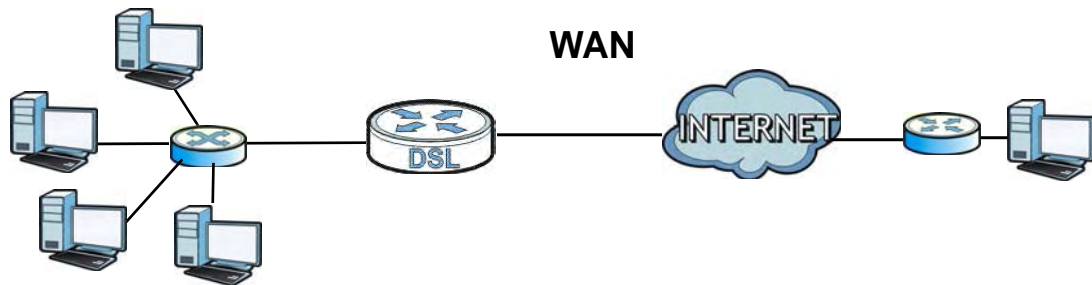
Broadband

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 19 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 63](#)).
- Use the **3G Backup** screen to configure 3G WAN connection ([Section 6.3 on page 71](#)).
- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions ([Section 6.4 on page 76](#)).
- Use the **Ethernet WAN** screen to convert LAN port number four as a WAN port or restore the Ethernet WAN port to a LAN port ([Section 6.5 on page 79](#)).
- Use the **802.1x** screen to view and configure the IEEE 802.1X settings on the VMG ([Section 6.6 on page 80](#)).

Table 6 WAN Setup Overview

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

6.1.2 What You Need to Know

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

WAN IP Address

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

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

ATM

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

PTM

Packet Transfer Mode (PTM) is packet-oriented and supported by the VDSL2 standard. In PTM, packets are encapsulated directly in the High-level Data Link Control (HDLC) frames. It is designed

to provide a low-overhead, transparent way of transporting packets over DSL links, as an alternative to ATM.

IPv6 Introduction

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

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

IPv6 Prefix and Prefix Length

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

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

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

IPv6 Subnet Masking

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

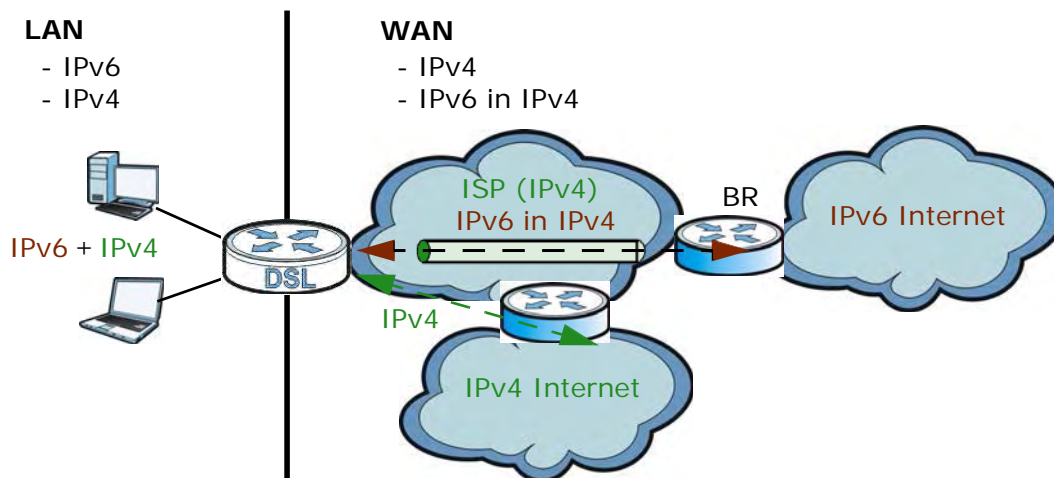
IPv6 Rapid Deployment

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

The VMG generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local

network can also use IPv4 services. The VMG uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 20 IPv6 Rapid Deployment

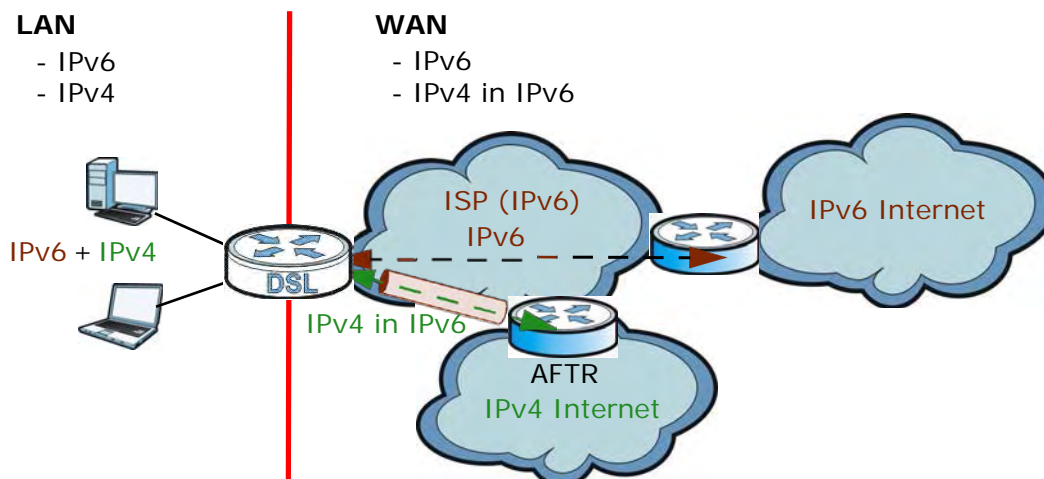


Dual Stack Lite

Use Dual Stack Lite when local network computers use IPv4 and the ISP has an IPv6 network. When the 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 21 Dual Stack Lite





6.1.3 Before You Begin

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

6.2 The Broadband Screen

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

Figure 22 Network Setting > Broadband

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

The following table describes the labels in this screen.

Table 7 Network Setting > Broadband

LABEL	DESCRIPTION
Add New WAN Interface	Click this button to create a new connection.
#	This is the index number of the entry.
Name	This is the service name of the connection.
Type	This shows whether it is an ATM, a PTM or an Ethernet connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays 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 ATM** connection type, **Routing** mode, and **PPPoE** encapsulation. The screen varies when you select other interface type, encapsulation, and IPv6/IPv4 mode.

Figure 23 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)

The screenshot shows the 'Add New WAN Interface' configuration window. The window is titled 'Add New WAN Interface' and has a close button (X) in the top right corner. The configuration is organized into several sections:

- General:**
 - Name: (text input field)
 - Type: (dropdown menu showing 'ADSL/VDSL over PTM')
 - Mode: (radio buttons for 'Routing' (selected) and 'Bridge')
 - Encapsulation: (dropdown menu showing 'PPPoE')
 - IPv4/IPv6 Mode: (dropdown menu showing 'IPv4 Only')
- PPP Information:**
 - PPP User Name: (text input field showing 'admin')
 - PPP Password: (password input field with masked characters '****')
 - password unmask: (checkbox, unchecked)
 - PPP Connection Trigger: (radio buttons for 'Auto Connect' (selected) and 'On Demand')
 - PPPoE Passthrough: (radio buttons for 'Enable' and 'Disable' (selected))
- IP Address:**
 - Obtain an IP Address Automatically: (radio button, selected)
 - Static IP Address: (radio button, unselected)
- VLAN:**
 - Active: (radio buttons for 'Enable' and 'Disable' (selected))
 - 802.1p: (dropdown menu showing '0')
 - 802.1q: (text input field showing '0' with a range '(0~4094)' next to it)
- MTU:**
 - MTU: (text input field showing '1492')
- Routing Feature:**
 - NAT Enable: (radio buttons for 'Enable' (selected) and 'Disable')
 - Fullcone NAT Enable: (radio buttons for 'Enable' and 'Disable' (selected))
 - IGMP Proxy Enable: (radio buttons for 'Enable' (selected) and 'Disable')
 - Apply as Default Gateway: (radio buttons for 'Enable' (selected) and 'Disable')
- DNS server:**
 - Obtain DNS Info Automatically: (radio button, selected)
 - Use Following Static DNS Address: (radio button, unselected)
- 6RD:**
 - 6RD: (radio buttons for 'Enable' and 'Disable' (selected))
 - Automatically configured by DHCP: (radio button, unselected)
 - Manually Configured: (radio button, selected)
 - Service Provider IPv6 Prefix: (text input field)
 - IPv4 Mask Length: (text input field)
 - Border Relay IPv4 Address: (text input field)
- Bridge and Routing mode in the same WAN:**
 - Enable Con-current WAN: (radio buttons for 'Enable' (selected) and 'Disable')
 - Bridge Port 1: (checkbox, unchecked)
 - Bridge Port 2: (checkbox, unchecked)
 - Bridge Port 3: (checkbox, unchecked)
 - Bridge Port 4: (checkbox, unchecked)

At the bottom right of the window are 'OK' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 8 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)

LABEL	DESCRIPTION
General	
Name	Specify a descriptive name for this connection.
Type	Select whether it is an ADSL/VDSL over PTM or ADSL over ATM connection.
Mode	Select Routing if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	<p>Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select Routing in the Mode field.</p> <p>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.</p>
IPv4/IPv6 Mode	<p>Select IPv4 Only if you want the VMG to run IPv4 only.</p> <p>Select IPv4 IPv6 DualStack to allow the VMG to run IPv4 and IPv6 at the same time.</p> <p>Select IPv6 Only if you want the VMG to run IPv6 only.</p>
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	<p>Select when to have the VMG establish the PPP connection.</p> <p>Auto Connect - select this to not let the connection time out.</p> <p>On Demand - select this to automatically bring up the connection when the VMG receives packets destined for the Internet.</p>
Idle Timeout	<p>This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.</p> <p>This field is not available if you select Auto Connect in the PPP Connection Trigger field.</p>
PPPoE Passthrough	<p>This field is available when you select PPPoE encapsulation.</p> <p>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.</p> <p>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.</p>
IP Address (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.

Table 8 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
Gateway IP Address	Enter the gateway IP address provided by your ISP.
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	<p>Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:</p> <ul style="list-style-type: none"> • LLC/SNAP-BRIDGING: In 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 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.
Service Category	<p>Select UBR Without PCR or UBR With PCR for applications that are non-time sensitive, such as e-mail.</p> <p>Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
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	<p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.</p> <p>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.</p>
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
MTU	
MTU	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Routing Feature (This is available only when you select 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	<p>Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p> <p>Select this option to have the VMG act as an IGMP proxy on this connection. This allows the VMG to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.</p>
Apply as Default Gateway	Select this option to have the VMG use the WAN interface of this connection as the system default gateway.

Table 8 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
DNS Server (This is available only when you select IPv4 Only or IPv4 IPv6 DualStack in the IPv4/IPv6 Mode field.)	
	<p>Select Obtain DNS Info Automatically if you want the VMG to use the DNS server addresses assigned by your ISP.</p> <p>Select Use Following Static DNS Address if you want the VMG to use the DNS server addresses you configure manually.</p>
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Tunnel	
<p>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 62 for more information.</p>	
Enabled 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	
<p>The 6RD (IPv6 rapid deployment) fields display when you set the IPv6/IPv4 Mode field to IPv4 Only. See IPv6 Rapid Deployment on page 61 for more information.</p>	
6RD	Select Enable to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
	<p>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.</p> <p>The Automatically configured by DHCP option is configurable only when you set the method of encapsulation to IPoE.</p>
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	<p>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.</p> <p>Select Option 121 to have the VMG push static routes to clients.</p>
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.

Table 8 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode) (continued)

LABEL	DESCRIPTION
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.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
IPv6 Default Gateway	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your VMG's interface(s). The gateway helps forward packets to their destinations.
IPv6 Routing Feature (This is available only when you select 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 checkbox to have the VMG act as an MLD proxy on this connection. This allows the VMG to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the VMG use the WAN interface of this connection as the system default gateway.
IPv6 DNS Server (This is available only when you select 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.
<p>Bridging and Routing in the same WAN</p> <p>Use this feature to bridge a LAN port(s) with the WAN interface. Traffic to/from LAN ports not in the bridge is routed from the WAN interface.</p> <p>ADSL use same VPI/VCI in Bridge and Route modes.</p> <p>VDSL use same VLAN in Bridge and Route modes.</p>	
Enable Concurrent WAN	<p>Enable this if you want to use the same VPI/VCI settings in different WAN interfaces. Select this and then choose the ports to bridge with the WAN interface.</p> <ul style="list-style-type: none"> ADSL concurrent WAN uses the same VCI/PVI in both routing and bridge modes. VDSL concurrent WAN uses same VLAN in both routing and bridge mode.
OK	Click OK 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 24 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM - Bridge Mode)

The following table describes the fields in this screen.

Table 9 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM - Bridge or Ethernet Mode)

LABEL	DESCRIPTION
General	
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	This section is available only when you select ADSL/VDSL over PTM in the Type field.
Active	Select the checkbox 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.

Table 9 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL/VDSL over PTM - Bridge or Ethernet Mode) (continued)

LABEL	DESCRIPTION
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 25 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

The following table describes the fields in this screen.

Table 10 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode)

LABEL	DESCRIPTION
General	
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 10 Network Setting > Broadband > Add New WAN Interface/Edit (ADSL over ATM-Bridge Mode) (continued)

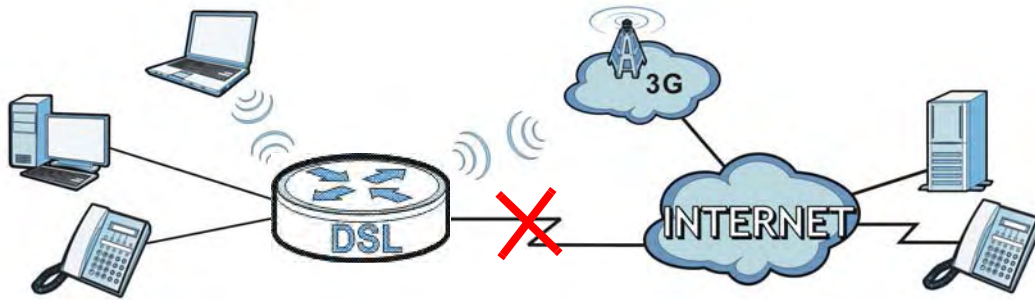
LABEL	DESCRIPTION
Encapsulation	<p>Select the method of multiplexing used by your ISP from the drop-down list box. Choices are:</p> <ul style="list-style-type: none"> • LLC/SNAP-BRIDGING: In LLC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. 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	<p>Select UBR Without PCR for applications that are non-time sensitive, such as e-mail.</p> <p>Select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic.</p> <p>Select Non Realtime VBR (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.</p> <p>Select Realtime VBR (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.</p>
VLAN	
Active	Select the checkbox to enable VLAN on this WAN interface.
802.1p	<p>IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service.</p> <p>Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.</p>
802.1q	Type the VLAN ID number (from 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 The 3G Backup Screen

The USB ports (at the left side panel of the VMG) allow you to attach a 3G dongle to wirelessly connect to a 3G network for Internet access. You can have the VMG use the 3G WAN connection as a backup. Disconnect the DSL and Ethernet WAN ports to use the 3G dongle as your primary WAN connection. The VMG automatically uses a wired WAN connection when available.

Note: This VMG supports connecting one 3G dongle at a time.

Figure 26 Internet Access Application: 3G WAN



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

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

Figure 27 Network Setting > Broadband > 3G Backup

General

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

trigger 3G backup when physical link of primary WAN is down

Ping Check
☐ Enable ☒ Disable

Check Cycle : Every 60 (20~180 Sec)

Consecutive Fail : 3 (2~5 times)

☐ Ping Default Gateway

☒ Ping the Host 8.8.8.8 (Host Name or IP address)

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

3G Connection Settings

Card description : N/A

Username : (Optional)

Password : (Optional)

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

Dial string : *99#

APN : internet

Connection : Nailed UP

☒ Obtain an IP Address Automatically
☐ Use the following static IP address
☒ Obtain DNS info Dynamically
☐ Use the following static DNS IP address

Enable E-mail Notification ☐ Enable ☒ Disable

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

Budget Setup

Enable Budget Control ☐ Enable ☒ Disable

☐ Time Budget: 0 hours per month

☐ Data Budget: 0 Mbytes Download/Upload per month

☐ Data Budget: 0 kPackets Download/Upload per month

Reset all budget counters on last day of the month

Reset time and data budget counters

Actions before over budget:

☐ Enable 0 % of time budget
☐ Enable 0 % of data budget (Mbytes)
☐ Enable 0 % of data budget (Packets)

Actions when over budget:

Current 3G connection: keep

Actions:

Enable E-mail Notification ☐ Enable ☒ Disable
☐ Enable Log: Interval 0 minutes

Note:
Budget Control is an approximate value.

[Basic](#)

Apply Cancel

The following table describes the labels in this screen.

Table 11 Network Setting > Broadband > 3G Backup

LABEL	DESCRIPTION
General	
3G Backup	Select Enable to have the VMG use the 3G connection as your WAN or a backup when the wired WAN connection fails.
Ping Check	Select Enable if you want the VMG to ping check the connection status of your WAN. You can configure the frequency of the ping check and number of consecutive failures before triggering 3G backup.
Check Cycle	Enter the frequency of the ping check in this field.
Consecutive Fail	Enter how many consecutive failures are required before 3G backup is triggered.
Ping Default Gateway	Select this to have the VMG ping the WAN interface's default gateway IP address.
Ping the Host	Select this to have the VMG ping the particular host name or IP address you typed in this field.
3G Connection Settings	
Card description	This field displays the manufacturer and model name of your 3G card if you inserted one in the VMG. Otherwise, it displays N/A .
Username	Type the user name (of up to 64 ASCII printable characters) given to you by your service provider.
Password	Type the password (of up to 64 ASCII printable characters) associated with the user name above.
PIN	A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card. If your ISP enabled PIN code authentication, enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, leave this field blank.
Dial string	Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number. For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan.
APN	Enter the APN (Access Point Name) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 32 ASCII printable characters. Spaces are allowed.
Connection	Select Nailed UP if you do not want the connection to time out. Select on Demand if you do not want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.
Max Idle Timeout	This value specifies the time in minutes that elapses before the VMG automatically disconnects from the ISP.
Obtain an IP Address Automatically	Select this option if your ISP did not assign you a fixed IP address.
Use the following static IP address	Select this option if the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected Use the following static IP address .

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

LABEL	DESCRIPTION
Subnet Mask	Enter the subnet mask of the IP address.
Obtain DNS info Dynamically	Select this to have the VMG get the DNS server addresses from the ISP automatically.
Use the following static DNS IP address	Select this to have the VMG use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Enable E-mail Notification	Select this to enable the e-mail notification function. The VMG will e-mail you a notification when the 3G connection is up.
Mail Account	Select an e-mail address you have configured in Maintenance > Email Notification . The VMG uses the corresponding mail server to send notifications. You must have configured a mail server already in the Maintenance > Email Notification screen.
3G Backup E-mail Title	Type a title that you want to be in the subject line of the e-mail notifications that the VMG sends.
Send Notification to E-mail	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail.
Advanced	Click this to show the advanced 3G backup settings.
Budget Setup	
Enable Budget Control	Select Enable to set a monthly limit for the user account of the installed 3G card. You can set a limit on the total traffic and/or call time. The VMG takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the 3G connection can be used within one month. If you change the value after you configure and enable budget control, the VMG resets the statistics.
Data Budget (Mbytes)	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month. Select Download/Upload to set a limit on the total traffic in both directions. Select Download to set a limit on the downstream traffic (from the ISP to the VMG). Select Upload to set a limit on the upstream traffic (from the VMG to the ISP). If you change the value after you configure and enable budget control, the VMG resets the statistics.
Data Budget (kPackets)	Select this and specify how much downstream and/or upstream data (in k Packets) can be transmitted via the 3G connection within one month. Select Download/Upload to set a limit on the total traffic in both directions. Select Download to set a limit on the downstream traffic (from the ISP to the VMG). Select Upload to set a limit on the upstream traffic (from the VMG to the ISP). If you change the value after you configure and enable budget control, the VMG resets the statistics.
Reset all budget counters on	Select the date on which the VMG resets the budget every month. Select last if you want the VMG to reset the budget on the last day of the month. Select specific and enter the number of the date you want the VMG to reset the budget

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

LABEL	DESCRIPTION
Reset time and data budget counters	Click this button to reset the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.
Actions before over budget	Specify the actions the VMG takes before the time or data limit exceeds.
Enable % of time budget/ data budget (Mbytes)/data budget (kPackets)	Select Enable and enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the VMG resets the statistics.
Actions when over budget	Specify the actions the VMG takes when the time or data limit is exceeded.
Current 3G connection	Select Keep to maintain an existing 3G connection or Drop to disconnect it.
Actions	
Enable E-mail Notification	Select Enable to enable the e-mail notification function. The VMG will e-mail you a notification when there over budget occurs.
Mail Account	Select an e-mail address you have configured in Maintenance > Email Notification . The VMG uses the corresponding mail server to send notifications. You must have configured a mail server already in the Maintenance > Email Notification screen.
3G Backup E-mail Title	Type a title that you want to be in the subject line of the e-mail notifications that the VMG sends.
Send Notification to E-mail	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail.
Enable Log	Select this to activate the logging function at the interval you set in this field.
Interval	Enter the interval of how many minutes you want the VMG to e-mail you.
Basic	Click this to hide the advanced settings of 3G backup.
Apply	Click Apply to save your changes back to the VMG.
Cancel	Click Cancel to return to the previous configuration.

6.4 The Advanced Screen

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 12 VDSL Profiles

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

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

Figure 28 Network Setting > Broadband > Advanced

DSL Capabilities

PhyR US : ☐ Enable ☒ Disable
PhyR DS : ☒ Enable ☐ Disable
Bitswap : ☒ Enable ☐ Disable
SRA : ☒ Enable ☐ Disable

ADSL 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

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
US0 : ☒ Enable ☐ Disable

Apply

Cancel

The following table describes the labels in this screen.

Table 13 Network Setting > Broadband > Advanced

LABEL	DESCRIPTION
DSL Capabilities	
PhyR US	Enable or disable PhyR US (upstream) for upstream transmission to the WAN. PhyR US should be enabled if data being transmitted upstream is sensitive to noise. However, enabling PhyR US can decrease the US line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
PhyR DS	Enable or disable PhyR DS (downstream) for downstream transmission from the WAN. PhyR DS should be enabled if data being transmitted downstream is sensitive to noise. However, enabling PhyR DS can decrease the DS line rate. Enabling or disabling PhyR will require the CPE to retrain. For PhyR to function, the DSLAM must also support PhyR and have it enabled.
Bitswap	Select Enable to allow the 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.
ADSL 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.
Annex M	Annex M is an optional specification in ITU-T recommendations G.992.3 (ADSL2) and G.992.5 (ADSL2+), also referred to as ADSL2 M and ADSL2+ M. This specification extends the capability of commonly deployed Annex A by more than doubling the number of upstream bits. The data rates can be as high as 12 or 24 Mbit/s downstream and 3 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises.
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.	

Table 13 Network Setting > Broadband > Advanced (continued)

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

6.5 The Ethernet WAN Screen

Use the **Ethernet WAN** screen to convert LAN port number four as a WAN port for Ethernet Internet access and to restore it back from a WAN port to a LAN port.

It's not enough to just enable LAN 4 as a WAN port here. You must also go to **Network Setting > Broadband** screen and create a new interface for it with the **Type** as **Ethernet** and **Encapsulation** as **IPoE**, and it's advisable to enable NAT.

Note: You cannot have DSL and Ethernet WAN connections working at the same time.

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

Figure 29 Network Setting > Broadband > Ethernet WAN

Active : ☒ Enable ☐ Disable

Notes:

1. Active Enable, the Ethernet Port is WAN Ethernet.
2. Active Disable, the Ethernet Port is LAN Ethernet.
3. Please don't connect Ethernet WAN cable and xDSL line at the same time.

Apply Cancel

The following table describes the labels in this screen.

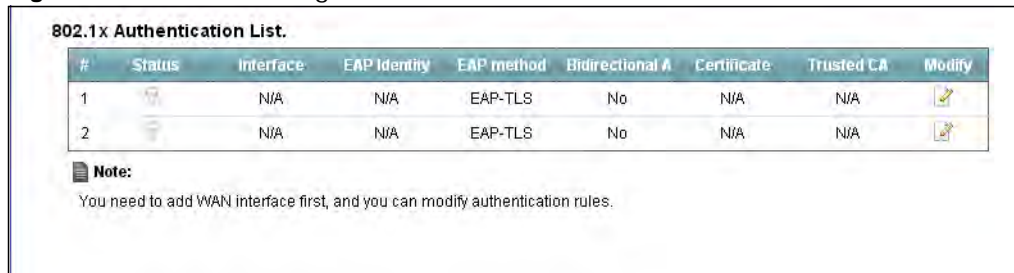
Table 14 Network Setting > Network Setting > Ethernet WAN

LABEL	DESCRIPTION
Active	Select Enable to convert LAN port number four to a WAN port. Select Disable to restore LAN port number four to a LAN port.
Apply	Click Apply to save your changes back to the VMG.
Cancel	Click Cancel to return to the previous configuration.

6.6 The 802.1x Screen

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

Figure 30 Network Setting > Broadband > 802.1x



#	Status	Interface	EAP Identity	EAP method	Bidirectional A	Certificate	Trusted CA	Modify
1		N/A	N/A	EAP-TLS	No	N/A	N/A	
2		N/A	N/A	EAP-TLS	No	N/A	N/A	

Note:
You need to add WAN interface first, and you can modify authentication rules.

The following table describes the labels in this screen.

Table 15 Network Setting > Network Setting > 802.1x

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field displays whether the authentication is active or not. A yellow bulb signifies that this authentication is active. A gray bulb signifies that this authentication is not active.
Interface	This is the interface that uses the authentication. This displays N/A when there is no interface assigned.
EAP Identity	This shows the EAP identity of the authentication. This displays N/A when there is no EAP identity assigned.
EAP method	This shows the EAP method used in the authentication. This displays N/A when there is no EAP method assigned.
Bidirectional Authentication	This shows whether bidirectional authentication is allowed.
Certificate	This shows the certificate used for this authentication. This displays N/A when there is no certificate assigned.
Trusted CA	This shows the Trusted CA used for this authentication. This displays N/A when there is no Trusted CA assigned.
Modify	Click this icon to edit an item.

6.6.1 Modify 802.1X Settings

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

Figure 31 Network Setting > Broadband > 802.1x > Modify

The following table describes the labels in this screen.

Table 16 Network Setting > Broadband > 802.1x: Edit

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

6.7 Technical Reference

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

Encapsulation

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

IP over Ethernet

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

PPP over ATM (PPPoA)

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

PPP over Ethernet (PPPoE)

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

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

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

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

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

RFC 1483

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

Multiplexing

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

VC-based Multiplexing

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

LLC-based Multiplexing

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

Traffic Shaping

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

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

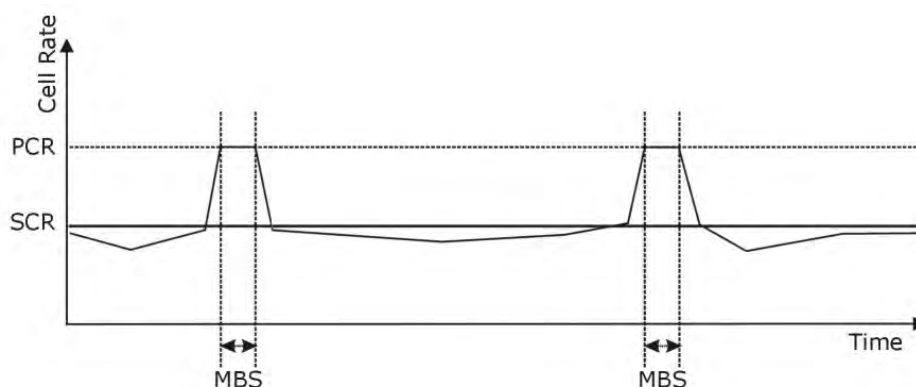
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

Figure 32 Example of Traffic Shaping



ATM Traffic Classes

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

Constant Bit Rate (CBR)

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

Variable Bit Rate (VBR)

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

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

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

Unspecified Bit Rate (UBR)

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

IP Address Assignment

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

Introduction to VLANs

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

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

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

Introduction to IEEE 802.1Q Tagged VLAN

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

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

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

Multicast

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

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

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

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely

important because without it, you must know the IP address of a computer before you can access it.

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

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

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

IPv6 Prefix and Prefix Length

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

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

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

Wireless

7.1 Overview

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

7.1.1 What You Can Do in this Chapter

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

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode ([Section 7.2 on page 88](#)).
- Use the **Guest/More AP** screen to set up multiple wireless networks on your VMG ([Section 7.3 on page 93](#)).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the VMG ([Section 7.4 on page 97](#)).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) ([Section 7.5 on page 98](#)).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications ([Section 7.6 on page 99](#)).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold ([Section 7.7 on page 100](#)).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results ([Section 7.8 on page 102](#)).

7.1.2 What You Need to Know

Wireless Basics

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

Finding Out More

See [Section 7.9 on page 103](#) for advanced technical information on wireless networks.

7.2 The General Screen

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

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

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

Figure 33 Network Setting > Wireless > General

Wireless Network Setup

Bandwidth: 2.4GHz ▾

Wireless: ☒ Enable ☐ Disable (settings are invalid when disabled)

Channel: Auto ▾ Current: 6

Bandwidth: 20MHz ▾

Control Sideband: None ▾

Passphrase Type: Fixed ▾

Passphrase Key:

Wireless Network Settings

Wireless Network Name: ZyXEL_0002

Max Clients: 32

☐ Hide SSID

☒ Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Note

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

BSSID: 02:10:18:01:00:02

Security Level

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

Security Mode: WPA2-PSK ▾

☒ Generate password automatically

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

Password: [hide](#)

☐ password unmask

Encryption: AES ▾

Group Key Update Timer: 3600 sec

Apply **Cancel**

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

Table 17 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless Network Setup	
Band	This shows the wireless band which this radio profile is using. 2.4GHz is the frequency used by IEEE 802.11b/g/n wireless clients.
Wireless	You can Enable or Disable the wireless LAN in this field.
Channel	Use Auto to have the VMG automatically determine a channel to use.

Table 17 Network Setting > Wireless > General (continued)

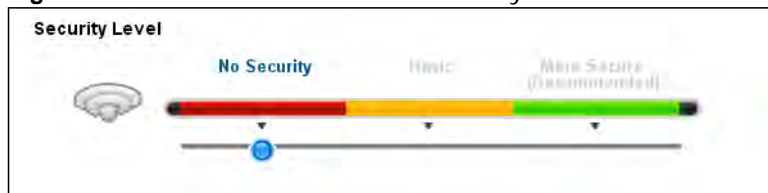
LABEL	DESCRIPTION
Bandwidth	<p>Select whether the VMG uses a wireless channel width of 20MHz or 40MHz.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>
Control Sideband	<p>This is available for some regions when you select a specific channel and set the Bandwidth field to 40MHz. Set whether the control channel (set in the Channel field) should be in the Lower or Upper range of channel bands.</p>
Passphrase Type	<p>If you set security for the wireless LAN and have the VMG generate a password, the setting in this field determines how the VMG generates the password.</p> <p>Select None to set the VMG's password generation to not be based on a passphrase.</p> <p>Select Fixed to use a 16 character passphrase for generating a password.</p> <p>Select Variable to use a 16 to 63 character passphrase for generating a password.</p>
Passphrase Key	<p>For a fixed type passphrase enter 16 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.</p> <p>For a variable type passphrase enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.</p>
Wireless Network Settings	
Wireless Network Name (SSID)	<p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID.</p> <p>Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.</p>
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Multicast Forwarding	Select this check box to allow the VMG to convert wireless multicast traffic into wireless unicast traffic.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the VMG when wireless LAN is enabled.
Security Level	<p>Select Basic (WEP) or More Secure (WPA-PSK, WPA2-PSK, WPA-WPA2-Personal) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the VMG. When you select to use a security, additional options appears in this screen.</p> <p>Or you can select No Security to allow any client to associate this network without any data encryption or authentication.</p> <p>See the following sections for more details about this field.</p>
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.2.1 No Security

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

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

Figure 34 Wireless > General: No Security



The following table describes the labels in this screen.

Table 18 Wireless > General: No Security

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

7.2.2 Basic (WEP Encryption)

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

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

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

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

Figure 35 Wireless > General: Basic (WEP)

Security Level

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

Security Mode: WEP

☒ Generate password automatically

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

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

☒ Password 1: E630549ED897C3432D [hide more](#)

☐ Password 2:

☐ Password 3:

☐ Password 4:

☒ password unmask

WEP Encryption: 128-bit

The following table describes the labels in this screen.

Table 19 Wireless > General: Basic (WEP)

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

7.2.3 More Secure (WPA(2)-PSK)

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

Click **Network Setting > Wireless** to display the **General** screen. Select **More Secure** as the security level.

Note: **WPA-PSK** or **WPA-WPA2-Personal** is not available if you enable WPS before you configure them.

Figure 36 Wireless > General: More Secure: WPA2-PSK

Security Level

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

Security Mode: WPA2-PSK

☒ Generate password automatically

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

Password: ***** [hide more](#)

☐ password unmask

Encryption: AES

Group Key Update Timer: 3600 sec

The following table describes the labels in this screen.

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

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

7.3 The Guest/More AP Screen

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

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

Figure 37 Network Setting > Wireless > Guest/More AP

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

The following table describes the labels in this screen.

Table 21 Network Setting > Wireless > Guest/More AP

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

7.3.1 Edit Guest/More AP

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

Figure 38 Network Setting > Wireless > Guest/More AP > Edit

More AP Edit

Wireless Network Setup

Wireless ☐ Enable ☒ Disable (settings are invalid when disabled)

Passphrase Type

Passphrase Key

Wireless Network Settings

Wireless Network Name(SSID):

☐ Hide SSID

☒ Multicast Forwarding

☒ Guest WLAN

Access Scenario:

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Note:

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

SSID Subnet: ☒ Enable ☐ Disable

DHCP Start Address:

DHCP End Address:

SSID Subnet Mask:

LAN IP Address:

Security Level

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

Security Mode

☒ Generate password automatically

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

Password

[more...](#)

The following table describes the fields in this screen.

Table 22 Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can Enable or Disable the wireless LAN in this field.
Passphrase Type	<p>If you set security for the wireless LAN and have the VMG generate a password, the setting in this field determines how the VMG generates the password.</p> <p>Select None to set the VMG's password generation to not be based on a passphrase.</p> <p>Select Fixed to use a 16 character passphrase for generating a password.</p> <p>Select Variable to use a 16 to 63 character passphrase for generating a password.</p>

Table 22 Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Passphrase Key	For a fixed type passphrase enter 16 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive. For a variable type passphrase enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Multicast Forwarding	Select this check box to allow the VMG to convert wireless multicast traffic into wireless unicast traffic.
Guest WLAN	Select this to create Guest WLANs for home and external clients. Select the WLAN type in the Access Scenario field.
Access Scenario	If you select Home Guest , clients connecting to the same SSID can communicate with each other directly. If you select External Guest , clients are blocked from connecting to each other directly. Move your mouse over the network icon next to the drop-down list box to view the corresponding network topology.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
SSID Subnet	Select Enable if you want the wireless network interface to assign DHCP IP addresses to the associated wireless clients.
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool. The VMG assigns IP addresses from this DHCP pool to wireless clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the VMG for the SSID subnet.
LAN IP Address	Specify the IP address of the VMG for the SSID subnet.
Security Level	
Security Mode	Select Basic (WEP) or More Secure (WPA-PSK, WPA2-PSK, WPA-WPA2-Personal) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the VMG. After you select to use a security, additional options appears in this screen. Or you can select No Security to allow any client to associate this network without any data encryption or authentication. See Section 7.2.1 on page 91 for more details about this field.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

7.4 The MAC Authentication Screen

This screen allows you to configure the VMG to give exclusive access to specific devices (Allow) or exclude specific devices from accessing the VMG (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:01:23:45. You need to know the MAC addresses of the devices to configure this screen.

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

Figure 39 Network Setting > Wireless > MAC Authentication

The screenshot shows the 'MAC Authentication' configuration screen. Under the 'General' tab, the 'SSID' is 'ZyXEL_0002' and 'MAC Restrict Mode' is 'Deny'. The 'MAC address List' section contains an 'Add new MAC address' button and a table with columns for index number, MAC address, and a 'Modify' button. The bottom of the screen has 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 23 Network Setting > Wireless > Authentication

LABEL	DESCRIPTION
General	
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	<p>Define the filter action for the list of MAC addresses in the MAC address list.</p> <p>Select Disable to turn off MAC filtering.</p> <p>Select Deny to block access to the VMG. MAC addresses not listed will be allowed to access the VMG.</p> <p>Select Allow to permit access to the VMG. MAC addresses not listed will be denied access to the VMG.</p>
MAC address List	
Add new MAC address	<p>Click this if you want to add a new MAC address entry to the MAC filter list below. This button is not configurable when you select Disable in the MAC Restrict Mode field.</p> <p>Enter the MAC addresses of the wireless devices that are allowed or denied access to the VMG. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.</p>
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the VMG.
Modify	<p>Click the Edit icon to change the MAC address.</p> <p>Click the Delete icon to remove the entry.</p>
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.5 The WPS Screen

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

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See [Section 7.9.8.3 on page 111](#) for more information about WPS.

Note: The VMG applies the security settings of the **SSID1** profile (see [Section 7.2 on page 88](#)). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA2-PSK** or **No Security**.

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

Figure 40 Network Setting > Wireless > WPS

The screenshot shows the 'General' tab of the WPS configuration screen. At the top, there's a 'WPS' section with 'Enable' selected and 'Disable' (settings are invalid when disabled) as an option. Below this is the 'Add a new device with WPS Method' section, which contains three panels: Method 1 (PBC), Method 2 (PIN), and Method 3 (AP's PIN). Each panel has 'Enable' and 'Disable' radio buttons. Method 1 instructions: Step 1. Click WPS button [WPS button icon]; Step 2. Press the WPS button on your new wireless client device within 120 seconds. Method 2 instructions: Step 1. Enter the PIN of your new wireless client device and then click Register [Register button]; Step 2. Press the WPS button on your new wireless client device within 120 seconds. Method 3 instructions: Enter AP's PIN Number in Wireless Client; Current state: Configured; 1. Please release configuration if you want to configure the wireless settings [Release Configuration button]; 2. Enter current PIN number on your wireless client [Generate New PIN button]. At the bottom, there's a 'Note' section with two points: 1. If you enable WPS, it will turn on UPnP service automatically. 2. This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured. 'Apply' and 'Cancel' buttons are at the bottom right.

The following table describes the labels in this screen.

Table 24 Network Setting > Wireless > WPS

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

Table 24 Network Setting > Wireless > WPS (continued)

LABEL	DESCRIPTION
Register	<p>Enter the PIN of the device that you are setting up a WPS connection with and click Register to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the VMG.</p>
Method 3	Use this section to set up a WPS wireless network by entering the PIN of the VMG into the client. Select Enable and click Apply to activate WPS method 3 on the VMG.
Release Configuration	<p>The default WPS status is configured.</p> <p>Click this button to remove all configured wireless and wireless security settings for WPS connections on the VMG.</p>
Generate New PIN Number	<p>If this method has been enabled, the PIN (Personal Identification Number) of the VMG is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS.</p> <p>The PIN is not necessary when you use WPS push-button method.</p> <p>Click the Generate New PIN button to have the VMG create a new PIN.</p>
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.6 The WMM Screen

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

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

Figure 41 Network Setting > Wireless > WMM

WMM of SSID1 : ☒ Enable ☐ Disable

WMM of SSID2 : ☒ Enable ☐ Disable

WMM of SSID3 : ☒ Enable ☐ Disable

WMM of SSID4 : ☒ Enable ☐ Disable

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

The following table describes the labels in this screen.

Table 25 Network Setting > Wireless > WMM

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

7.7 The Others Screen

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

See [Section 7.9.2 on page 105](#) for detailed definitions of the terms listed in this screen.

Figure 42 Network Setting > Wireless > Others

The screenshot displays the 'Network Setting > Wireless > Others' configuration screen. It contains the following settings:

- RTS/CTS Threshold : 2347
- Fragmentation Threshold : 2346
- Auto Channel Timer : 0 min
- Output Power : 100% ▼
- Beacon Interval : 100 ms
- DTIM Interval : 1 ms
- 802.11 Mode : 802.11b/g/n Mixed ▼
- 802.11 Protection : Off ▼
- RIFS Advertisement : Auto ▼
- Preamble : Long ▼
- RX Chain Power Save : ☒ Enable ☐ Disable
- OBSS Coexistence : ☒ Enable ☐ Disable
- XPress™ Technology : ☒ Enable ☐ Disable
- WPS 2.0 : ☒ Enable ☐ Disable

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

The following table describes the labels in this screen.

Table 26 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Auto Channel Timer	If you set the channel to Auto in the Network Setting > Wireless > General screen, specify the interval in minutes for how often the VMG scans for the best channel. Enter 0 to disable the periodical scan.
Output Power	Set the output power of the VMG. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: 20% , 40% , 60% , 80% or 100% .
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50ms to 1000ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
802.11 Mode	Select 802.11b Only to allow only IEEE 802.11b compliant WLAN devices to associate with the VMG. Select 802.11g Only to allow only IEEE 802.11g compliant WLAN devices to associate with the VMG. Select 802.11n Only to allow only IEEE 802.11n compliant WLAN devices to associate with the VMG. 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. 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.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select Auto to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select Off to disable 802.11 protection. The transmission rate of your VMG might be reduced in a mixed-mode network. This field displays Off and is not configurable when you set 802.11 Mode to 802.11b Only .
RIFS Advertisement	Select Auto to enable the Reduced Inter-frame Spacing (RIFS) feature. It improves the Device's performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable the feature.
Preamble	Select a preamble type from the drop-down list box. Choices are Long or Short . See Section 7.9.7 on page 109 for more information. This field is configurable only when you set 802.11 Mode to 802.11b .
RX Chain Power Save	Select Enable to activate the RX Chain Power Save feature. It turns off one of the Receive chains to save power when it is not in use. Select Disabled to disable this feature.

Table 26 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
OBSS Coexistence	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.
XPress™ Technology	Select Enable for higher speeds, especially if you have both IEEE 802.11b and IEEE 802.11g wireless clients. The wireless clients do not have to support XPress™ Technology, although the performance enhancement is greater if they do. Select Disabled to disable this feature.
WPS 2.0	Select Enable to support WPS 2.0 which enhances WPS security and flexibility on configuration. Select Disabled to disable this feature.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

7.8 The Channel Status Screen

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

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

Figure 43 Network Setting > Wireless > Channel Status

7.9 Technical Reference

This section discusses wireless LANs in depth. For more information, see [Appendix B on page 267](#).

7.9.1 Wireless Network Overview

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

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

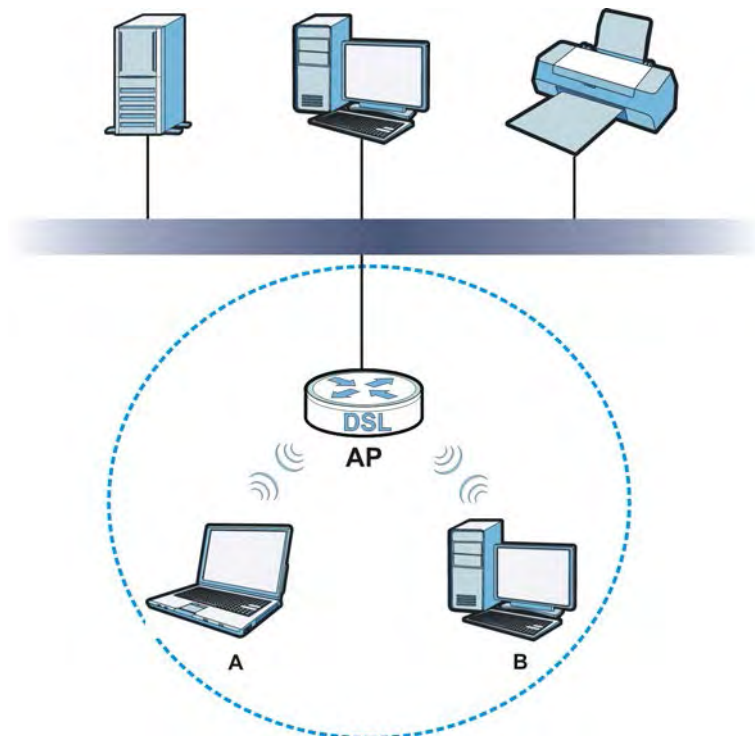
Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.

- An “ad-hoc” type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 44 Example of a Wireless Network



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

Every wireless network must follow these basic guidelines.

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

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

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

7.9.2 Additional Wireless Terms

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

Table 27 Additional Wireless Terms

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

7.9.3 Wireless Security Overview

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

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

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

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

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

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

7.9.3.1 SSID

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

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

7.9.3.2 MAC Address Filter

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

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

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

7.9.3.3 User Authentication

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

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

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

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


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

7.9.3.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See [Section 7.9.3.3 on page 106](#) for information about this.)

Table 28 Types of Encryption for Each Type of Authentication

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

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

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

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

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

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

7.9.4 Signal Problems

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

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

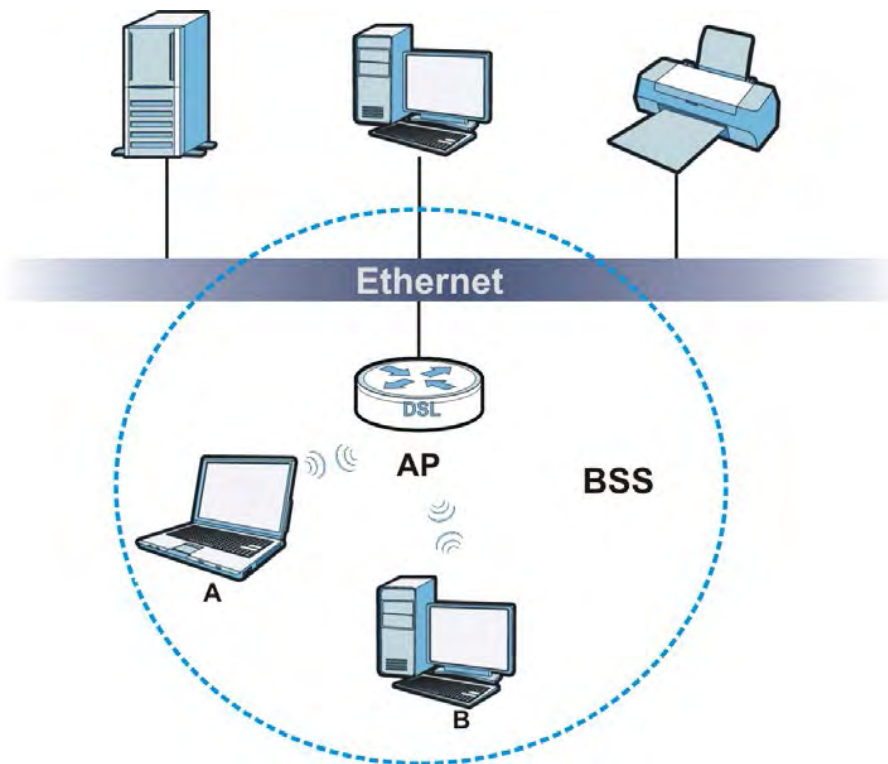
coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.9.5 BSS

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

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

Figure 45 Basic Service set



7.9.6 MBSSID

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

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

7.9.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.

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

7.9.7 Preamble Type

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

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

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

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

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

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

7.9.8 WiFi Protected Setup (WPS)

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

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

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

7.9.8.1 Push Button Configuration

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

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

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

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

- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the VMG, see [Section 7.6 on page 99](#)).
- 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 three seconds.
- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

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

7.9.8.2 PIN Configuration

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

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

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

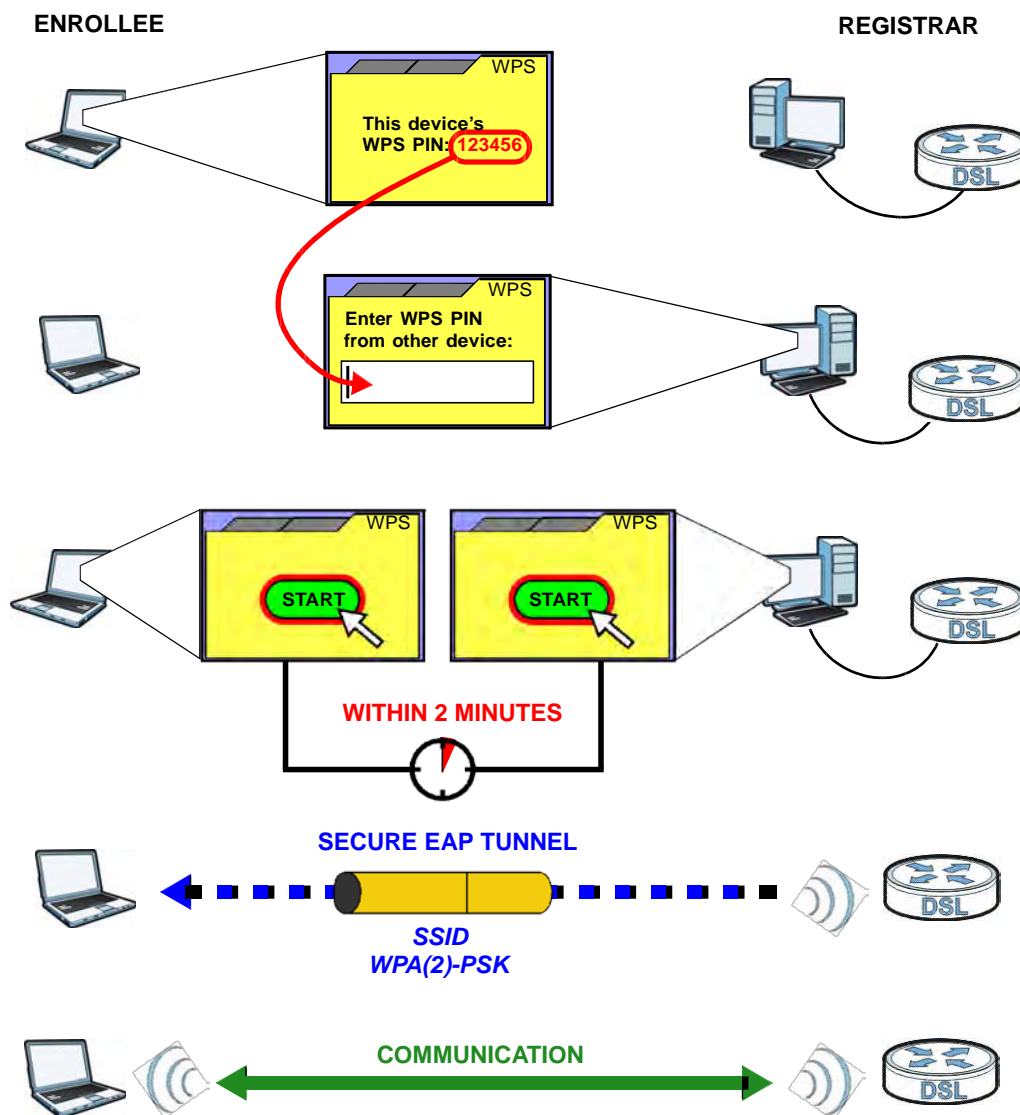
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the VMG, see [Section 7.5 on page 98](#)).
- 4 Enter the client's PIN in the AP's configuration interface.
- 5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6 Start WPS on both devices within two minutes.
- 7 Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

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

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

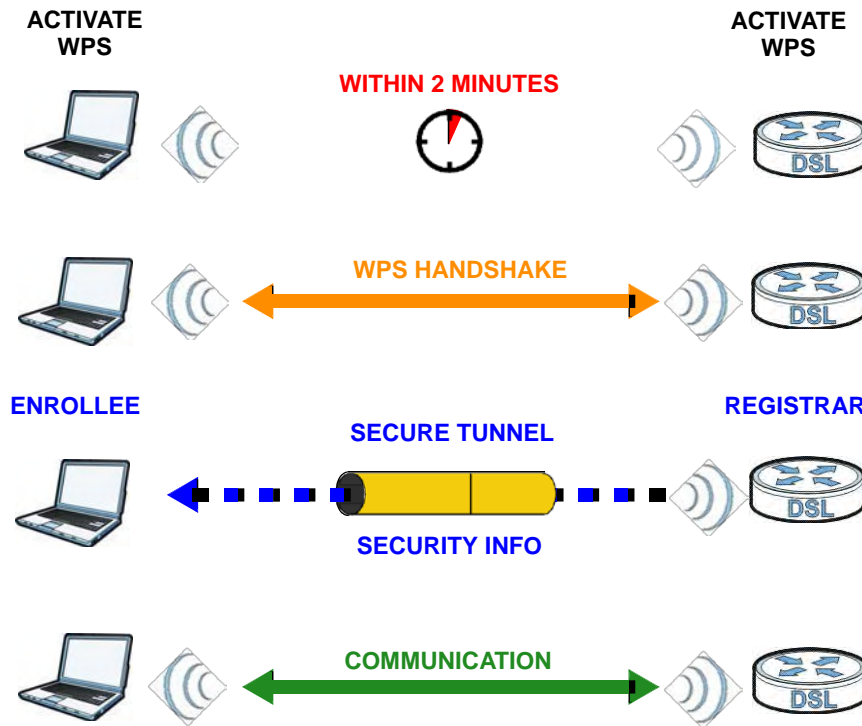
Figure 46 Example WPS Process: PIN Method



7.9.8.3 How WPS Works

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

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

Figure 47 How WPS works

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

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

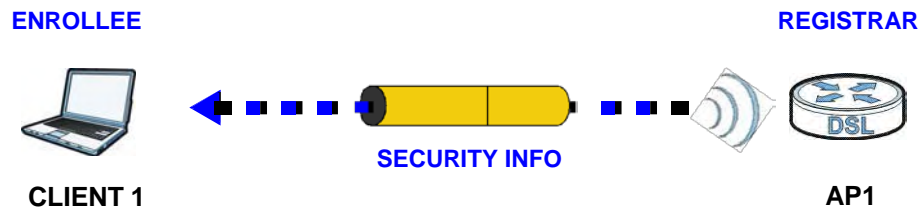
Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

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

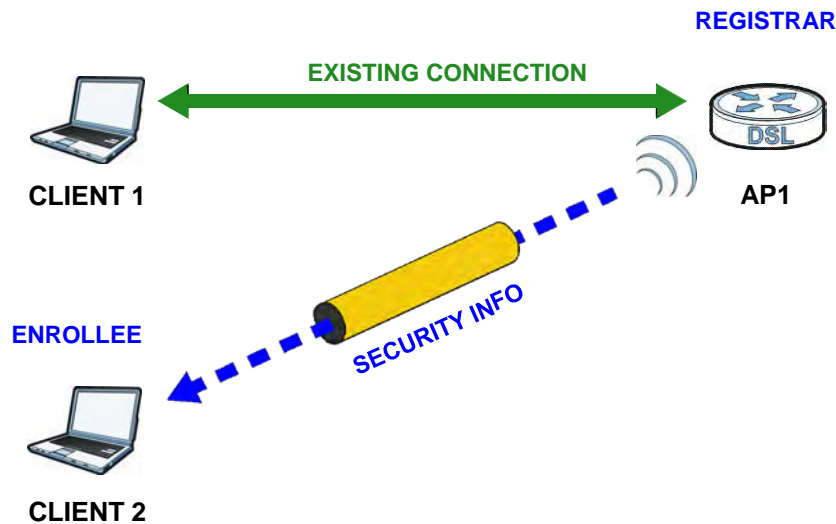
7.9.8.4 Example WPS Network Setup

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

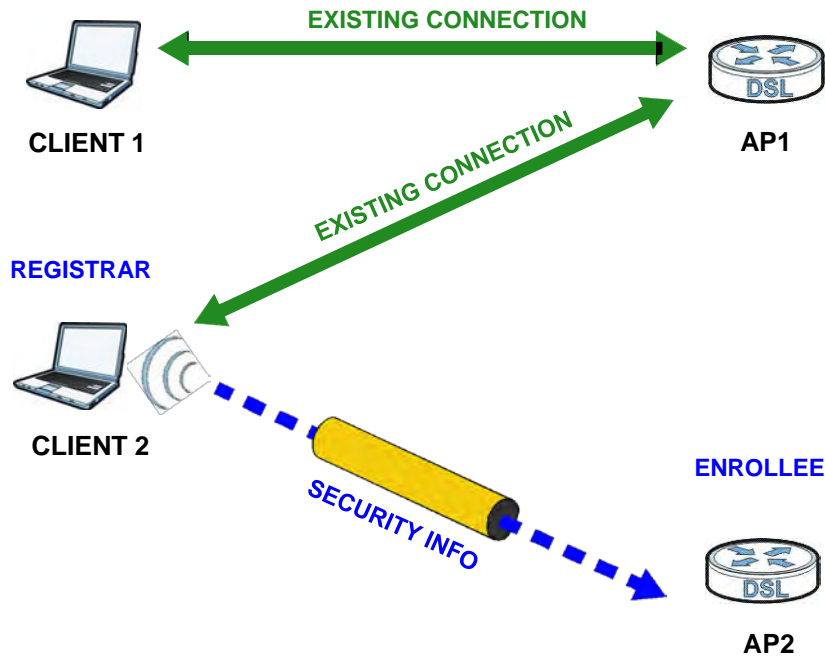
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 48 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 49 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 50 WPS: Example Network Step 3

7.9.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

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

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

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

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

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

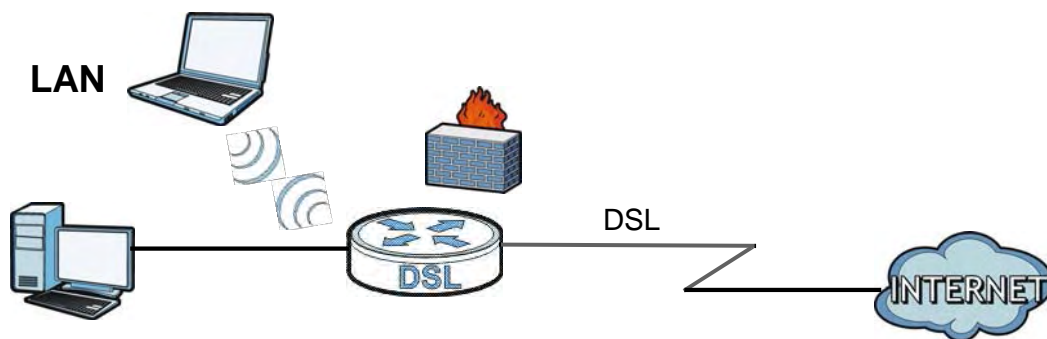
access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an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

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 127](#)).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. ([Section 8.7 on page 127](#)).
- 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 128](#)).

8.1.2 What You Need To Know

8.1.2.1 About LAN

IP Address

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

Subnet Mask

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

DHCP

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

DNS

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

RADVD (Router Advertisement Daemon)

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

8.1.2.2 About UPnP

Identifying UPnP Devices

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

NAT Traversal

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

- Dynamic port mapping
- Learning public IP addresses

- Assigning lease times to mappings

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

See the [Chapter 11 on page 157](#) 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 124](#) for examples of installing and using UPnP.

Finding Out More

See [Section 8.9 on page 128](#) for technical background information on LANs.

8.1.3 Before You Begin

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

8.2 The LAN Setup Screen

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

Follow these steps to configure your LAN settings.

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

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

Figure 51 Network Setting > Home Networking > LAN Setup

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

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 Address Setup
☒ Delegate prefix from WAN: Default ▼
☐ Static

MLD Snooping
Active: ☒ Enable ☐ Disable

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 29 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 14 on page 179 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).
IGMP Snooping	
Active	Select Enable to allows the VMG to passively learn multicast group.
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.
LAN IPv6 Mode Setup	
IPv6 Active	Select Enable to activate the IPv6 mode and configure IPv6 settings on the VMG.
Link Local Address Type	

Table 29 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
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 Address Setup	
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the VMG's LAN IPv6 address.
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.
LAN IPv6 Address Assign Setup	<p>Select how you want to obtain an IPv6 address:</p> <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. • Stateless and Stateful: The VMG uses both IPv6 stateless and stateful autoconfiguration. The LAN IPv6 clients can obtain IPv6 addresses either through router advertisements or through DHCPv6.
LAN IPv6 DNS Assign Setup	<p>Select how the VMG provide DNS server and domain name information to the clients:</p> <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	<p>Select From ISP if your ISP dynamically assigns IPv6 DNS server information.</p> <p>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.</p> <p>Select None if you do not want to configure IPv6 DNS servers.</p>

Table 29 Network Setting > Home Networking > LAN Setup (continued)

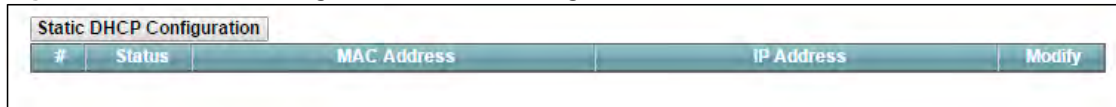
LABEL	DESCRIPTION
DNS Query Scenario	<p>Select how the VMG handles clients' DNS information requests.</p> <ul style="list-style-type: none"> • IPv4/IPv6 DNS Server: The VMG forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. • IPv6 DNS 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 The Static DHCP Screen

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

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AO: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 52 Network Setting > Home Networking > Static DHCP


Static DHCP Configuration				
#	Status	MAC Address	IP Address	Modify

The following table describes the labels in this screen.

Table 30 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>
IP Address	This field displays the IP address relative to the # field listed above.
Modify	<p>Click the Edit icon to have the IP address field editable and change it.</p> <p>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.</p>

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 53 Static DHCP: Static DHCP Configuration/Edit

The following table describes the labels in this screen.

Table 31 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 14 on page 179 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 The UPnP Screen

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

See [page 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 54 Network Setting > Home Networking > UPnP

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

Apply Cancel

The following table describes the labels in this screen.

Table 32 Network Setting > Home Networking > UPnP

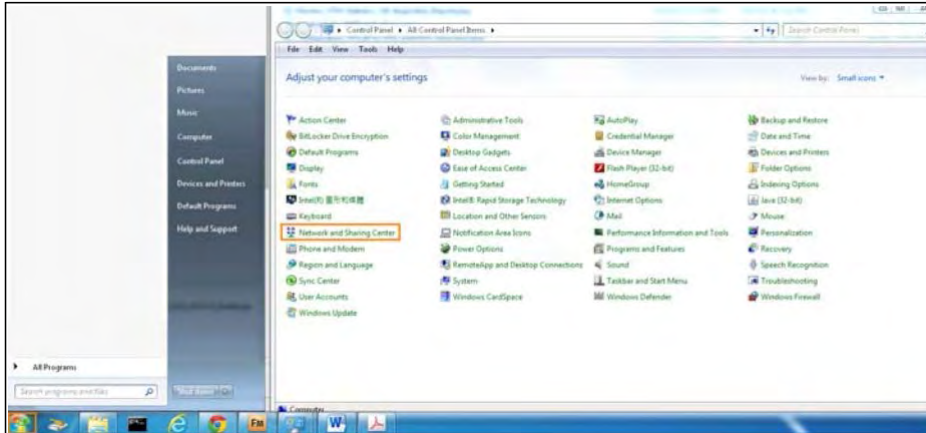
LABEL	DESCRIPTION
UPnP	Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the VMG's IP address (although you must still enter the password to access the web configurator).
UPnP NAT-T	Select Enable to allow UPnP-enabled 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 Turning On UPnP in Windows 7 Example

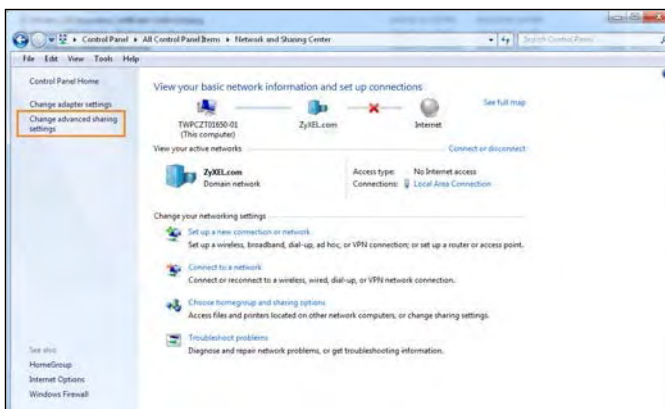
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the VMG.

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

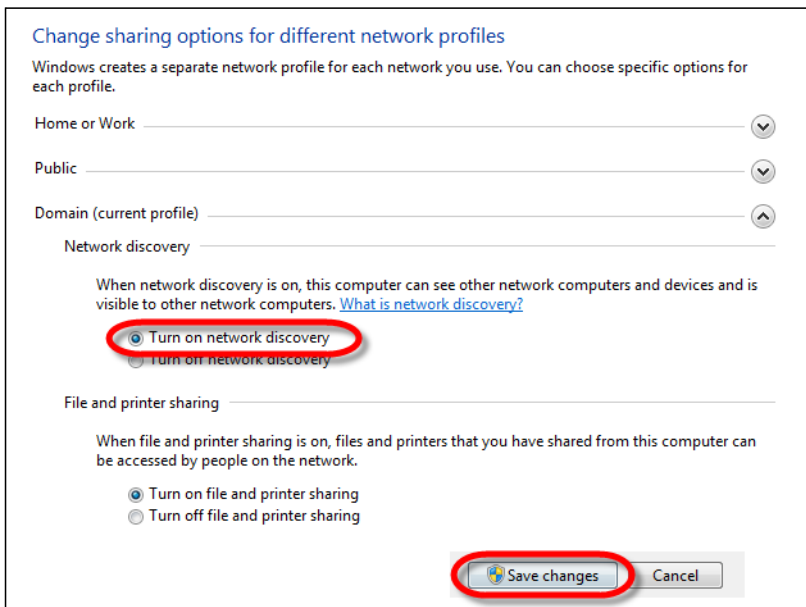
- 1 Click the start icon, **Control Panel** and then the **Network and Sharing Center**.



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



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



8.5 The Additional Subnet Screen

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

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

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

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

Figure 55 Network Setting > Home Networking > Additional Subnet

The following table describes the labels in this screen.

Table 33 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 14 on page 179 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 turn on the Public LAN feature. Your ISP must support Public LAN and Static IP.
IPv4 Address	Enter the public IP address provided by your ISP.
Subnet Mask	Enter the public IP subnet mask provided by your ISP.
Offer Public IP by DHCP	Select Enable to allow the VMG to provide public IP addresses by DHCP server.
Enable ARP Proxy	Select Enable to activate the ARP (Address Resolution Protocol) proxy.

Table 33 Network Setting > Home Networking > Additional Subnet (continued)

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

8.6 The STB Vendor ID Screen

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

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

Figure 56 Network Setting > Home Networking > STB Vendor ID

The following table describes the labels in this screen.

Table 34 Network Setting > Home Networking > STB Vendor ID

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

8.7 The Wake on LAN Screen

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

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

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

Figure 57 Network Setting > Home Networking > Wake on LAN

The following table describes the labels in this screen.

Table 35 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 The TFTP Server Name Screen

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

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

Figure 58 Network Setting > Home Networking > TFTP Server Name



The following table describes the labels in this screen.

Table 36 Network Setting > Home Networking > TFTP Server Name

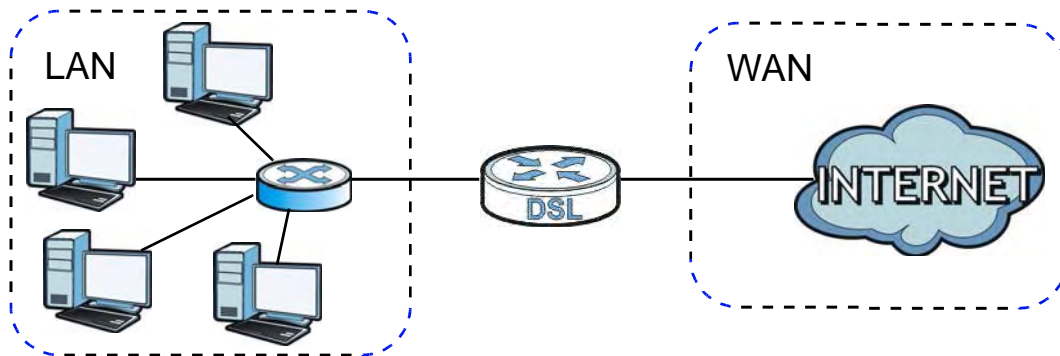
LABEL	DESCRIPTION
TFTP Server Name	Enter the IP address or the domain name of a single TFTP server.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

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 59 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".

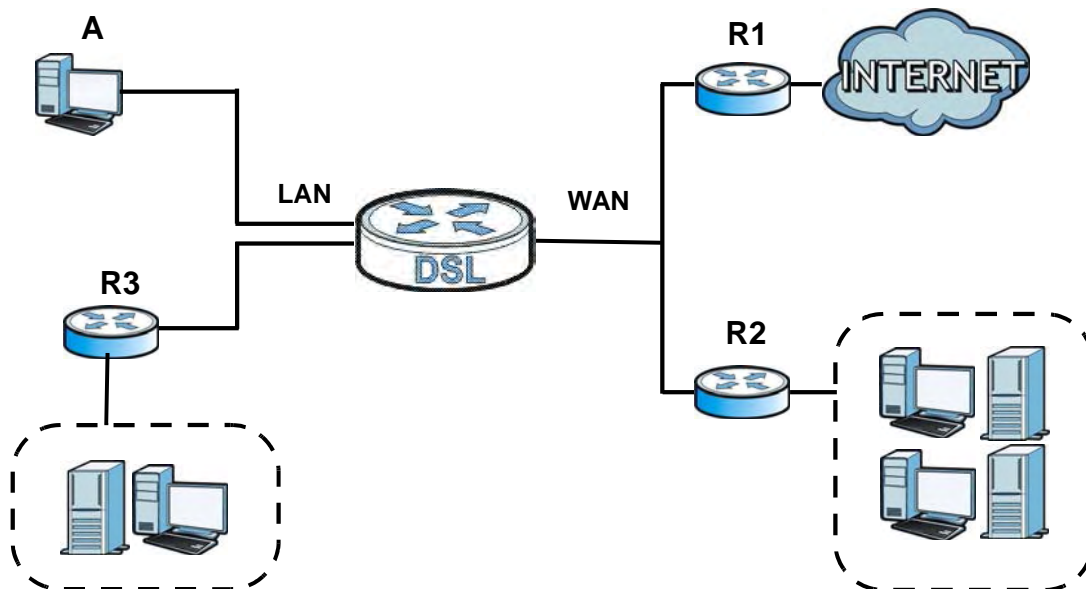
Routing

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 60 Example of Routing Topology



9.2 The Routing Screen

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

Figure 61 Network Setting > Routing > Static Route

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

The following table describes the labels in this screen.

Table 37 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	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 62 Routing: Add/Edit

The following table describes the labels in this screen.

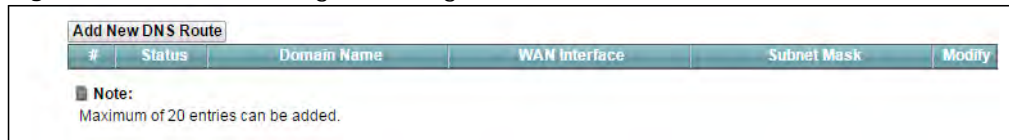
Table 38 Routing: Add/Edit

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 The DNS Route Screen

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

Figure 63 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

Table 39 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.

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

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

9.3.1 The DNS Route Add Screen

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

Figure 64 DNS Route Add

The following table describes the labels in this screen.

Table 40 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.
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. WWAN means the wireless 3G interface.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving any changes.

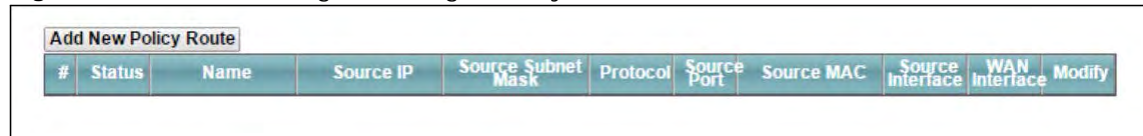
9.4 The Policy Route Screen

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

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

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

Figure 65 Network Setting > Routing > Policy Route



The following table describes the labels in this screen.

Table 41 Network Setting > Routing > Policy Route

LABEL	DESCRIPTION
Add New Policy Route	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.
Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	This is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Source MAC	This is the source MAC address.
Source Interface	This is the interface from which the matched traffic is sent.
WAN Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the Edit icon to edit this policy. Click the Delete icon to remove a policy from the 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 66 Policy Route: Add/Edit

The following table describes the labels in this screen.

Table 42 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. WWAN means the wireless 3G interface.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

9.5 RIP

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

9.5.1 The RIP Screen

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

Figure 67 RIP

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

The following table describes the labels in this screen.

Table 43 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	<p>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.</p> <p>Select Active to have the VMG advertise its route information and also listen for routing updates from neighboring routers.</p>
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.

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 141](#)).
- Use the **Queue Setup** screen to configure QoS queue assignment ([Section 10.4 on page 142](#)).
- 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 149](#)).
- Use the **Policer Setup** screen to control incoming traffic transmission rate and bursts ([Section 10.6 on page 149](#)).

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.

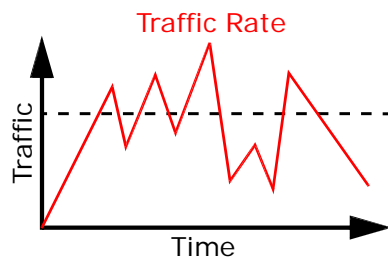
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

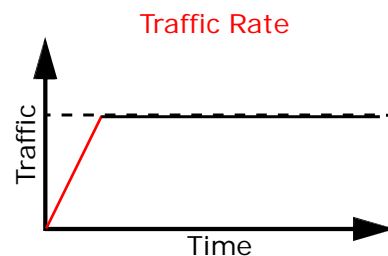
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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



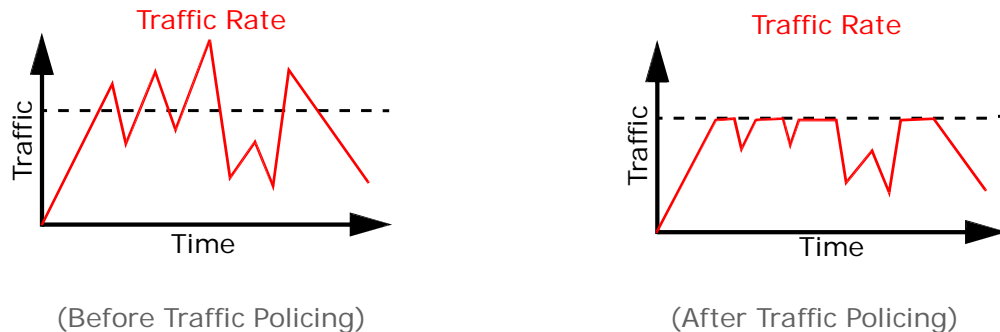
(Before Traffic Shaping)



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

10.3 The Quality of Service General Screen

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

Use this screen to enable or disable QoS and set the upstream bandwidth. See [Section 10.1 on page 139](#) for more information.

Figure 68 Network Settings > QoS > General

QoS

☐ Enable
 ☒ Disable (settings are invalid when disabled)

WAN Managed Upstream Bandwidth : (kbps)

LAN Managed Downstream Bandwidth : (kbps)

Upstream Traffic Priority Assigned by: None

Note

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

If Upstream Auto-Priority mapping criteria 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

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

The following table describes the labels in this screen.

Table 44 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 The Queue Setup Screen

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

Use this screen to configure QoS queue assignment.

Figure 69 Network Setting > QoS > Queue Setup

Add New Queue								
#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit (kbps)	Modify
1		default queue	WAN	8	1	DT		
2		default queue	WAN	1	1	DT		

Note
Maximum 8 configurable entries for WAN port.
Priority level 1 is the highest priority for QoS.
Rate limit 0 is max bandwidth.

The following table describes the labels in this screen.

Table 45 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 70 Queue Setup: Add

The following table describes the labels in this screen.

Table 46 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 The Classification Setup Screen

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

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

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

Figure 71 Network Setting > QoS > Classification Setup

Order	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
<div>Add New Classification</div>								

The following table describes the labels in this screen.

Table 47 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 72 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"/> ~ <input type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	<input type="text"/> - - - - -	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"/> ~ <input type="text"/>			<input type="checkbox"/> Exclude
<input type="checkbox"/> MAC	<input type="text"/> - - - - -	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"/> ~ <input type="text"/>	<input type="checkbox"/> Exclude
<input type="checkbox"/> DSCP	<input type="text"/> (0~63)	<input type="checkbox"/> Exclude
<input type="checkbox"/> 802.1P	<input type="text" value="0 BE"/> ▼	<input type="checkbox"/> Exclude
<input type="checkbox"/> VLAN ID	<input type="text"/> (1~4095)	<input type="checkbox"/> Exclude
<input type="checkbox"/> TCP ACK		<input type="checkbox"/> Exclude

Step3: Packet Modification

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

DSCP Mark ▼ (0~63)

802.1P Mark ▼

VLAN ID Tag ▼ (1~4095)

Step4: Class Routing

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

Forward To Interface ▼

Step5: Outgoing Queue Selection

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

To Queue Index: ▼

OK Cancel

The following table describes the labels in this screen.

Table 48 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	
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the From Interface drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select IP , you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select 802.1Q , you can configure an 802.1p priority level.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	Enter the source subnet mask.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the 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.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.

Table 48 Classification Setup: Add/Edit (continued)

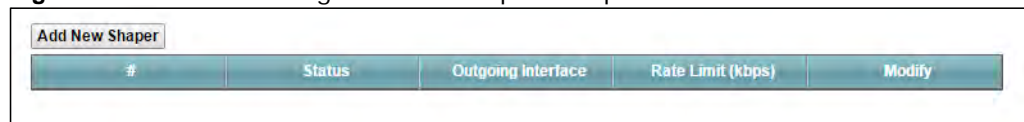
LABEL	DESCRIPTION
Others	
Service	<p>This field is available only when you select IP in the Ether Type field.</p> <p>This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter 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>
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 48 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 The QoS Shaper Setup Screen

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

Figure 73 Network Setting > QoS > Shaper Setup

The following table describes the labels in this screen.

Table 49 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>

10.6.1 Add/Edit a QoS Shaper

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

Figure 74 Shaper Setup: Add/Edit

The following table describes the labels in this screen.

Table 50 Shaper Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this shaper.
Interface	Select the VMG's interface through which traffic in this shaper applies.
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

10.7 The QoS Policer Setup Screen

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

Figure 75 Network Setting > QoS > Policer Setup

The following table describes the labels in this screen.

Table 51 Network Setting > QoS > Policer Setup

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

Table 51 Network Setting > QoS > Policer Setup (continued)

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

10.7.1 Add/Edit a QoS Policer

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

Figure 76 Policer Setup: Add/Edit

The following table describes the labels in this screen.

Table 52 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select enable or disable this policer.
Name	Enter the descriptive name of this policer.

Table 52 Policer Setup: Add/Edit

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

10.8 Technical Reference

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

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

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

Table 53 IEEE 802.1p Priority Level and Traffic Type

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

DiffServ

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

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

DSCP and Per-Hop Behavior

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

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

DSCP (6 bits)	Unused (2 bits)
---------------	-----------------

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

IP Precedence

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

Automatic Priority Queue Assignment

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

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

Table 54 Internal Layer2 and Layer3 QoS Mapping

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

Token Bucket

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

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

In traffic shaping:

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

In traffic policing:

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

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

Single Rate Three Color Marker

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

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

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

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

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

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.

- If there are not enough tokens in the CBS bucket, the VMG checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

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

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

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

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

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

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the VMG checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

Network Address Translation (NAT)

11.1 Overview

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

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network ([Section 11.2 on page 158](#)).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network ([Section 11.3 on page 161](#)).
- Use the **Port Triggering** screen to add and configure the VMG's trigger port settings ([Section 11.4 on page 162](#)).
- Use the **DMZ** screen to configure a default server ([Section 11.5 on page 165](#)).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the VMG ([Section 11.6 on page 166](#)).
- Use the **Address Mapping** screen to configure the VMG's address mapping settings ([Section 11.7 on page 166](#)).
- Use the **Sessions** screen to configure the VMG's maximum number of NAT sessions ([Section 11.8 on page 168](#)).

11.1.2 What You Need To Know

Inside/Outside

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

Global/Local

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

NAT

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

Port Forwarding

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

Finding Out More

See [Section 11.9 on page 169](#) for advanced technical information on NAT.

11.2 The Port Forwarding Screen

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

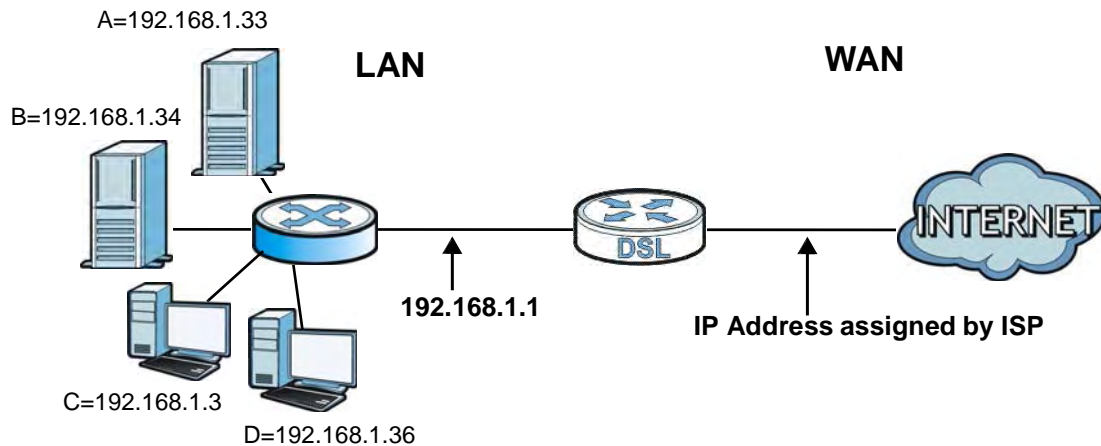
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more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

The most often used port numbers and services are shown in [Appendix D on page 288](#). Please refer to RFC 1700 for further information about port numbers.

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

Configuring Servers Behind Port Forwarding (Example)

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

Figure 77 Multiple Servers Behind NAT Example

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

See [Appendix D on page 288](#) for port numbers commonly used for particular services.

Figure 78 Network Setting > NAT > Port Forwarding

Add New Rule										
#	Status	Service Name	WAN Interface	WAN IP	Server IP Address	Start Port	End Port	Translation Start Port	Translation End Port	Protocol Modify
Note: The TCP port 7547 is reserved for TR069 connection request port.										

The following table describes the fields in this screen.

Table 55 Network Setting > NAT > Port Forwarding

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

11.2.1 Add/Edit Port Forwarding

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

Figure 79 Port Forwarding: Add/Edit

Add New Rule

Active ☒ Enable ☐ Disable

Service Name

WAN Interface

Start Port

End Port

Translation Start Port

Translation End Port

Server IP Address

Protocol

☐ Wake up this target by Wake On Lan(WOL)

MAC address of WOL device

Note

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

OK Cancel

The following table describes the labels in this screen.

Table 56 Port Forwarding: Add/Edit

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

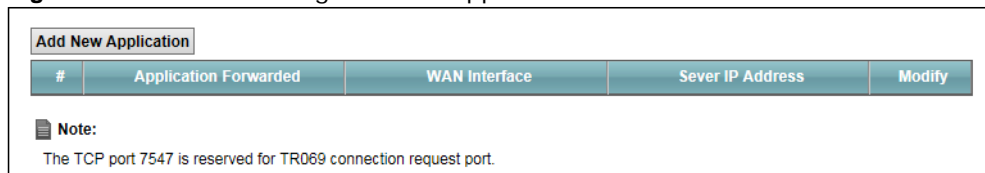
Table 56 Port Forwarding: Add/Edit (continued)

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

11.3 The Applications Screen

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

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

Figure 80 Network Setting > NAT > Applications


The screenshot shows the 'Applications' screen in the VMG1312-B10D interface. At the top left is a button labeled 'Add New Application'. Below it is a table with five columns: '#', 'Application Forwarded', 'WAN Interface', 'Server IP Address', and 'Modify'. The table is currently empty. Below the table, there is a 'Note' section with a document icon and the text: 'The TCP port 7547 is reserved for TR069 connection request port.'

The following table describes the labels in this screen.

Table 57 Network Setting > NAT > Applications

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

11.3.1 Add New Application

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

Figure 81 Applications: Add

The following table describes the labels in this screen.

Table 58 Applications: Add

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

11.4 The Port Triggering Screen

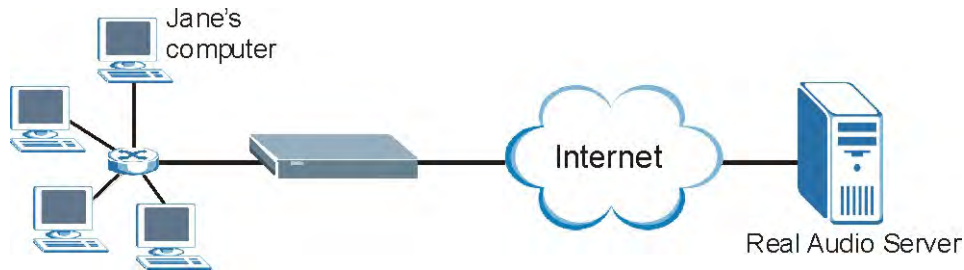
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem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

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

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

For example:

Figure 82 Trigger Port Forwarding Process: Example



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

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

Figure 83 Network Setting > NAT > Port Triggering

#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Proto.	Modify
Note: 1. The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice. 2. The TCP port 7547 is reserved for TR069 connection request port.										

The following table describes the labels in this screen.

Table 59 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.

Table 59 Network Setting > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the VMG to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The VMG forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Proto.	This is the open transport layer protocol.
Modify	Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule.

11.4.1 Add/Edit Port Triggering Rule

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

Figure 84 Port Triggering: Add/Edit

The following table describes the labels in this screen.

Table 60 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the VMG to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.

Table 60 Port Triggering: Configuration Add/Edit (continued)

LABEL	DESCRIPTION
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from TCP or UDP .
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The VMG forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from TCP or UDP .
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

11.5 The DMZ Screen

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

Figure 85 Network Setting > NAT > DMZ

Default Server Address :

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

The following table describes the fields in this screen.

Table 61 Network Setting > NAT > DMZ

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

11.6 The ALG Screen

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

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

Figure 86 Network Setting > NAT > ALG

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

The following table describes the fields in this screen.

Table 62 Network Setting > NAT > ALG

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

11.7 The Address Mapping Screen

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

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

Figure 87 Network Setting > NAT > Address Mapping

Add New Rule							
Rule Name	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	WAN Interface :	Modify

The following table describes the fields in this screen.

Table 63 Network Setting > NAT > Address Mapping

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

11.7.1 Add/Edit Address Mapping Rule

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

Figure 88 Address Mapping: Add/Edit

The following table describes the fields in this screen.

Table 64 Address Mapping: Add/Edit

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

11.8 The Sessions Screen

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

Figure 89 Network Setting > NAT > Sessions

MAX NAT Session Per Host:

Note:
 Enter session number and click "Apply" to activate this feature.
 Clear the session number field and click "Apply" to deactivate this feature.

The following table describes the fields in this screen.

Table 65 Network Setting > NAT > Sessions

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

11.9 Technical Reference

This part contains more information regarding NAT.

11.9.1 NAT Definitions

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

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

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 66 NAT Definitions

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

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

11.9.2 What NAT Does

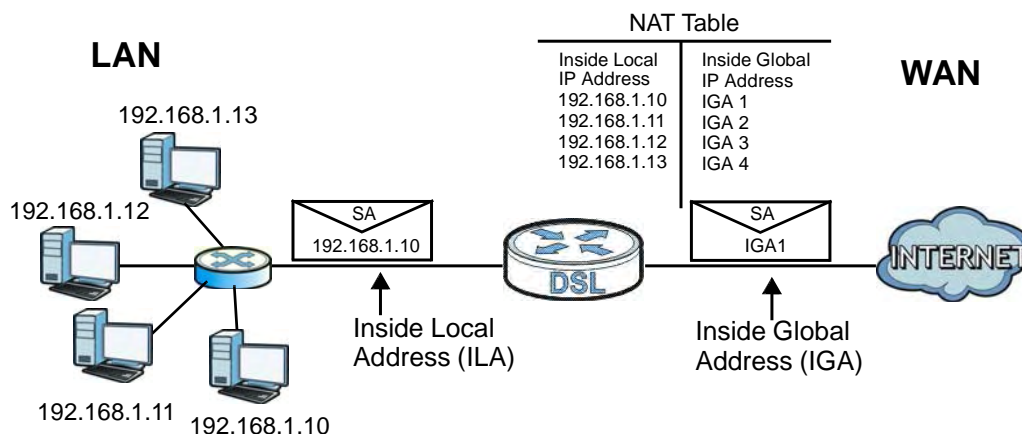
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

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

11.9.3 How NAT Works

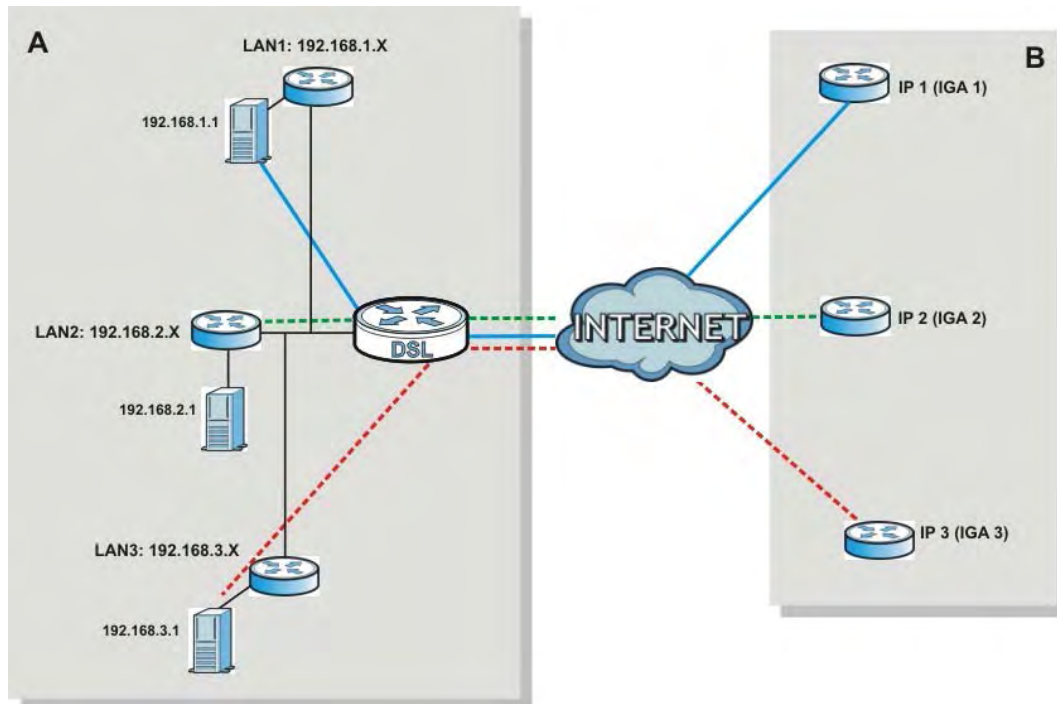
Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN,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

Figure 90 How NAT Works



11.9.4 NAT Application

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

Figure 91 NAT Application With IP Alias

Port Forwarding: Services and Port Numbers

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

Table 67 Services and Port Numbers

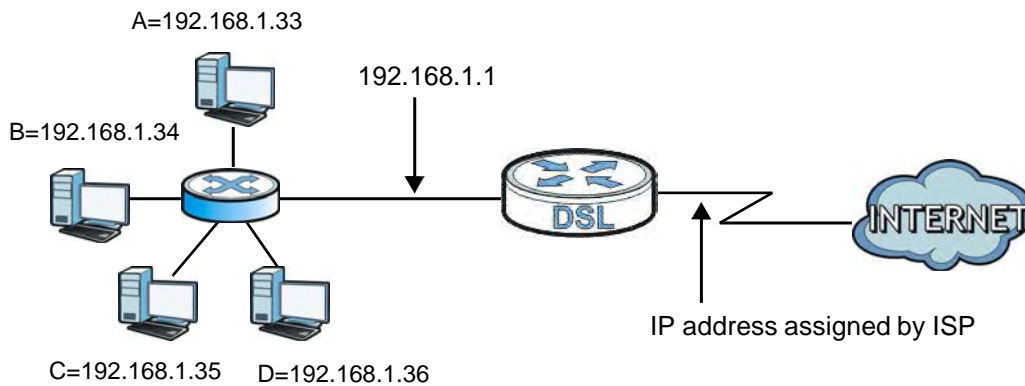
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)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

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a

third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 92 Multiple Servers Behind NAT Example



Dynamic DNS Setup

12.1 Overview

DNS

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

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

Dynamic DNS

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

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

12.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes ([Section 12.2 on page 174](#)).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the VMG ([Section 12.3 on page 175](#)).

12.1.2 What You Need To Know

DYNDNS Wildcard

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

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

12.2 The DNS Entry Screen

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

Figure 93 Network Setting > DNS > DNS Entry

Add New DNS Entry

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

The following table describes the fields in this screen.

Table 68 Network Setting > DNS > DNS Entry

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

12.2.1 Add/Edit DNS Entry

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

Figure 94 DNS Entry: Add/Edit

DNS Entry Configuration

Host Name :

IPv4 Address :

OK Cancel

The following table describes the labels in this screen.

Table 69 DNS Entry: Add/Edit

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

12.3 The Dynamic DNS Screen

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

Figure 95 Network Setting > DNS > Dynamic DNS

The following table describes the fields in this screen.

Table 70 Network Setting > DNS > > Dynamic DNS

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

Table 70 Network Setting > DNS > > Dynamic DNS (continued)

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

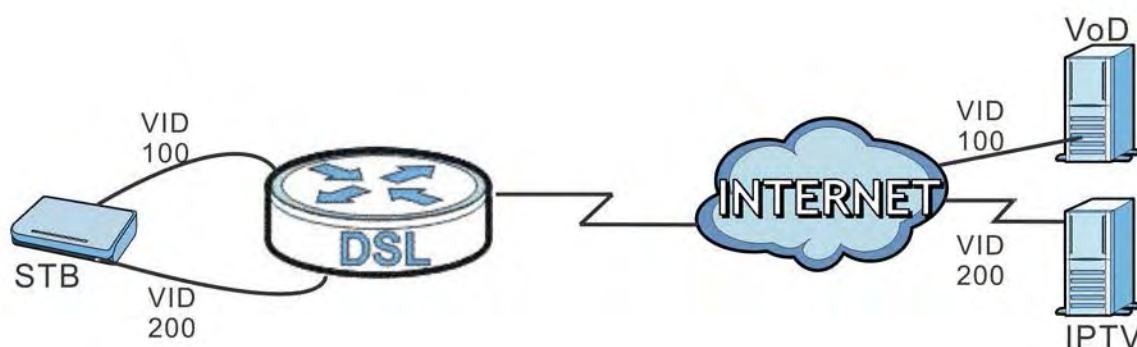
VLAN Group

13.1 Overview

Virtual LAN IDs are used to identify different traffic types over the same physical link.

In the following example, the VMG (DSL) can use VLAN IDs (VID) 100 and 200 to identify Video-on-Demand and IPTV traffic respectively coming from the two VoD and IPTV multicast servers. The VMG (DSL) can also tag outgoing requests to these servers with these VLAN IDs.

Figure 96 VLAN Group Example





13.1.1 What You Can Do in this Chapter

Use these screens to group separate VLAN groups together to be treated as one VLAN group.

13.2 The VLAN Group Screen

Click **Network Setting > Vlan Group** to open the following screen.

Figure 97 Network Setting > Vlan Group

Add New VLAN Group				
#	Group Name	VLAN ID	Interfaces	Modify
1	VG123	123	LAN3U	 

The following table describes the fields in this screen.

Table 71 Network Setting > Vlan Group

LABEL	DESCRIPTION
Add New VLAN Group	Click this button to create a new VLAN group.
#	This is the index number of the VLAN group.
Group Name	This shows the descriptive name of the VLAN group.
VLAN ID	This shows the unique ID number that identifies the VLAN group.
Interfaces	This shows the LAN ports included in the VLAN group and if traffic leaving the port will be tagged with the VLAN ID.
Modify	Click the Edit icon to change an existing VLAN group setting or click the Delete icon to remove the VLAN group.

13.2.1 Add/Edit a VLAN Group

Click the **Add New VLAN Group** button in the **Vlan Group** screen to open the following screen. Use this screen to create a new VLAN group.

Figure 98 Add/Edit VLAN Group

The following table describes the fields in this screen.

Table 72 Add/Edit VLAN Group

LABEL	DESCRIPTION
VLAN Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
VLAN ID	Enter a unique ID number, from 1 to 4,094, to identify this VLAN group. Outgoing traffic is tagged with this ID if Tx Tagging is selected below.
LAN	Select Include to add the associated LAN interface to this VLAN group. Select Tx Tagging to tag outgoing traffic from the associated LAN port with the VLAN ID number entered above.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

Interface Grouping

14.1 Overview

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

14.1.1 What You Can Do in this Chapter

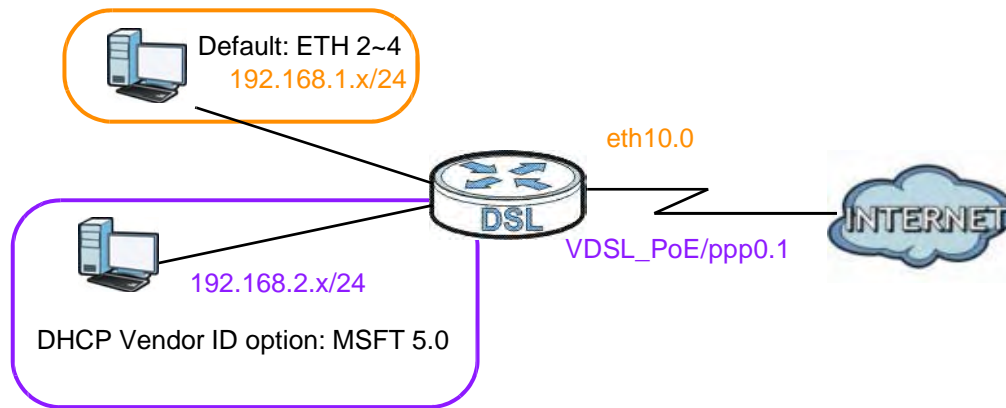
The **Interface Grouping** screens let you create multiple networks on the VMG ([Section 14.2 on page 179](#)).

14.2 The Interface Group Screen

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

Use the **LAN** screen to configure the private IP addresses the DHCP server on the VMG assigns to the clients in the default and/or user-defined groups. If you set the VMG to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See [Chapter 8 on page 116](#) for more information.

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

Figure 99 Interface Grouping Application

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

Figure 100 Network Setting > Interface Grouping

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

The following table describes the fields in this screen.

Table 73 Network Setting > Interface Grouping

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

14.2.1 Interface Group Configuration

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

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

Figure 101 Interface Group Configuration

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

Group Name

WAN Interfaces used in the grouping

PTM type -

ATM type -

ETH type -

WWAN type -

Available LAN Interfaces

Available LAN Interfaces

Automatically Add Clients With the following DHCP Vendor IDs

#	Filter Criteria	WildCard Support	Modify
<input type="button" value="Add"/>			

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

OK Cancel

The following table describes the fields in this screen.

Table 74 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interface used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface, up to one ETH interface, and up to one WWAN interface.
Available LAN Interfaces	<p>Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the Available LAN Interfaces list on the right side and use the left arrow to move them to the Available LAN Interfaces list on the left side to add the interfaces to this group.</p> <p>To remove a LAN or wireless LAN interface from the Available LAN Interfaces on the left side, use the right-facing arrow.</p>
Automatically Add Clients With the following DHCP Vendor IDs	Click Add to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 14.2.2 on page 182 for more information.
#	This shows the index number of the rule.

Table 74 Interface Group Configuration (continued)

LABEL	DESCRIPTION
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
Wildcard Support	This shows if wildcard on DHCP option 60 is enabled.
Modify	Click the Edit icon to change the group setting Click the Delete icon to delete this group from the VMG.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

14.2.2 Interface Grouping Criteria

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

Figure 102 Interface Grouping Criteria

The following table describes the fields in this screen.

Table 75 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	Select this option and enter the source MAC address of the packet.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.

Table 75 Interface Grouping Criteria (continued)

LABEL	DESCRIPTION
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first three bytes of the MAC address.
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
VLAN Group	Select this and the VLAN group of the matched traffic from the drop-down list box.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

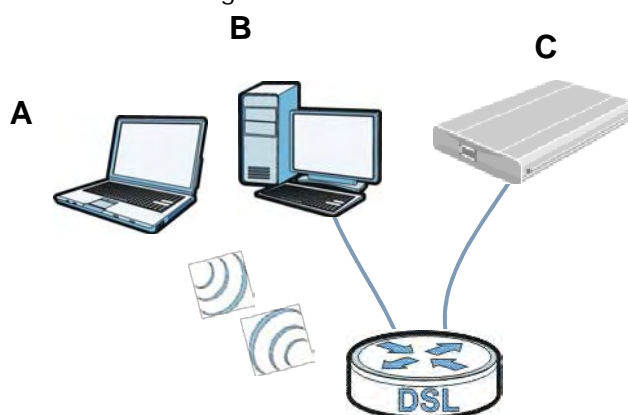
USB Service

15.1 Overview

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

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

Figure 103 File Sharing Overview



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

15.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to enable file-sharing server ([Section 15.1.3 on page 185](#)).
- Use the **Media Server** screen to enable or disable the sharing of media files ([Section 15.3 on page 187](#)).

15.1.2 What You Need To Know

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

15.1.2.1 About File Sharing

Workgroup name

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

Shares

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

File Systems

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

Common Internet File System

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

15.1.3 Before You Begin

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

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

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

15.2 The File Sharing Screen

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

Figure 104 Network Setting > USB Service > File Sharing

Information

Volume	Capacity	Used Space
--------	----------	------------

Server Configuration

File Sharing Services: ☒ Enable ☐ Disable

Account Management

Add New User

Active	Status	User Name	Modify
<input checked="" type="checkbox"/>		guest	

Apply **Cancel**

Each field is described in the following table.

Table 76 Network Setting > USB Service > File Sharing

LABEL	DESCRIPTION
Information	
Volume	This is the volume name the VMG gives to an inserted USB device.
Capacity	This is the total available memory size (in megabytes) on the USB device.
Used Space	This is the memory size (in megabytes) already used on the USB device.
Server Configuration	
File Sharing Services	Select Enable to activate file sharing through the VMG.
Account Management	
Add New User	Click this button to create a user account to access the secured shares.
Active	Select this to allow the user to access the secured shares.
Status	<p>This field shows the status of the user.</p> <p> : The user account is not activated for the share.</p> <p> : The user account is activated for the share.</p>
User Name	This is the name of a user who is allowed to access the secured shares on the USB device.
Modify	<p>Click the Edit icon to modify the user account.</p> <p>Click the Delete icon to remove the user account from the VMG.</p>
Apply	Click this to save your changes to the VMG.
Cancel	Click this to restore your previously saved settings.

15.2.1 The Add New User Screen

Use this screen to create a user account that can access the secured shares on the USB device. To access this screen, click the **Add New User** button in the **Network Setting > USB Service > File Sharing** screen.

Figure 105 Network Setting > USB Service > File Sharing > Add new user

Each field is described in the following table.

Table 77 Network Setting > USB Service > File Sharing > Add new user

LABEL	DESCRIPTION
User Name	Enter a user name. You can enter up to 16 characters. Only letters and numbers allowed.
New Password	Enter the password used to access the secured share. The password must be 5 to 15 characters long. Only letters and numbers are allowed. The password is case sensitive.
Retype New Password	Retype the password that you entered above.
Apply	Click Apply to save your changes to the VMG.
Cancel	Click Cancel to exit this screen without saving.

15.3 The Media Server Screen

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

The VMG media server enables you to:

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

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

To change your VMG's media server settings, click **Network Setting > USB Service > Media Server**. The screen appears as shown.

Figure 106 Network Setting > USB Service > Media Server

Media Server: ☒ Enable ☐ Disable

Interface: Default ▼

Media Library Path: /mnt/

Apply Cancel

The following table describes the labels in this menu.

Table 78 Network Setting > USB Service > Media Server

LABEL	DESCRIPTION
Media Server	Select Enable to have the VMG function as a DLNA-compliant media server. Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares.
Interface	Select an interface on which you want to enable the media server function.
Media Library Path	Enter the path clients use to access the media files on a USB storage device connected to the VMG.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

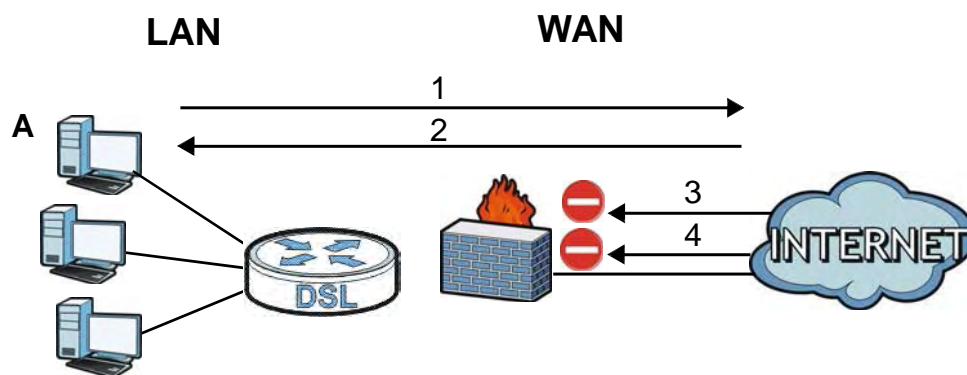
16.1 Overview

This chapter shows you how to enable and configure the VMG's security settings. Use the firewall to protect your VMG and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 107 Default Firewall Action



16.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the VMG ([Section 16.2 on page 190](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 16.3 on page 191](#)).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules ([Section 16.4 on page 193](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 16.5 on page 195](#)).

16.1.2 What You Need to Know

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The VMG is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

16.2 The Firewall Screen

Use this screen to set the security level of the firewall on the VMG. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Security > Firewall** to display the **General** screen.

Figure 108 Security > Firewall > General

IPv4 Firewall : ☒ Enable ☐ Disable

IPv6 Firewall : ☒ Enable ☐ Disable

Medium (Recommended)

LAN to WAN ☒

WAN to LAN ☐

Note:

(1) LAN to WAN: Allow access to all Internet services

(2) WAN to LAN: Allow access from other computers on the Internet

(3) When the security level is set to 'High', access to the following services is allowed: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP

Apply Cancel

The following table describes the labels in this screen.

Table 79 Security > Firewall > General

LABEL	DESCRIPTION
Firewall	Select Enable to activate the firewall feature on the VMG.
Easy	Select Easy to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select Medium to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select High to deny LAN to WAN and WAN to LAN packet directions.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

16.3 The Protocol Screen

You can configure customized services and port numbers in the **Protocol** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See [Appendix D on page 288](#) for some examples.

Click **Security > Firewall > Protocol** to display the following screen.

Figure 109 Security > Firewall > Protocol

Add New Protocol Entry

Name	Description	Ports/Protocol Number	Modify

Note:

If a protocol rule is removed, related ACL rules will also be removed.

The following table describes the labels in this screen.

Table 80 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to add a new service.
Name	This is the name of your customized service.
Description	This is the description of your customized service.
Ports/Protocol Number	This shows the IP protocol (TCP , UDP , ICMP , or TCP/UDP) and the port number or range of ports that defines your customized service. Other and the protocol number displays if the service uses another IP protocol.
Modify	Click the Edit icon to edit the entry. Click the Delete icon to remove this entry.

16.3.1 Add/Edit a Service

Use this screen to add a customized service rule that you can use in the firewall's ACL rule configuration. Click **Add new service entry** or the edit icon next to an existing service rule in the **Service** screen to display the following screen.

Figure 110 Security > Firewall > Protocol: Add/Edit

The following table describes the labels in this screen.

Table 81 Security > Firewall > Protocol: Add/Edit

LABEL	DESCRIPTION
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Description	Enter a description for your customized port.
Protocol	Choose the IP protocol (TCP , UDP , ICMP , or Other) that defines your customized port from the drop-down list box. Select Other to be able to enter a protocol number.
Protocol Number	This field is displayed if you select Other as the protocol. Enter the protocol number of your customized port.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

16.4 The Access Control Screen

Click **Security > Firewall > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 111 Security > Firewall > Access Control

#	Name	Src IP	Dst IP	Service	Action	Modify
---	------	--------	--------	---------	--------	--------

The following table describes the labels in this screen.

Table 82 Security > Firewall > Access Control

LABEL	DESCRIPTION
Add New ACL Rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
#	This is the index number of the entry.
Name	This displays the name of the rule.
Src IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to Any .
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to Any .
Service	This displays the transport layer protocol that defines the service and the direction of traffic to which this rule applies.
Action	This field displays whether the rule silently discards packets (DROP), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (REJECT) or allows the passage of packets (ACCEPT).
Modify	Click the Edit icon to edit the rule. Click the Delete icon to delete an existing rule. Note that subsequent rules move up by one when you take this action. Click the Move To icon to change the order of the rule. Enter the number in the # field.

16.4.1 Add/Edit an ACL Rule

Click **Add new ACL rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 112 Access Control: Add/Edit

The following table describes the labels in this screen.

Table 83 Access Control: Add/Edit

LABEL	DESCRIPTION
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Order	Select the order of the ACL rule.
Select Source Device	Select the source device to which the ACL rule applies. If you select Specific IP Address , enter the source IP address in the field below.
Source IP Address	Enter the source IP address.
Select Destination Device	Select the destination device to which the ACL rule applies. If you select Specific IP Address , enter the destination IP address in the field below.
Destination IP Address	Enter the destination IP address.
IP Type	Select whether your IP type is IPv4 or IPv6 .
Select Service	Select the service rule that defines your customized port from the drop-down list box. The specific service rule you add in the Security > Firewall > Protocol screen display in this list. If you want to configure a customized service, select Specific Service .

Table 83 Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Protocol	This field is displayed only when you select Specific Service in the Select Service field. Choose the transport layer protocol (TCP/UDP , TCP , UDP , ICMP , or ICMPv6) that defines your customized port from the drop-down list box.
Custom Source Port	This field is displayed only when you select Specific Service in the Select Service field. Enter a single port number or the range of port numbers of the source.
Custom Destination Port	This field is displayed only when you select Specific Service in the Select Service field. Enter a single port number or the range of port numbers of the destination.
Policy	Use the drop-down list box to select whether to discard (DROP), deny and send an ICMP destination-unreachable message to the sender of (REJECT) or allow the passage of (ACCEPT) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies.
Enable Rate Limit	Select Enable to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packets per minute or second the transmission rate is.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click Add New Rule . This will bring you to the Security > Scheduler Rules screen.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving.

16.5 The DoS Screen

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Use the **DoS** screen to activate protection against DoS attacks. Click **Security > Firewall > DoS** to display the following screen.

Figure 113 Security > Firewall > DoS

DoS Protection Blocking : ☒ Enable ☐ Disable (settings are invalid when disabled)

Apply Cancel

The following table describes the labels in this screen.

Table 84 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select Enable to enable protection against DoS attacks.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to exit this screen without saving.

MAC Filter

17.1 Overview

You can configure the VMG to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

17.2 The MAC Filter Screen

Use this screen to allow wireless and LAN clients access to the VMG. Click **Security > MAC Filter**. The screen appears as shown.

Figure 114 Security > MAC Filter

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

MAC Restrict Mode ☒ Allow ☐ Deny

Set	Active	Host Name	MAC Address
1	<input type="checkbox"/>		- - - - -
2	<input type="checkbox"/>		- - - - -
3	<input type="checkbox"/>		- - - - -
4	<input type="checkbox"/>		- - - - -
5	<input type="checkbox"/>		- - - - -
6	<input type="checkbox"/>		- - - - -
7	<input type="checkbox"/>		- - - - -
8	<input type="checkbox"/>		- - - - -
9	<input type="checkbox"/>		- - - - -
10	<input type="checkbox"/>		- - - - -
31	<input type="checkbox"/>		- - - - -
32	<input type="checkbox"/>		- - - - -

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

Apply Cancel

The following table describes the labels in this screen.

Table 85 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select Enable to activate the MAC filter function.
MAC Restrict Mode	Select Allow to only permit the listed MAC addresses access to the VMG. Select Deny to permit anyone access to the VMG except the listed MAC addresses.
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Active is not selected.
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the VMG.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the VMG in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

Parental Control

18.1 Overview

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the VMG performs parental control on a specific user.

18.2 The Parental Control Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Security** > **Parental Control** to open the following screen.

Figure 115 Security > Parental Control

#	Status	PCP Name	Home Network User MAC	Internet Access Schedule	Network Service	Website Blocked	Modify
---	--------	----------	-----------------------	--------------------------	-----------------	-----------------	--------

The following table describes the fields in this screen.

Table 86 Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Select Enable to activate parental control.
Add New PCP	Click this if you want to configure a new Parental Control Profile (PCP).
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User MAC	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the day(s) and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, None will be shown.
Website Blocked	This shows whether the website block is configured. If not, None will be shown.

Table 86 Security > Parental Control (continued)

LABEL	DESCRIPTION
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

18.2.1 Add/Edit a Parental Control Profile

Click **Add New PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 116 Parental Control Rule: Add/Edit Rule

Add New PCP

General

Active: ☐ Enable ☒ Disable (Settings are invalid when disabled)

Parental Control Profile Name:

Home Network User:

Rule List

User MAC Address	Delete

Internet Access Schedule

Day: ☐ Everyday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Time (Start - End): 09:30 - 24:00

00:00 - 24:00

00:00 24:00

Authorized Access

Network Service

Network Service Setting: Selected Service(s)

#	Service Name	Protocol:Port	Modify

Site/URL Keyword

Block or Allow the Web Site:

#	webSite	Modify

☐ Redirect blocked site to ZyXEL Family Safety page

Figure 117 Parental Control Rule: Add/Edit Rule > Add Service

Figure 118 Parental Control Rule: Add/Edit Rule > Add Keyword

The following table describes the fields in this screen.

Table 87 Parental Control Rule: Add/Edit

LABEL	DESCRIPTION
General	
Active	Select to enable or disable this parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select Custom , enter the LAN user's MAC address. If you select All , the rule applies to all LAN users.
Rule List	In Home Network User , select Custom , enter the LAN user's MAC address, then click the Add icon to enter a computer MAC address for this PCP. Up to five are allowed. Click the Delete icon to remove one.
Internet Access Schedule	
Day	Select check boxes for the days that you want the VMG to perform parental control.
Time	Drag the time bar to define the time that the LAN user is allowed access (Authorized access) or denied access (No access). Click the Add icon above the time bar to add a new time bar. Up to three are allowed.
Network Service	
Network Service Setting	If you select Block , the VMG prohibits the users from viewing the Web sites with the URLs listed below. If you select Allow , the VMG blocks access to all URLs except ones listed below.