VMG5313-B10A / VMG5313-B30A

Wireless N VDSL2 VoIP IAD with USB

Version 1.00
Edition 3, 09/2014

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.1
Login	admin, zyuser
Password	1234, 1234
Default URL	http://192.168.1.1

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.

Contents Overview

Table of Contents

PART I
User's Guide

Introducing the VMG

1.1 Overview

In this guide we refer to all models in the series as the VMG. The exact model name is used for explicit references.

The VMG is a combo WAN (DSL, Ethernet and 3G in order of priority) gateway with VoIP capabilities and high speed LAN and WAN access for business users. It is equipped with four LAN ports, of which port number four can be converted into a WAN port, two phone ports that can be connected to make VoIP calls and one USB 2.0 port for file sharing. It is backward compatible with ADSL, ADSL2 and ADSL2+ in case VDSL is not available. The VMG is also a wireless access point and is compatible with IEEE 802.11b/g/n wireless standard.

- The VMG5313-B10A works over the analog telephone system, POTS (Plain Old Telephone Service).
- The VMG5313-B30A works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

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

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.
- TR-069. This is an auto-configuration server used to remotely configure your device.

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.

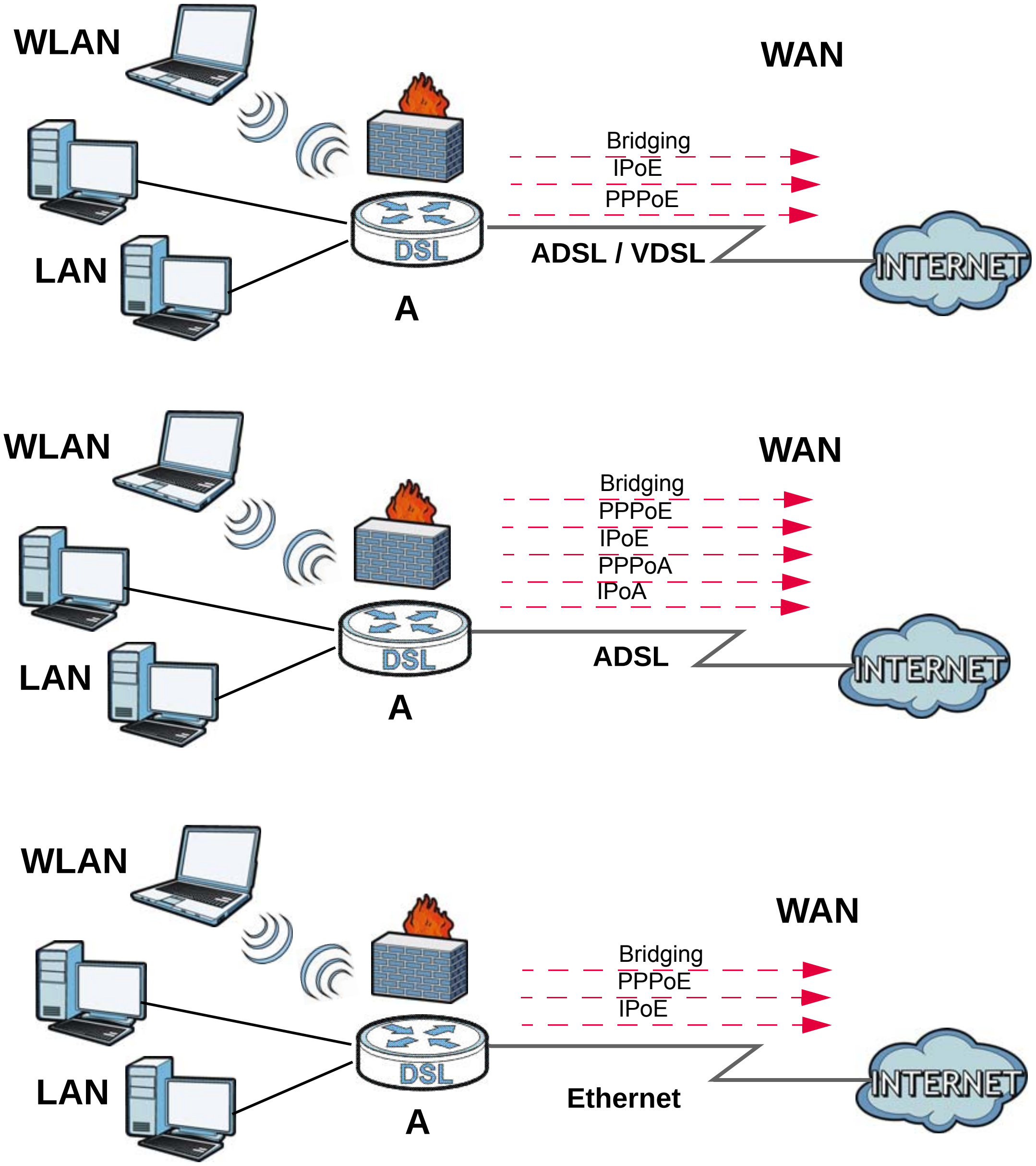
1.4 Applications for the VMG

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

1.4.1 Internet Access

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, VDSL or Ethernet connection at the same time. However, the VMG cannot work in ADSL and VDSL mode simultaneously. 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 83 for the **Network Setting > Broadband** screen. Computers can connect to the VMG's LAN ports (or wirelessly).

Figure 1 VMG's Internet Access Application



You can also configure IP filtering on the VMG for secure Internet access. Click **Security** > **MAC Filter** to set the IP Filtering. 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.

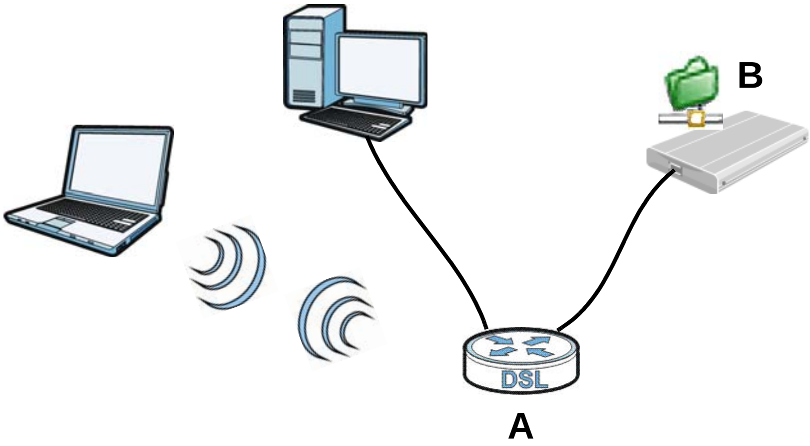
1.5 VMG's USB Support

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

File Sharing

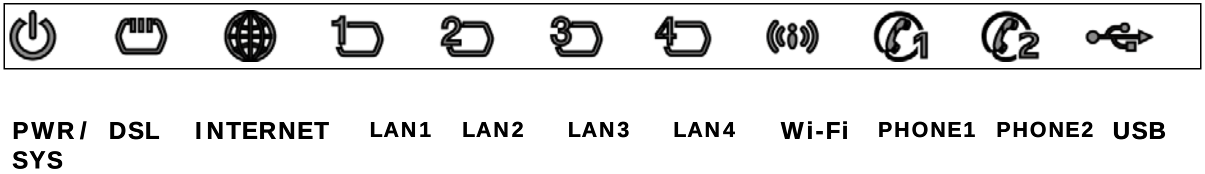
Use the built-in USB 2.0 port to share files on a USB memory stick or a USB hard drive (**B**). You can connect one USB hard drive to the VMG at a time. Use FTP to access the files on the USB device.

Figure 2 USB File Sharing Application



1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.



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

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	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 ADSL line is up.
		Blinking	The VMG is initializing the ADSL line.
	Orange	On	The VDSL line is up.
		Blinking	The VMG is initializing the VDSL line.
		Off	The DSL line is down.

Table 1 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
INTERNET	Green	On	The VMG has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The VMG is sending or receiving IP traffic.
		Off	There is no Internet connection or the gateway is in bridged mode.
	Red	On	The VMG attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
LAN	Green	On	The VMG has a successful 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 100 Mbps.
		Off	The VMG does not have an Ethernet connection with the LAN.
WiFi 2.4G	Green	On	The 2.4 GHz wireless network is activated.
		Blinking	The VMG is communicating with other wireless clients.
	Orange	Blinking	The VMG is setting up a WPS connection.
		Off	The 2.4 GHz wireless network is not activated.
Phone1, Phone2	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
		Off	The phone port does not have a SIP account registered.
USB	Green	On	The VMG recognizes a USB connection through the USB1 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 USB1 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 default login names and passwords will be reset (see the cover page).

1 Make sure the **PWR/SYS** LED is on (not blinking).

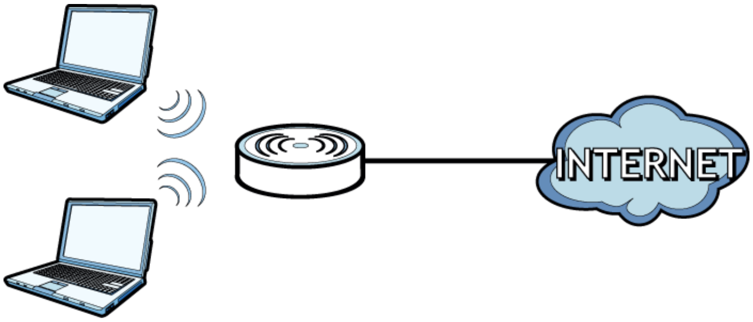
2 To set the device back to the factory default settings, press the **RESET** button for five seconds or until the **PWR/SYS** LED begins to blink and then release it. When the **PWR/SYS** LED begins to blink, the defaults have been restored and the device restarts.

1.8 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 3 Wireless Access Example



1.8.1 Using the Wi-Fi and WPS Buttons

If the wireless network is turned off, press the **Wi-Fi** button for one second. Once the **WiFi** 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 **PWR/SYS** LED is on and not blinking.

2 Press the **WPS** button for five seconds and release it.

3 Press the WPS button on another WPS-enabled device within range of the VMG. The **WiFi** LED flashes orange while the VMG sets up a WPS connection with the other wireless device.

4 Once the connection is successfully made, the **WiFi** LED shines green.

To turn off the wireless network, press the **Wi-Fi** button for one to five seconds. The **WiFi** LED turns off when the wireless network is off.

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy 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).

See Appendix D on page 399 if you need to make sure these functions are allowed in Internet Explorer.

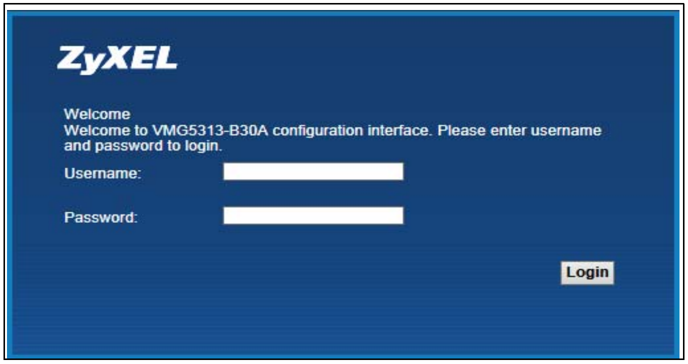
2.1.1 Accessing the Web Configurator

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 advanced account security is enabled (see Section 29.2 on page 313) the number of dots that appears when you type the password changes randomly to prevent anyone watching the password field from knowing the length of your password. If you have changed the password, enter your password and click **Login**.

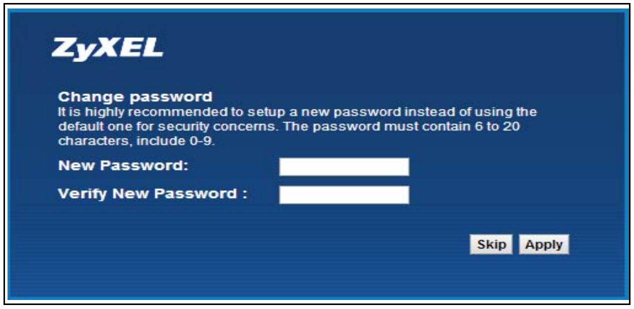
Figure 4 Password Screen



Welcome
Welcome to VMG5313-B30A configuration interface. Please enter username and password to login.
Username:
Password:

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

Figure 5 Change Password Screen



ZyXEL

Change password

It is highly recommended to setup a new password instead of using the default one for security concerns. The password must contain 6 to 20 characters, include 0-9.

New Password:

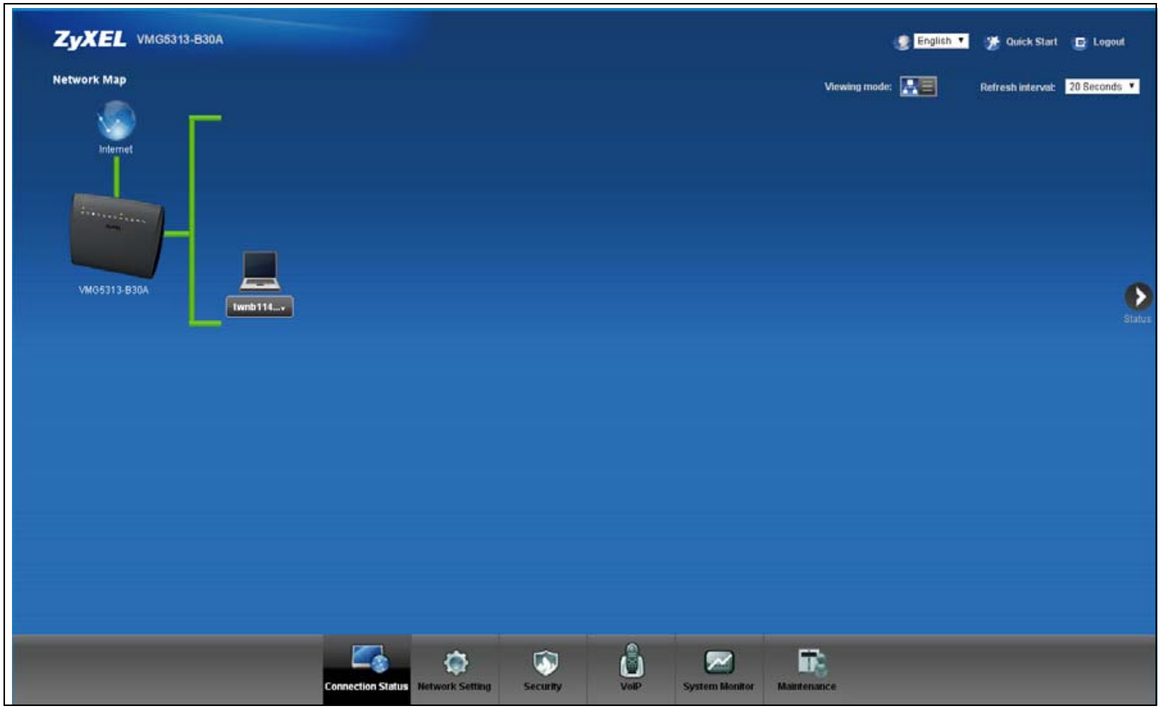
Verify New Password :

Skip Apply

5 The **Quick Start Wizard** screen appears. You can configure the VMG's time zone, basic Internet access, and wireless settings. See Chapter 3 on page 33 for more information.

6 After you finished or closed the **Quick Start Wizard** screen, the **Network Map** page appears.

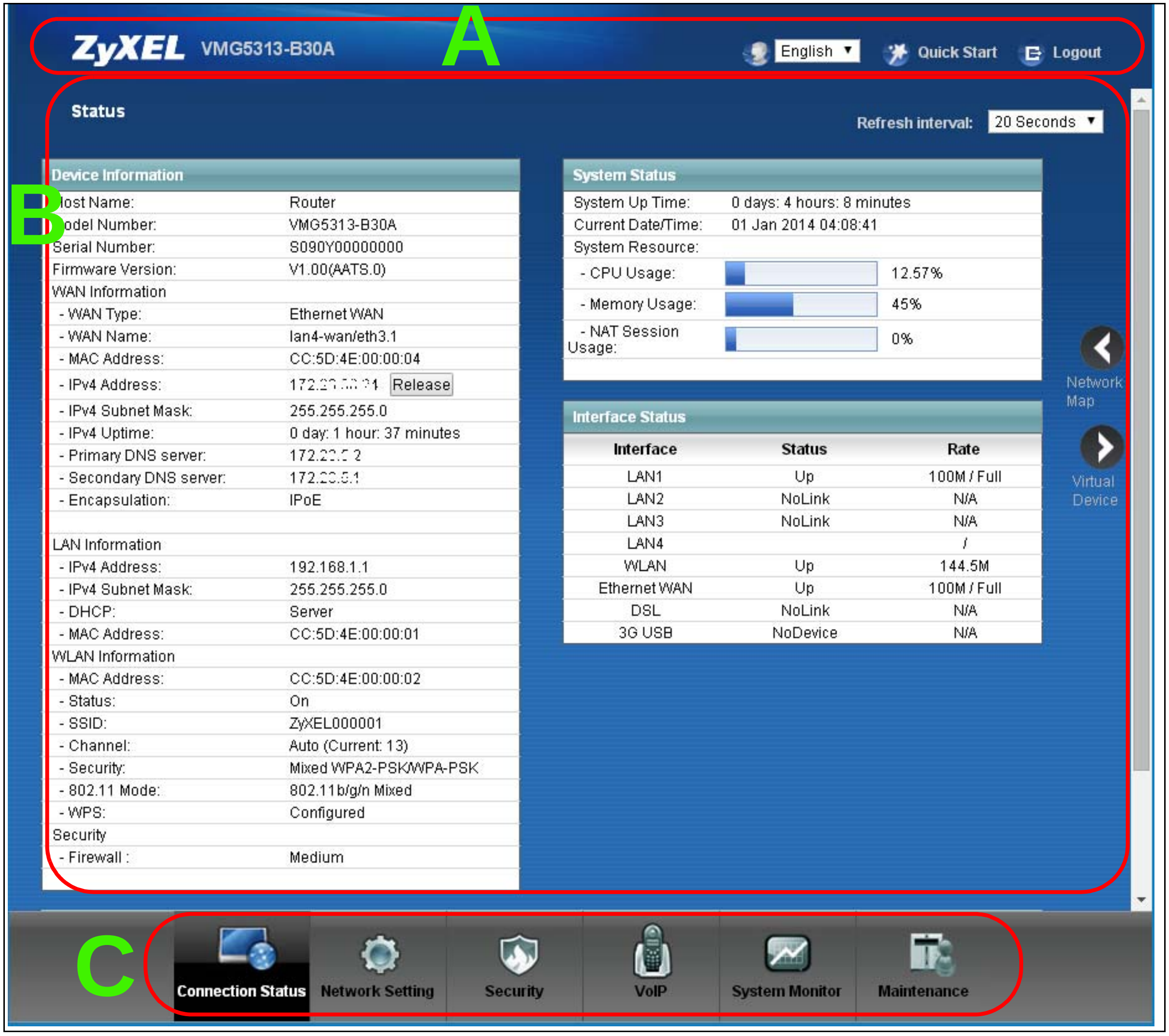
Figure 6 Network Map



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

2.2 Web Configurator Layout

Figure 7 Screen Layout



Status

Refresh interval: 20 Seconds

Device Information	
Host Name:	Router
Model Number:	VMG5313-B30A
Serial Number:	S090Y00000000
Firmware Version:	V1.00(AATS.0)
WAN Information	
- WAN Type:	Ethernet WAN
- WAN Name:	lan4-wan/eth3.1
- MAC Address:	CC:5D:4E:00:00:04
- IPv4 Address:	172.2[illegible]1 Release
- IPv4 Subnet Mask:	255.255.255.0
- IPv4 Uptime:	0 day: 1 hour: 37 minutes
- Primary DNS server:	172.2[illegible]2
- Secondary DNS server:	172.2[illegible].1
- Encapsulation:	IPoE
LAN Information	
- IPv4 Address:	192.168.1.1
- IPv4 Subnet Mask:	255.255.255.0
- DHCP:	Server
- MAC Address:	CC:5D:4E:00:00:01
WLAN Information	
- MAC Address:	CC:5D:4E:00:00:02
- Status:	On
- SSID:	ZyXEL000001
- Channel:	Auto (Current: 13)
- Security:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Security	
- Firewall :	Medium

System Status	
System Up Time:	0 days: 4 hours: 8 minutes
Current Date/Time:	01 Jan 2014 04:08:41
System Resource:	
- CPU Usage:	12.57%
- Memory Usage:	45%
- NAT Session Usage:	0%

Interface Status

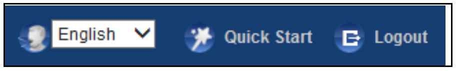
Interface	Status	Rate
LAN1	Up	100M / Full
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4		/
WLAN	Up	144.5M
Ethernet WAN	Up	100M / Full
DSL	NoLink	N/A
3G USB	NoDevice	N/A

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

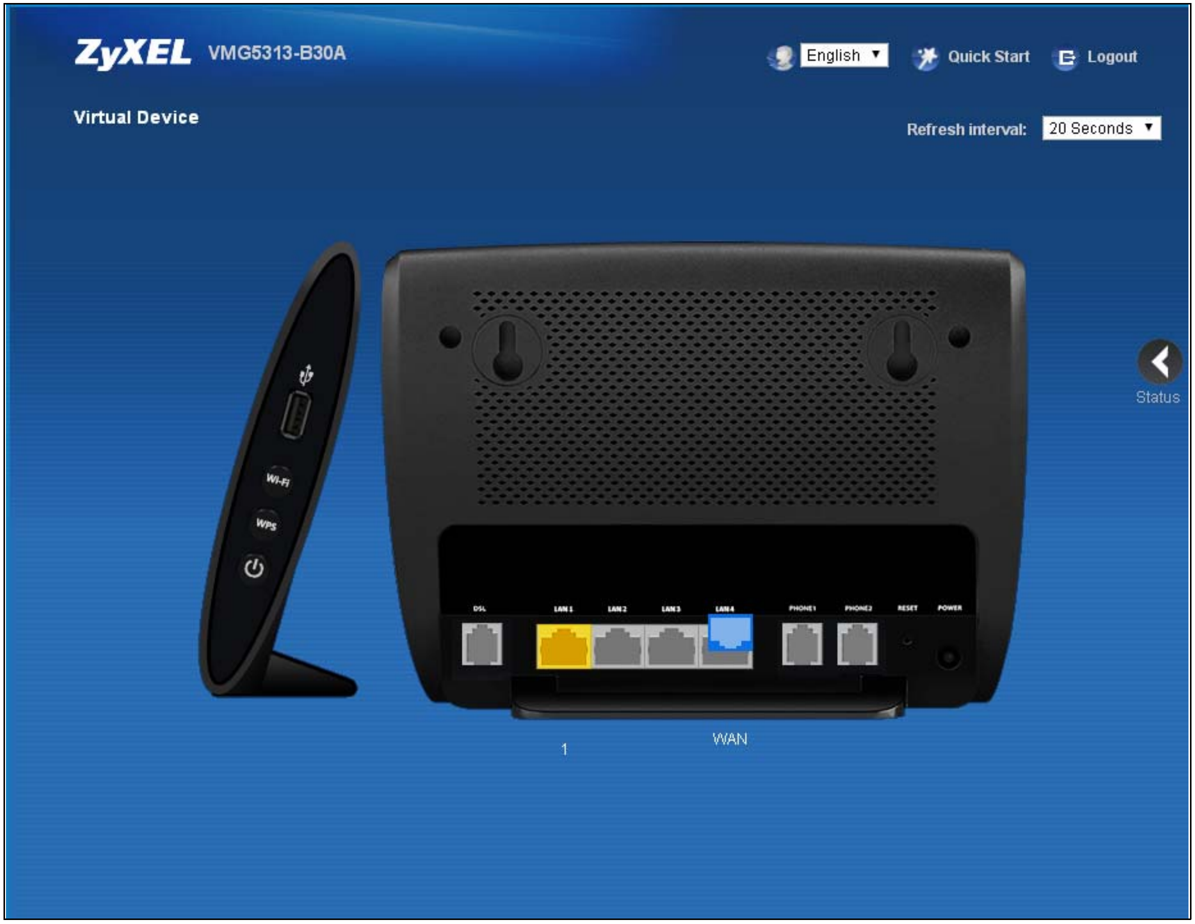
2.2.2 Main Window

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

After you click **Status** on the **Connection Status** page, the **Status** screen is displayed. See Chapter 5 on page 74 for more information about the **Status** screen.

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

Figure 8 Virtual Device



Refresh interval: 20 Seconds

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 WAN connection.
	Advanced	Use this screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions.
	802.1x	Use this screen to view and configure the IEEE 802.1x settings on the VMG.
	Ethernet WAN	Use this screen to convert Ethernet LAN 4 port as WAN port, or restore the WAN port to LAN port.
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.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to turn UPnP and UPnP NAT-T on or off.
	Additional Subnet	Use this screen to configure IP alias and public static IP.
	STB Vendor ID	Use this screen to have the VMG automatically create static DHCP entries for Set Top Box (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	Use DHCP option 66 to identify a TFTP server name.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Routing	Static Route	Use this screen to view and set up static routes on the VMG.
	DNS Route	Use this screen to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s).
	Policy Forwarding	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.
	Class Setup	Use this screen to define a classifier.
	Policer Setup	Use these screens to configure QoS policers.
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 Device'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.
DDNS	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.
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.
	Print Server	Use this screen to enable the print server on the VMG and get the model name of the associated printer.
Power Management	Power Management	This screen is only available for administrators. Use this screen to manually turn on/off specific interface(s) and/or all LEDs immediately.
	Auto Switch Off	This screen is only available for administrators. Use this screen to configure schedules to have the VMG automatically turn on/off specific interface(s) and/or all LEDs.
Security Settings		

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
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 Rules	Scheduler Rules	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.
IPSec VPN	Setup	Use this screen to add or edit VPN policies.
	Monitor	Use this screen to view the status of all IPSec VPN tunnels. You can also manually initiate a tunnel in this screen.
VoIP		
SIP	SIP Account	Use this screen to set up information about your SIP account and configure audio settings such as volume levels for the phones connected to the VMG.
	SIP Service Provider	Use this screen to configure your VMG's Voice over IP settings.
Phone	Phone	Use this screen to select your location and a call service mode.
Call Rule	Call Rule	
Call History	Call History Summary	Use this screen to view a call history list.
	Call History Outgoing	Use this screen to view detailed information for each outgoing call you made.
	Call History Incoming	Use this screen to view detailed information for each incoming call from someone calling you.
System Monitor		

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Log	System Log	Use this screen to view the status of events that occurred to the VMG. You can export or e-mail the logs.
	Security Log	Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window. Levels include: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging Category include: • 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.
VoIP Status	VoIP Status	Use this screen to view VoIP registration, current call status and phone numbers for the phone ports.
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.
IGMP/MLD Group Status	IGMP/MLD Group Status	Use this screen to view the status of all IGMP settings on the VMG.
xDSL Statistics	xDSL Statistics	Use this screen to view the Device's xDSL traffic statistics.
3G Statistics	3G Statistics	Use this screen to look at 3G Internet connection status.
Maintenance		
User Account	User Account	Use this screen to change user password on the VMG.
Remote MGMT		
	Remote MGMT	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to grant access to local management service by adding IP address.
TR-069 Client	TR-069 Client	Use this screen to configure the VMG to be managed by an Auto Configuration Server (ACS).
TR-064	TR-064	Use this screen to enable management via TR-064 on the LAN.
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.

Table 3 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
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.
Configuration	Configuration	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

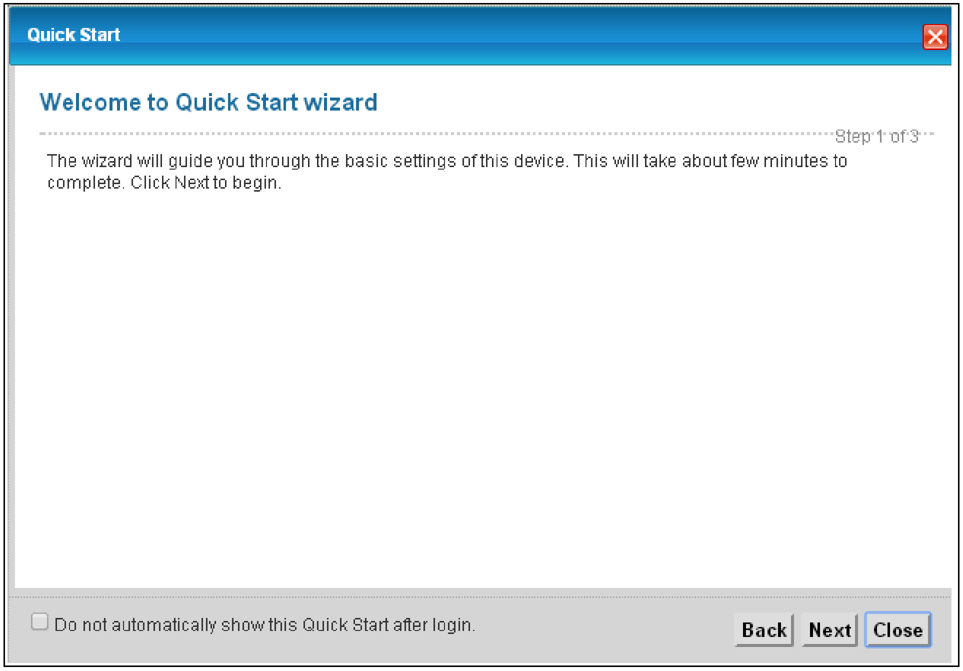
Use the Quick Start screens to configure the VMG’s time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on Chapter 4 on page 35) for background information on the features in this chapter.

3.2 Quick Start Setup

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

Figure 9 Quick Start - Welcome

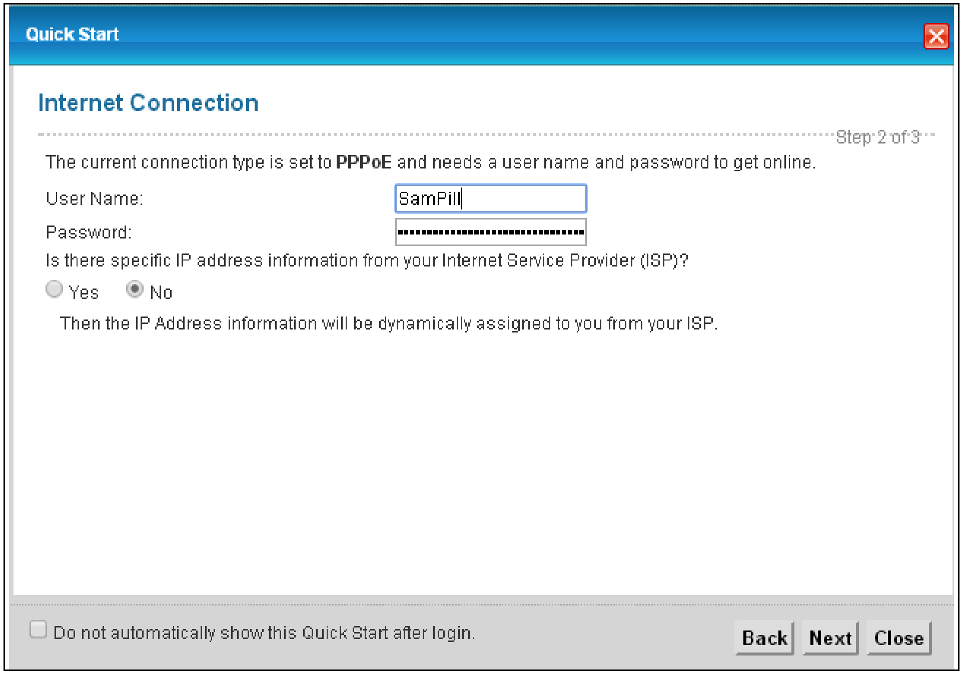


Welcome to Quick Start wizard

The wizard will guide you through the basic settings of this device. This will take about few minutes to complete. Click Next to begin.

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

Figure 10 Quick Start - Internet Connection



Internet Connection

Step 2 of 3

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

User Name: SamPill

Password: ••••••••••••••••••••••••••••••••

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

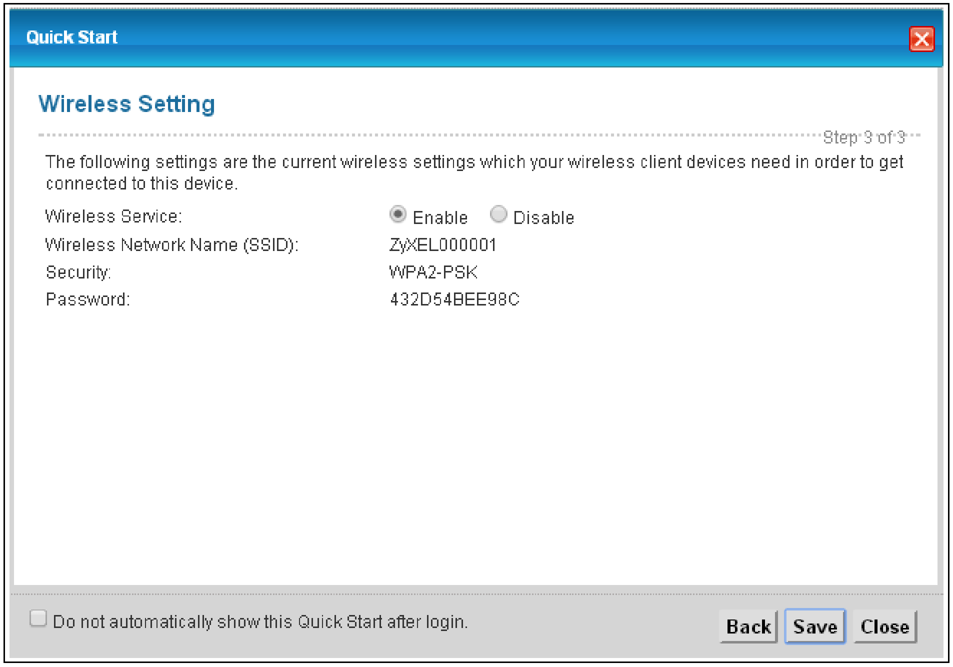
○ Yes ● No

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

□ Do not automatically show this Quick Start after login.

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 11 Quick Start - Wireless



Wireless Setting

Step 3 of 3

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

Wireless Service: ● Enable ○ Disable

Wireless Network Name (SSID): ZyXEL000001

Security: WPA2-PSK

Password: 432D54BEE98C

□ Do not automatically show this Quick Start after login.

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

4

Tutorials

4.1 Overview

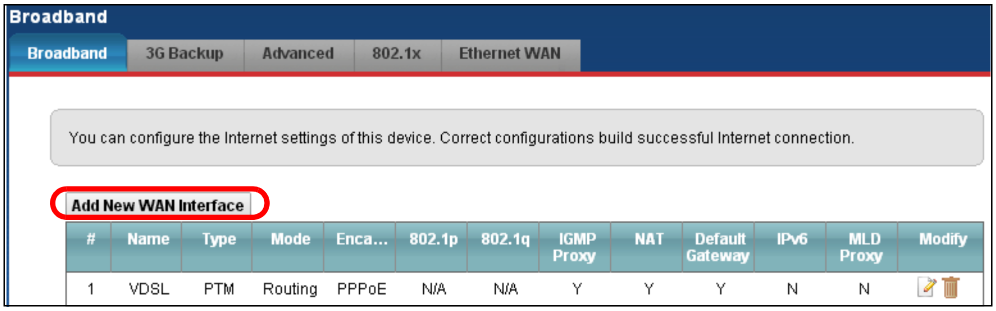
This chapter shows you how to use the VMG's various features.

- Setting Up an Ethernet WAN Connection, see page 35
- Configure the Broadband screen as follows., see page 35
- Setting Up a Secure Wireless Network, see page 41
- Setting Up Multiple Wireless Groups, see page 47
- Configuring Static Route for Routing to Another Network, see page 50
- Configuring QoS Queue and Class Setup, see page 53
- Access the VMG Using DDNS, see page 56
- Configuring the MAC Address Filter, see page 57
- Access Your Shared Files From a Computer, see page 58
- Using the Media Server Feature, see page 60
- Using the Print Server Feature, see page 65

4.2 Setting Up an Ethernet WAN Connection

This tutorial shows you how to use LAN port 4 as an alternative or backup Internet connection using the Web Configurator.

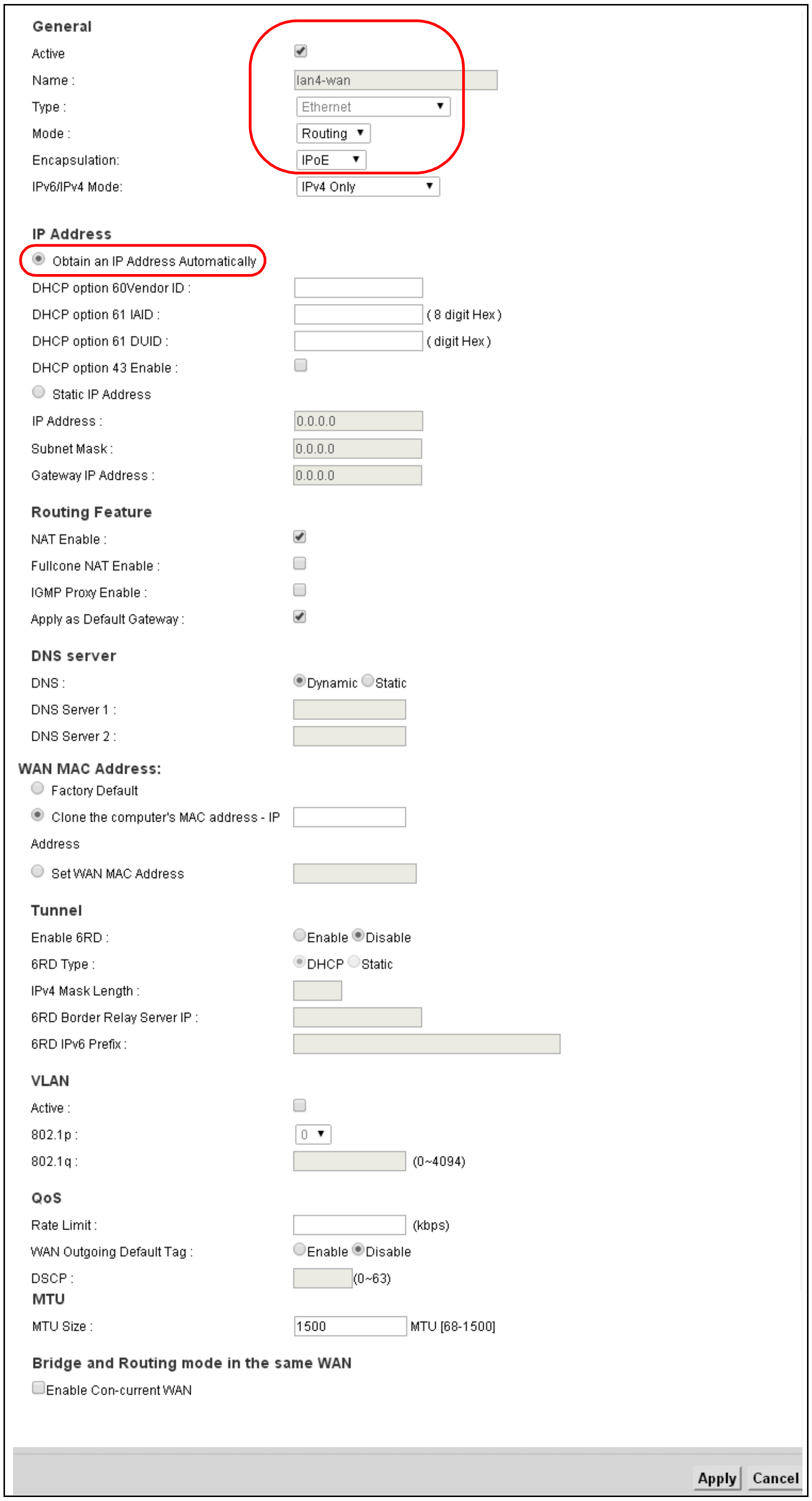
1 Click **Network Setting > Broadband** to open the following screen. Click **Add New WAN Interface**.



You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

#	Name	Type	Mode	Enca...	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	VDSL	PTM	Routing	PPPoE	N/A	N/A	Y	Y	Y	N	N	✎ 🗑

2 Configure the **Broadband** screen as follows.



General

Active ☑

Name : lan4-wan

Type : Ethernet ▼

Mode : Routing ▼

Encapsulation: IPoE ▼

IPv6/IPv4 Mode: IPv4 Only ▼

IP Address

● Obtain an IP Address Automatically

DHCP option 60Vendor ID :

DHCP option 61 IAID : (8 digit Hex)

DHCP option 61 DUID : (digit Hex)

DHCP option 43 Enable : □

○ Static IP Address

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway IP Address : 0.0.0.0

Routing Feature

NAT Enable : ☑

Fullcone NAT Enable : □

IGMP Proxy Enable : □

Apply as Default Gateway : ☑

DNS server

DNS : ● Dynamic ○ Static

DNS Server 1 :

DNS Server 2 :

WAN MAC Address:

○ Factory Default

● Clone the computer's MAC address - IP Address

○ Set WAN MAC Address

Tunnel

Enable 6RD : ○ Enable ● Disable

6RD Type : ● DHCP ○ Static

IPv4 Mask Length :

6RD Border Relay Server IP :

6RD IPv6 Prefix :

VLAN

Active : □

802.1p : 0 ▼

802.1q : (0~4094)

QoS

Rate Limit : (kbps)

WAN Outgoing Default Tag : ○ Enable ● Disable

DSCP : (0~63)

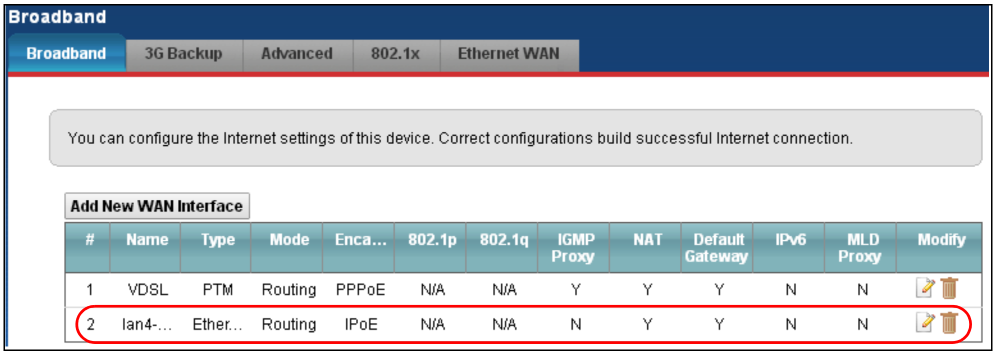
MTU

MTU Size : 1500 MTU [68-1500]

Bridge and Routing mode in the same WAN

□ Enable Con-current WAN

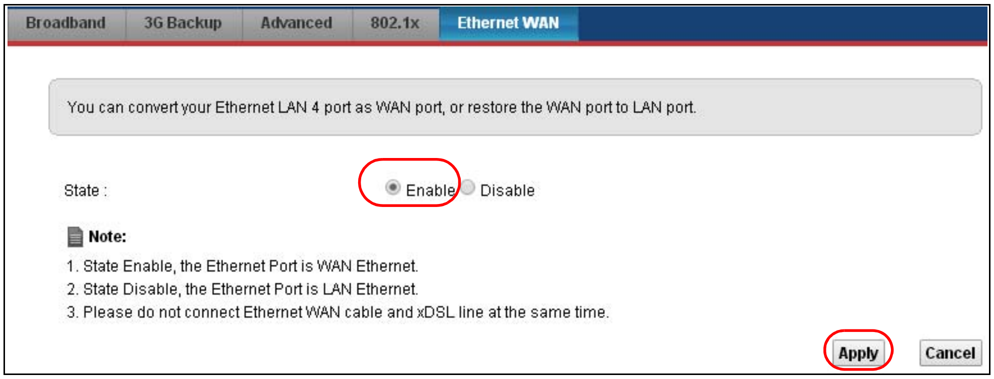
3 The **Broadband** summary screen then appears as follows.



You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

#	Name	Type	Mode	Enca...	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	VDSL	PTM	Routing	PPPoE	N/A	N/A	Y	Y	Y	N	N	
2	lan4-...	Ether...	Routing	IPoE	N/A	N/A	N	Y	Y	N	N	

4 Next, go to **Broadband > Ethernet WAN**, select **Enable** and then click **Apply**.



You can convert your Ethernet LAN 4 port as WAN port, or restore the WAN port to LAN port.

State : ● Enable ○ Disable

Note:

1. State Enable, the Ethernet Port is WAN Ethernet.
2. State Disable, the Ethernet Port is LAN Ethernet.
3. Please do not connect Ethernet WAN cable and xDSL line at the same time.

5 After the connection is set up, connect LAN port 4 to a broadband router or modem for Internet access.

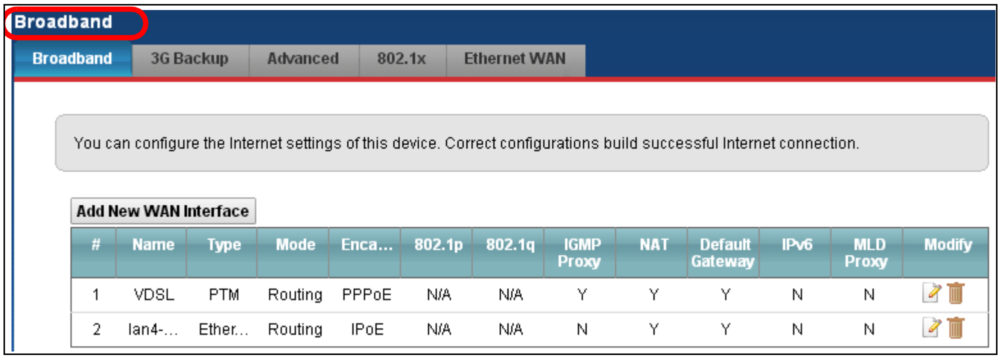
Note: The DSL Internet connection and the Ethernet Internet connection cannot operate at the same time.

4.3 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**.



You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

#	Name	Type	Mode	Enca...	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	VDSL	PTM	Routing	PPPoE	N/A	N/A	Y	Y	Y	N	N	
2	lan4-...	Ether...	Routing	IPoE	N/A	N/A	N	Y	Y	N	N	

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

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

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

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

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

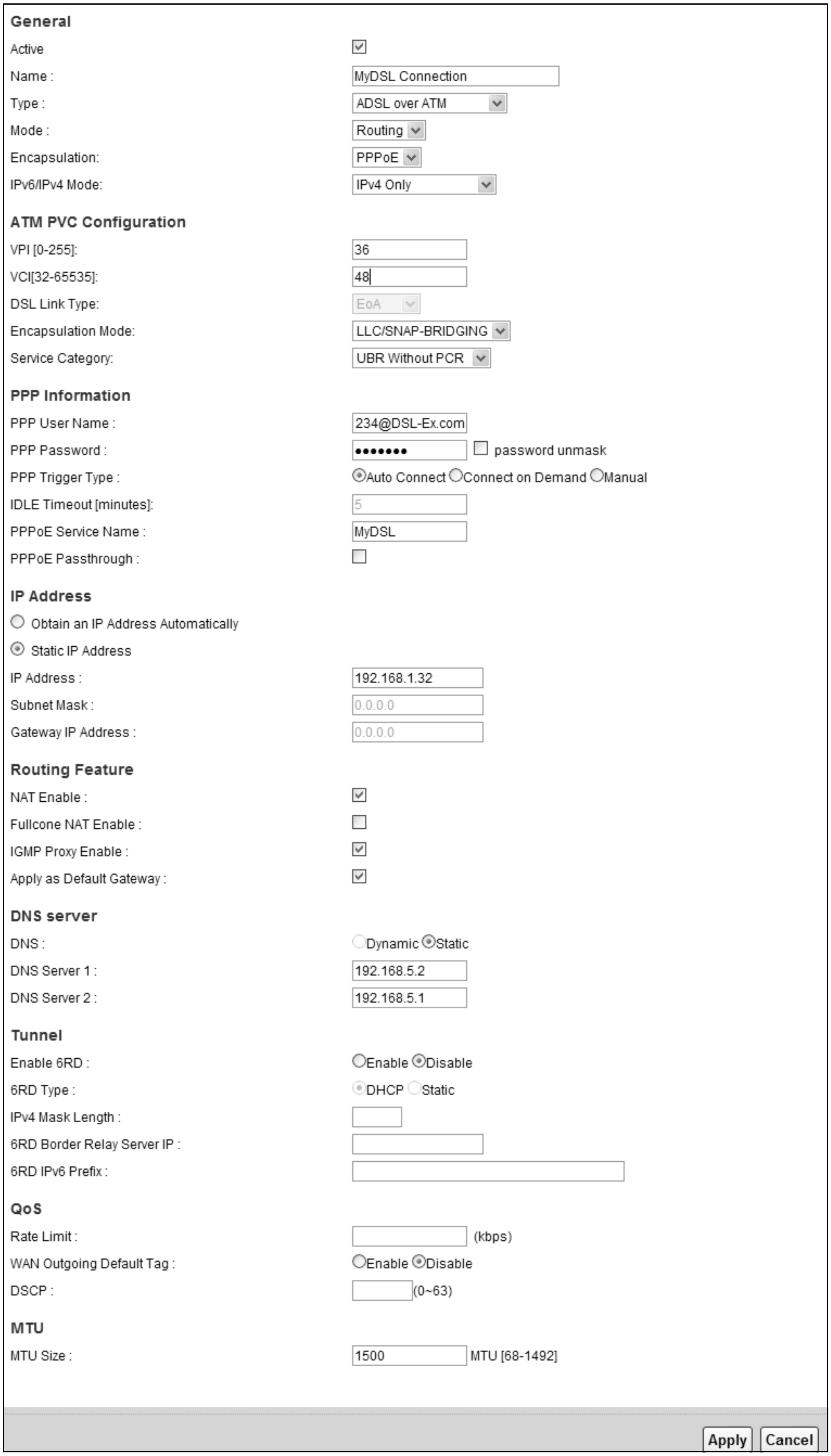
Set the **IPv6/IPv4 Mode** to **IPv4 Only**.

4 Enter the account information provided to you by your DSL service provider.

5 Configure this rule as your default Internet connection by selecting the **Apply as Default Gateway** check box. Then select DNS as **Static** and enter the DNS server addresses provided to you, such as **192.168.5.2** (DNS server1)/**192.168.5.1** (DNS server2).

6 Leave the rest of the fields to the default settings.

7 Click **Apply** to save your settings.



General

Active	☑
Name :	MyDSL Connection
Type :	ADSL over ATM
Mode :	Routing
Encapsulation:	PPPoE
IPv6/IPv4 Mode:	IPv4 Only

ATM PVC Configuration

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

PPP Information

PPP User Name :	234@DSL-Ex.com
PPP Password :	••••••• □ password unmask
PPP Trigger Type :	● Auto Connect ○ Connect on Demand ○ Manual
IDLE Timeout [minutes]:	5
PPPoE Service Name :	MyDSL
PPPoE Passthrough :	□

IP Address

○ Obtain an IP Address Automatically

● Static IP Address

IP Address :	192.168.1.32
Subnet Mask :	0.0.0.0
Gateway IP Address :	0.0.0.0

Routing Feature

NAT Enable :	☑
Fullcone NAT Enable :	□
IGMP Proxy Enable :	☑
Apply as Default Gateway :	☑

DNS server

DNS :	○ Dynamic ● Static
DNS Server 1 :	192.168.5.2
DNS Server 2 :	192.168.5.1

Tunnel

Enable 6RD :	○ Enable ● Disable
6RD Type :	● DHCP ○ Static
IPv4 Mask Length :	
6RD Border Relay Server IP :	
6RD IPv6 Prefix :	

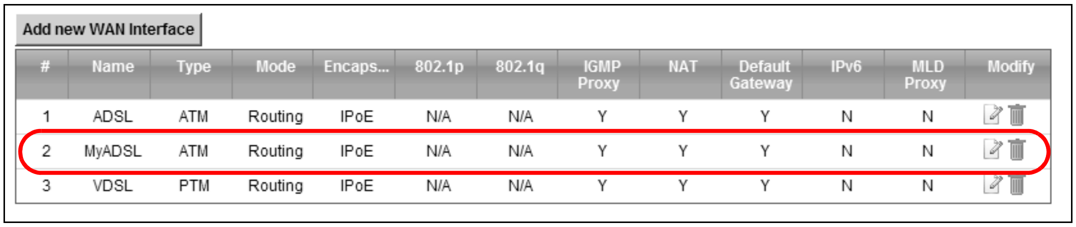
QoS

Rate Limit :	(kbps)
WAN Outgoing Default Tag :	○ Enable ● Disable
DSCP :	(0~63)

MTU

MTU Size :	1500 MTU [68-1492]

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



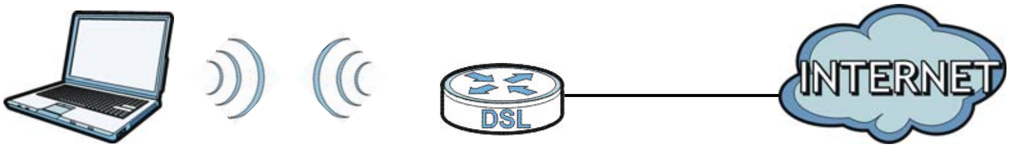
Add new WAN Interface

#	Name	Type	Mode	Encaps...	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
2	MyADSL	ATM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	
3	VDSL	PTM	Routing	IPoE	N/A	N/A	Y	Y	Y	N	N	

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

4.4 Setting Up a Secure Wireless Network

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



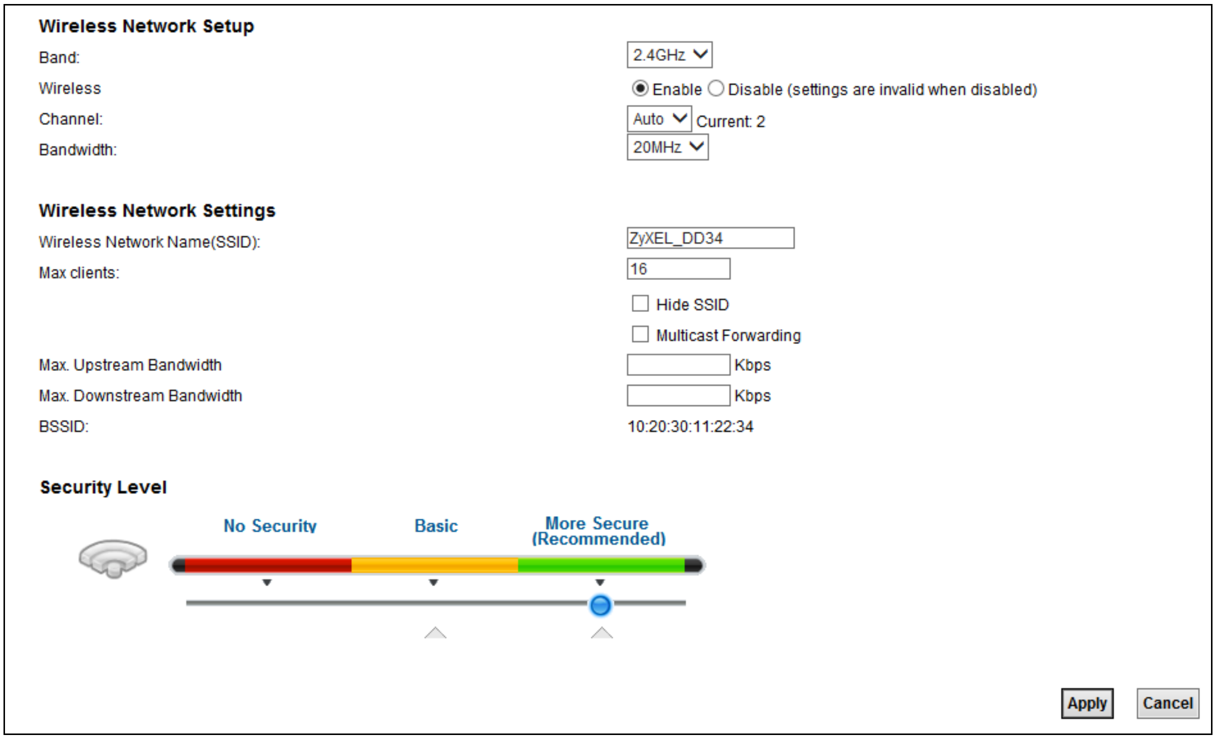
Thomas has to configure the wireless network settings on the VMG. Then he can set up a wireless network using WPS (Section 4.4.2 on page 42) or manual configuration (Section 4.4.3 on page 46).

4.4.1 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 41). Click **Apply**.



Wireless Network Setup

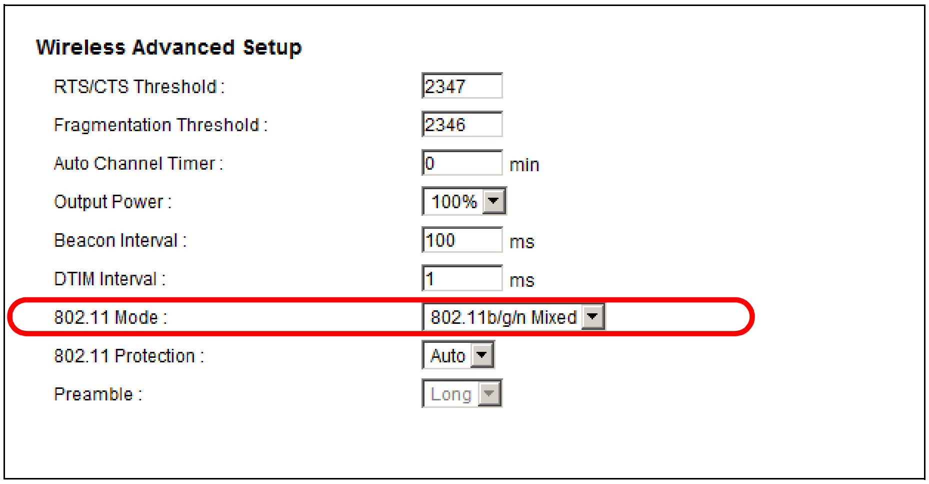
Band:	2.4GHz
Wireless	● Enable ○ Disable (settings are invalid when disabled)
Channel:	Auto Current: 2
Bandwidth:	20MHz

Wireless Network Settings

Wireless Network Name(SSID):	ZyXEL_DD34
Max clients:	16
	□ Hide SSID
	□ Multicast Forwarding
Max. Upstream Bandwidth	Kbps
Max. Downstream Bandwidth	Kbps
BSSID:	10:20:30:11:22:34

Security Level

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



Wireless Advanced Setup

RTS/CTS Threshold :	2347
Fragmentation Threshold :	2346
Auto Channel Timer :	0 min
Output Power :	100%
Beacon Interval :	100 ms
DTIM Interval :	1 ms
802.11 Mode :	802.11b/g/n Mixed
802.11 Protection :	Auto
Preamble :	Long

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the VMG (see Section 4.4.2 on page 42). He can also use the notebook's wireless client to search for the VMG (see Section 4.4.3 on page 46).

4.4.2 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.

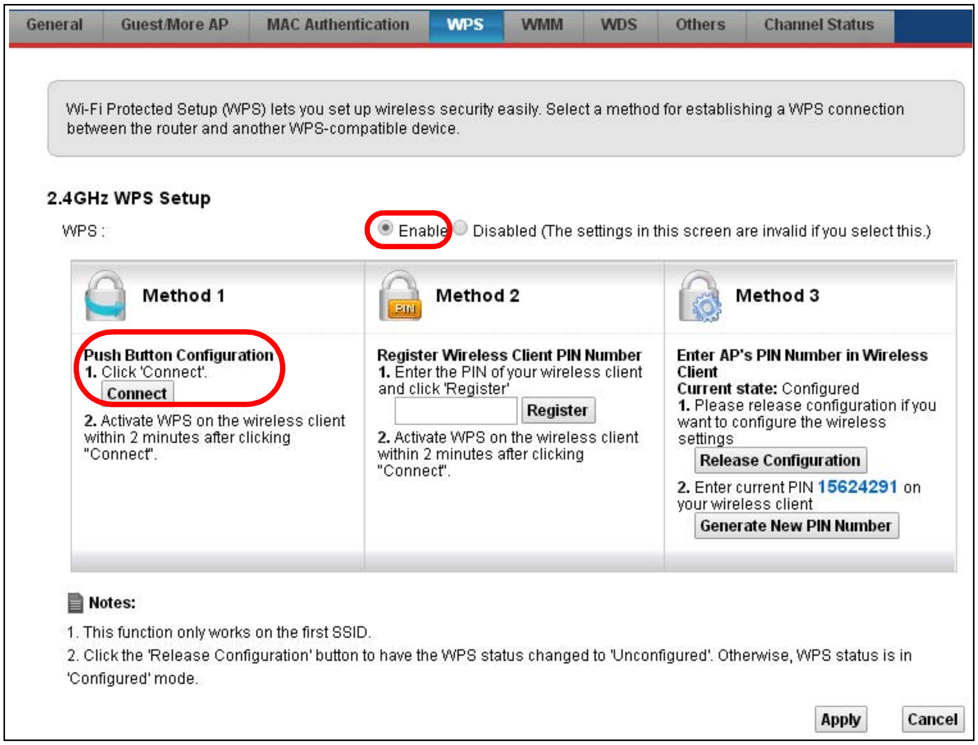
Push Button Configuration (PBC)

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 and click **Apply**. Then click the **Connect** button.



Wi-Fi Protected Setup (WPS) lets you set up wireless security easily. Select a method for establishing a WPS connection between the router and another WPS-compatible device.

2.4GHz WPS Setup

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

Method 1

Push Button Configuration
1. Click 'Connect'.
Connect
2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client PIN Number
1. Enter the PIN of your wireless client and click 'Register'
Register
2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

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
2. Enter current PIN 15624291 on your wireless client
Generate New PIN Number

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

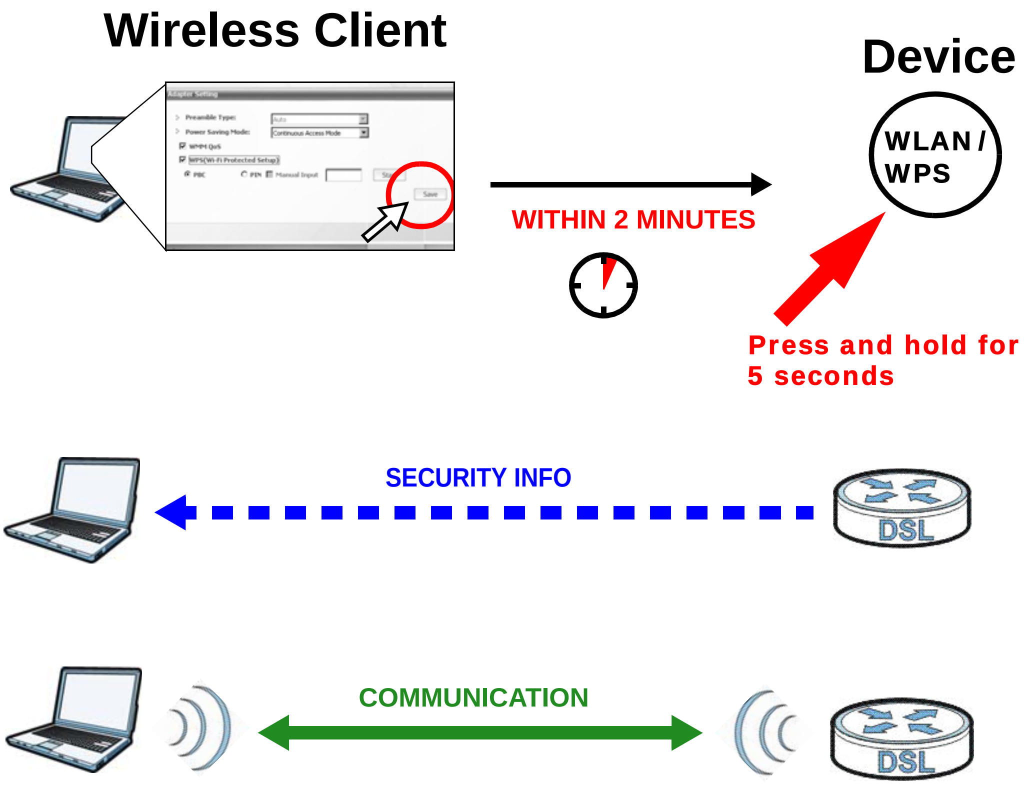
Apply Cancel

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

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

The 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.

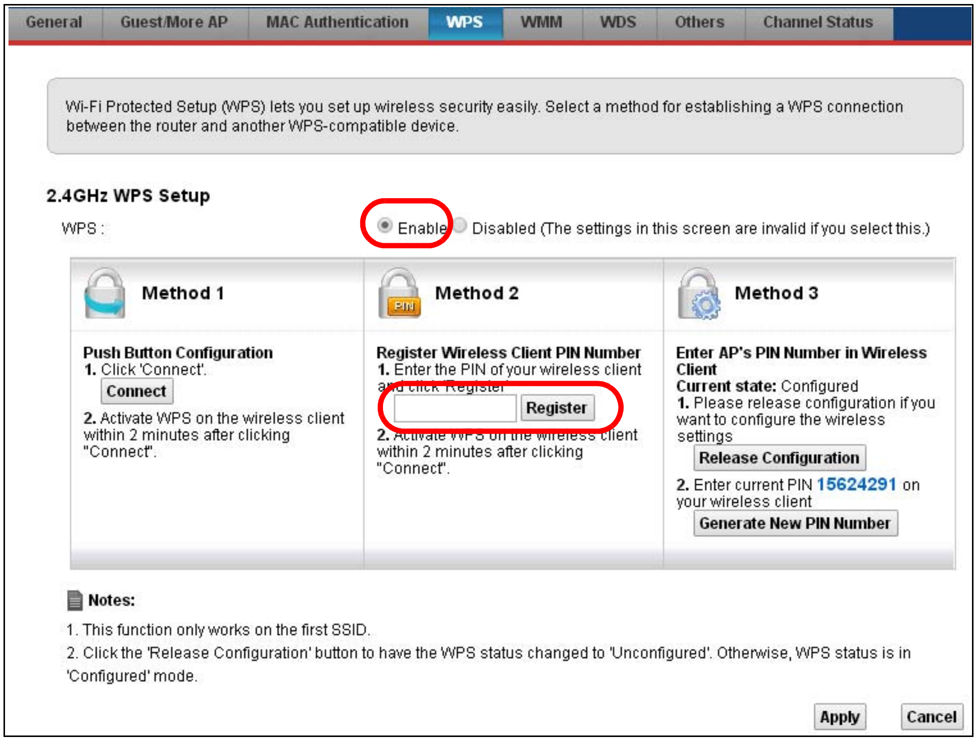


PIN Configuration

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**.



Wi-Fi Protected Setup (WPS) lets you set up wireless security easily. Select a method for establishing a WPS connection between the router and another WPS-compatible device.

2.4GHz WPS Setup

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

Method 1	Method 2	Method 3
Push Button Configuration **1.** Click 'Connect'. Connect **2.** Activate WPS on the wireless client within 2 minutes after clicking "Connect".	**Register Wireless Client PIN Number** **1.** Enter the PIN of your wireless client and click 'Register' Register **2.** Activate WPS on the wireless client within 2 minutes after clicking "Connect".	**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 **2.** Enter current PIN 15624291 on your wireless client Generate New PIN Number

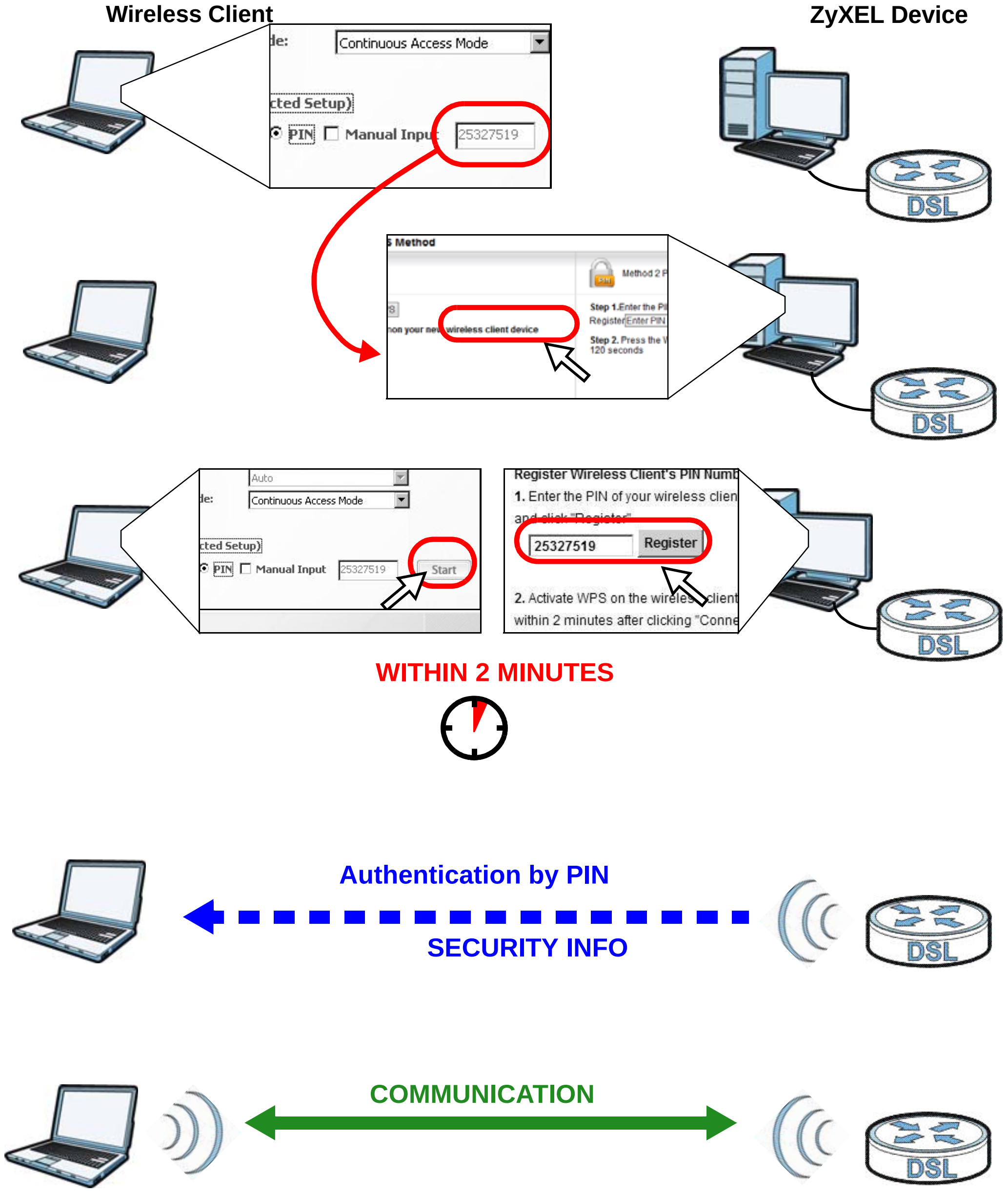
Notes:

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

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

The 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.



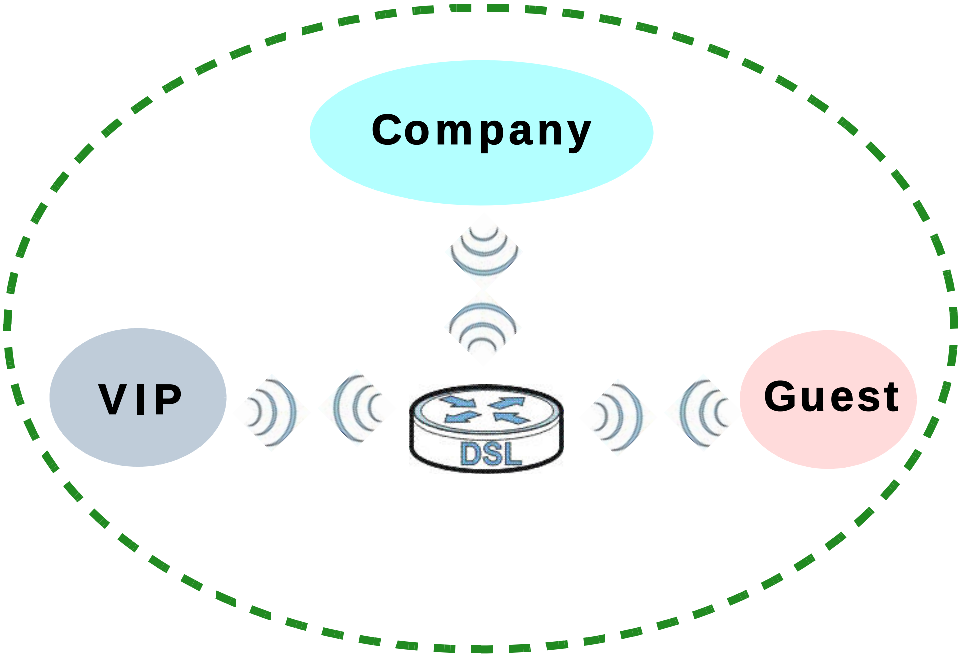
4.4.3 Without WPS

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.

4.5 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.

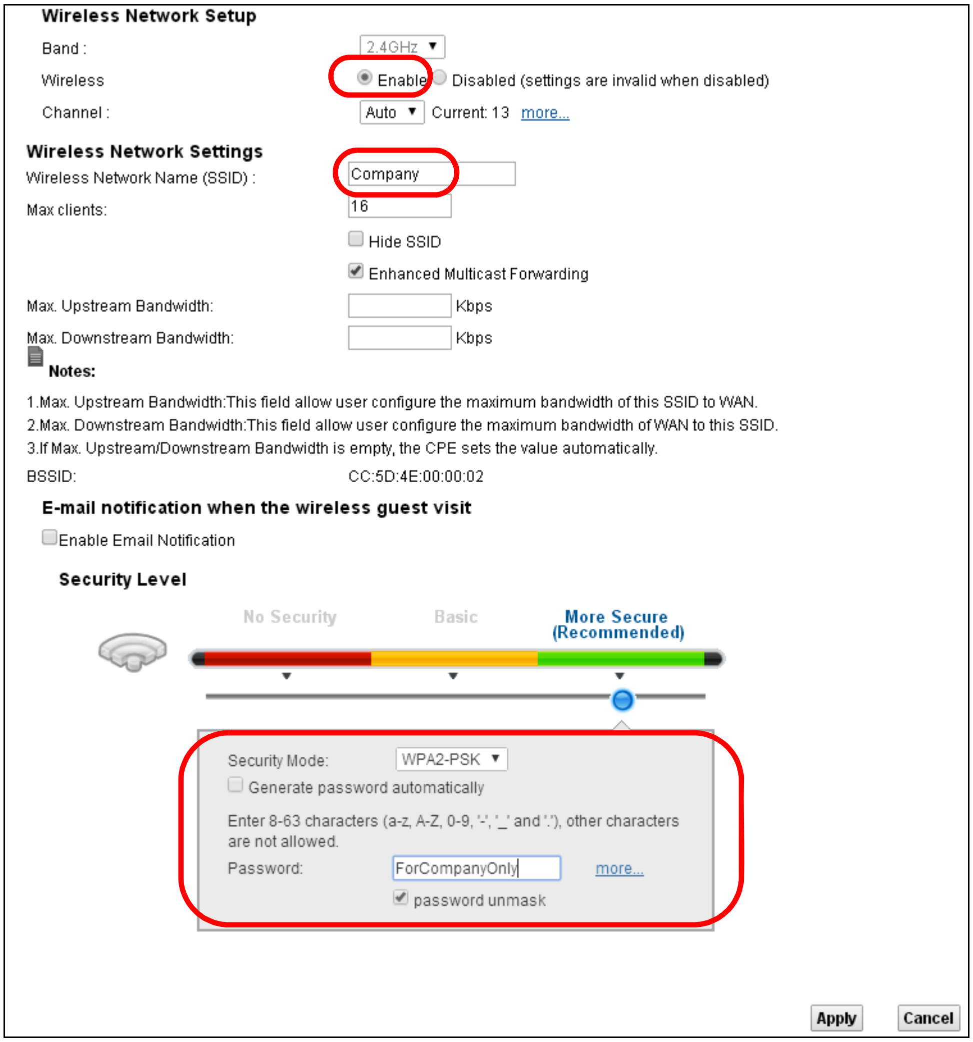


- Employees in Company A will use a general **Company** wireless network group.
- Higher management level and important visitors will use the **VIP** group.
- Visiting guests will use the **Guest** group, which has a different SSID and password.

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

Security Mode: WPA2-PSK

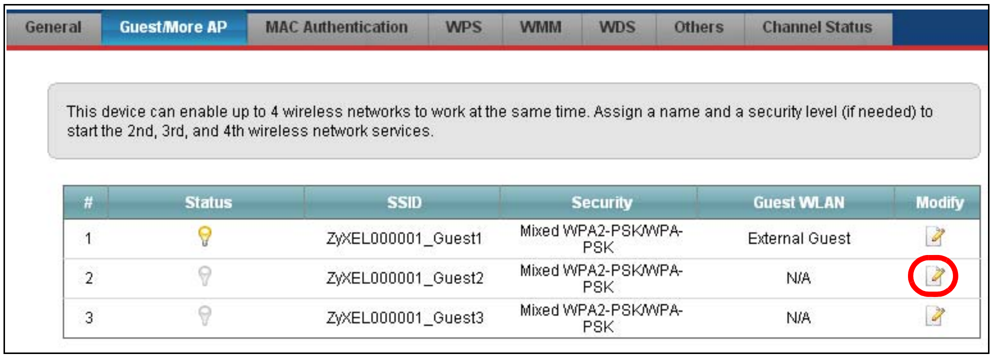
□ Generate password automatically

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

Password: ForCompanyOnly more...

☑ password unmask

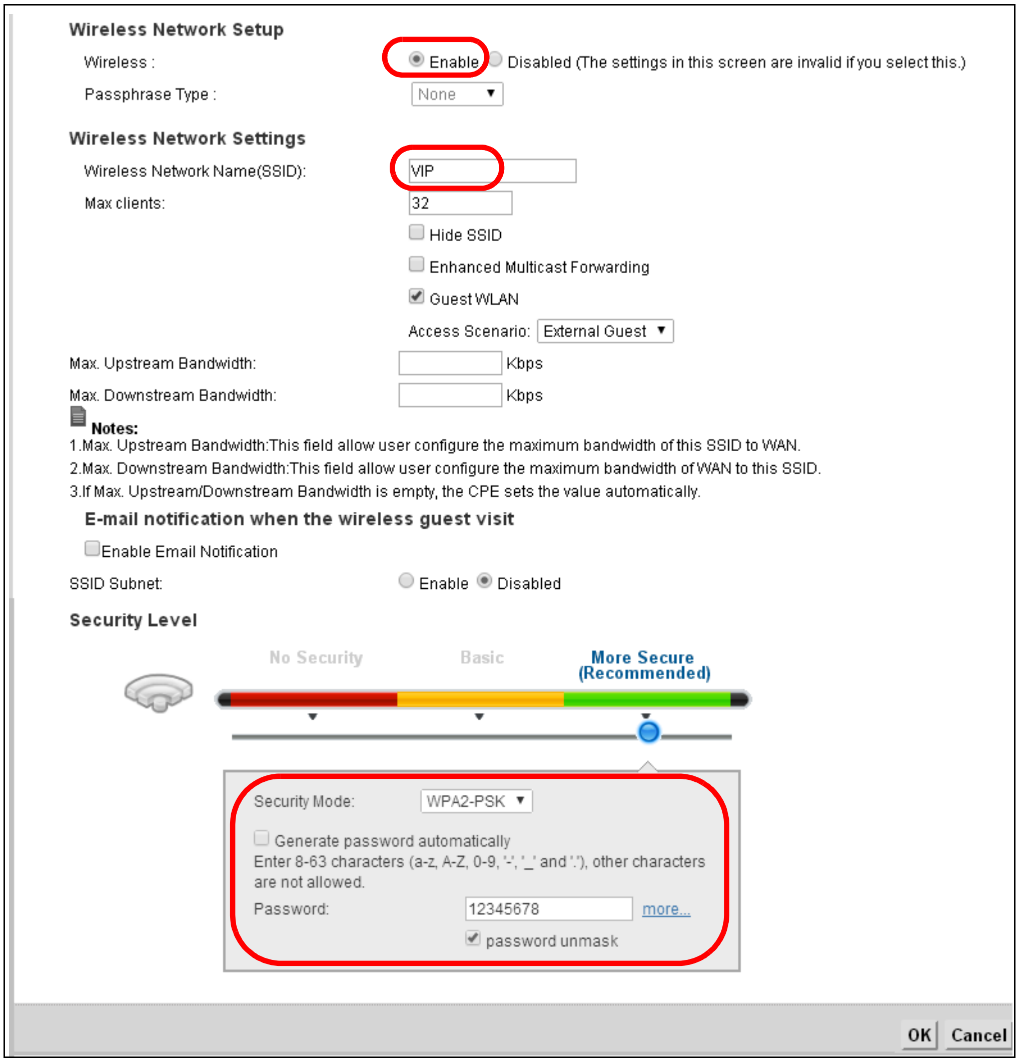
2 Click **Network Setting > Wireless > Guest/More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group.



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 : None

Wireless Network Settings

Wireless Network Name(SSID): VIP

Max clients: 32

□ Hide SSID

□ Enhanced Multicast Forwarding

☑ Guest WLAN

Access Scenario: External Guest

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

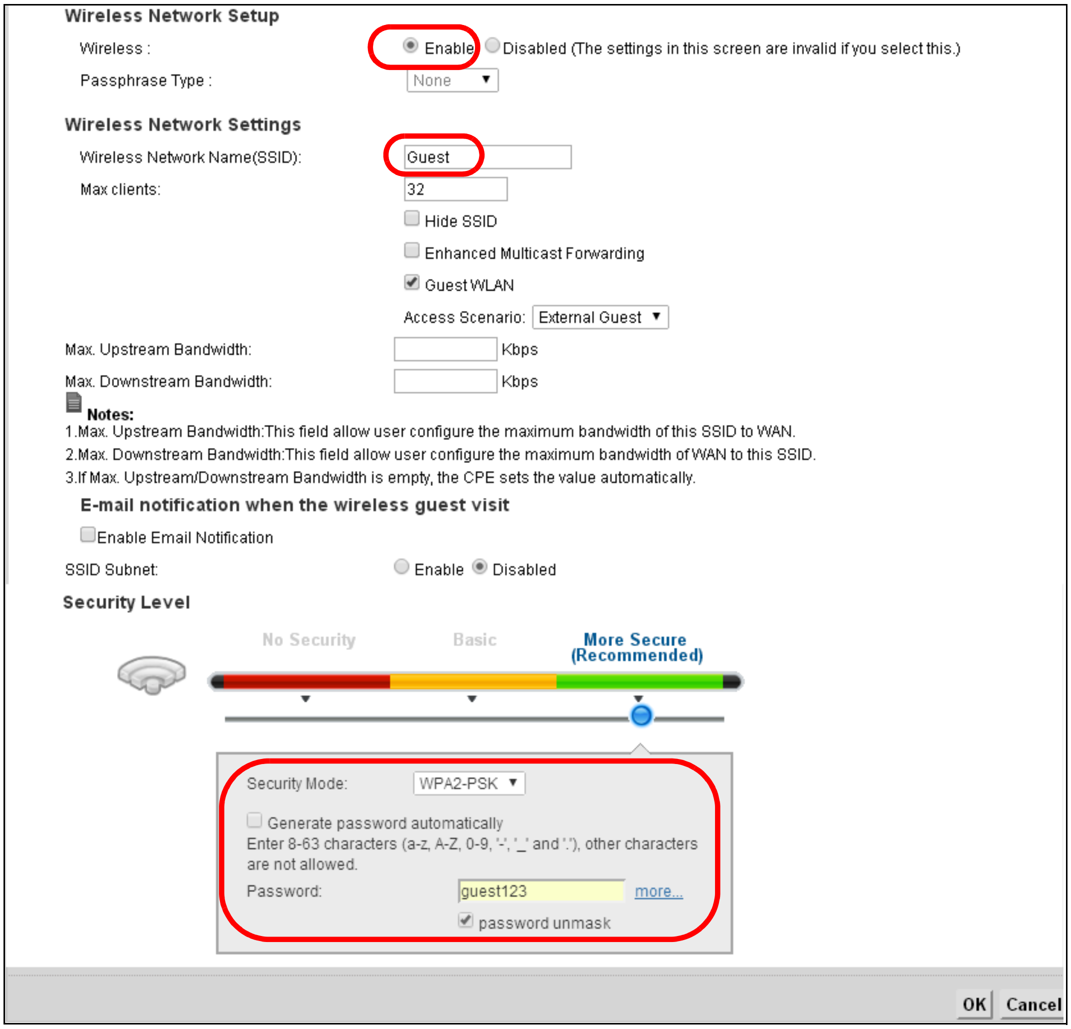
Security Mode: WPA2-PSK

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

Password: 12345678 more...

☑ password unmask

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 : None ▼

Wireless Network Settings

Wireless Network Name(SSID): Guest

Max clients: 32

☐ Hide SSID

☐ Enhanced Multicast Forwarding

☑ Guest WLAN

Access Scenario: External Guest ▼

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

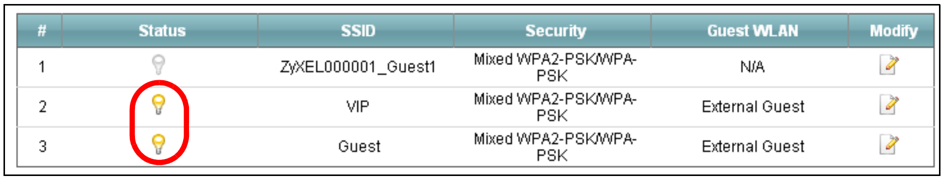
Security Mode: WPA2-PSK ▼

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

Password: guest123 more...

☑ password unmask

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.

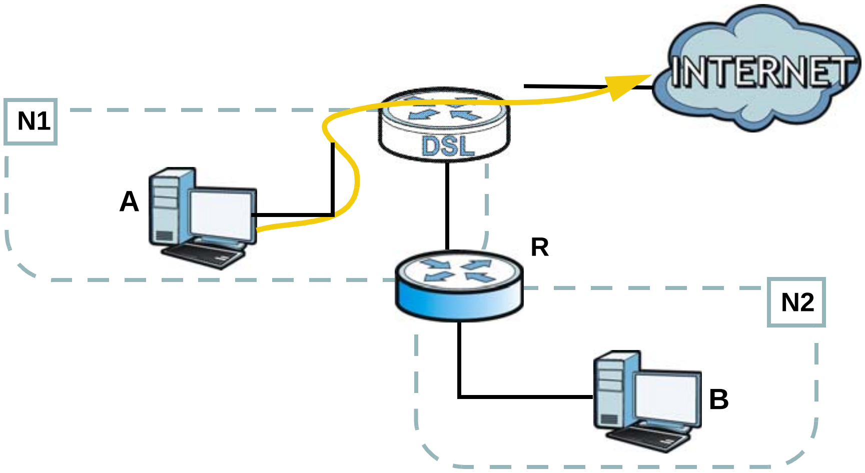


#	Status	SSID	Security	Guest WLAN	Modify
1	○	ZyXEL000001_Guest1	Mixed WPA2-PSK/WPA-PSK	N/A	✎
2	●	VIP	Mixed WPA2-PSK/WPA-PSK	External Guest	✎
3	●	Guest	Mixed WPA2-PSK/WPA-PSK	External Guest	✎

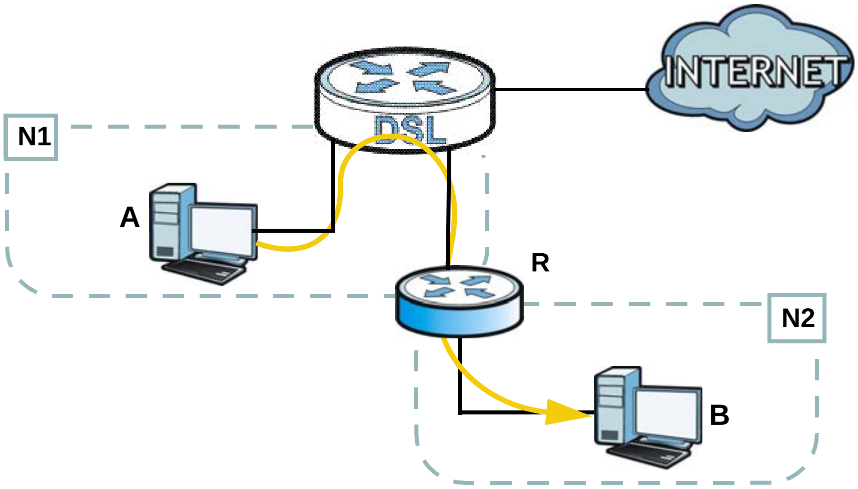
4.6 Configuring Static Route for Routing to Another Network

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

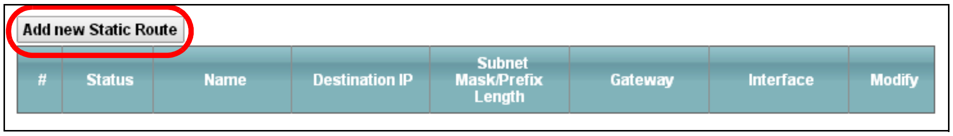
DEVICE / COMPUTER	IP ADDRESS
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

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.



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

4 Configure the **Static Route Setup** screen using the following settings:

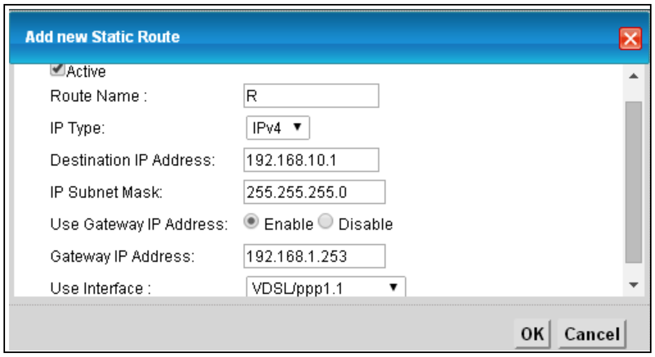
4a Select the **Active** check box. Enter the **Route Name** as **R**.

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**.



☑ Active

Route Name :	R
IP Type:	IPv4
Destination IP Address:	192.168.10.1
IP Subnet Mask:	255.255.255.0
Use Gateway IP Address:	● Enable ○ Disable
Gateway IP Address:	192.168.1.253
Use Interface :	VDSL/ppp1.1

4a Click **OK**.

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

4.7 Configuring QoS Queue and Class Setup

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

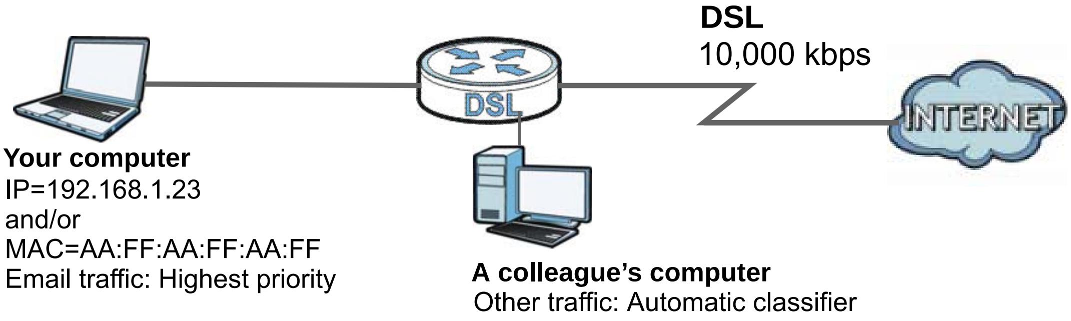
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues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

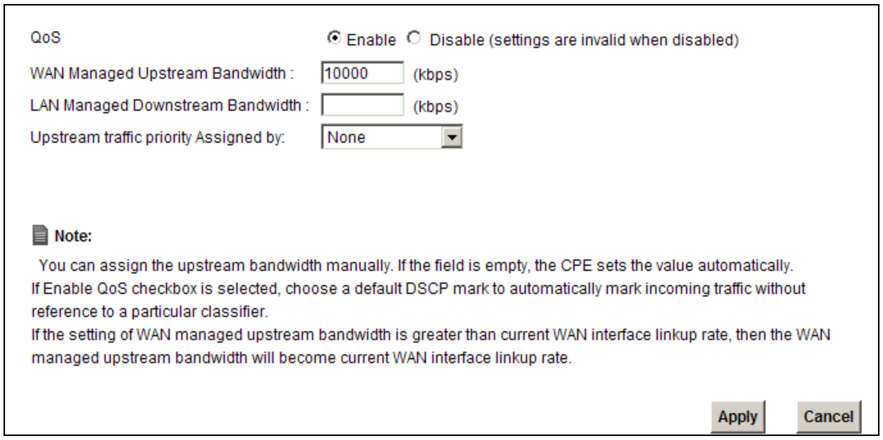
- Configure a queue to assign the highest priority queue (1) to e-mail traffic going to the WAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer 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 : 10000 (kbps)

LAN Managed Downstream Bandwidth : (kbps)

Upstream traffic priority Assigned by: None

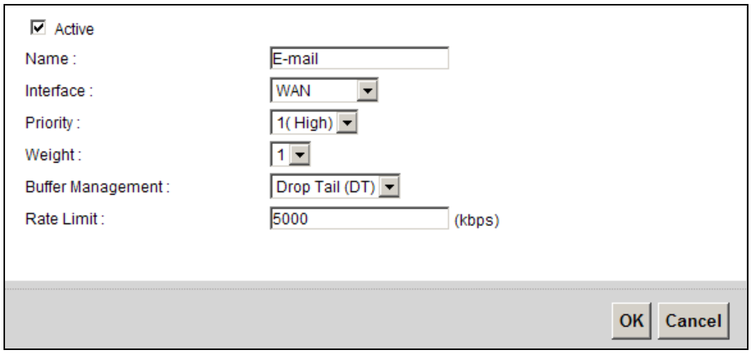
Note:

You can assign the upstream bandwidth manually. If the field is empty, the CPE sets the value automatically.
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

2 Click **Queue Setup** > **Add new Queue** to cr

3 eate a new queue. In the screen that opens, check **Active** and enter or select the following values:

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



☑ Active

Name : E-mail

Interface : WAN

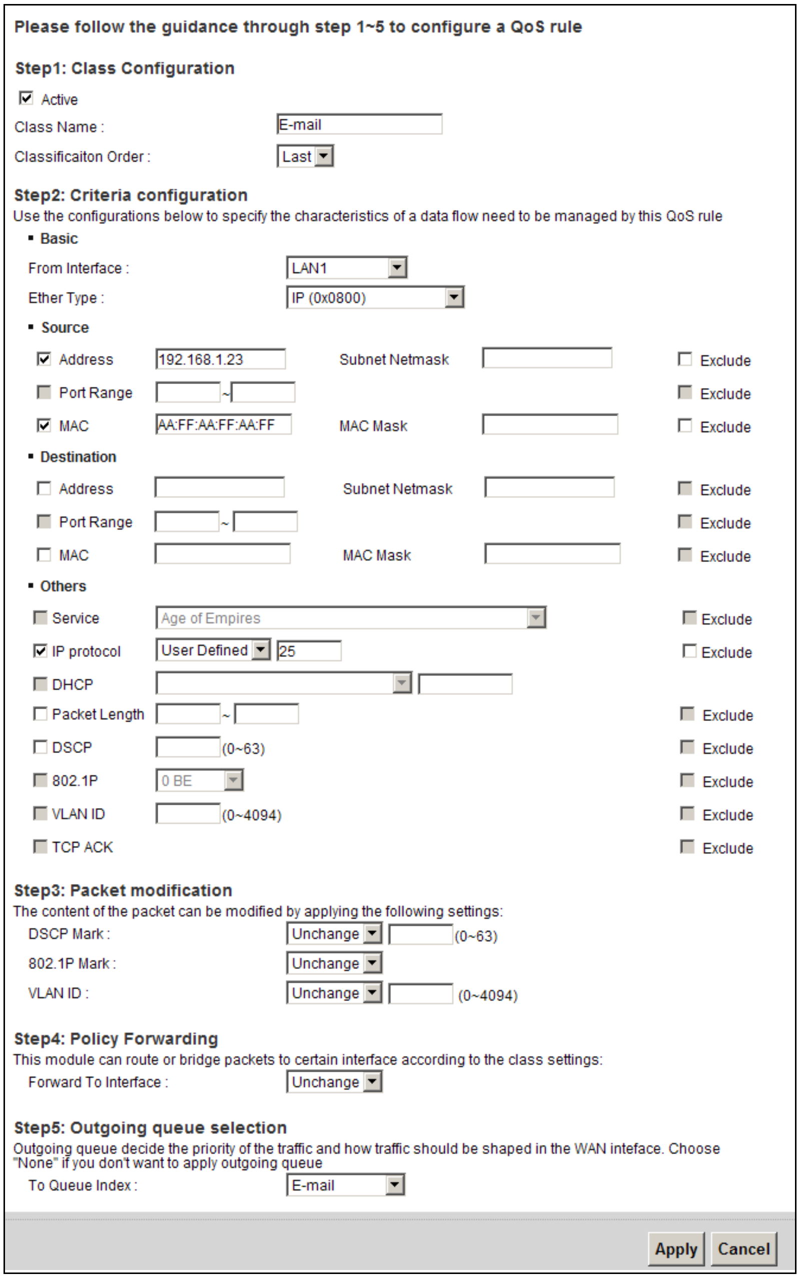
Priority : 1(High)

Weight : 1

Buffer Management : Drop Tail (DT)

Rate Limit : 5000 (kbps)

4 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 : E-mail

Classificaiton Order : Last

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 : LAN1

Ether Type : IP (0x0800)

- **Source**

☑ Address 192.168.1.23 Subnet Netmask □ Exclude

□ Port Range ~ □ Exclude

☑ MAC AA:FF:AA:FF:AA:FF MAC Mask □ Exclude

- **Destination**

□ Address Subnet Netmask □ Exclude

□ Port Range ~ □ Exclude

□ MAC MAC Mask □ Exclude

- **Others**

□ Service Age of Empires □ Exclude

☑ IP protocol User Defined 25 □ Exclude

□ DHCP

□ Packet Length ~ □ Exclude

□ DSCP (0~63) □ Exclude

□ 802.1P 0 BE □ 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 : Unchange (0~63)

802.1P Mark : Unchange

VLAN ID : Unchange (0~4094)

Step4: Policy Forwarding

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

Forward To Interface : Unchange

Step5: Outgoing queue selection

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

To Queue Index : E-mail

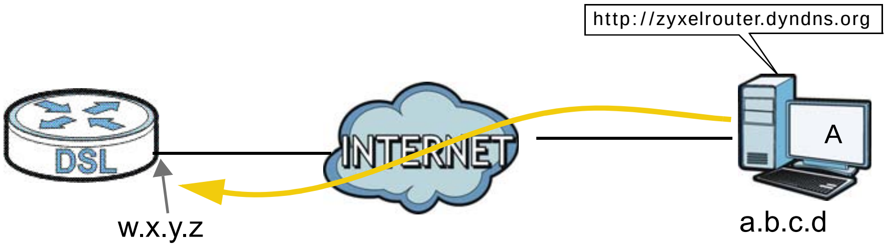
Class Name	Give a class name to this traffic, such as **E-mail** in this example.
From Interface	This is the interface from which the traffic will be coming from. Select **LAN1** for this example.
Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.
IP Address	Type 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).

5 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.

4.8 Access the VMG Using DDNS

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



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

This tutorial covers:

- Registering a DDNS Account on 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.

4.8.1 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.

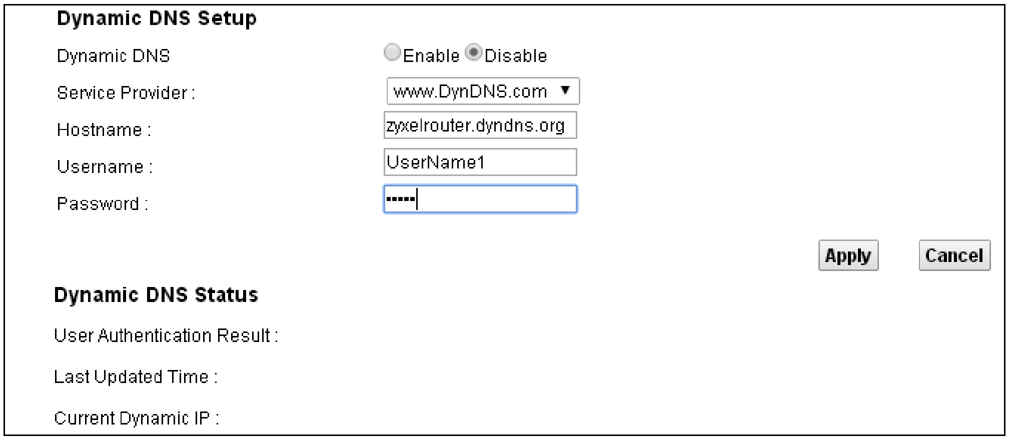
- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your VMG is currently using. You can find the IP address on the VMG's Web Configurator **Status** page.

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

4.8.2 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 : www.DynDNS.com ▼

Hostname : zyxelrouter.dyndns.org

Username : UserName1

Password : •••••

Dynamic DNS Status

User Authentication Result :

Last Updated Time :

Current Dynamic IP :

Click **Apply**.

4.8.3 Testing the DDNS Setting

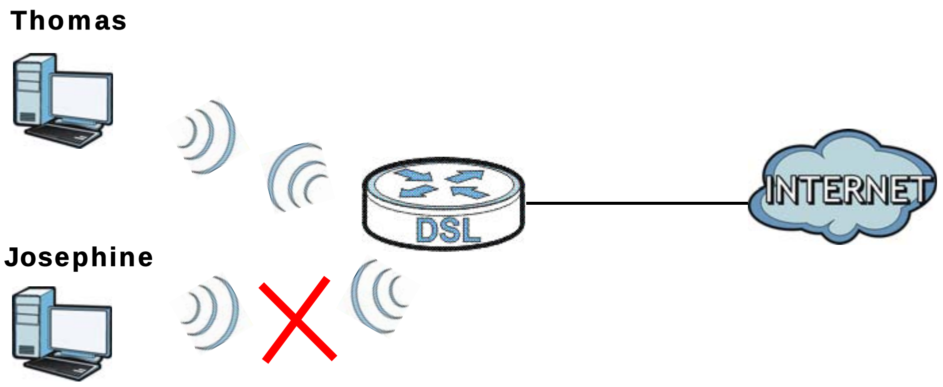
Now you should be able to access the VMG from the Internet. To test this:

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.

4.9 Configuring the MAC Address Filter

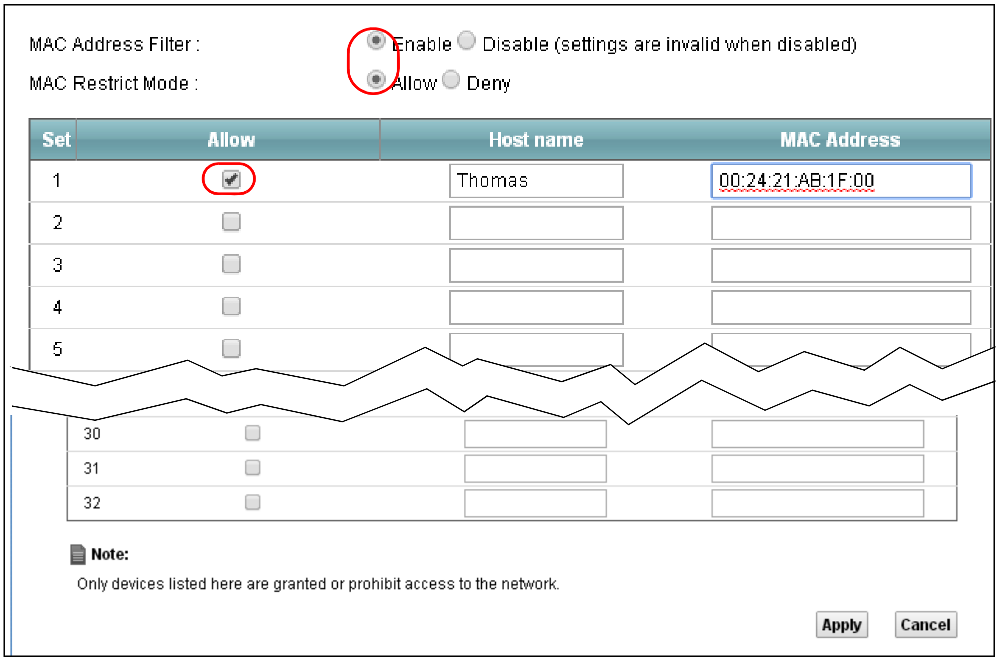
Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

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	☑	Thomas	00:24:21:AB:1F:00
2	□		
3	□		
4	□		
5	□		
30	□		
31	□		
32	□		

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

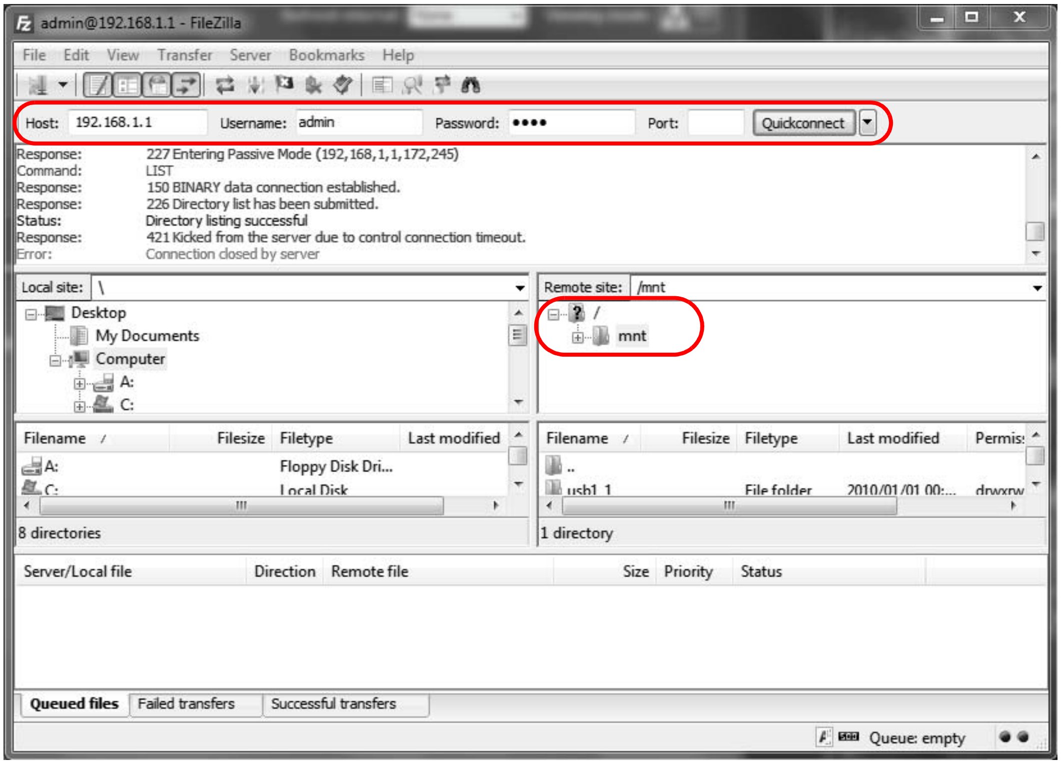
Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the VMG.

4.10 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.



admin@192.168.1.1 - FileZilla
File Edit View Transfer Server Bookmarks Help
Quickconnect
Queued files
Failed transfers
Successful transfers
Queue: empty

Host: 192.168.1.1 Username: admin Password: •••• Port:

```
Response:    227 Entering Passive Mode (192,168,1,1,172,245)
Command:     LIST
Response:    150 BINARY data connection established.
Response:    226 Directory list has been submitted.
Status:      Directory listing successful
Response:    421 Kicked from the server due to control connection timeout.
Error:       Connection closed by server
```

Local site: \

- Desktop
  - My Documents
  - Computer
    - A:
    - C:

Remote site: /mnt

- /
  - mnt

Filename /	Filesize	Filetype	Last modified
A:		Floppy Disk Dri...	
C:		Local Disk	

8 directories

Filename /	Filesize	Filetype	Last modified	Permis:
..				
usb1_1		File folder	2010/01/01 00:...	drwxrw

1 directory

Server/Local file	Direction	Remote file	Size	Priority	Status

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

4.11 Using the Media Server Feature

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

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

- Microsoft (MS) Windows Media Player

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

- ZyXEL DMA-2500, a digital media adapter

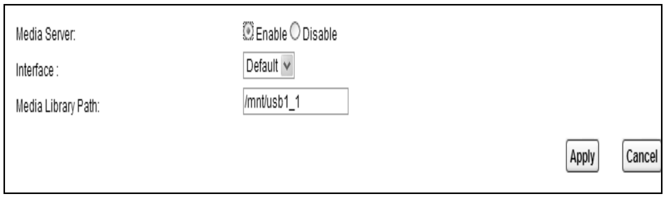
  You need to set up the DMA-2500 to work with your television (TV). Refer to the DMA-2500 Quick Start Guide for the correct hardware connections.

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

4.11.1 Configuring the VMG

Note: The Media Server feature is enabled by default.

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

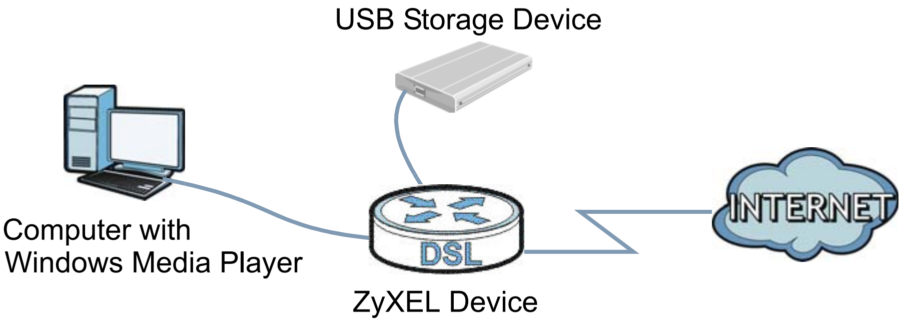


Media Server:	● Enable ○ Disable
Interface :	Default
Media Library Path:	/mnt/usb1_1

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

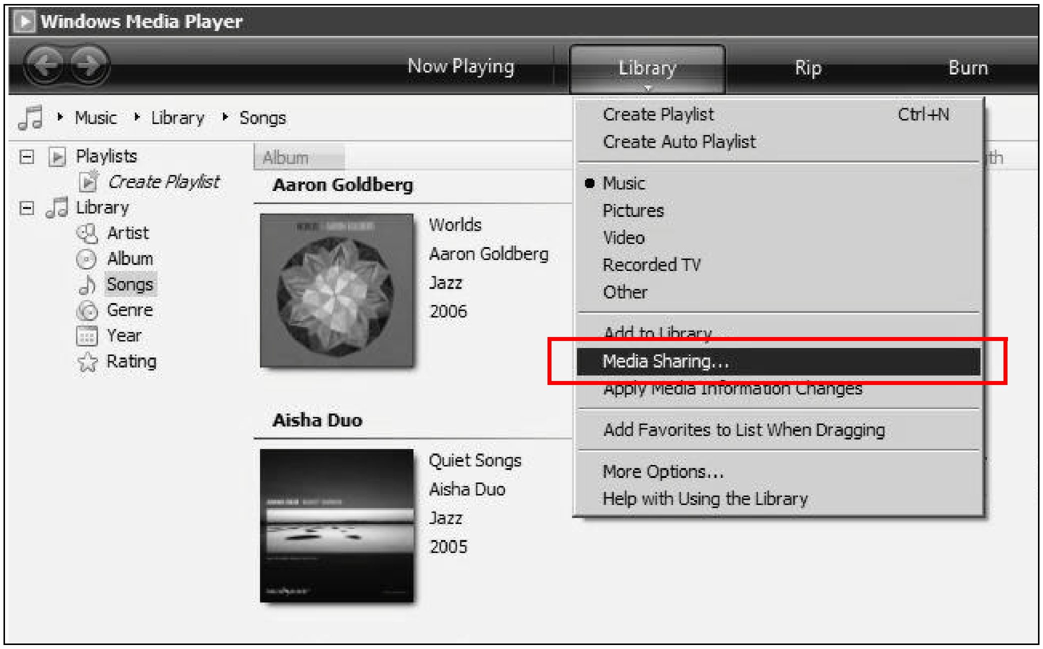
4.11.2 Using Windows Media Player

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

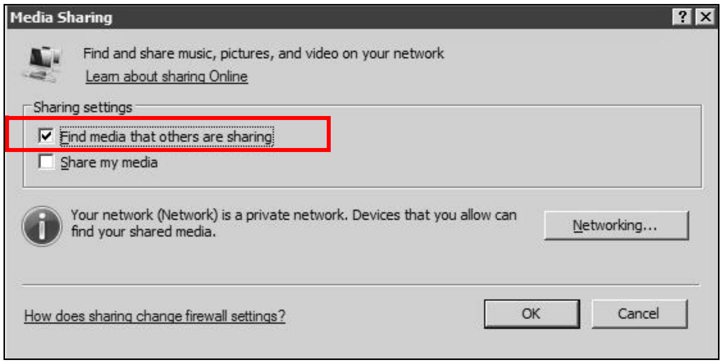


Windows Vista

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



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


Media Sharing

Find and share music, pictures, and video on your network

Learn about sharing Online

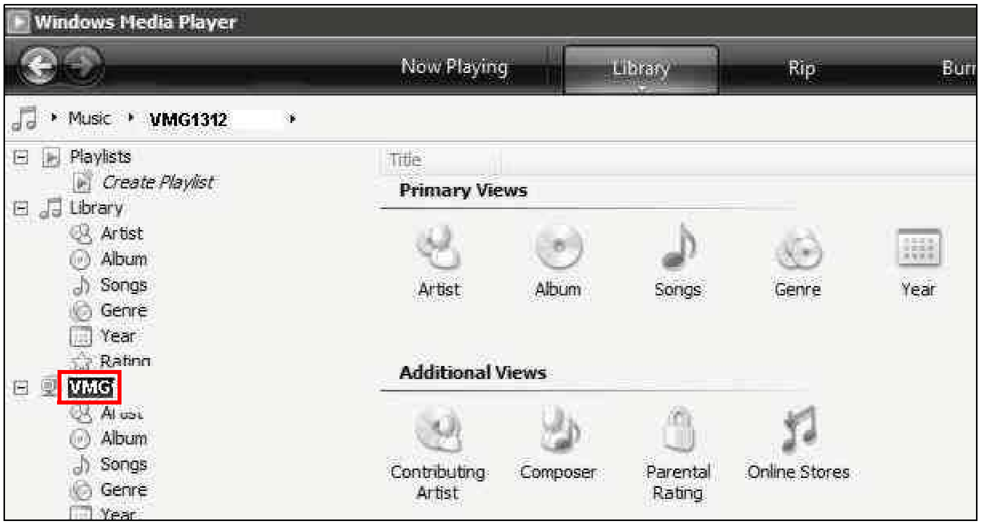
Sharing settings

☑ Find media that others are sharing

□ Share my media

Your network (Network) is a private network. Devices that you allow can find your shared media.

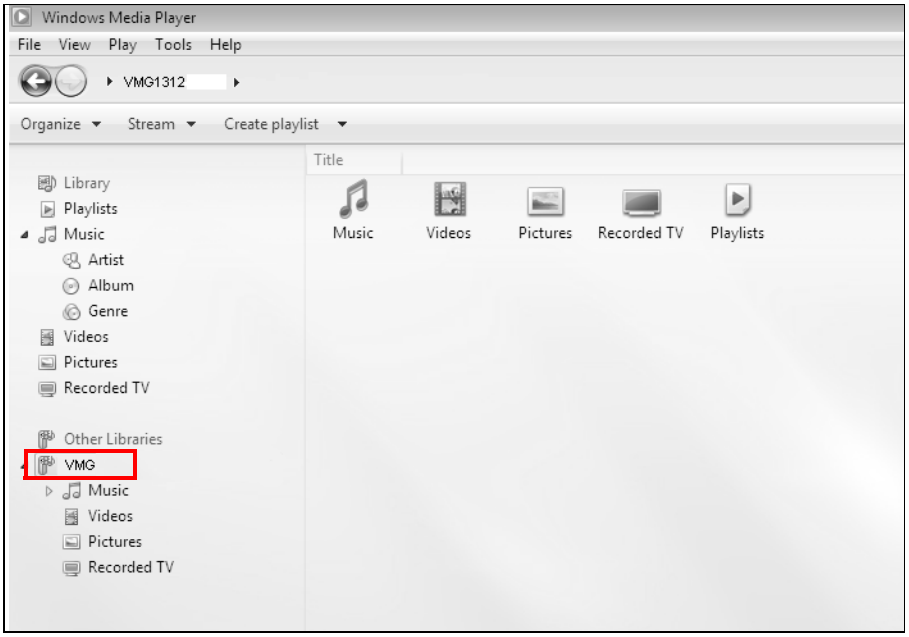
3 In the **Library** screen, check the left panel. The Windows Media Player should detect the VMG.



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

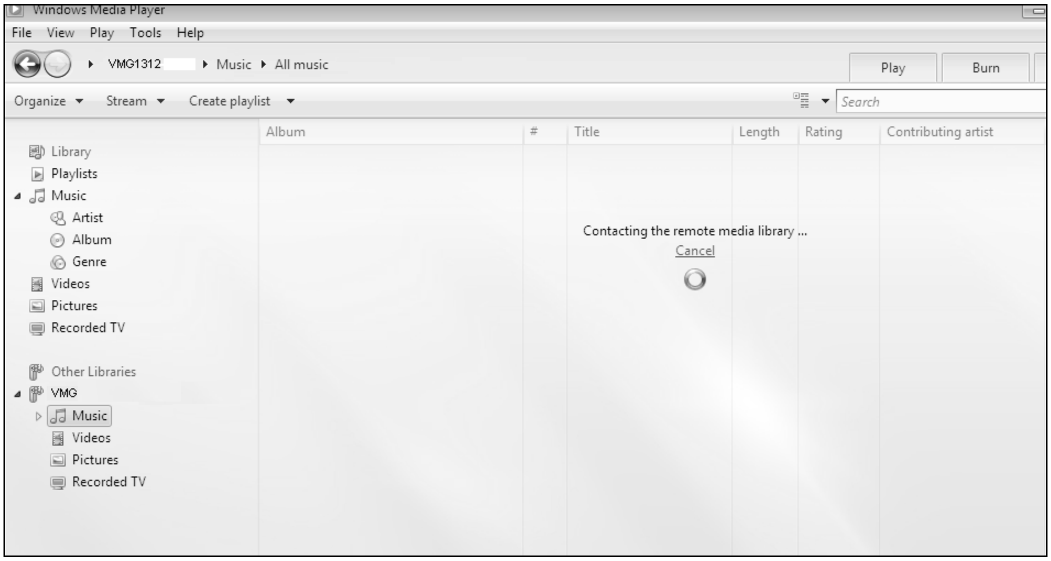
Windows 7

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



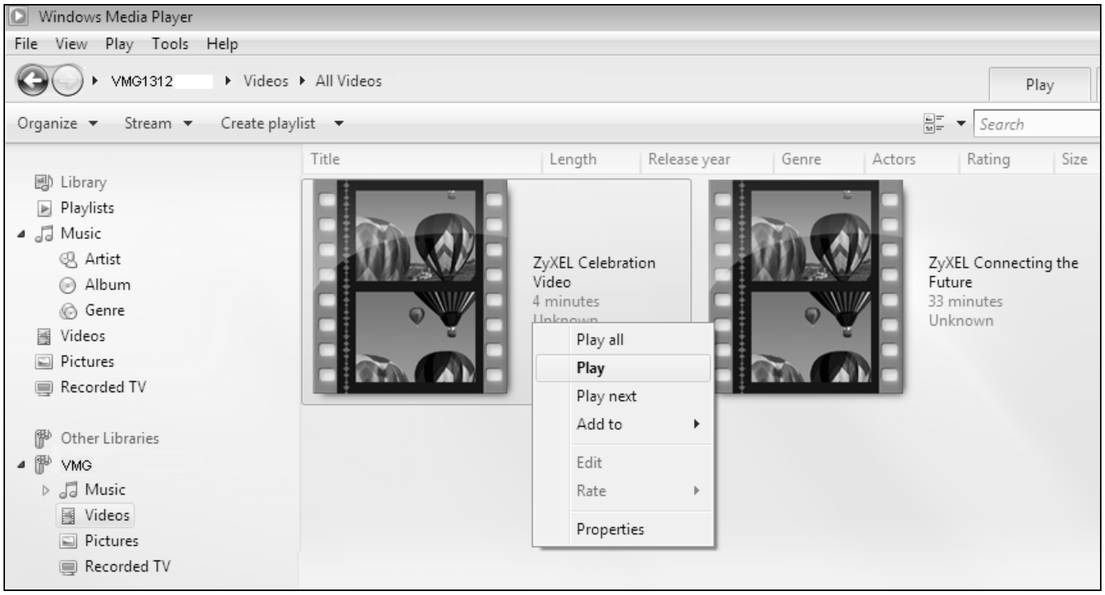
If you cannot see the VMG in the left panel as shown above, right-click **Other Libraries > Refresh Other Libraries**.

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



Contacting the remote media library ...

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

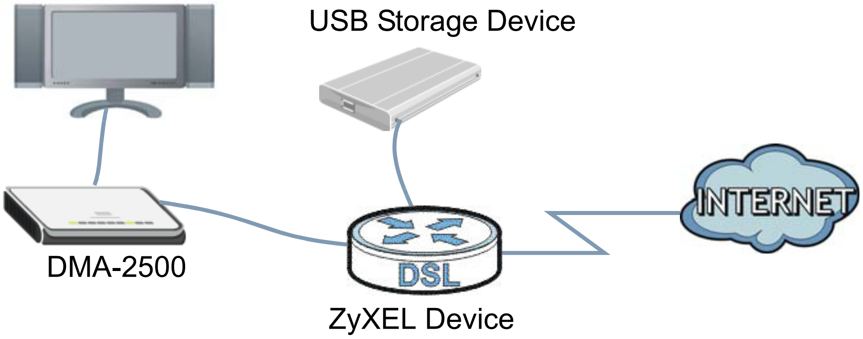


4.11.3 Using a Digital Media Adapter

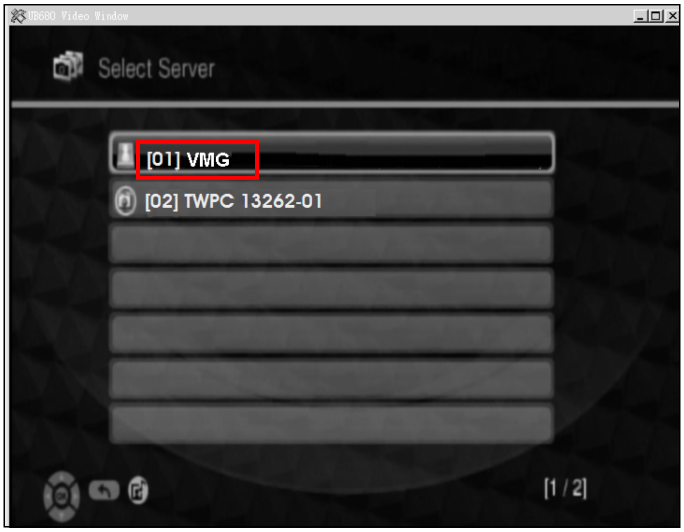
This section shows you how you can use the VMG with a ZyXEL DMA-2500 to play media files stored in the USB storage device in your TV screen.

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

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

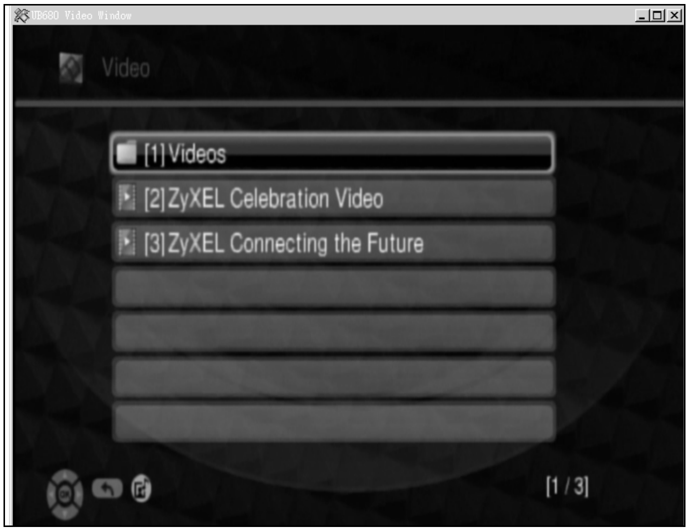


2 Turn on the TV and wait for the DMA-2500 **Home** screen to appear. Using the remote control, go to **MyMedia** to open the following screen. Select the VMG as your media server.



[01] VMG
[02] TWPC 13262-01

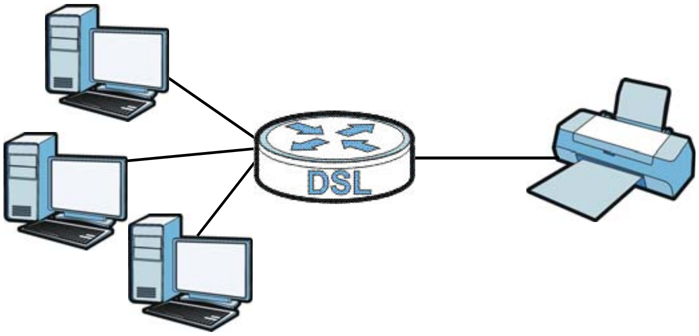
3 The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button in the remote control.



[1] Videos
[2] ZyXEL Celebration Video
[3] ZyXEL Connecting the Future

4.12 Using the Print Server Feature

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



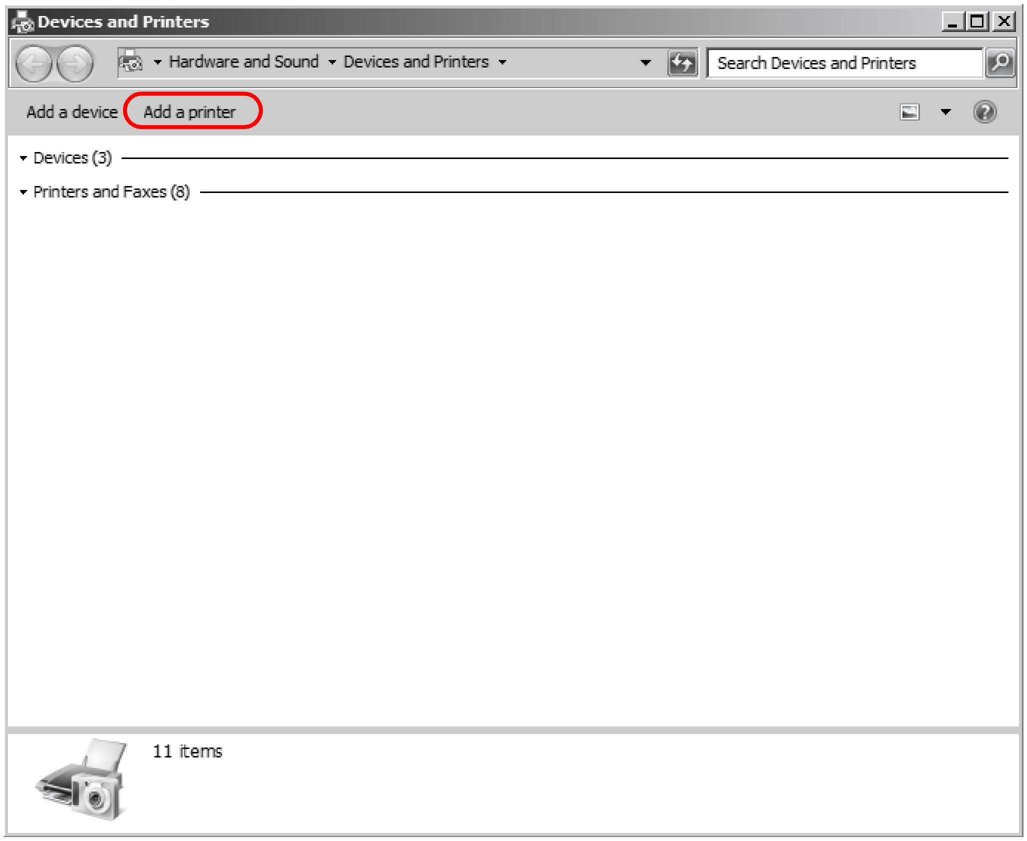
In this section you can:

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

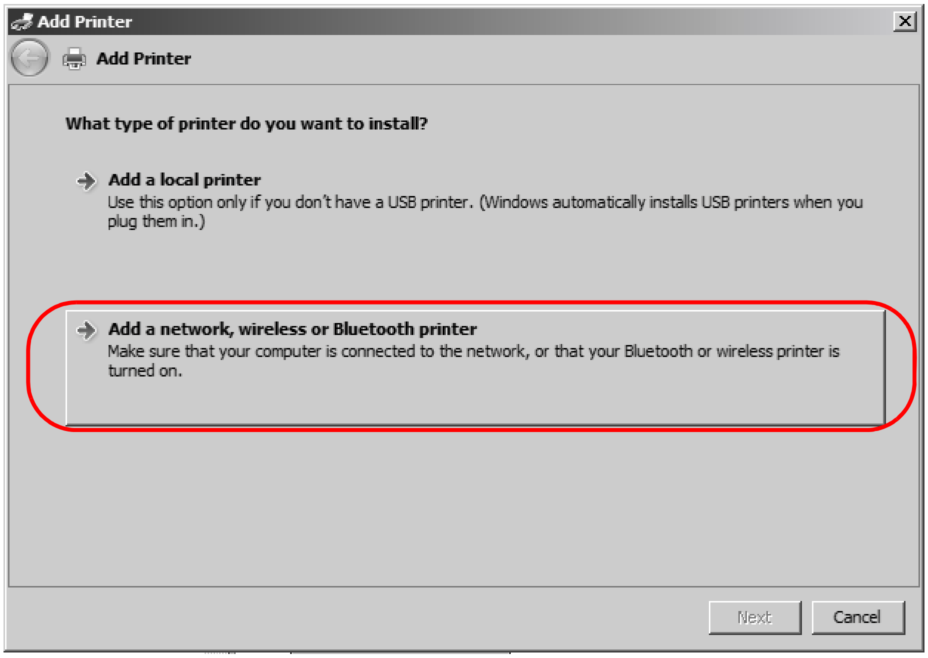
Add a New Printer Using Windows

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

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



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

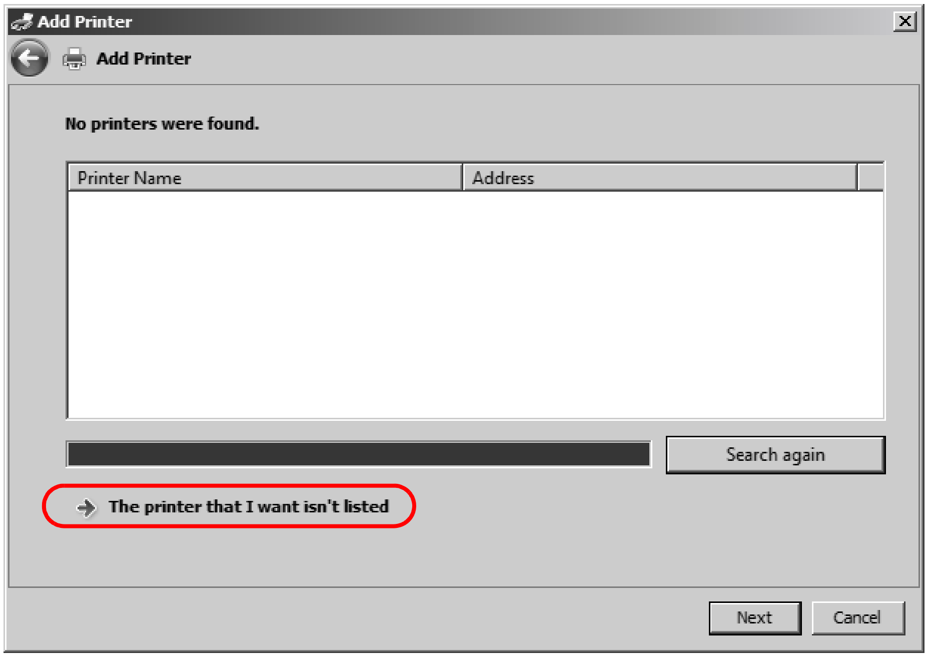


What type of printer do you want to install?

Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

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



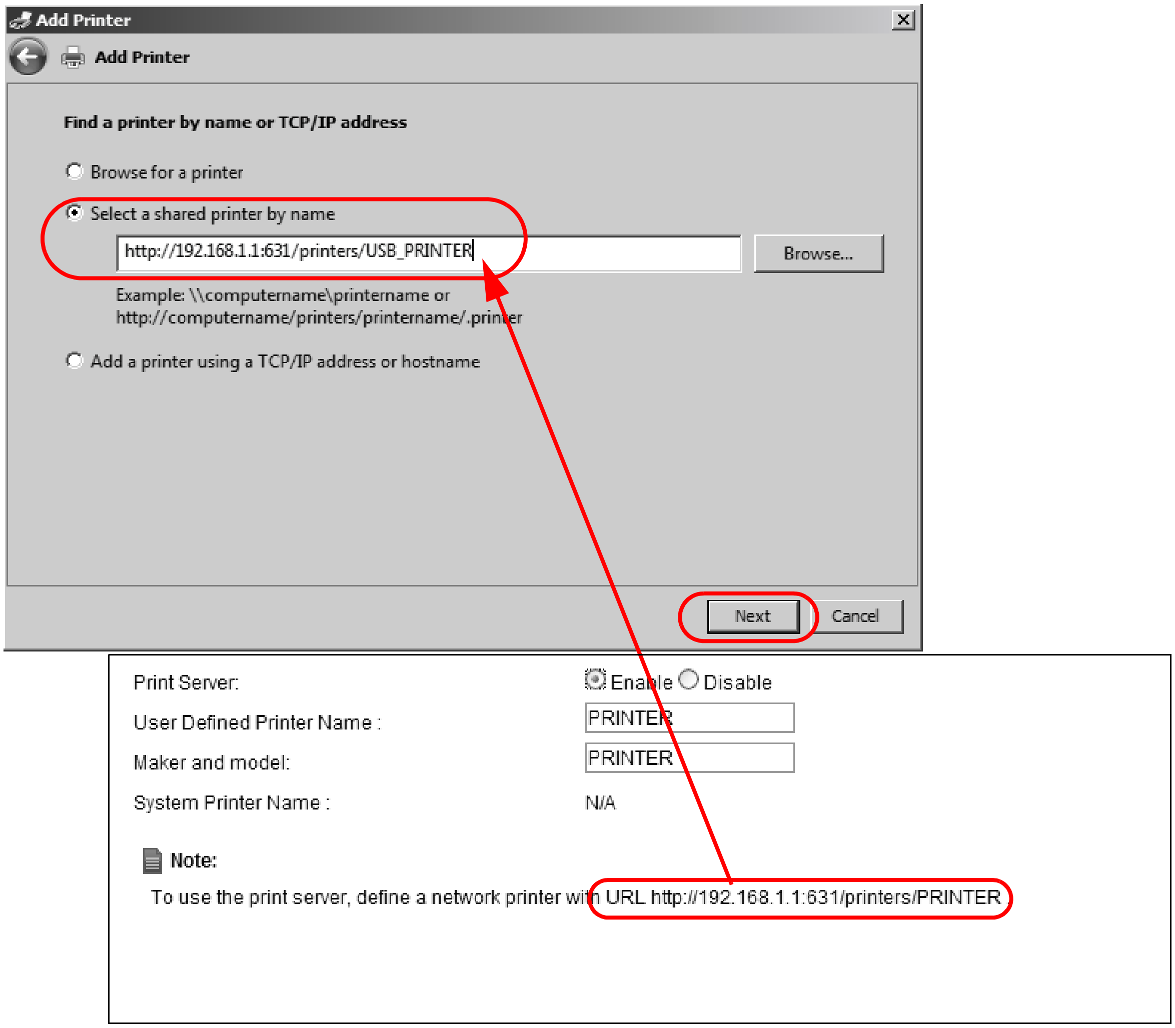
Add Printer

Add Printer

No printers were found.

Printer Name	Address

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



Find a printer by name or TCP/IP address

○ Browse for a printer

● Select a shared printer by name

http://192.168.1.1:631/printers/USB_PRINTER

Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

Print Server:	● Enable ○ Disable
User Defined Printer Name :	PRINTER
Maker and model:	PRINTER
System Printer Name :	N/A

Note:

To use the print server, define a network printer with URL http://192.168.1.1:631/printers/PRINTER

5 Install the printer driver. Please check the Windows CD if it includes the printer driver. If not, please install the driver from the CD included with your printer or by downloading it from the printer vendor's website.

6 After the printer driver installs successfully, choose if you want to set this printer to be the default.

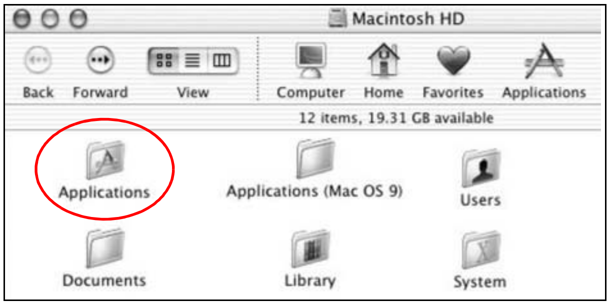
Add a New Printer Using Macintosh OS X

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

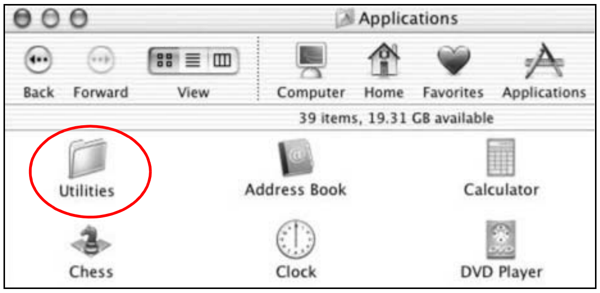
1 Click the **Print Center** icon located in the Macintosh Dock (a place holding a series of icons/ shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.

2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.

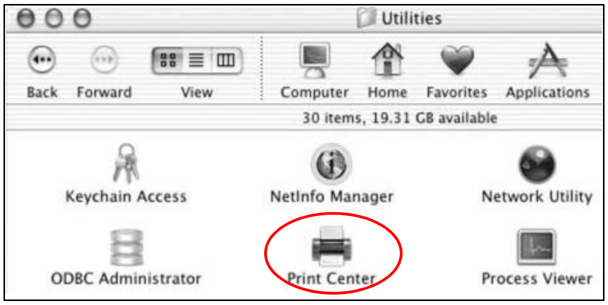
3 Double-click the **Applications** folder.



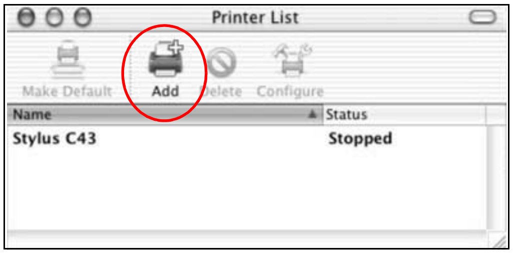
4 Double-click the **Utilities** folder.



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



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



Name	Status
Stylus C43	Stopped

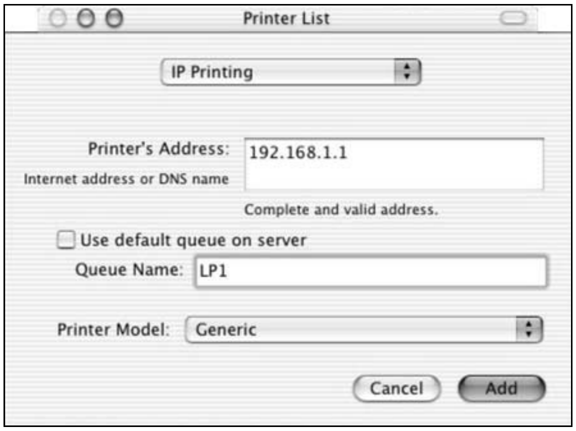
7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.

8 In the **Printer's Address** field, type the IP address of your VMG.

9 Deselect the **Use default queue on server** check box.

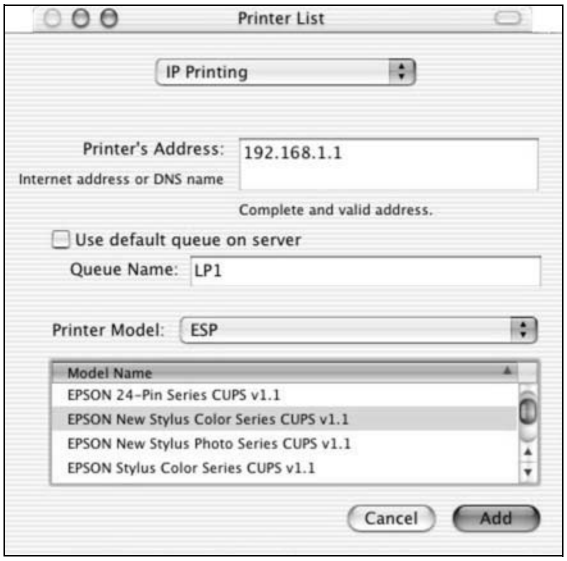
10 Type **LP1** in the **Queue Name** field.

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



Printer's Address: 192.168.1.1
Internet address or DNS name
Complete and valid address.
□ Use default queue on server
Queue Name: LP1
Printer Model: Generic

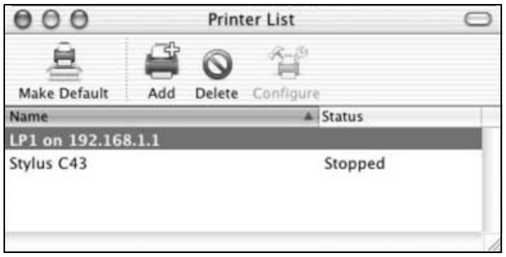
12 Click **Add** to select a printer model, save and close the **Printer List** configuration screen.



Printer's Address: 192.168.1.1
Internet address or DNS name
Complete and valid address.
□ Use default queue on server
Queue Name: LP1
Printer Model: ESP

Model Name
EPSON 24-Pin Series CUPS v1.1
EPSON New Stylus Color Series CUPS v1.1
EPSON New Stylus Photo Series CUPS v1.1
EPSON Stylus Color Series CUPS v1.1

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



Name	Status
LP1 on 192.168.1.1	
Stylus C43	Stopped

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

PART II

Technical Reference

Network Map and Status Screens

5.1 Overview

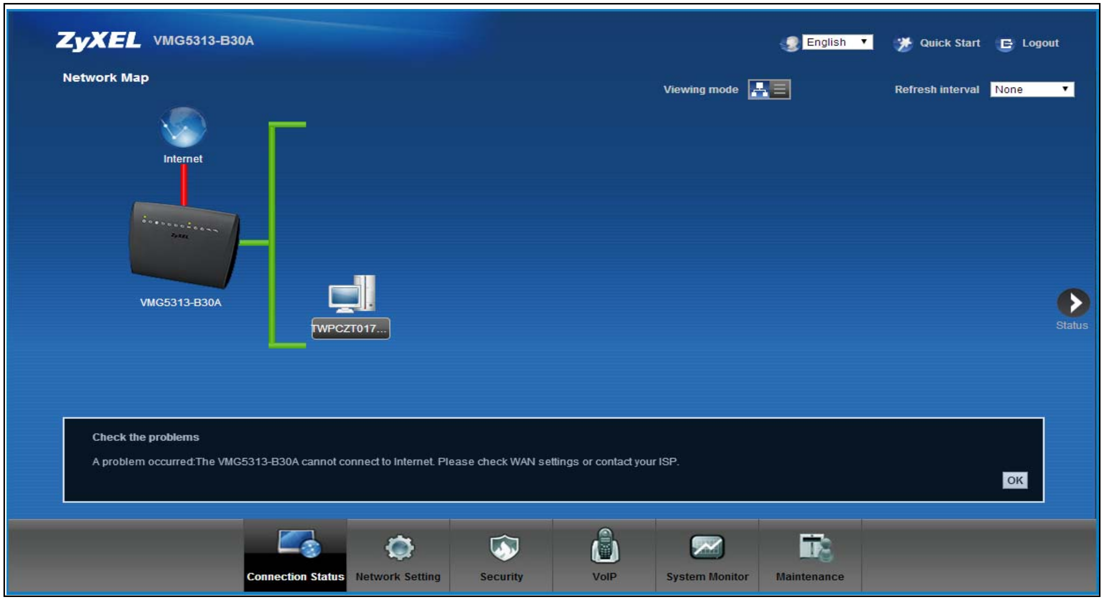
After you log into the Web Configurator, the **Network Map** screen appears. This shows the network connection status of the Device and clients connected to it.

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

5.2 The Network Map Screen

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

Figure 12 Network Map: Icon View Mode

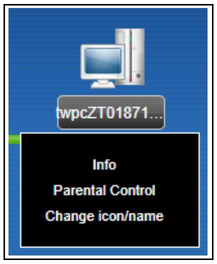


Check the problems

A problem occurred:The VMG5313-B30A cannot connect to Internet. Please check WAN settings or contact your ISP.

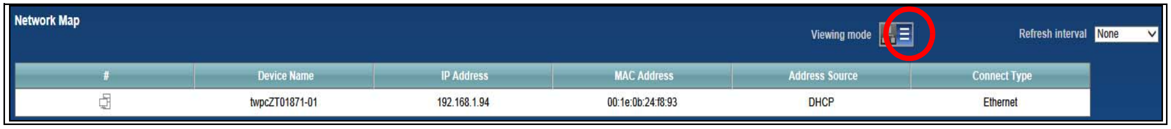
OK

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



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

Figure 13 Network Map: List View Mode

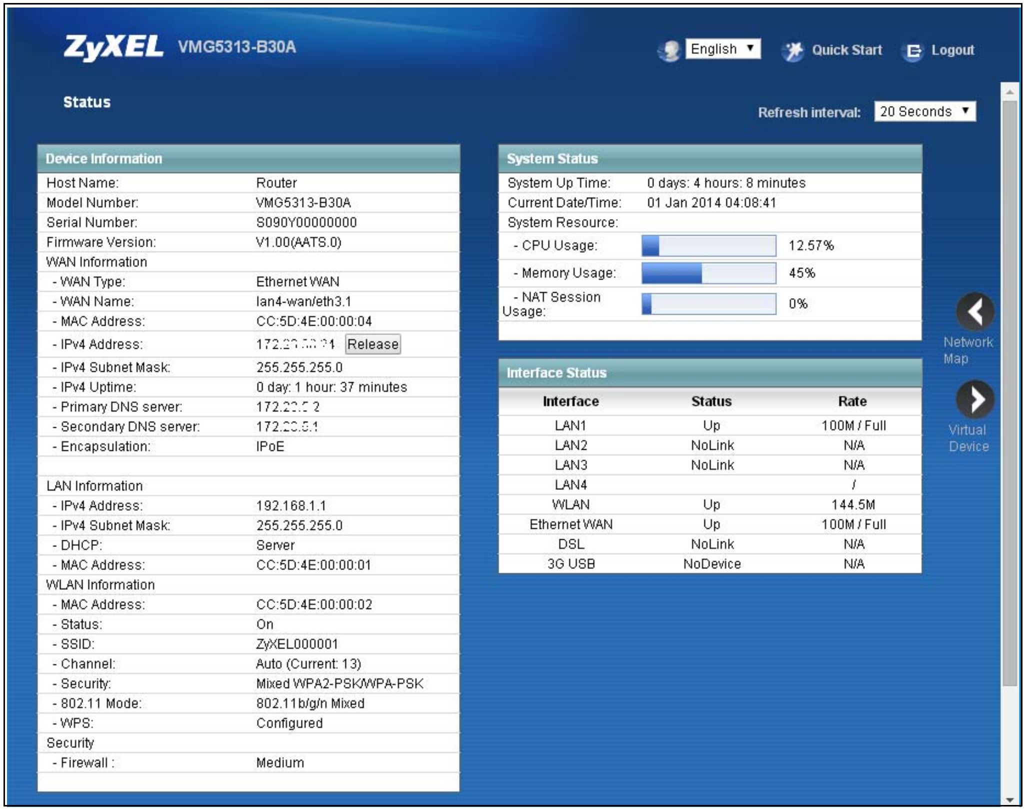


#	Device Name	IP Address	MAC Address	Address Source	Connect Type
	twpcZT01871-01	192.168.1.94	00:1e:0b:24:f8:93	DHCP	Ethernet

5.3 The Status Screen

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

Figure 14 Status Screen



Refresh interval: 20 Seconds

Device Information

Host Name:	Router
Model Number:	VMG5313-B30A
Serial Number:	S090Y00000000
Firmware Version:	V1.00(AATS.0)
WAN Information	
- WAN Type:	Ethernet WAN
- WAN Name:	lan4-wan/eth3.1
- MAC Address:	CC:5D:4E:00:00:04
- IPv4 Address:	172.2[illegible]1 Release
- IPv4 Subnet Mask:	255.255.255.0
- IPv4 Uptime:	0 day: 1 hour: 37 minutes
- Primary DNS server:	172.2[illegible]2
- Secondary DNS server:	172.2[illegible].1
- Encapsulation:	IPoE
LAN Information	
- IPv4 Address:	192.168.1.1
- IPv4 Subnet Mask:	255.255.255.0
- DHCP:	Server
- MAC Address:	CC:5D:4E:00:00:01
WLAN Information	
- MAC Address:	CC:5D:4E:00:00:02
- Status:	On
- SSID:	ZyXEL000001
- Channel:	Auto (Current: 13)
- Security:	Mixed WPA2-PSK/WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Configured
Security	
- Firewall :	Medium

System Status

System Up Time:	0 days: 4 hours: 8 minutes
Current Date/Time:	01 Jan 2014 04:08:41
System Resource:	
- CPU Usage:	12.57%
- Memory Usage:	45%
- NAT Session Usage:	0%

Interface Status

Interface	Status	Rate
LAN1	Up	100M / Full
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4		/
WLAN	Up	144.5M
Ethernet WAN	Up	100M / Full
DSL	NoLink	N/A
3G USB	NoDevice	N/A

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 unique 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.)	
WAN Type	This shows wherther it's a DSL, Ethernet or 3G WAN connection..
WAN Name	This is the namke of the interface.
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) Address of your VMG.
IP v4 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**.
IPv4 Subnet Mask	This field displays the current subnet mask in the WAN.
IPv4 Uptime	This shows how long the VMG has had the IP address.
Primary DNS server	This shows the primary DNS server IP address.
Secondary DNS server	This shows the secondary DNS server IP address.
Encapsulation	This field displays the current encapsulation method.
LAN Information	
IPv4 Address	This is the current IP address of the VMG in the LAN.
IPv4 Subnet Mask	This is the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the VMG is providing to the LAN. Choices are: **Server** - The VMG is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The VMG acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The VMG is not providing any DHCP services to the LAN.
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your VMG.
WLAN Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of your VMG.
Status	This displays whether 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 VMG now.
Security	This displays the type of security mode the VMG is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the VMG is using in the wireless LAN.
WPS	This displays whether WPS is activated.
Security	
Firewall	This displays the firewall's current security level.
System Status	

Table 5 Status Screen (continued)

LABEL	DESCRIPTION
System Up Time	This field displays how long the VMG has been running since it last started up. The VMG starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it.
Current Date/ Time	This field displays the current date and time in the VMG. You can change this in **Maintenance> Time Setting**.
System Resource	
CPU Usage	This field displays what percentage of the VMG's processing ability is currently used. When this percentage is close to 100%, the VMG is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 10 on page 163).
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 38.2 on page 337, 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.
Interface Status	
Interface	This column displays each interface the VMG has.
Status	This field indicates the interface's use status. For the DSL interface, this field displays **Down** (line down), **Up** (line up or connected) and **Drop** (dropping a call) if you're using PPPoE encapsulation. For the Ethernet WAN and LAN interface, this field displays **Up** when using the interface and **NoLink** when not using the interface. For the WLAN interface, this field displays the enabled (**Active**) or disabled (**InActive**) state of the interface. For the 3G USB interface, this field displays **Up** when using the interface and **NoDevice** when no device is detected in any USB slot.
Rate	For the Ethernet WAN and LAN interface, this displays the port speed and duplex setting. For the DSL interface, it displays the downstream and upstream transmission rate. For the WLAN interface, it displays the maximum transmission rate or **N/A** with WLAN disabled. For the 3G USB interface, this field displays **Up** when a 3G USB device is installed in a USB slot and **NoDevice** when no device is detected in any USB slot.
Registration Status	
Account	This column displays each SIP account in the VMG.
Action	If the SIP account is already registered with the SIP server, the **Account Status** field displays **Registered**. Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. If the SIP account is not registered with the SIP server, the **Account Status** field displays **Not Registered**. Click **Register** to have the VMG attempt to register the SIP account with the SIP server. The button is grayed out if the SIP account is disabled.

Table 5 Status Screen (continued)

LABEL	DESCRIPTION
Account Status	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Account**. **Not Registered** - The last time the VMG tried to register the SIP account with the SIP server, the attempt failed. Use the **Register** button to register the account again. The VMG automatically tries to register the SIP account when you turn on the VMG or when you activate it. **Registered** - The SIP account is already registered with the SIP server. You can use it to make a VoIP call.
Service-Provider	This column displays the service provider name and SIP number for each SIP account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP > SIP** screens.

6

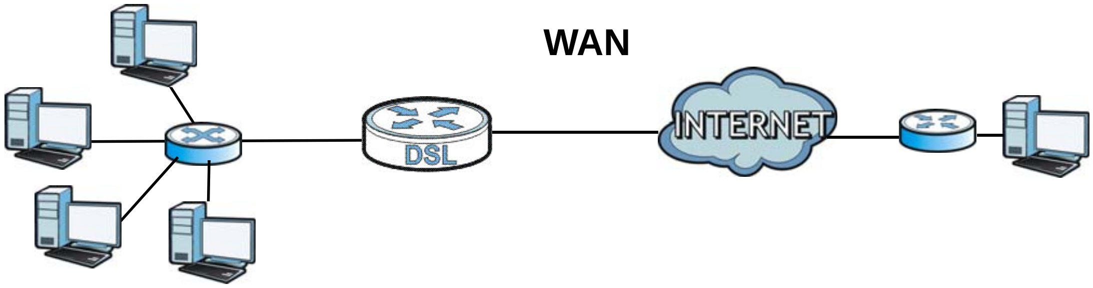
Broadband

6.1 Overview

This chapter discusses the VMG's **Broadband** screens. Use these screens to configure your VMG for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 15 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 83).
- Use the **Advanced** screen to enable or disable PTM over ADSL, Annex M/Annex J, and DSL PhyR functions (Section 6.4 on page 95).
- Use the **Ethernet WAN** screen to convert LAN port number four as a WAN port or restore the WAN to a LAN port. This is for Ethernet connection.

Table 6 WAN Setup Overview

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

Table 6 WAN Setup Overview

LAYER-2 INTERFACE		INTERNET CONNECTION		
CONNECTION	**DSL LINK TYPE**	**MODE**	**ENCAPSULATION**	**CONNECTION SETTINGS**
ADSL over ATM	EoA	Routing	PPPoE/PPP0A	ATM PVC configuration, PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
			IPoE/IPoA	ATM PVC configuration, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	ATM PVC configuration, and QoS
Ethernet	N/A	Routing	IPoE/PPPoE	PPP information, IPv4/IPv6 IP address, routing feature, DNS server, VLAN, QoS, and MTU
		Bridge	N/A	VLAN and QoS

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 x 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

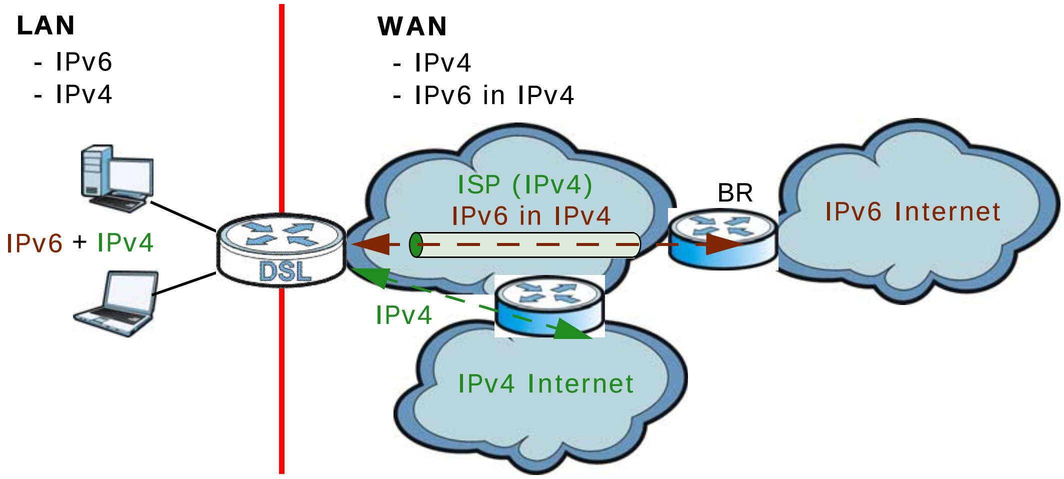
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block’s 16 bits are then represented by four hexadecimal characters. For example, 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 **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP’s IPv4 network.

The 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 it’s configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 16 IPv6 Rapid Deployment

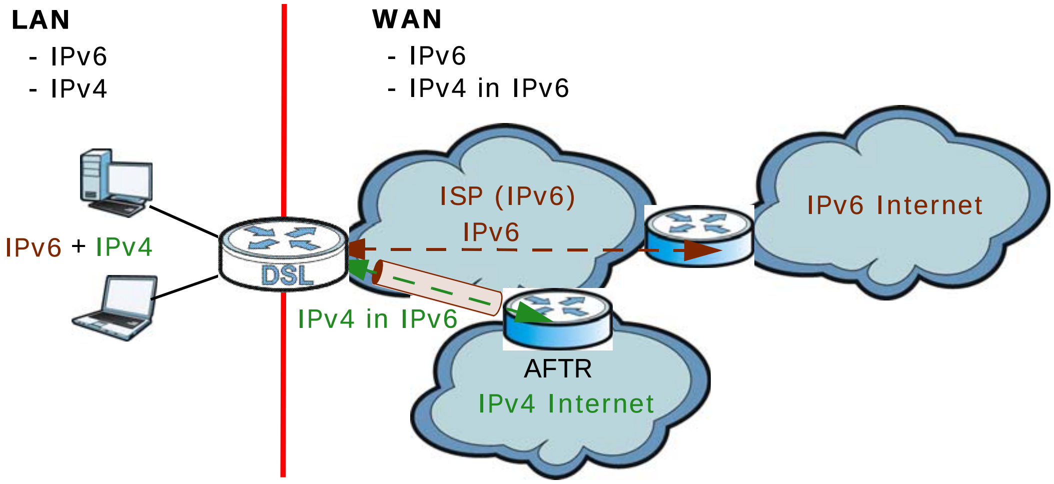


Dual Stack Lite

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 **IPv6 / IPv4 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 it's configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 17 Dual Stack Lite



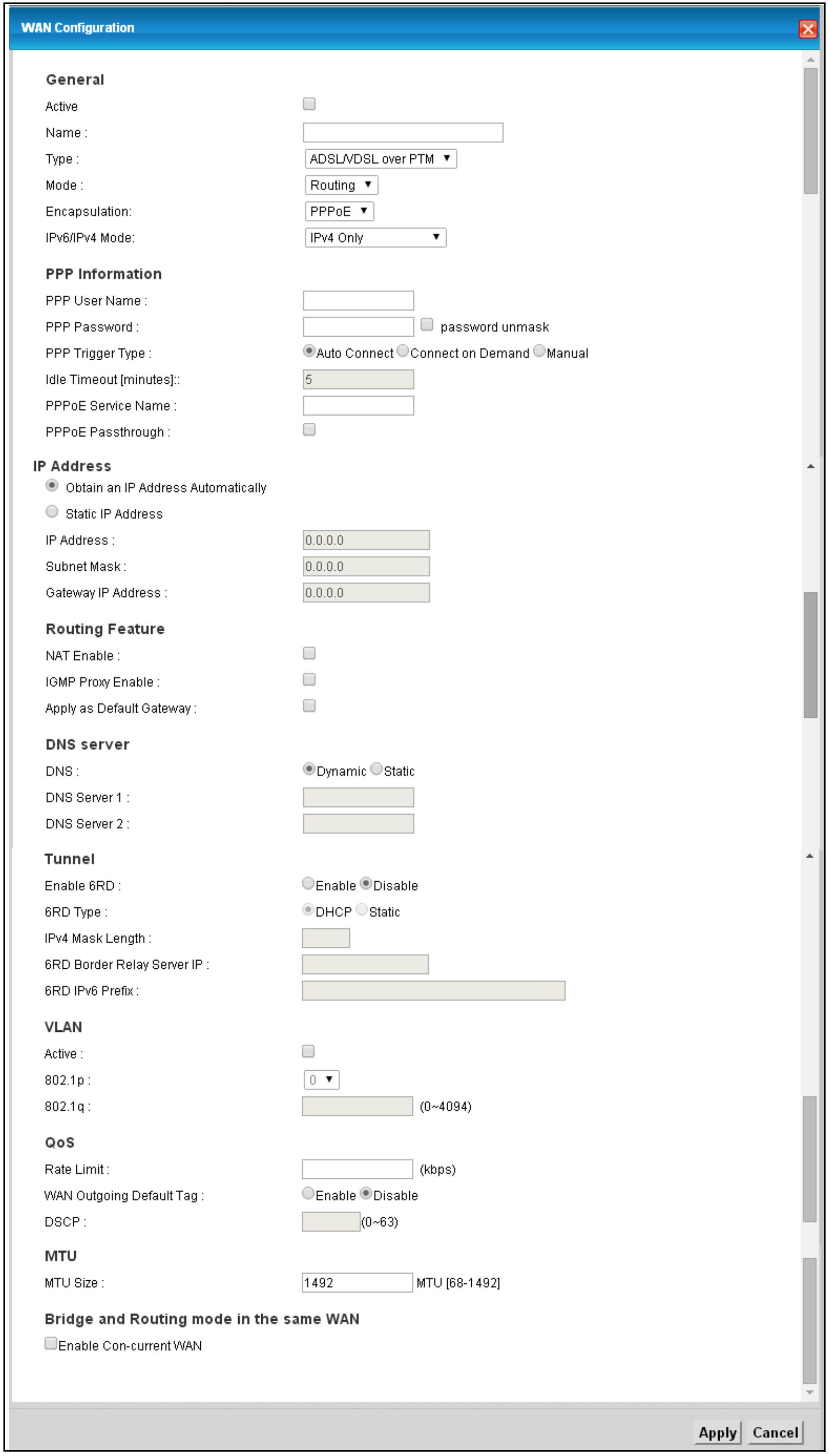
6.1.3 Before You Begin

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 18 Network Setting > Broadband



WAN Configuration

General

Active □

Name :

Type : ADSL/VDSL over PTM ▼

Mode : Routing ▼

Encapsulation: PPPoE ▼

IPv6/IPv4 Mode: IPv4 Only ▼

PPP Information

PPP User Name :

PPP Password : □ password unmask

PPP Trigger Type : ● Auto Connect ○ Connect on Demand ○ Manual

Idle Timeout [minutes]:: 5

PPPoE Service Name :

PPPoE Passthrough : □

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway IP Address : 0.0.0.0

Routing Feature

NAT Enable : □

IGMP Proxy Enable : □

Apply as Default Gateway : □

DNS server

DNS : ● Dynamic ○ Static

DNS Server 1 :

DNS Server 2 :

Tunnel

Enable 6RD : ○ Enable ● Disable

6RD Type : ● DHCP ○ Static

IPv4 Mask Length :

6RD Border Relay Server IP :

6RD IPv6 Prefix :

VLAN

Active : □

802.1p : 0 ▼

802.1q : (0~4094)

QoS

Rate Limit : (kbps)

WAN Outgoing Default Tag : ○ Enable ● Disable

DSCP : (0~63)

MTU

MTU Size : 1492 MTU [68-1492]

Bridge and Routing mode in the same WAN

□ Enable Con-current WAN

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, Ethernet or a PTM connection.
Mode	This shows whether the connection is in routing or bridge mode.
Encapsulation	This is the method of encapsulation used by this connection.
802.1p	This indicates the 802.1p priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
802.1q	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IGMP Proxy	This shows whether the VMG act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the VMG use the WAN interface of this connection as the system default gateway.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
MLD Proxy	This shows whether Multicast Listener Discovery (MLD) is activated or not for this connection. MLD is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Delete** icon to remove the WAN connection.

6.2.1 Add/Edit Internet Connection

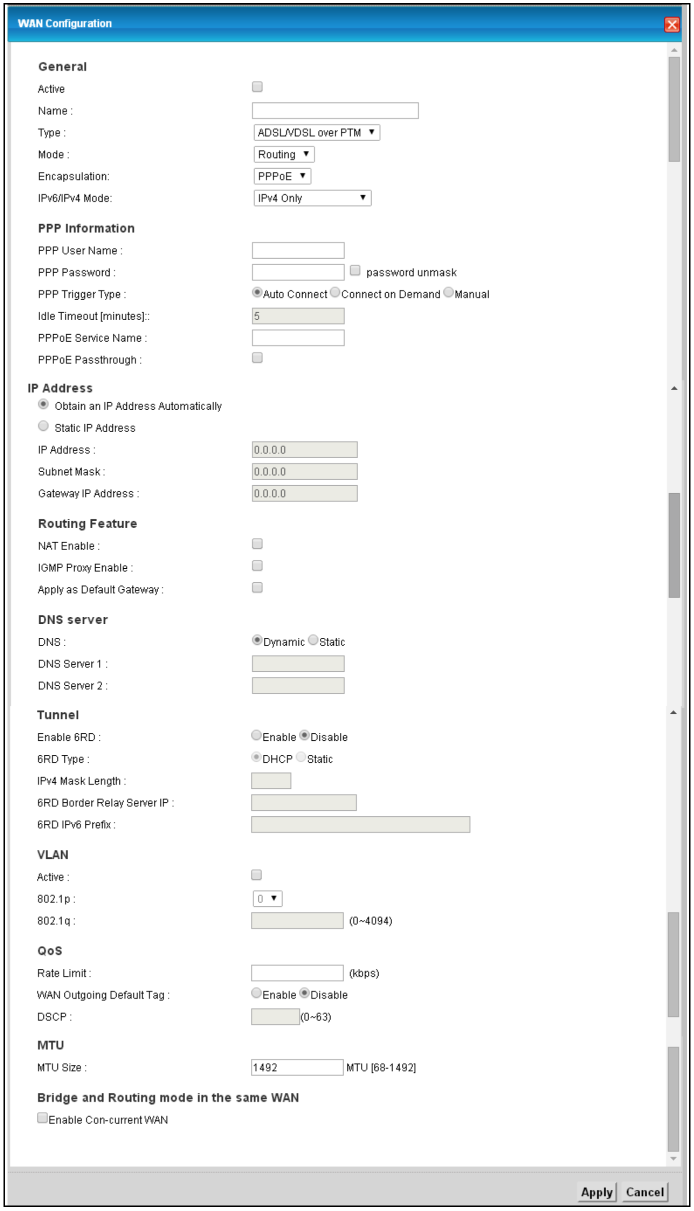
Click **Add New WAN Interface** in the **Broadband** screen or the **Edit** icon next to an existing WAN interface to configure a WAN connection. The screen varies depending on the interface type, mode, encapsulation, and IPv6/IPv4 mode you select.

6.2.1.1 Routing Mode

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

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

Figure 19 Network Setting > Broadband > Add New WAN Interface/Edit (Routing Mode)



WAN Configuration

General

Active □

Name :

Type : ADSL/VDSL over PTM ▼

Mode : Routing ▼

Encapsulation: PPPoE ▼

IPv6/IPv4 Mode: IPv4 Only ▼

PPP Information

PPP User Name :

PPP Password : □ password unmask

PPP Trigger Type : ● Auto Connect ○ Connect on Demand ○ Manual

Idle Timeout [minutes]:: 5

PPPoE Service Name :

PPPoE Passthrough : □

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway IP Address : 0.0.0.0

Routing Feature

NAT Enable : □

IGMP Proxy Enable : □

Apply as Default Gateway : □

DNS server

DNS : ● Dynamic ○ Static

DNS Server 1 :

DNS Server 2 :

Tunnel

Enable 6RD : ○ Enable ● Disable

6RD Type : ● DHCP ○ Static

IPv4 Mask Length :

6RD Border Relay Server IP :

6RD IPv6 Prefix :

VLAN

Active : □

802.1p : 0 ▼

802.1q : (0~4094)

QoS

Rate Limit : (kbps)

WAN Outgoing Default Tag : ○ Enable ● Disable

DSCP : (0~63)

MTU

MTU Size : 1492 MTU [68-1492]

Bridge and Routing mode in the same WAN

□ Enable Con-current WAN

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
General	
Active	Select this to enable the interface.
Name	Specify a descriptive name for this connection.
Type	Select whether it is an ADSL/VDSL over PTM, ADSL over ATM connection or Ethernet.
Mode	Select **Routing** if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. The choices depend on the connection type you selected. If your connection type is **ADSL/VDSL over PTM**, the choices are **PPPoE** and **IPoE**. If your connection type is **ADSL over ATM**, the choices are **PPPoE**, **PPPoA**, **IPoE** and **IPoA**.
IPv6/IPv4 Mode	Select **IPv4 Only** if you want the Device to run IPv4 only. Select **IPv6/IPv4 DualStack** to allow the Device to run IPv4 and IPv6 at the same time. Select **IPv6 Only** if you want the Device to run IPv6 only.
ATM PVC Configuration (These fields appear when the **Type** is set to **ADSL over ATM**.)	
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	The choices in this field change according to the **Encapsulation** method chosen above. This field is not editable. **PPPoA** and **IPoA** encapsulation use the same named **DSL Link Type**. Ethernet-over-ATM (**EoA**) is used for **PPPoE**, and **IPoE** encapsulation. **EoA** a protocol for data transfer between Ethernet LAN and WAN over the ATM protocol. It creates a bridged connection between the VMG and the ISP. It uses an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. EoA supports ENET ENCAP (IPoE), PPPoE and RFC1483/2684 bridging encapsulation methods. **PPPoA** (PPP over ATM) allows just one PPPoA connection over a PVC. **IPoA** (IP over ATM) allows just one RFC 1483 routing connection over a PVC.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: • **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **IPoE** or **PPPoE** in the **Select DSL Link Type** field. • **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the VMG needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. • **LLC/ENCAPSULATION:** More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Encapsulation** field. • **LLC/SNAP-ROUTING:** In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select **IPoA** in the **Encapsulation** field.

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

LABEL	DESCRIPTION
Service Category	Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
PPP Information (This is available only when you select **PPPoE** or **PPPoA** in the **Mode** field.)	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above. Select **password unmask** to show your entered password in plain text.
PPP Trigger Type	Select when to have the VMG establish the PPP connection. **Auto Connect** - select this to not let the connection time out. **Connect on Demand** - select this to automatically bring up the connection when the Device receives packets destined for the Internet.**Manual** - select this if you want to manually trigger the connection up.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not configurable if you select **Auto Connect** in the **PPP Trigger Type** field.
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation. In addition to the VMG's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the VMG. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
PPPoE Service Name	Enter the name of your PPPoE service here.
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation. In addition to the VMG's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the VMG. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
IP Address (This is available only when you select **IPv4 Only** or **IPv6/IPv4 DualStack** in the **IPv6/IPv4 Mode** field.)	
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
DHCP option 60/ Vendor ID	This field displays when editing an existing WAN interface. Type the class vender ID you want the VMG to add in the DHCP Discovery packets that go to the DHCP server.

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

LABEL	DESCRIPTION
DHCP option 43 Enable	This field displays when editing an existing WAN interface. Type the vender specific information you want the VMG to add in the DHCP Offer packets. The information is used, for example, for configuring an ACS's (Auto Configuration Server) URL.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
Routing Feature (This is available only when you select **IPv4 Only** or **IPv6 / IPv4 DualStack** in the **IPv6 / IPv4 Mode** field.)	
NAT Enable	Select this option to activate NAT on this connection.
Full cone NAT enable	Select this option to enable full cone NAT on this connection. This field is available only when you activate NAT. In full cone NAT, the VMG maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The VMG also maps packets coming to that external IP address and port to the internal IP address and port.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the VMG act as an IGMP proxy on this connection. This allows the VMG to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the VMG use the WAN interface of this connection as the system default gateway.
DNS Server (This is available only when you select **IPv4 Only** or **IPv6 / IPv4 DualStack** in the **IPv6 / IPv4 Mode** field.)	
DNS	Select **Obtain DNS Info Automically** if you want the VMG to use the DNS server addresses assigned by your ISP. Select **Use Following Static DNS Address** if you want the VMG to use the DNS server addresses you configure manually.
DNS server1	Enter the first DNS server address assigned by the ISP.
DNS server 2	Enter the second DNS server address assigned by the ISP.
Tunnel (This is available only when you select **IPv4 Only** or **IPv6 Only** in the **IPv6 / IPv4 Mode** field.) The DS-Lite (Dual Stack Lite) fields display when you set the **IPv6 / IPv4 Mode** field to **IPv6 Only**. Enable Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network. See Dual Stack Lite on page 82 for more information. The 6RD (IPv6 rapid deployment) fields display when you set the **IPv6 / IPv4 Mode** field to **IPv4 Only**. See IPv6 Rapid Deployment on page 81 for more information.	
Enable DS-Lite	This is available only when you select **IPv6 Only** in the **IPv6 / IPv4 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.
Enable 6RD	This is available only when you select **IPv4 Only** in the **IPv6 / IPv4 Mode** field. Select **Enable** to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
6RD Type	Select **Static** if you have the IPv4 address of the relay server, otherwise select **DHCP** to have the Device detect it automatically through DHCP.

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

LABEL	DESCRIPTION
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
6RD Border Relay Server IP	When you set the **6RD Type** to **Static**, specify the relay server's IPv4 address in this field.
6RD IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
IPv6 Address (This is available only when you select **IPv6/IPv4 DualStack** or **IPv6 Only** in the **IPv6/IPv4 Mode** field.)	
IPv6 Address	Select **Automatic** if you want to have the VMG use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address. • Select **Get IPv6 Address From DHCPv6 Server(IA_NA)** if you want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the VMG using the IPv6 prefix from an RA. This option is available only when you choose to get your IPv6 address automatically. • Select **Prefix Delegation(IA_PD)** to use DHCP PD (Prefix Delegation) which enables the Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses. Select **Static** if you have a fixed IPv6 address assigned by your ISP. Select **None** to not assign any IPv6 address to this WAN connection.
Prefix Length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Next Hop	Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your VMG's interface(s). The gateway helps forward packets to their destinations.
IPv6 Routing Feature (This is available only when you select **IPv6/IPv4 DualStack** or **IPv6 Only** in the **IPv6/IPv4 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	Configure the IPv6 DNS server in the following section.
IPv6 DNS	Select **Dynamic** to have the VMG get the IPv6 DNS server addresses from the ISP automatically. Select **Static** to have the VMG use the IPv6 DNS server addresses you configure manually.
IPv6 DNS Server 1	Enter the first IPv6 DNS server address assigned by the ISP.
IPv6 DNS Server 2	Enter the second IPv6 DNS server address assigned by the ISP.
VLAN (These fields appear when the **Type** is set to **ADSL/VDSL over PTM**.)	
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
QoS	

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

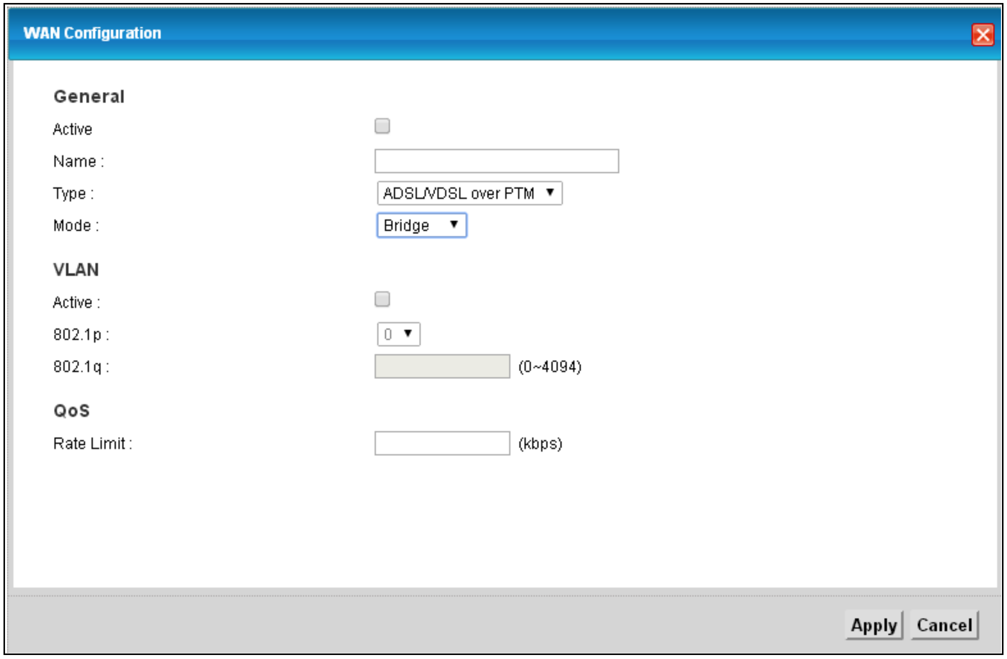
LABEL	DESCRIPTION
Rate Limit	Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection.
WAN Outgoing Default Tag	Select **Enable** and enter a **DSCP** (DiffServ Code Point) value to have the VMG add it in the packets sent by this WAN interface.
DSCP	If you enable Select **WAN Outgoing Default Tag**, enter a **DSCP** (DiffServ Code Point) value to have the VMG add it in the packets sent by this WAN interface.
MTU	
MTU Size	Enter the MTU (Maximum Transfer Unit) size for this traffic.
Bridging and Routing in the same WAN	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. ADSL use same VPI/VCI in Bridge and Route modes. VDSL use same VLAN in Bridge and Route modes.
Enable Con-current WAN	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. \\ • 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.
Apply	Click **Apply** to save your changes back to the VMG.
Cancel	Click **Cancel** to exit this screen without saving.

6.2.1.2 Bridge Mode

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

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

Figure 20 Network Setting > Broadband > Add New WAN Interface/Edit (Bridge Mode)



WAN Configuration

General

Active □

Name :

Type : ADSL/VDSL over PTM

Mode : Bridge

VLAN

Active : □

802.1p : 0

802.1q : (0~4094)

QoS

Rate Limit : (kbps)

The following table describes the fields in this screen.

Table 9 Network Setting > Broadband > Add New WAN Interface/Edit (Bridge Mode)

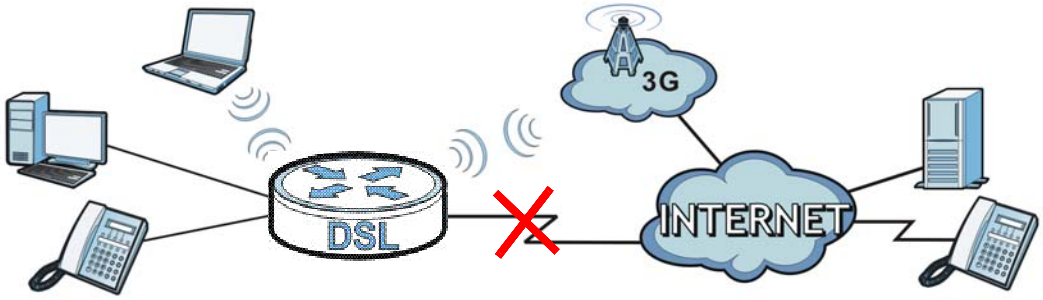
LABEL	DESCRIPTION
General	
Active	Select this to enable the interface.
Name	Enter a service name of the connection.
Type	Select **ADSL/VDSL over PTM** as the interface that you want to configure. The VMG uses the VDSL technology for data transmission over the DSL port.
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
VLAN	This section is available only when you select **ADSL/VDSL over PTM** in the **Type** field.
802.1p	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Select the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
802.1q	Type the VLAN ID number (from 0 to 4094) for traffic through this connection.
QoS	
Rate Limit	Enter the rate limit for the connection. This is the maximum transmission rate allowed for traffic on this connection.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

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.

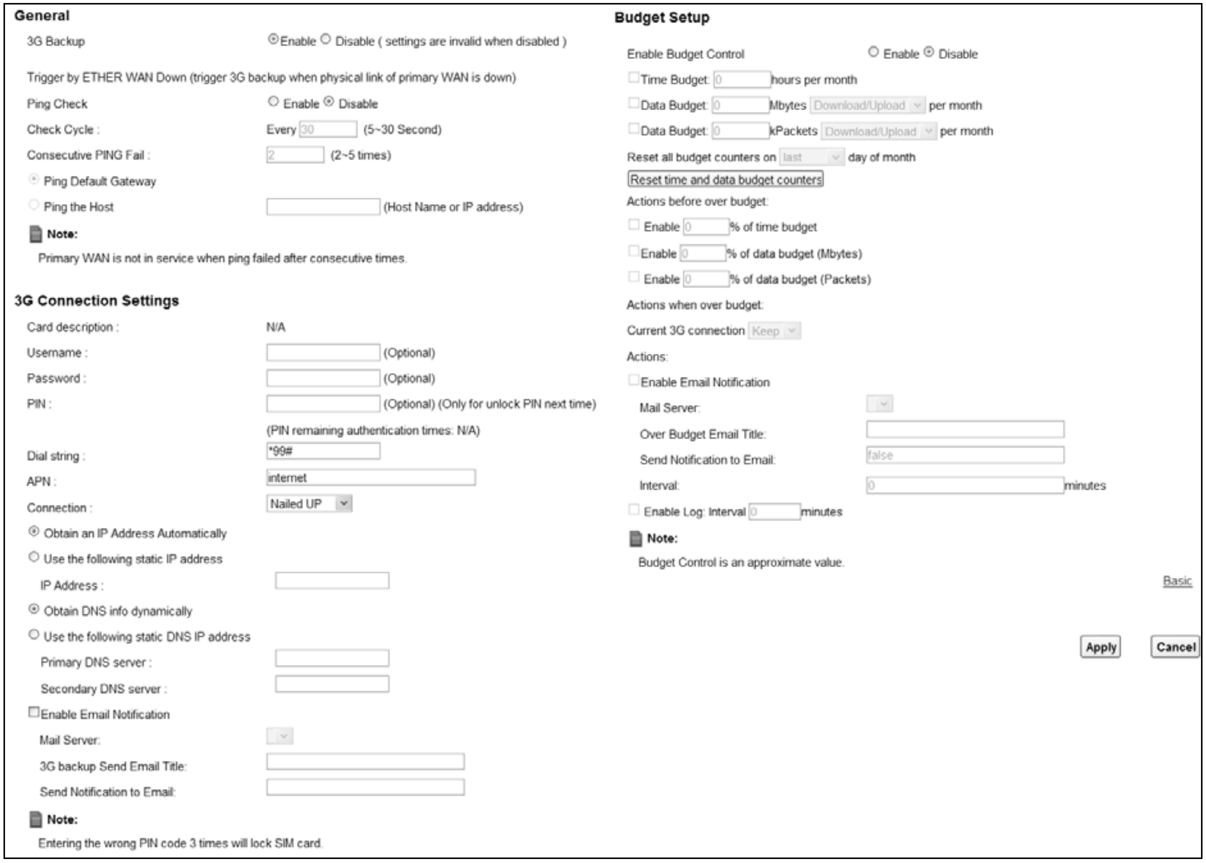
Figure 21 Internet Access Application: 3G WAN



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 22 Network Setting **>** Broadband > 3G Backup



General

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

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

Ping Check ○ Enable ● Disable

Check Cycle : Every 30 (5~30 Second)

Consecutive PING Fail : 2 (2~5 times)

● Ping Default Gateway

○ Ping the Host (Host Name or IP address)

Note:

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

3G Connection Settings

Card description : N/A

Username : (Optional)

Password : (Optional)

PIN : (Optional) (Only for unlock PIN next time)

(PIN remaining authentication times: N/A)

Dial string : *99#

APN : internet

Connection : Nailed UP

● Obtain an IP Address Automatically

○ Use the following static IP address

IP Address :

● Obtain DNS info dynamically

○ Use the following static DNS IP address

Primary DNS server :

Secondary DNS server :

□ Enable Email Notification

Mail Server:

3G backup Send Email Title:

Send Notification to Email:

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 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 Email Notification

Mail Server:

Over Budget Email Title:

Send Notification to Email: false

Interval: 0 minutes

□ Enable Log: Interval 0 minutes

Note:

Budget Control is an approximate value.

The following table describes the labels in this screen.

Table 10 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 PING 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**.

Table 10 Network Setting **>** Broadband > 3G Backup (continued)

LABEL	DESCRIPTION
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**.
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 Email 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 Server	Select a mail server for the e-mail address specified below. If you do not select a mail server, e-mail notifications cannot be sent via e-mail. You must have configured a mail server already in the **Maintenance** > **Email Notification** screen.
3G backup Send Email Title	Type a title that you want to be in the subject line of the e-mail notifications that the VMG sends.

Table 10 Network Setting **>** Broadband > 3G Backup (continued)

LABEL	DESCRIPTION
Send Notification to Email	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail.
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
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 Email Notification	Select this to enable the e-mail notification function. The VMG will e-mail you a notification when there over budget occurs.

Table 10 Network Setting > Broadband > 3G Backup (continued)

LABEL	DESCRIPTION
Mail Server	Select a mail server for the e-mail address specified below. If you do not select a mail server, e-mail notifications cannot be sent via e-mail. You must have configured a mail server already in the **Maintenance** > **Email Notification** screen.
Over Budget Email Title	Type a title that you want to be in the subject line of the e-mail notifications that the VMG sends.
Send Notification to Email	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail.
Interval	Enter the interval of how many minutes you want the VMG to e-mail you.
Enable Log	Select this to activate the logging function at the interval you set in this field.
Basic	Click this to hide the advanced settings of 3G backup.
Apply	Click **Apply** to save your changes back to the 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.

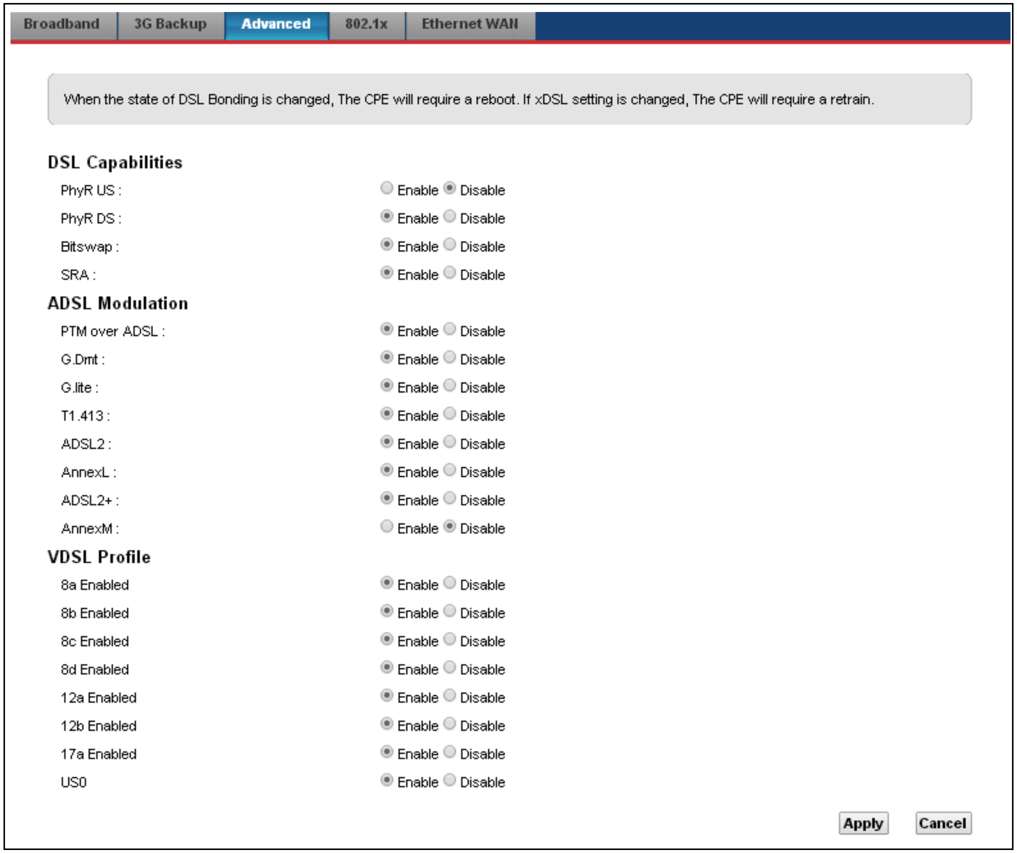
ITU-T G.993.2 standard defines a wide range of settings for various parameters, some of which are encompassed in profiles as shown in the next table.

Table 11 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 23 Network Setting **>** Broadband > Advanced



When the state of DSL Bonding is changed, The CPE will require a reboot. If xDSL setting is changed, The CPE will require a retrain.

DSL Capabilities

PhyR US : ○ Enable ● Disable

PhyR DS : ● Enable ○ Disable

Bitswap : ● Enable ○ Disable

SRA : ● Enable ○ Disable

ADSL Modulation

PTM over ADSL : ● Enable ○ Disable

G.Dmt : ● Enable ○ Disable

G.lite : ● Enable ○ Disable

T1.413 : ● Enable ○ Disable

ADSL2 : ● Enable ○ Disable

AnnexL : ● Enable ○ Disable

ADSL2+ : ● Enable ○ Disable

AnnexM : ○ Enable ● Disable

VDSL Profile

8a Enabled ● Enable ○ Disable

8b Enabled ● Enable ○ Disable

8c Enabled ● Enable ○ Disable

8d Enabled ● Enable ○ Disable

12a Enabled ● Enable ○ Disable

12b Enabled ● Enable ○ Disable

17a Enabled ● Enable ○ Disable

US0 ● Enable ○ Disable

The following table describes the labels in this screen.

Table 12 Network Setting **>** Broadband > Advanced

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

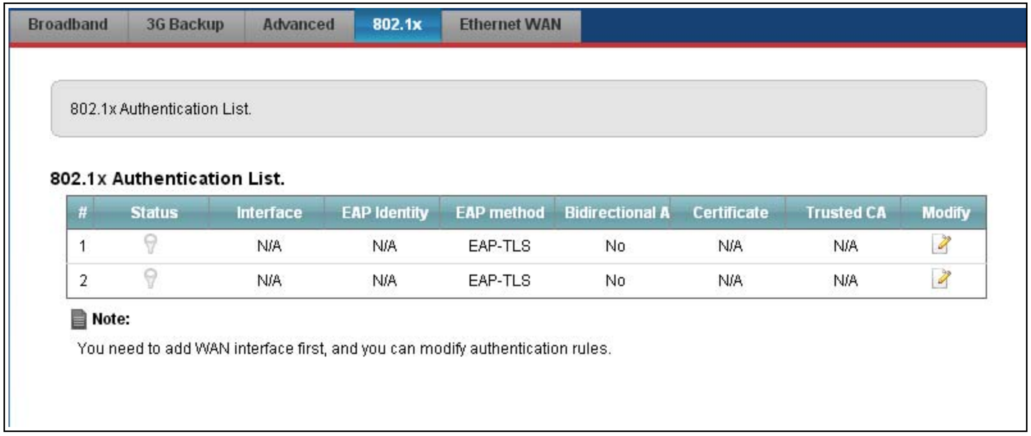
Table 12 Network Setting **>** Broadband > Advanced (continued)

LABEL	DESCRIPTION
G.lite :	ITU G.992.2 (better known as G.lite) is an ITU standard for ADSL using discrete multitone modulation. G.lite does not strictly require the use of DSL filters, but like all variants of ADSL generally functions better with splitters.
T1.413 :	ANSI T1.413 is a technical standard that defines the requirements for the single asymmetric digital subscriber line (ADSL) for the interface between the telecommunications network and the customer installation in terms of their interaction and electrical characteristics.
ADSL2 :	It optionally extends the capability of basic ADSL in data rates to 12 Mbit/s downstream and, depending on Annex version, up to 3.5 Mbit/s upstream (with a mandatory capability of ADSL2 transceivers of 8 Mbit/s downstream and 800 kbit/s upstream).
AnnexL :	Annex L is an optional specification in the ITU-T ADSL2 recommendation G.992.3 titled Specific requirements for a Reach Extended ADSL2 (READSL2) system operating in the frequency band above POTS, therefore it is often referred to as Reach Extended ADSL2 or READSL2.The main difference between this specification and commonly deployed Annex A is the maximum distance that can be used. The power of the lower frequencies used for transmitting data is boosted up to increase the reach of this signal up to 7 kilometers (23,000 ft).
ADSL2+ :	ADSL2+ extends the capability of basic ADSL by doubling the number of downstream channels. The data rates can be as high as 24 Mbit/s downstream and up to 1.4 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises.
AnnexM :	Annex M is an optional specification in ITU-T recommendations G.992.3 (ADSL2) and G.992.5 (ADSL2+), also referred to as ADSL2 M and ADSL2+ M. This specification extends the capability of commonly deployed Annex A by more than doubling the number of upstream bits. The data rates can be as high as 12 or 24 Mbit/s downstream and 3 Mbit/s upstream depending on the distance from the DSLAM to the customer's premises.
VDSL Profile	VDSL2 profiles differ in the width of the frequency band used to transmit the broadband signal. Profiles that use a wider frequency band can deliver higher maximum speeds.
8a, 8b, 8c, 8d, 12a, 12b, 17a, 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 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 24 Network Setting > Broadband > 802.1x



802.1x Authentication List.

802.1x Authentication List.

#	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.

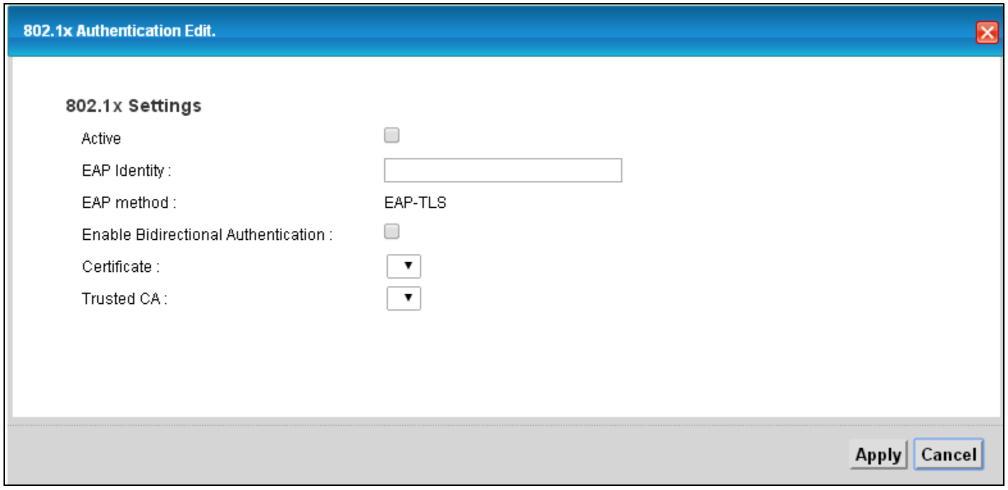
Table 13 Network Setting > Network Setting > 802.1x

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

6.5.1 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 25 Network Setting **>** Broadband > 802.1x > Modify



802.1x Authentication Edit.

802.1x Settings

Active □

EAP Identity :

EAP method : EAP-TLS

Enable Bidirectional Authentication : □

Certificate : ▼

Trusted CA : ▼

The following table describes the labels in this screen.

Table 14 Network Setting **>** Broadband > 802.1x: Edit

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

6.6 Ethernet WAN

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

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

You cannot have DSL Ethernet and 3G WAN connections working at the same time. The order of priority for the WAN connections are:

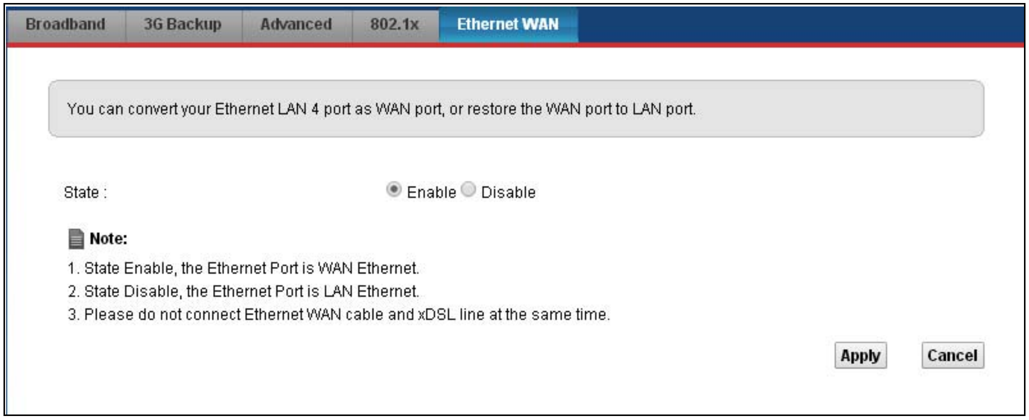
1 DSL

2 Ethernet

3 3G

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

Figure 26 Network Setting > Broadband > Ethernet WAN



You can convert your Ethernet LAN 4 port as WAN port, or restore the WAN port to LAN port.

State : ● Enable ○ Disable

Note:
1. State Enable, the Ethernet Port is WAN Ethernet.
2. State Disable, the Ethernet Port is LAN Ethernet.
3. Please do not connect Ethernet WAN cable and xDSL line at the same time.

The following table describes the fields in the above screen.

Table 15 Network Setting > Broadband > Ethernet WAN

LABEL	DESCRIPTION
Enable	Click the radio button to convert LAN port number four to a WAN port.
Disable	Click the radio button to restore LAN port number four to a LAN port.

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.

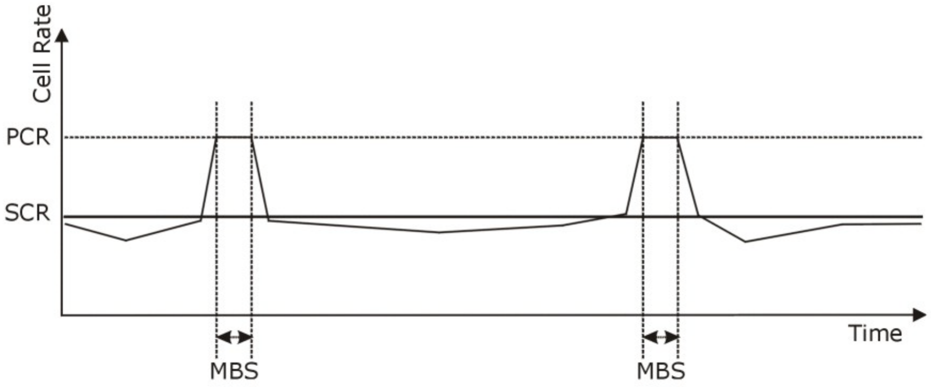
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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 27 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.

7

Wireless

7.1 Overview

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

7.1.1 What You Can Do in this Chapter

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

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 7.2 on page 108).
- Use the **Guest / More AP** screen to set up multiple wireless networks on your VMG (Section 7.3 on page 114).
- 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 117).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 7.5 on page 118).
- 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 119).
- Use the **WDS** screen to set up a Wireless Distribution System, in which the VMG acts as a bridge with other ZyXEL access points (Section 7.7 on page 120).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold (Section 7.8 on page 122).
- Use the **Channel Status** screen to scan wireless LAN channel noises and view the results (Section 7.9 on page 124).

7.1.2 What You Need to Know

Wireless Basics

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

Finding Out More

See Section 7.10 on page 125 for advanced technical information on wireless networks.

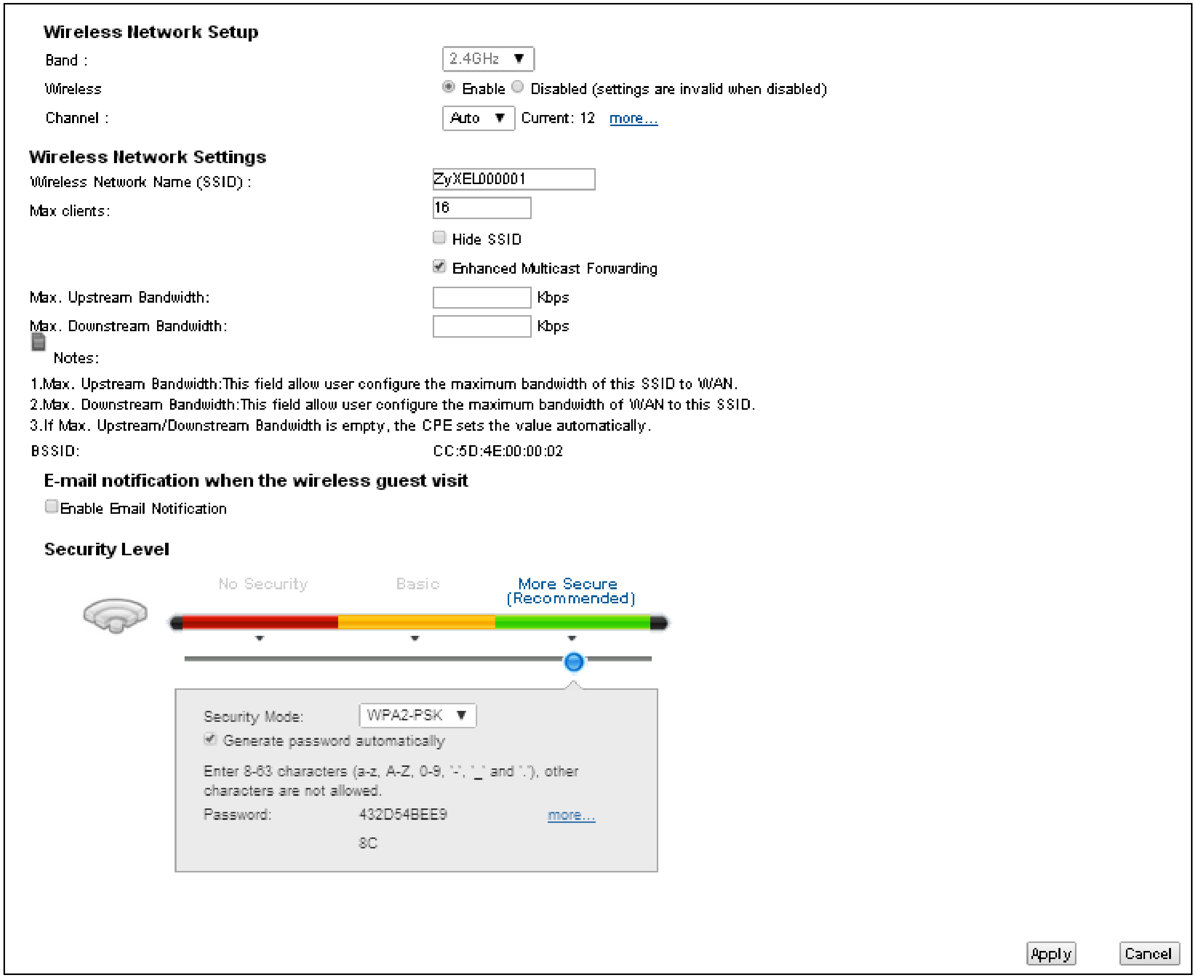
7.2 The General Screen

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 28 Network Setting > Wireless > General



Wireless Network Setup

Band : 2.4GHz ▼

Wireless ● Enable ○ Disabled (settings are invalid when disabled)

Channel : Auto ▼ Current: 12 more...

Wireless Network Settings

Wireless Network Name (SSID) : ZyXEL000001

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

Security Mode: WPA2-PSK ▼

☑ Generate password automatically

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

Password: 432D54BEE9 8C more...

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

Table 16 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can **Enable** or **Disable** the wireless LAN in this field.
Band	This shows the wireless band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n wireless clients.
Channel	Use **Auto** to have the VMG automatically determine a channel to use.
more.../less	Click **more...** to show more information. Click **less** to hide them.
Bandwidth	Select whether the VMG uses a wireless channel width of **20MHz** or **40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.

Table 16 Network Setting > Wireless > General (continued)

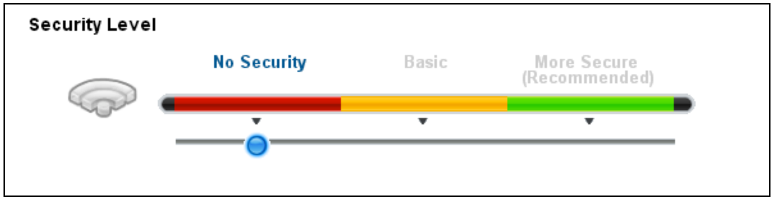
LABEL	DESCRIPTION
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Passphrase Type	If you set security for the wireless LAN and have the VMG generate a password, the setting in this field determines how the VMG generates the password. Select **None** to set the VMG's password generation to not be based on a passphrase. Select **Fixed** to use a 16 character passphrase for generating a password. Select **Variable** to use a 16 to 63 character passphrase for generating a password.
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.
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.
Enhanced Multicast Forwarding	Select this check box to allow the VMG to convert wireless multicast traffic into wireless unicast traffic.
Maximum Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Maximum 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	
Security Mode	Select **Basic (WEP, 802.1X)** or **More Secure (WPA(2)-PSK)** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the VMG. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Apply	Click **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 29 Wireless > General: No Security



The following table describes the labels in this screen.

Table 17 Wireless > General: No Security

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

7.2.2 Basic (WEP Encryption)

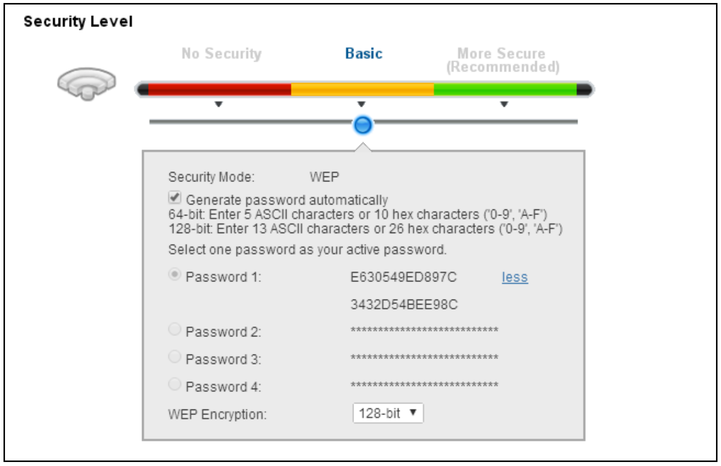
WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

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

Your 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 30 Wireless > General: Basic (WEP)



Security Mode: WEP

☑ Generate password automatically
64-bit: Enter 5 ASCII characters or 10 hex characters ('0-9', 'A-F')
128-bit: Enter 13 ASCII characters or 26 hex characters ('0-9', 'A-F')

Select one password as your active password.

● Password 1: E630549ED897C less
3432D54BEE98C

○ Password 2: ***************************

○ Password 3: ***************************

○ Password 4: ***************************

WEP Encryption: 128-bit ▼

The following table describes the labels in this screen.

Table 18 Wireless > General: Basic (WEP)

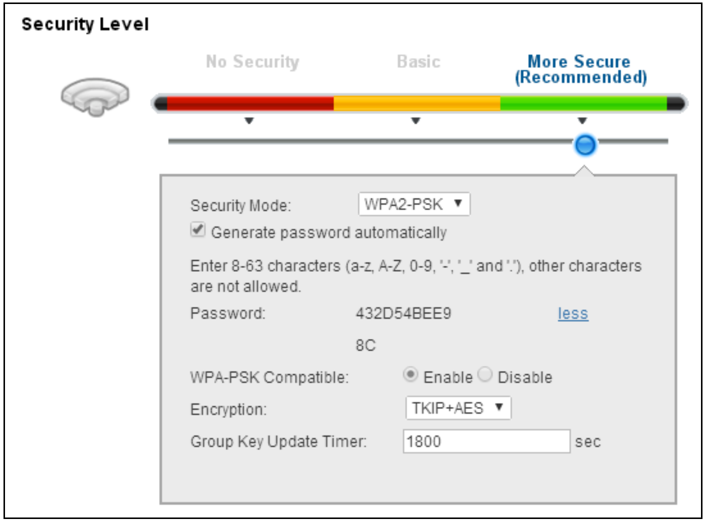
LABEL	DESCRIPTION
Security Level	Select **Basic** to enable WEP data encryption.
Generate password automatically	Select this option to have the VMG automatically generate a password. The password field will not be configurable when you select this option.
Password 1~4	The password (WEP keys) are used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

7.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the 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. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 31 Wireless > General: More Secure: WPA(2)-PSK



Security Level

Security Mode: WPA2-PSK ▼

☑ Generate password automatically

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

Password: 432D54BEE9 8C less

WPA-PSK Compatible: ● Enable ○ Disable

Encryption: TKIP+AES ▼

Group Key Update Timer: 1800 sec

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Generate password automatically	Select this option to have the VMG automatically generate a password. The password field will not be configurable when you select this option.
Password	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. If you did not select **Generate password automatically**, you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
more.../less	Click **more...** to show more fields in this section. Click **less** to hide them.
WPA-PSK Compatible	This field appears when you choose **WPA-PSK2** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your VMG. The VMG supports WPA-PSK and WPA2-PSK simultaneously.

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

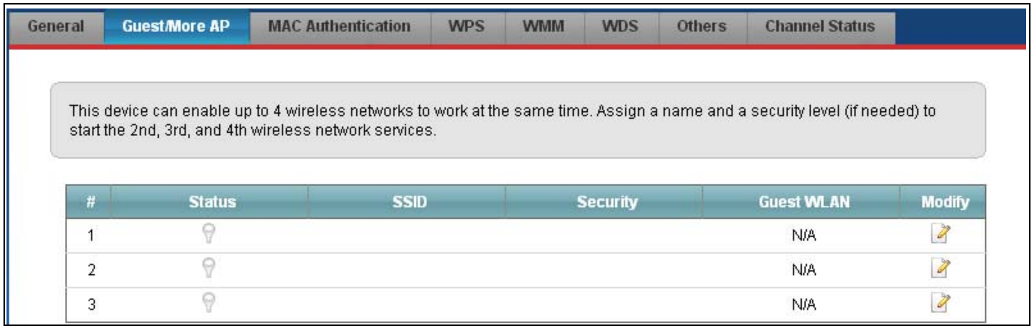
LABEL	DESCRIPTION
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or 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 32 Network Setting > Wireless > Guest / More AP



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	💡			N/A	✎
2	💡			N/A	✎
3	💡			N/A	✎

The following table describes the labels in this screen.

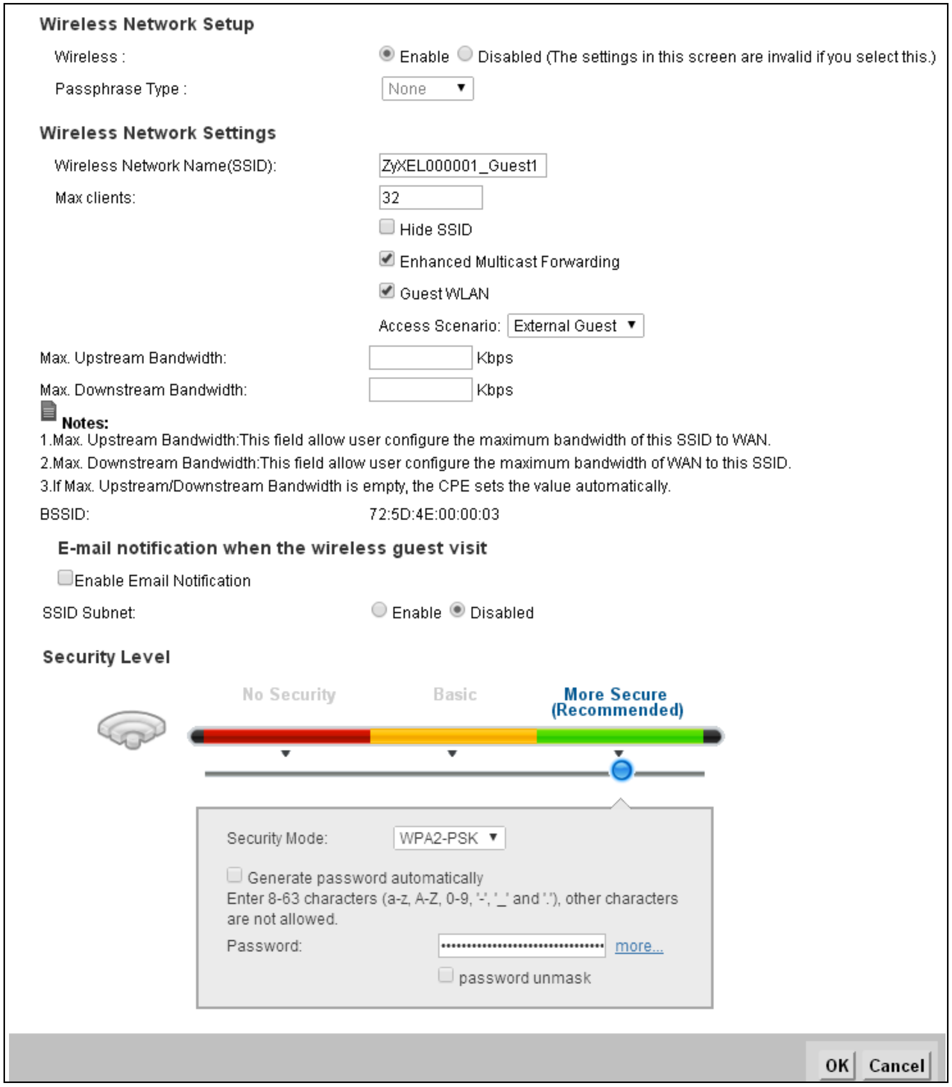
Table 20 Network Setting > Wireless > Guest / More AP

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 can connect to 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 33 Network Setting > Wireless > Guest / More AP > Edit



Wireless Network Setup

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

Passphrase Type : None ▼

Wireless Network Settings

Wireless Network Name(SSID): ZyXEL000001_Guest1

Max clients: 32

□ Hide SSID

☑ Enhanced Multicast Forwarding

☑ Guest WLAN

Access Scenario: External Guest ▼

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: 72:5D:4E:00:00:03

E-mail notification when the wireless guest visit

□ Enable Email Notification

SSID Subnet: ○ Enable ● Disabled

Security Level

Security Mode: WPA2-PSK ▼

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

Password: •••••••••••••••••••••••••••••••• more...

□ password unmask

The following table describes the fields in this screen.

Table 21 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	Passphrase type cannot be changed. The default is **None**.
Wireless Network Settings	

Table 21 Network Setting > Wireless > Guest / More AP > Edit (continued)

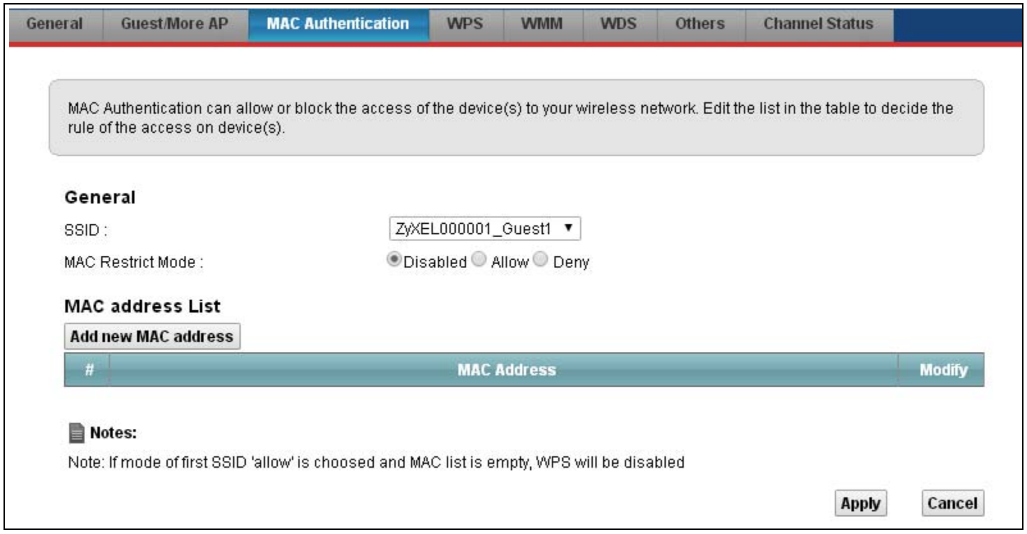
LABEL	DESCRIPTION
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
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.
Enhanced 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 can connect to each other directly. If you select **External Guest**, clients are blocked from connecting to each other directly.
Maximum Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Maximum 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.
E-mail notification when the wireless guest visit	
Enable Email Notification	Select this to have the VMG e-mail you a notification when a wireless client is connected to the wireless network.
Mail Server	Select a mail server for the e-mail address specified below. If you do not select a mail server, e-mail notifications cannot be sent via e-mail. You must have configured a mail server already in the **Maintenance** > **Email Notification** screen.
Email 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 Email	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications cannot be sent via e-mail.
Security Level	
Security Mode	Select **Basic (WEP, 802.1X)** or **More Secure (WPA(2)-PSK)** 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 110 for more details about this field.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

7.4 MAC Authentication

This screen allows you to configure the ZyXEL Device to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the ZyXEL Device **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

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

Figure 34 Wireless > MAC Authentication



MAC Authentication can allow or block the access of the device(s) to your wireless network. Edit the list in the table to decide the rule of the access on device(s).

General

SSID : ZyXEL000001_Guest1

MAC Restrict Mode : ● Disabled ○ Allow ○ Deny

MAC address List

#	MAC Address	Modify

Notes:

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

The following table describes the labels in this screen.

Table 22 Wireless > MAC Authentication

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Deny** to block access to the VMG. MAC addresses not listed will be allowed to access the VMG. Select **Allow** to permit access to the VMG. MAC addresses not listed will be denied access to the VMG.
Add new MAC address	Click this if you want to add a new MAC address entry to the MAC filter list below. Enter the MAC addresses of the wireless devices that are allowed or denied access to the 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.
#	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.
Delete	Click the **Delete** icon to delete the entry.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

7.5 The WPS Screen

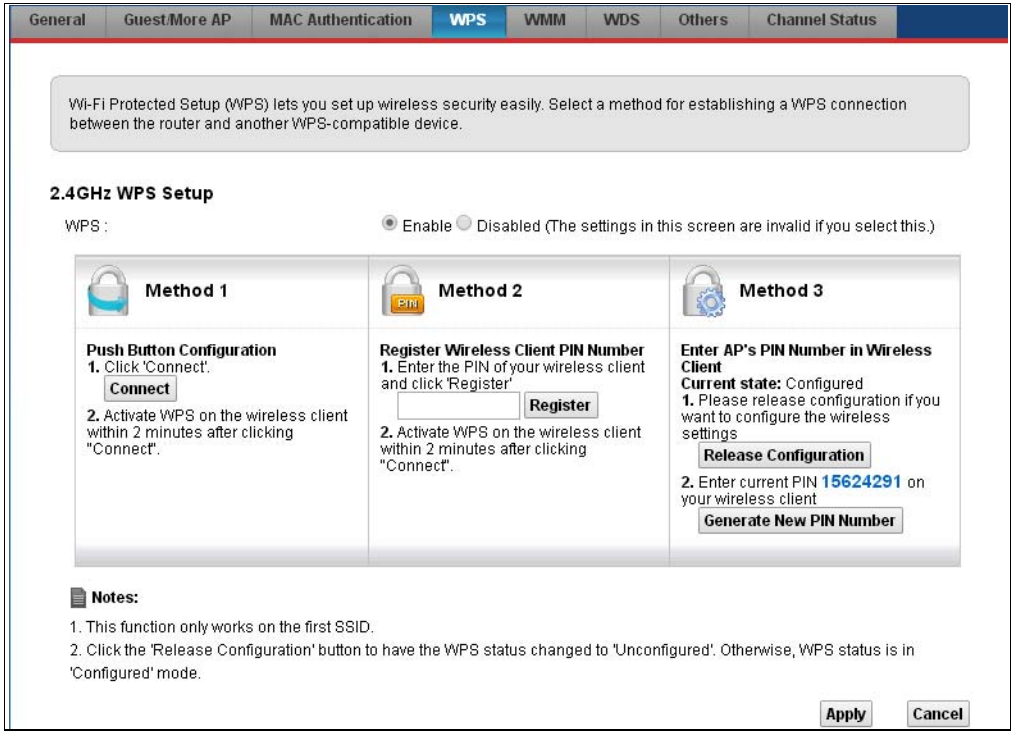
Use this screen to configure WiFi Protected Setup (WPS) on your VMG.

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 7.10.9.3 on page 134 for more information about WPS.

Note: The VMG applies the security settings of the **SSID1** profile (see Section 7.2 on page 108). 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 35 Network Setting > Wireless > WPS



Wi-Fi Protected Setup (WPS) lets you set up wireless security easily. Select a method for establishing a WPS connection between the router and another WPS-compatible device.

2.4GHz WPS Setup

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

Method 1

Push Button Configuration
1. Click 'Connect'.
2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client PIN Number
1. Enter the PIN of your wireless client and click 'Register'
2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

Enter AP's PIN Number in Wireless Client
Current state: Configured
1. Please release configuration if you want to configure the wireless settings
2. Enter current PIN **15624291** on your wireless client

Notes:

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

The following table describes the labels in this screen.

Table 23 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
WPS	Select **Enable** to activate WPS on the VMG.
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
Connect	Click this button to add another WPS-enabled wireless device (within wireless range of the 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 **Connect** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.

Table 23 Network Setting > Wireless > WPS (continued)

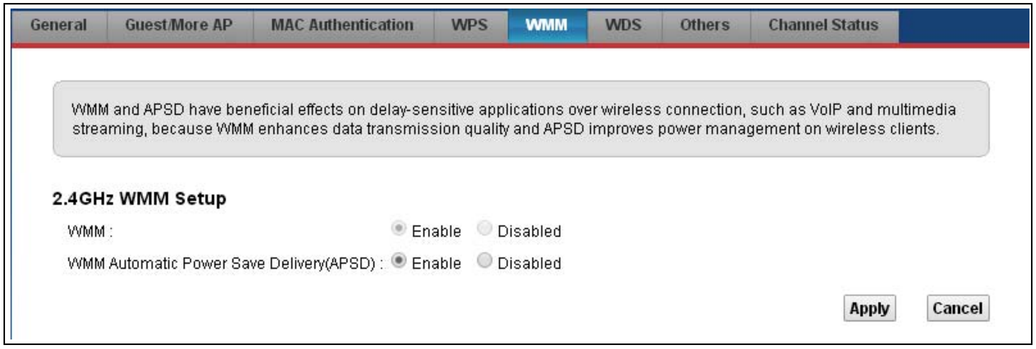
LABEL	DESCRIPTION
Method 2	Use this section to set up a WPS wireless network by entering the PIN of the client into the VMG.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the VMG.
Method 3	Use this section to set up a WPS wireless network by entering the PIN of the VMG into the client.
Release Configuration	The default WPS status is configured. Click this button to remove all configured wireless and wireless security settings for WPS connections on the VMG.
Generate New PIN Number	The PIN (Personal Identification Number) of the VMG is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the **Generate New PIN Number** button to have the VMG create a new PIN.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.6 The WMM Screen

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

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

Figure 36 Network Setting > Wireless > WMM



WMM and APSD have beneficial effects on delay-sensitive applications over wireless connection, such as VoIP and multimedia streaming, because WMM enhances data transmission quality and APSD improves power management on wireless clients.

2.4GHz WMM Setup

WMM : ● Enable ○ Disabled

WMM Automatic Power Save Delivery(APSD) : ● Enable ○ Disabled

The following table describes the labels in this screen.

Table 24 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
WMM	Select **On** to have the VMG automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
WMM Automatic Power Save Delivery	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The 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: 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 WDS Screen

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

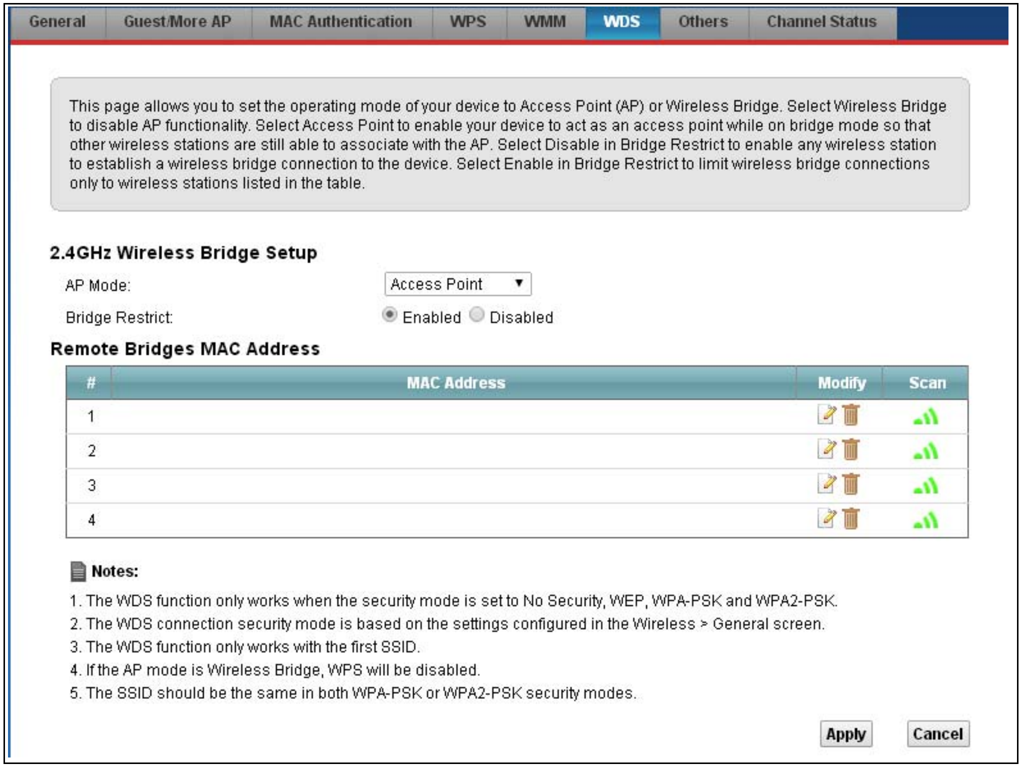
Use this screen to set up your WDS (Wireless Distribution System) links between the VMG and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made.

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

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

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

Figure 37 Network Setting > Wireless > WDS



This page allows you to set the operating mode of your device to Access Point (AP) or Wireless Bridge. Select Wireless Bridge to disable AP functionality. Select Access Point to enable your device to act as an access point while on bridge mode so that other wireless stations are still able to associate with the AP. Select Disable in Bridge Restrict to enable any wireless station to establish a wireless bridge connection to the device. Select Enable in Bridge Restrict to limit wireless bridge connections only to wireless stations listed in the table.

2.4GHz Wireless Bridge Setup

AP Mode: Access Point ▼

Bridge Restrict: ● Enabled ○ Disabled

Remote Bridges MAC Address

#	MAC Address	Modify	Scan
1			
2			
3			
4			

Notes:

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

The following table describes the labels in this screen.

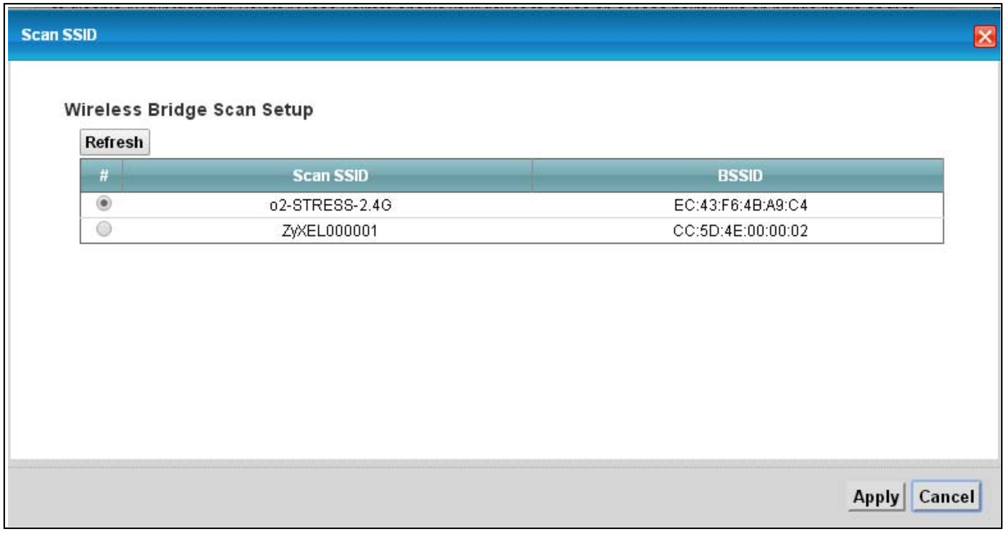
Table 25 Network Setting > Wireless > WDS

LABEL	DESCRIPTION
Wireless Bridge Setup	
AP Mode	Select the operating mode for your VMG. • **Access Point** - The VMG functions as a bridge and access point simultaneously. • **Wireless Bridge** - The VMG acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the VMG wirelessly.
Bridge Restrict	This field is available only when you set operating mode to **Access Point**. Select **Enabled** to turn on WDS and enter the peer device's MAC address manually in the table below. Select **Disable** to turn off WDS.
Remote Bridge MAC Address	You can enter the MAC address of the peer device by clicking the **Edit** icon under **Modify**.
#	This is the index number of the entry.
MAC Address	This shows the MAC address of the peer device. You can connect to up to 4 peer devices.
Modify	Click the **Edit** icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the **Delete** icon to remove this entry.
Scan	Click the **Scan** icon to search and display the available APs within range.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.7.1 WDS Scan

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

Figure 38 WDS: Scan



#	Scan SSID	BSSID
●	o2-STRESS-2.4G	EC:43:F6:4B:A9:C4
○	ZyXEL000001	CC:5D:4E:00:00:02

The following table describes the labels in this screen.

Table 26 WDS: Scan

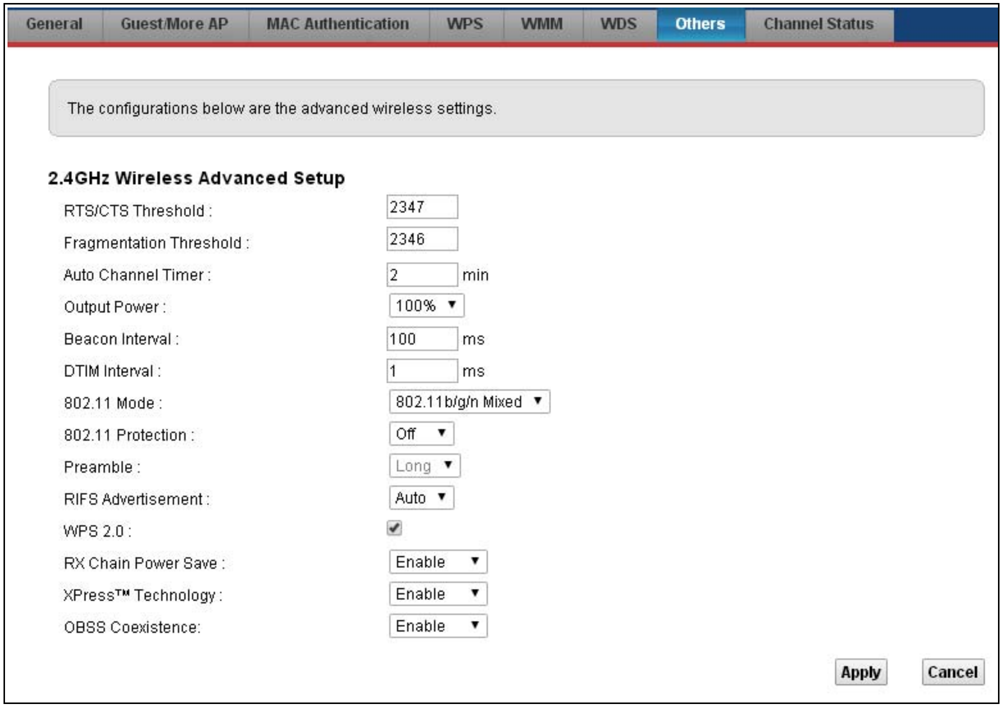
LABEL	DESCRIPTION
Wireless Bridge Scan Setup	
Refresh	Click **Refresh** to update the table.
#	This is the index number of the entry.
SSID	This shows the SSID of the available wireless device within range.
BSSID	This shows the MAC address of the available wireless device within range.
Apply	Click **Apply**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

7.8 The Others Screen

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

See Section 7.10.2 on page 127 for detailed definitions of the terms listed in this screen.

Figure 39 Network Setting > Wireless > Others



The configurations below are the advanced wireless settings.

2.4GHz Wireless Advanced Setup

RTS/CTS Threshold : 2347

Fragmentation Threshold : 2346

Auto Channel Timer : 2 min

Output Power : 100%

Beacon Interval : 100 ms

DTIM Interval : 1 ms

802.11 Mode : 802.11b/g/n Mixed

802.11 Protection : Off

Preamble : Long

RIFS Advertisement : Auto

WPS 2.0 : ☑

RX Chain Power Save : Enable

XPress™ Technology : Enable

OBSS Coexistence: Enable

The following table describes the labels in this screen.

Table 27 Network Setting > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
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.

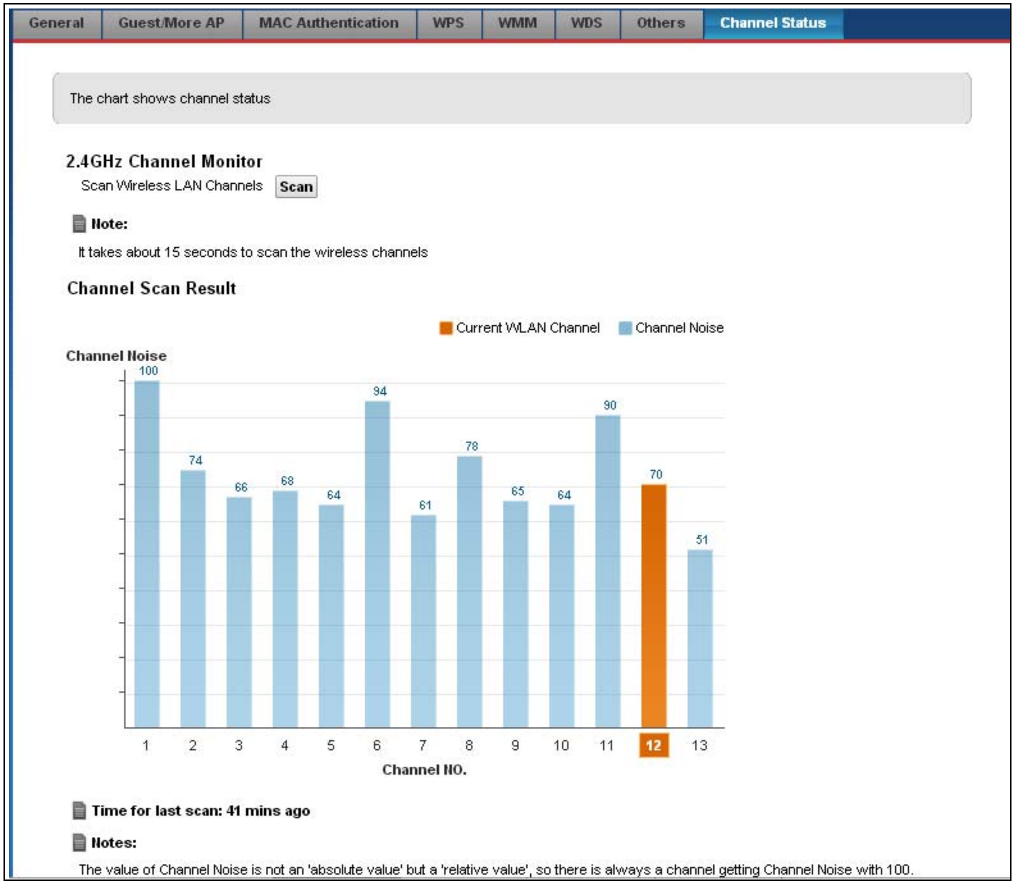
Table 27 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
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**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 7.10.7 on page 131 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.9 The Channel Status Screen

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

Figure 40 Network Setting > Wireless > Channel Status



The chart shows channel status

2.4GHz Channel Monitor

Scan Wireless LAN Channels

Note:

It takes about 15 seconds to scan the wireless channels

Channel Scan Result

Time for last scan: 41 mins ago

Notes:

The value of Channel Noise is not an 'absolute value' but a 'relative value', so there is always a channel getting Channel Noise with 100.

7.10 Technical Reference

This section discusses wireless LANs in depth. For more information, see Appendix E on page 375.

7.10.1 Wireless Network Overview

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

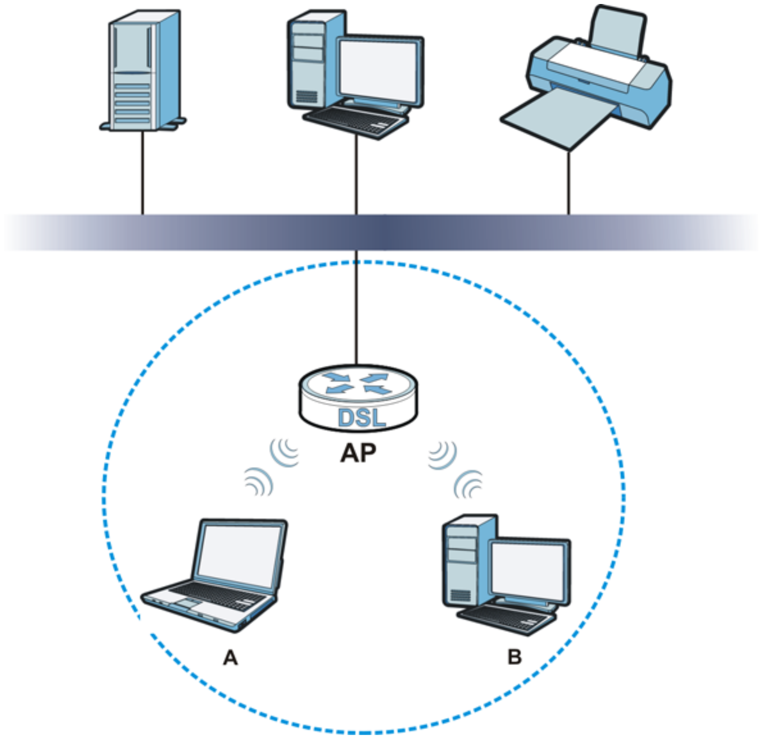
- A wireless client is a radio connected to a user’s computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients,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

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

- An “infrastructure” type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An “ad-hoc” type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 41 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.

7.10.2 Additional Wireless Terms

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

Table 28 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	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. 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. 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.
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.

7.10.3 Wireless Security Overview

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

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

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

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

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

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

7.10.3.1 SSID

Normally, the 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.

7.10.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; 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.

7.10.3.3 User Authentication

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

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

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

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

7.10.3.4 Encryption

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

The types of encryption you can choose depend on the type of authentication. (See Section 7.10.3.3 on page 128 for information about this.)

Table 29 Types of Encryption for Each Type of Authentication

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

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

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

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

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

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

7.10.4 Signal Problems

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

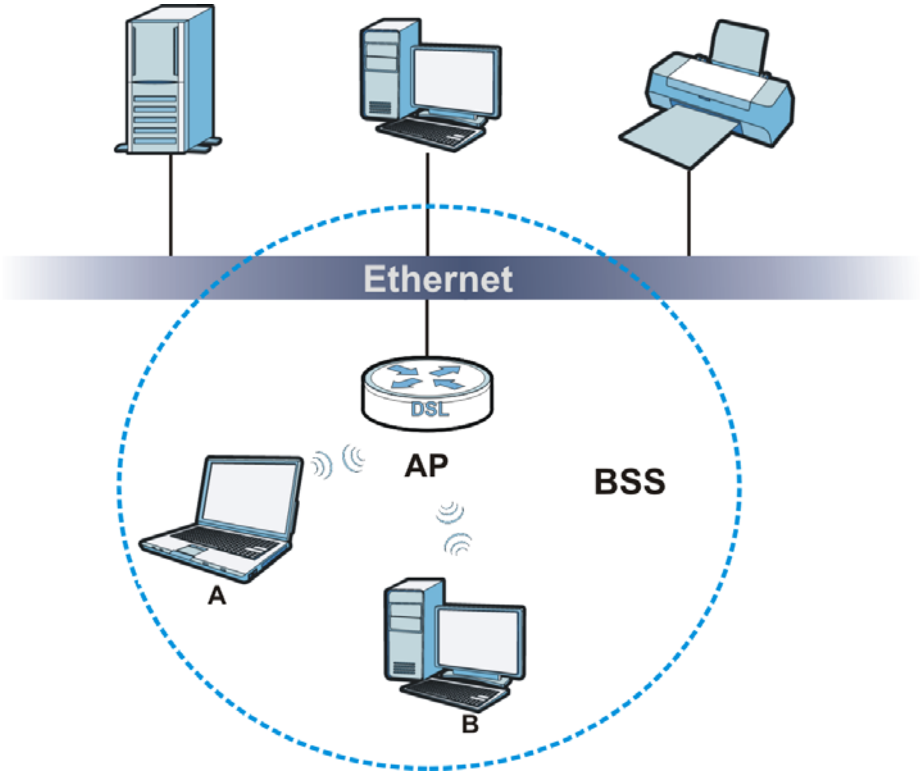
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.10.5 BSS

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

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

Figure 42 Basic Service set



7.10.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The 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.

7.10.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).

- MBSSID should not replace but rather be used in conjunction with 802.1x security.

7.10.7 Preamble Type

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

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

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

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

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

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

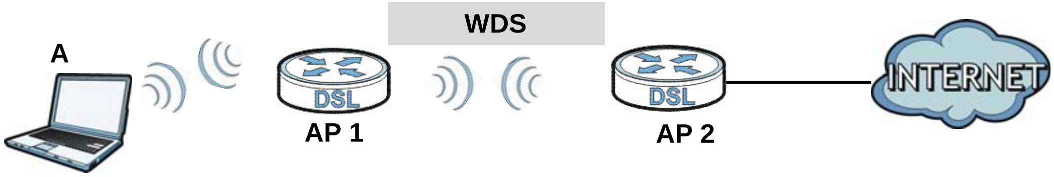
7.10.8 Wireless Distribution System (WDS)

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

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

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

Figure 43 WDS Link Example



7.10.9 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.

7.10.9.1 Push Button Configuration

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

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

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

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the VMG, see Section 7.6 on page 119).
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.

7.10.9.2 PIN Configuration

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

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

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

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

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client’s WPS PIN; it will be displayed either on the device, or in the WPS section of the client’s configuration interface (see the device’s User’s Guide for how to find the WPS PIN - for the VMG, see Section 7.5 on page 118).

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.

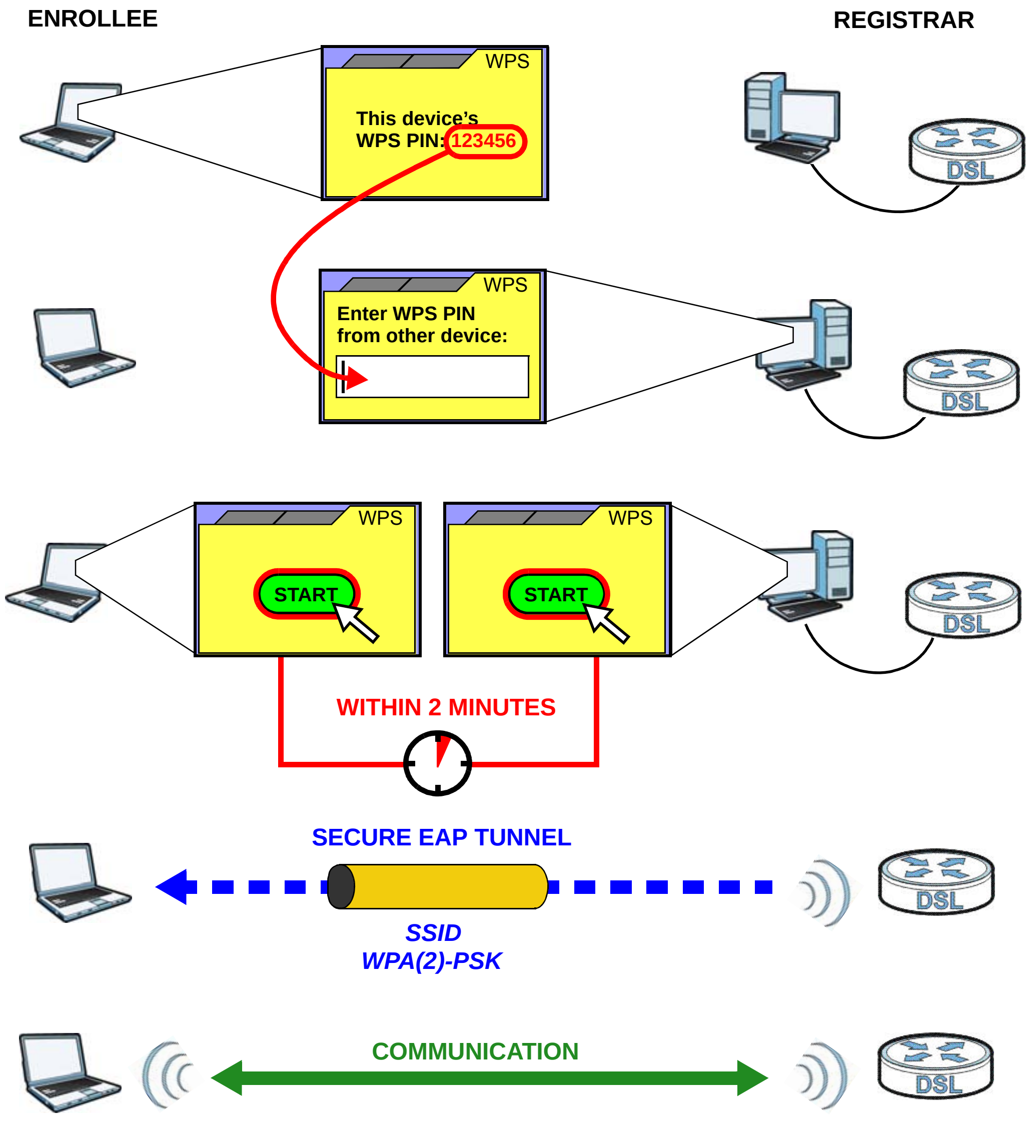
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

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 44 Example WPS Process: PIN Method

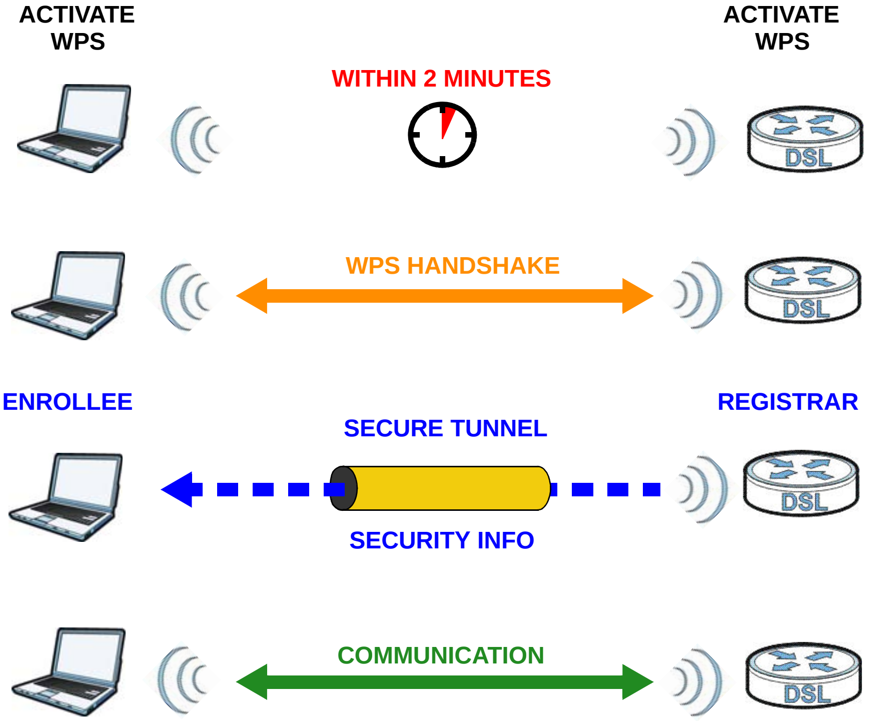


7.10.9.3 How WPS Works

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

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

Figure 45 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.

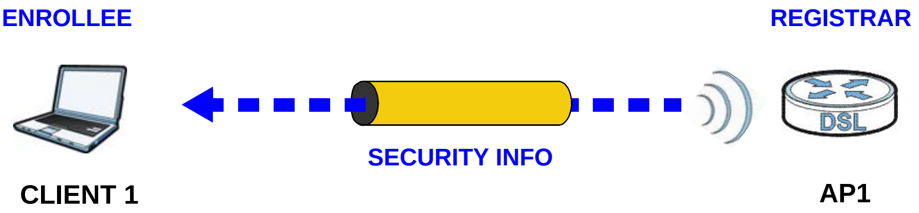
By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled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

7.10.9.4 Example WPS Network Setup

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

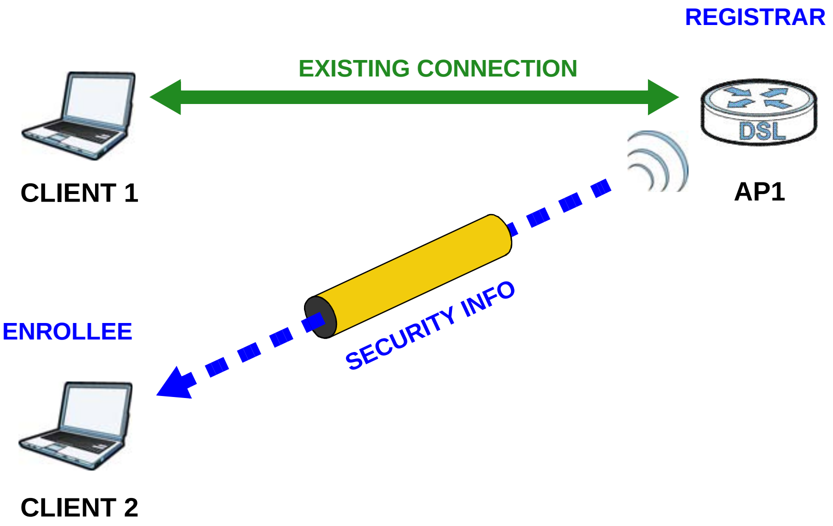
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information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

Figure 46 WPS: Example Network Step 1



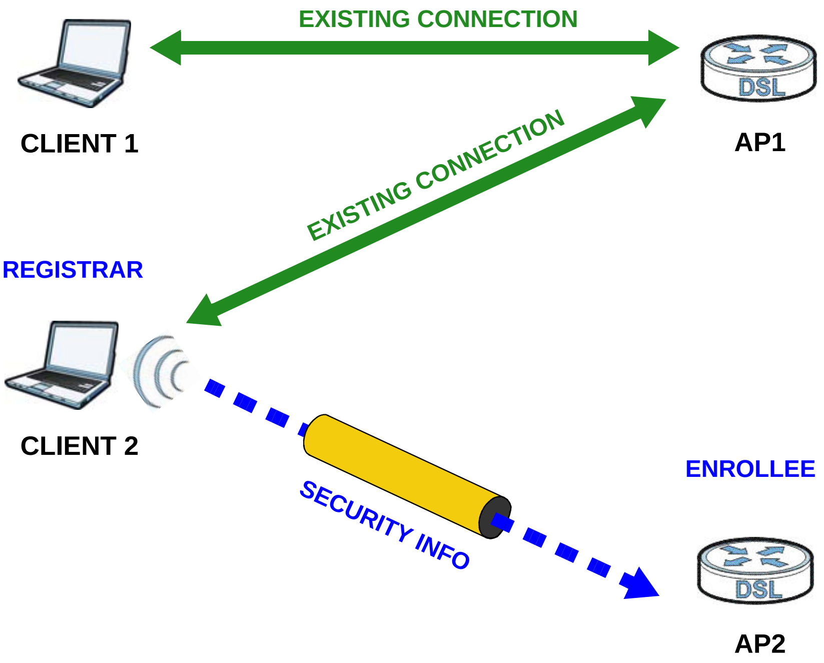
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the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

Figure 47 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 48 WPS: Example Network Step 3



7.10.9.5 Limitations of WPS

WPS has some limitations of which you should be aware.

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

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

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

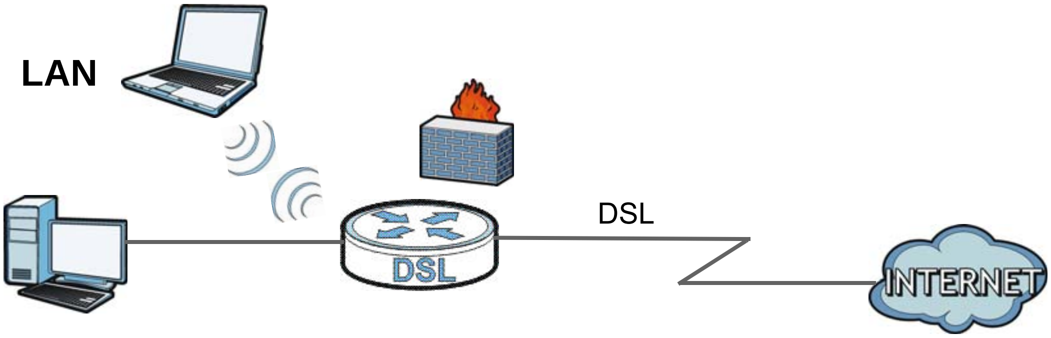
8

Home Networking

8.1 Overview

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

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



8.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your VMG (Section 8.2 on page 141).
- 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 144).
- Use the **UPnP** screen to enable UPnP and UPnP NAT traversal on the VMG (Section 8.4 on page 146).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 8.5 on page 148).
- Use the **STB Vendor ID** screen to have the VMG automatically create static DHCP entries for Set Top Box (STB) devices when they request IP addresses (Section 8.6 on page 150)
- Use the **Wake on Lan** screen to remotely turn on a device on the network. (Section 8.7 on page 150).
- Use the **TFTP Server** screen to identify a TFTP server for configuration file download using DHCP option 66. (Section 8.8 on page 151).

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 181 for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the 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 147 for examples of installing and using UPnP.

Finding Out More

See Section 8.9 on page 152 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.

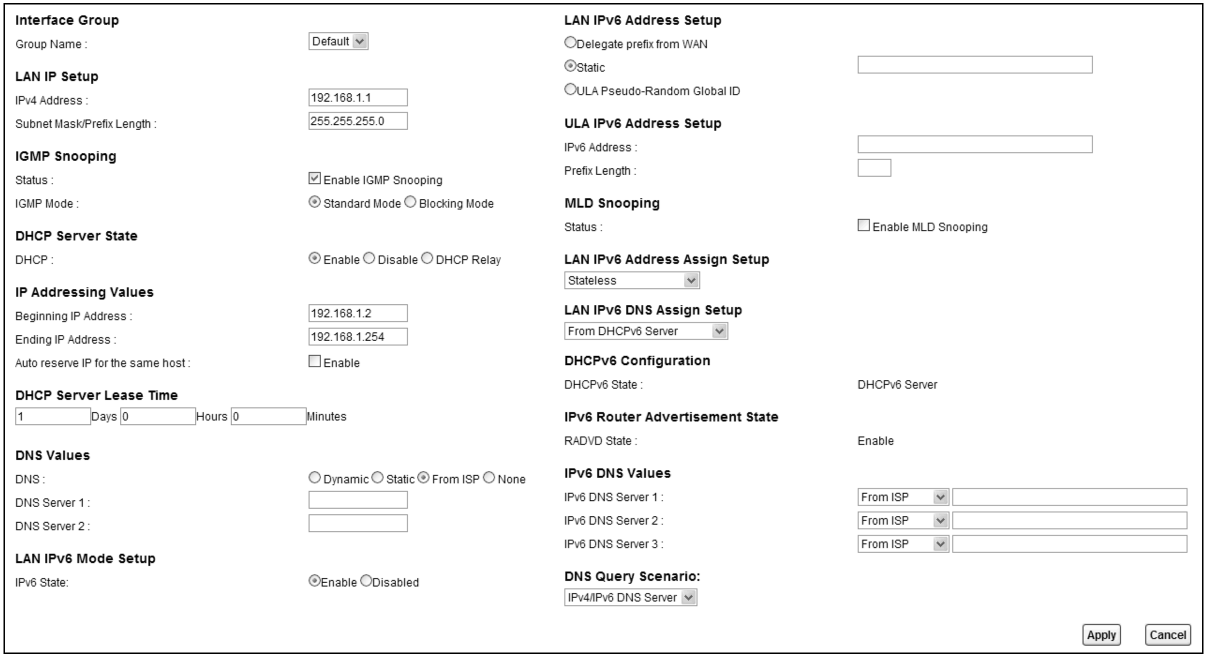
Follow these steps to configure your LAN settings.

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 49 Network Setting > Home Networking > LAN Setup



Interface Group

Group Name : Default

LAN IP Setup

IPv4 Address : 192.168.1.1

Subnet Mask/Prefix Length : 255.255.255.0

IGMP Snooping

Status : ☑ Enable IGMP Snooping

IGMP Mode : ● Standard Mode ○ Blocking Mode

DHCP Server State

DHCP : ● Enable ○ Disable ○ DHCP Relay

IP Addressing Values

Beginning IP Address : 192.168.1.2

Ending IP Address : 192.168.1.254

Auto reserve IP for the same host : □ Enable

DHCP Server Lease Time

1 Days 0 Hours 0 Minutes

DNS Values

DNS : ○ Dynamic ○ Static ● From ISP ○ None

DNS Server 1 :

DNS Server 2 :

LAN IPv6 Mode Setup

IPv6 State: ● Enable ○ Disabled

LAN IPv6 Address Setup

○ Delegate prefix from WAN

● Static

○ ULA Pseudo-Random Global ID

ULA IPv6 Address Setup

IPv6 Address :

Prefix Length :

MLD Snooping

Status : □ Enable MLD Snooping

LAN IPv6 Address Assign Setup

Stateless

LAN IPv6 DNS Assign Setup

From DHCPv6 Server

DHCPv6 Configuration

DHCPv6 State : DHCPv6 Server

IPv6 Router Advertisement State

RADVD State : 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

The following table describes the fields in this screen.

Table 30 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group name for which you want to configure LAN settings. See Chapter 14 on page 205 for how to create a new interface group.
LAN IP Setup	
IPv4 Address	Enter the LAN IPv4 IP address you want to assign to your VMG in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask/ Prefix Length	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your VMG automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
IGMP Snooping	
Status	Select the **Enable IGMP Snooping** checkbox to allows the VMG to passively learn multicast group.
IGMP Mode	Select **Standard Mode** to have the VMG forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to have the VMG block all unknown multicast packets from the WAN.
DHCP Server State	
DHCP	Select **Enable** to have the VMG act as a DHCP server or DHCP relay agent. Select **Disable** to stop the DHCP server on the VMG. Select **DHCP Relay** to have the VMG forward DHCP request to the DHCP server.
DHCP Relay Server Address	This field is only available when you select **DHCP Relay** in the **DHCP** field.
IPv4 Address	Enter the IPv4 IP address of the actual remote DHCP server in this field.

Table 30 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
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 the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic** if you have the Dynamic DNS service. Select **Static** if you have the Static DNS service.
DNS Server 1 DNS Server 2	Enter the first and second DNS (Domain Name System) server IP address the VMG passes to the DHCP clients.
LAN IPv6 Mode Setup	
IPv6 State	Select **Enable** to activate the IPv6 mode and configure IPv6 settings on the VMG.
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.
ULA Pseudo-Random Global ID	A unique local address (ULA) is a unique IPv6 address for use in private networks but not routable in the global IPv6 Internet. Select this to have the VMG automatically generate a globally unique address for the LAN IPv6 address. The address format is like fdxx:xxxx:xxxx:xxxx::/64.
ULA IPv6 Address Setup	
IPv6 Address	If you select static IPv6 address, enter the IPv6 address prefix that the VMG uses for the LAN IPv6 address.
Prefix Length	If you select static IPv6 address, enter the IPv6 prefix length that the VMG uses to generate the LAN IPv6 address. An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
MLD Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network. Select **Enable MLD Snooping** to activate MLD Snooping on the VMG. This allows the VMG to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.

Table 30 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
MLD Mode	Select **Standard Mode** to have the VMG forward IPv6 multicast packets to a port that joins the IPv6 multicast group and broadcast unknown IPv6 multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to have the VMG block all unknown IPv6 multicast packets from the WAN.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: • **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	Select how the VMG provide DNS server and domain name information to the clients: • **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 State	This shows the status of the DHCPv6.
IPv6 Router Advertisement State	
RADVD State	This shows whether RADVD is enabled or not.
IPv6 DNS Values	
IPv6 DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns IPv6 DNS server information. Select **User-Defined** if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the VMG passes to the DHCP clients. Select **None** if you do not want to configure IPv6 DNS servers.
DNS Query Scenario	Select how the VMG handles clients' DNS information requests. • **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.

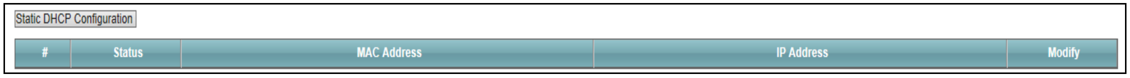
8.3 The Static DHCP Screen

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:A0:C5:00:00:02.

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

Figure 50 Network Setting > Home Networking > Static DHCP



Static DHCP Configuration

#	Status	MAC Address	IP Address	Modify

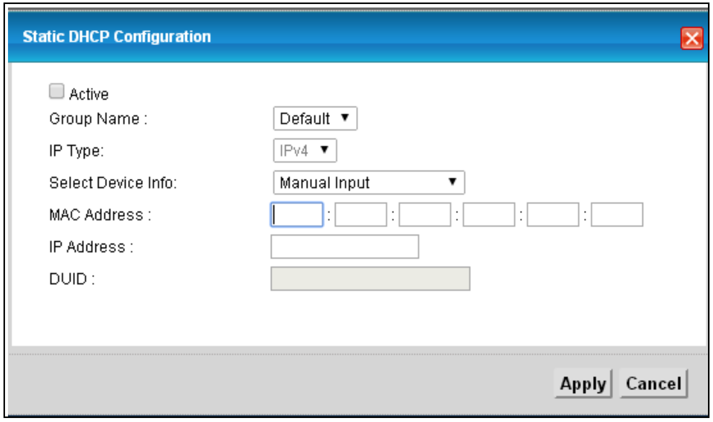
The following table describes the labels in this screen.

Table 31 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the VMG.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the **Edit** icon to have the IP address field editable and change it. Click the **Delete** icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

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

Figure 51 Static DHCP: Add/Edit



Static DHCP Configuration

□ Active

Group Name : Default

IP Type: IPv4

Select Device Info: Manual Input

MAC Address : __ : __ : __ : __ : __ : __

IP Address :

DUID :

The following table describes the labels in this screen.

Table 32 Static DHCP: Add/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 205 for how to create a new interface group.
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.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

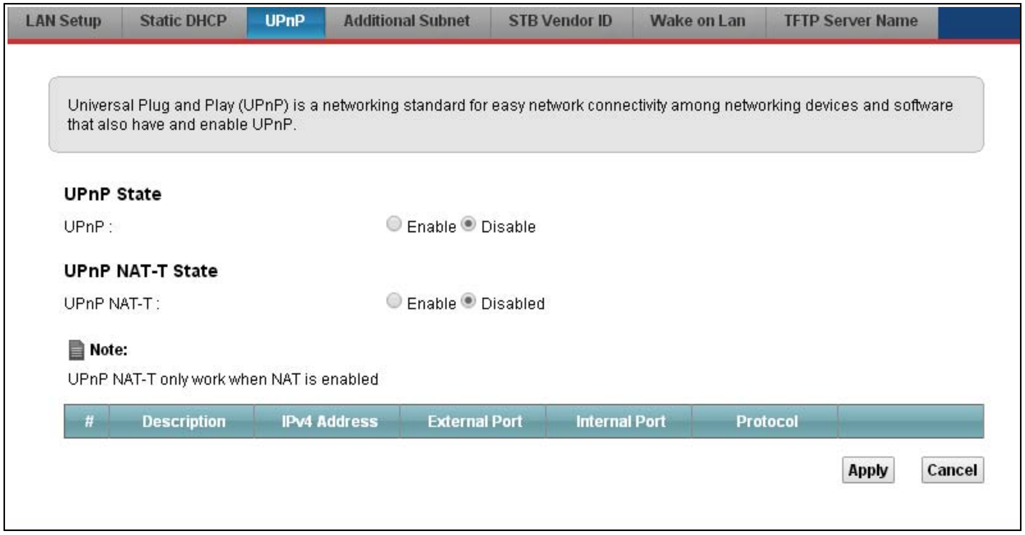
8.4 The UPnP Screen

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

See page 140 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 52 Network Setting > Home Networking > UPnP



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

UPnP State

UPnP : ○ Enable ● Disable

UPnP NAT-T State

UPnP NAT-T : ○ Enable ● Disabled

Note:

UPnP NAT-T only work when NAT is enabled

#	Description	IPv4 Address	External Port	Internal Port	Protocol

The following table describes the labels in this screen.

Table 33 Network Setting > Home Networking > UPnP

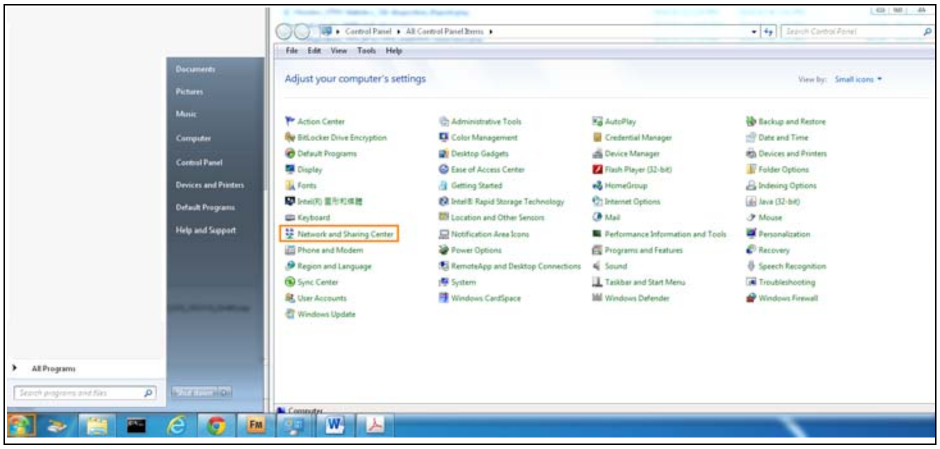
LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the VMG's IP address (although you must still enter the password to access the web configurator).
UPnP NAT-T	Select **Enable** to allow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

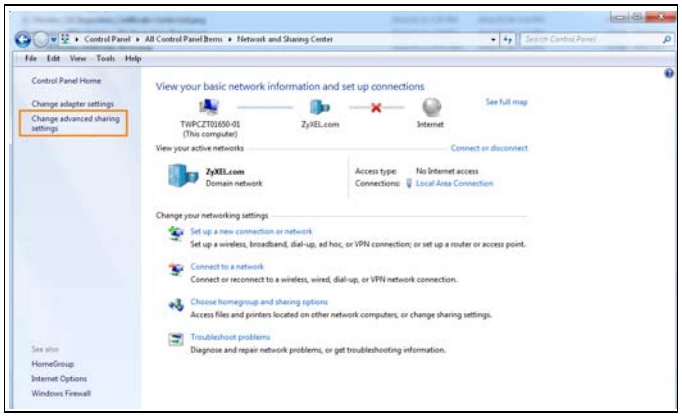
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the VMG.

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**.



View your basic network information and set up connections

View your active networks

ZyXEL.com
Domain network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

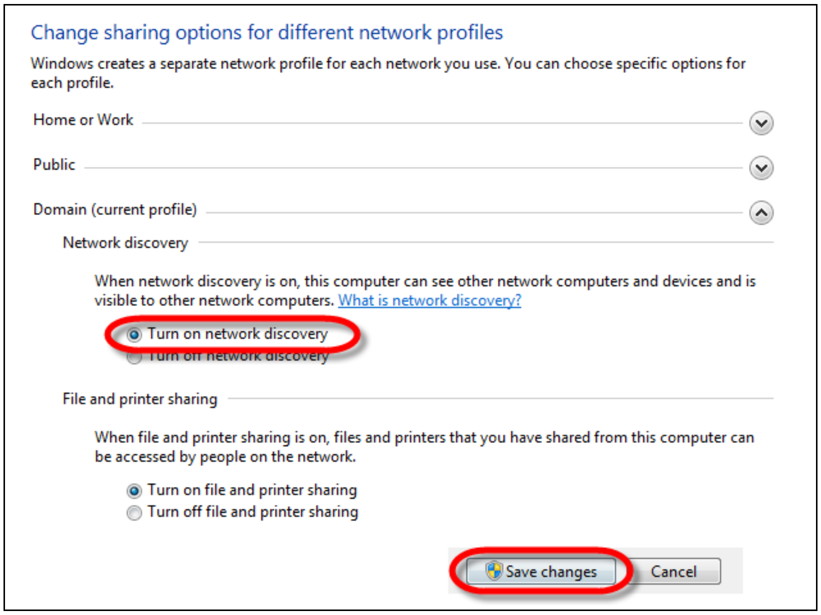
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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.



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public

Domain (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

8.5 The Additional Subnet Screen

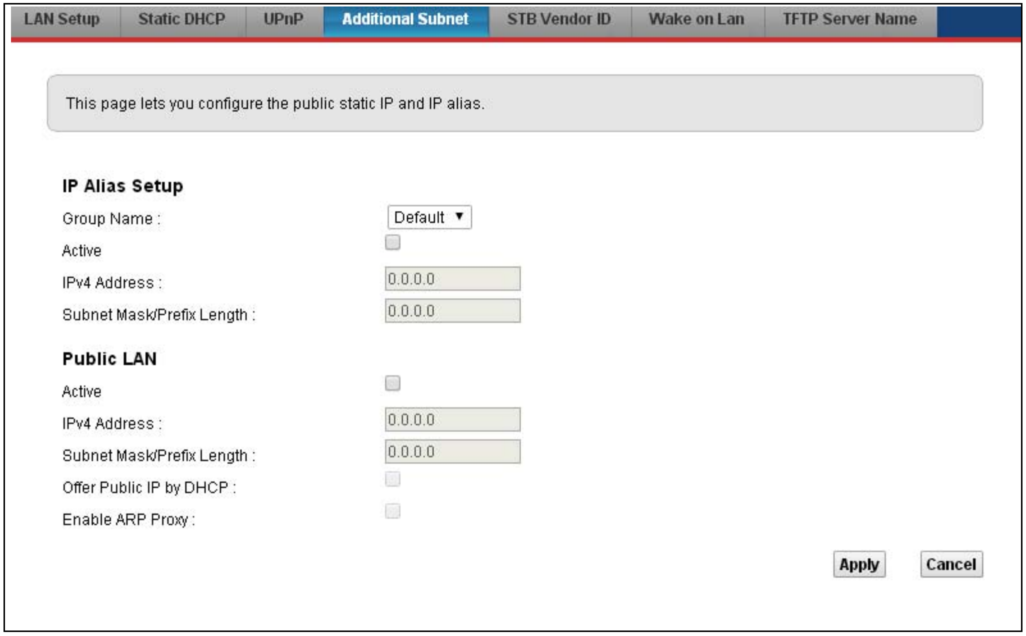
Use the **Additional Subnet** screen to configure IP alias and public static IP.

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 53 Network Setting > Home Networking > Additional Subnet



This page lets you configure the public static IP and IP alias.

IP Alias Setup

Group Name : Default ▼

Active □

IPv4 Address : 0.0.0.0

Subnet Mask/Prefix Length : 0.0.0.0

Public LAN

Active □

IPv4 Address : 0.0.0.0

Subnet Mask/Prefix Length : 0.0.0.0

Offer Public IP by DHCP : □

Enable ARP Proxy : □

The following table describes the labels in this screen.

Table 34 Network Setting > Home Networking > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings. See Chapter 14 on page 205 for how to create a new interface group.
Active	Select the checkbox to configure a LAN network for the VMG.
IP Address	Enter the IP address of your VMG in dotted decimal notation.
IP Subnet Mask	Your VMG will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the VMG.
Public LAN	
Active	Select the checkbox to enable the Public LAN feature. Your ISP must support Public LAN and Static IP.
IP Address	Enter the public IP address provided by your ISP.
IP Subnet Mask	Enter the public IP subnet mask provided by your ISP.
Offer Public IP by DHCP	Select the checkbox to enable the VMG to provide public IP addresses by DHCP server.
Enable ARP Proxy	Select the checkbox to enable the ARP (Address Resolution Protocol) proxy.

Table 34 Network Setting > Home Networking > Additional Subnet (continued)

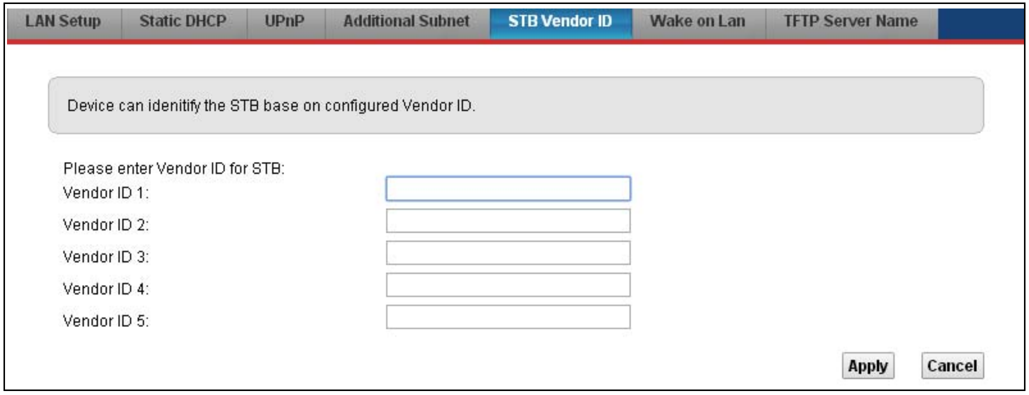
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

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 list the Vendor IDs of connected STBs to have the VMG automatically create static DHCP entries for them when they request IP addresses.

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

Figure 54 Network Setting > Home Networking > STB Vendor ID



Device can idenitify the STB base on configured Vendor ID.

Please enter Vendor ID for STB:

Vendor ID 1:

Vendor ID 2:

Vendor ID 3:

Vendor ID 4:

Vendor ID 5:

The following table describes the labels in this screen.

Table 35 Network Setting > Home Networking > STB Vendor ID

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

Note: The VMG needs to restart to make the role change take effect.

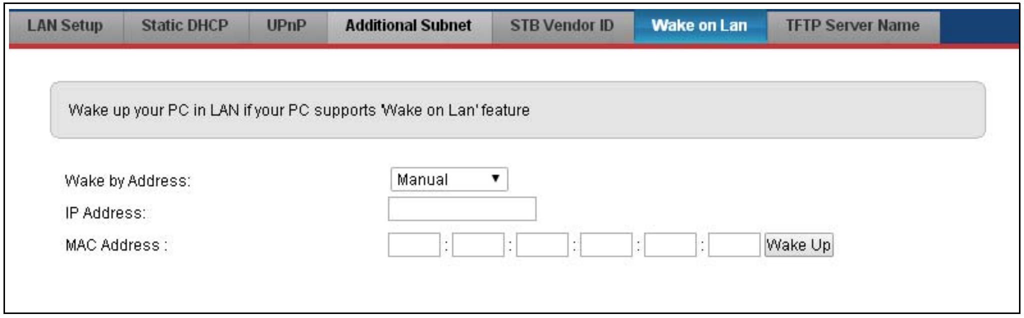
8.7 The Wake on LAN Screen

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 55 Network Setting > Home Networking > Wake on Lan



Wake up your PC in LAN if your PC supports 'Wake on Lan' feature

Wake by Address: Manual

IP Address:

MAC Address : : : : : :

The following table describes the labels in this screen.

Table 36 Network Setting > Home Networking > Wake on Lan

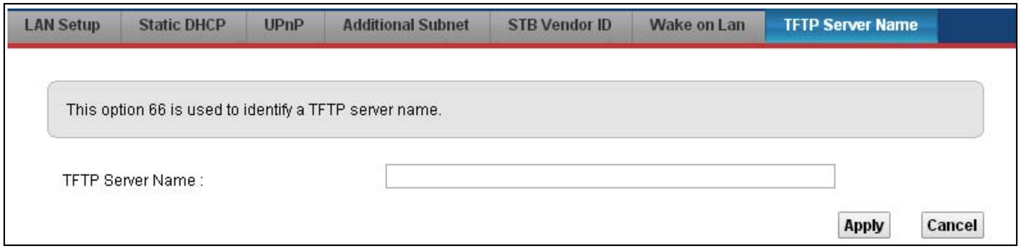
LABEL	DESCRIPTION
Wake by Address	Select **Manual** and enter the IP address or MAC address of the device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the VMG's ARP table. Select an IP address and it will then automatically update the IP address and MAC 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** screen to identify a TFTP server for configuration file download using DHCP option 66. RFC 2132 defines the option 66 open standard. DHCP option 66 supports the IP address or the hostname of a single TFTP server.

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

Figure 56 Network Setting > Home Networking > TFTP Server Name



This option 66 is used to identify a TFTP server name.

TFTP Server Name :

The following table describes the labels in this screen.

Table 37 Network Setting > Home Networking > TFTP Server Name

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

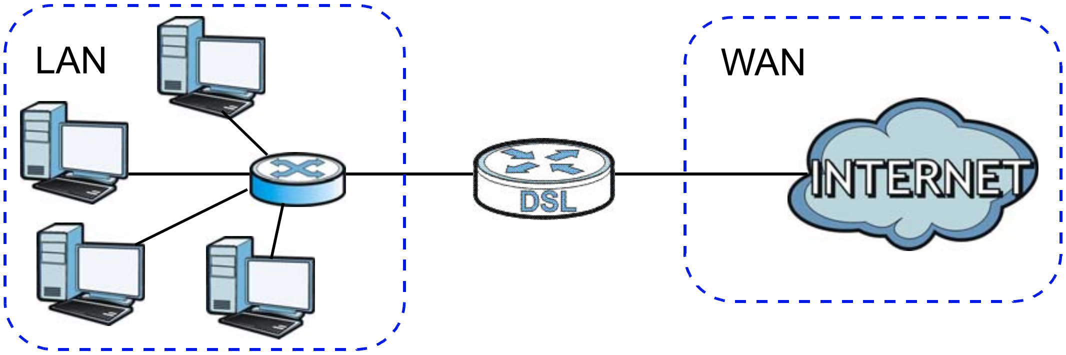
8.9 Technical Reference

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 57 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”.

9

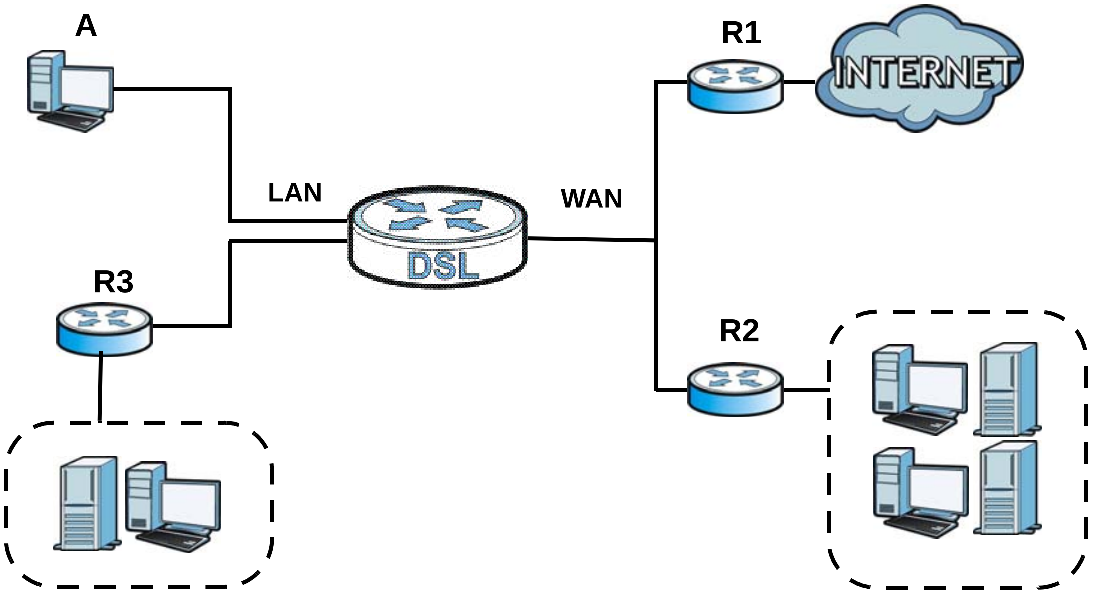
Routing

9.1 Overview

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

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

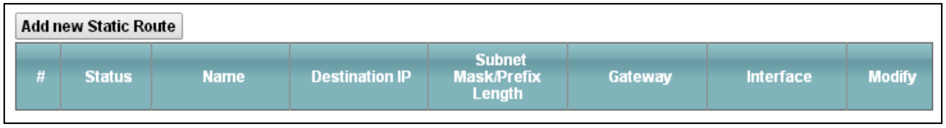
Figure 58 Example of Routing Topology



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 59 Network Setting > Routing > Static Route



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

The following table describes the labels in this screen.

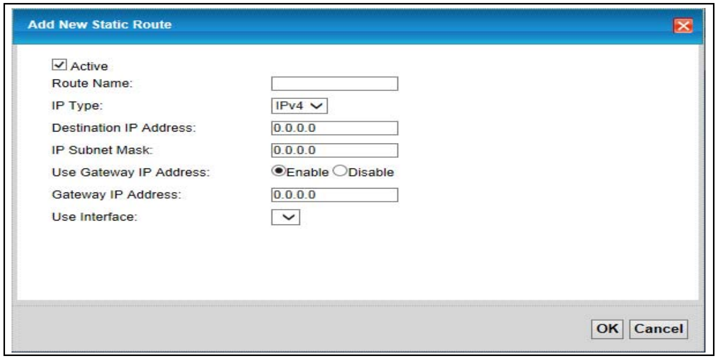
Table 38 Network Setting > Routing > Static Route

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 60 Routing: Add/Edit



☑ Active

Route Name:

IP Type: IPv4

Destination IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

Use Gateway IP Address: ● Enable ○ Disable

Gateway IP Address: 0.0.0.0

Use Interface:

The following table describes the labels in this screen.

Table 39 Routing: Add/Edit (Sheet 1 of 2)

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route. Select this to enable the static route. Clear this to disable 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.

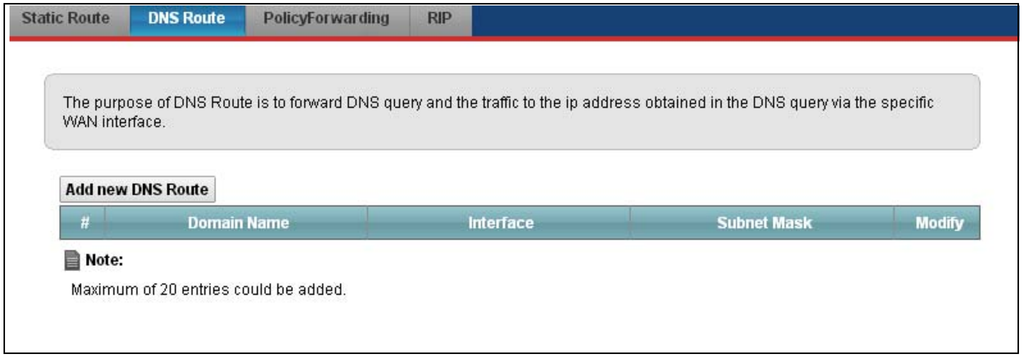
Table 39 Routing: Add/Edit (Sheet 2 of 2)

LABEL	DESCRIPTION
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.
Apply	Click **Apply** 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 61 Network Setting > Routing > DNS Route



The purpose of DNS Route is to forward DNS query and the traffic to the ip address obtained in the DNS query via the specific WAN interface.

#	Domain Name	Interface	Subnet Mask	Modify

Note:

Maximum of 20 entries could be added.

The following table describes the labels in this screen.

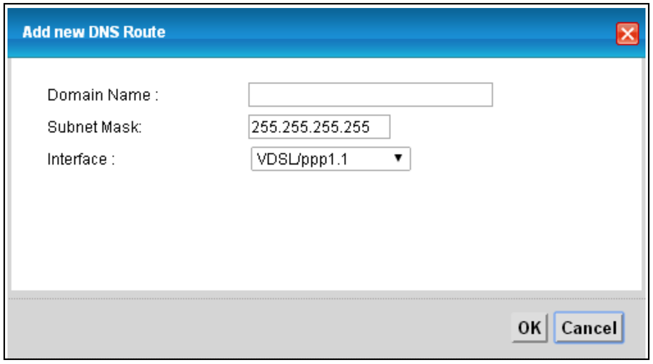
Table 40 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add new DNS Route	Click this to add a new DNS route.
#	This is the index number of a DNS route.
Domain Name	This is the host name or domain name of the DNS route entry.
Interface	This is the WAN connection through which the VMG forwards DNS requests for this domain name.
Subnet Mask	This is the subnet mask of the DNS route entry.
Modify	Click the **Edit** icon to modify the DNS route. Click the **Delete** icon to delete the DNS route.

9.3.1 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 62 DNS Route Add



Add new DNS Route

Domain Name :

Subnet Mask: 255.255.255.255

Interface : VDSL/ppp1.1

The following table describes the labels in this screen.

Table 41 DNS Route Add

LABEL	DESCRIPTION
Domain Name	Enter the domain name of the DNS route entry.
Interface	Select the WAN connection through which the VMG forwards DNS requests for this domain name.
Subnet Mask	Enter the subnet mask of the DNS route entry.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving any changes.

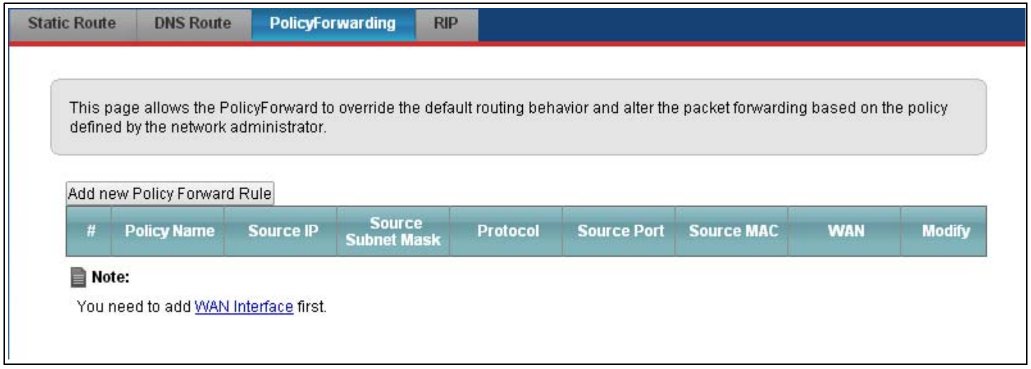
9.4 The Policy Forwarding Screen

Traditionally, routing is based on the destination address only and the VMG takes the shortest path to forward a packet. Policy forwarding 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 Forwarding** screen let you view and configure routing policies on the VMG. Click **Network Setting > Routing > Policy Forwarding** to open the following screen.

Figure 63 Network Setting > Routing > Policy Forwarding



This page allows the PolicyForward to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

#	Policy Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	WAN	Modify

Note:

You need to add WAN Interface first.

The following table describes the labels in this screen.

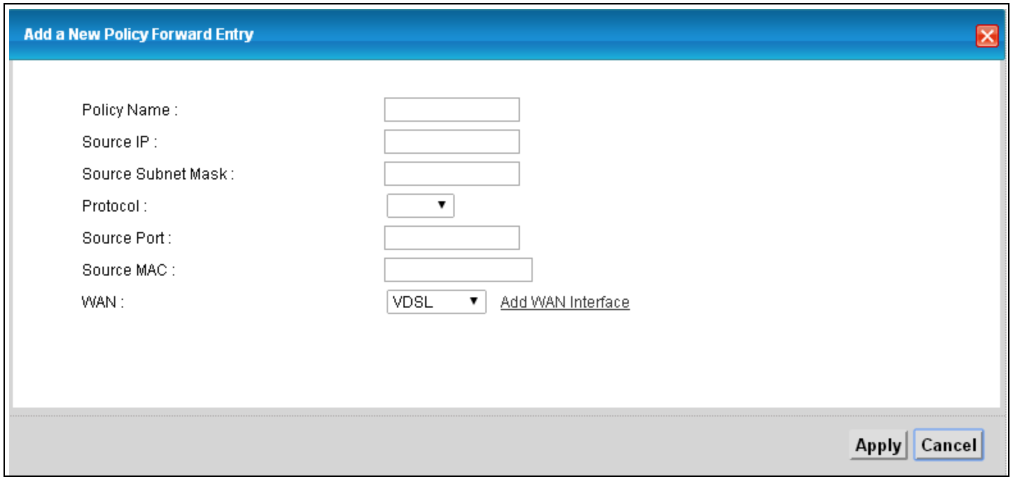
Table 42 Network Setting > Routing >Policy Forwarding

LABEL	DESCRIPTION
Add new Policy Forward Rule	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.
Policy Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	his is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
WAN	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 Forwarding

Click **Add new Policy Forward Rule** in the **Policy Forwarding** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 64 Policy Forwarding: Add/Edit



Add a New Policy Forward Entry

Policy Name :	
Source IP :	
Source Subnet Mask :	
Protocol :	
Source Port :	
Source MAC :	
WAN :	VDSL

The following table describes the labels in this screen.

Table 43 Policy Forwarding: Add/Edit

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP	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.
WAN	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screens.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

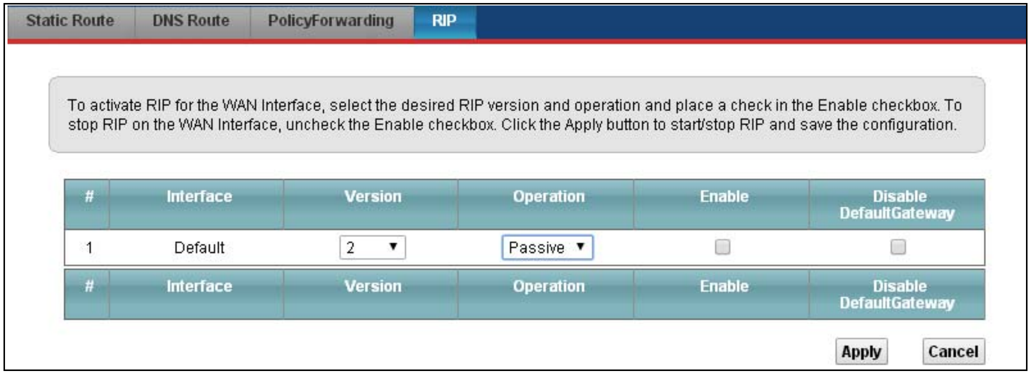
9.5 RIP

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 65 RIP



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

#	Interface	Version	Operation	Enable	Disable DefaultGateway
1	Default	2 ▼	Passive ▼	□	□
#	Interface	Version	Operation	Enable	Disable DefaultGateway

The following table describes the labels in this screen.

Table 44 RIP

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

10

Quality of Service (QoS)

10.1 Overview

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

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

1 Configure classifiers to sort traffic into different flows.

2 Assign priority and define actions to be performed for a classified traffic flow.

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

This chapter contains information about configuring QoS and editing classifiers.

10.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 10.3 on page 165).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 10.4 on page 166).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 10.5 on page 168).
- The **Policer Setup** screen lets you add, edit or delete QoS policers (Section 10.5 on page 168).

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.

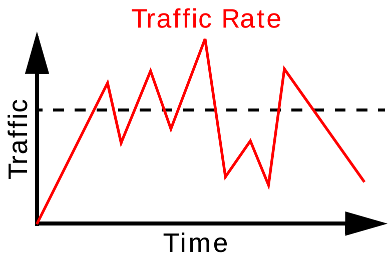
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

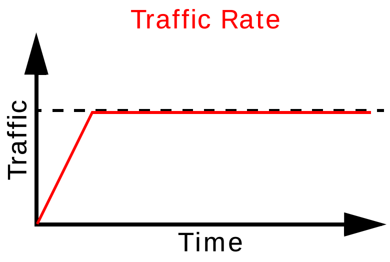
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or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



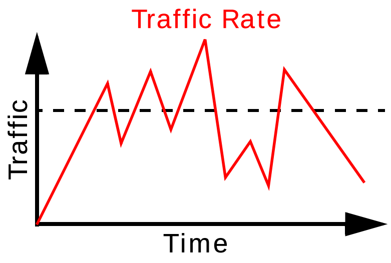
(Before Traffic Shaping)



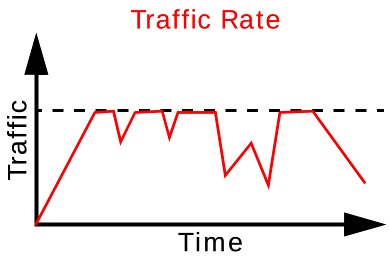
(After Traffic Shaping)

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.



(Before Traffic Policing)



(After Traffic Policing)

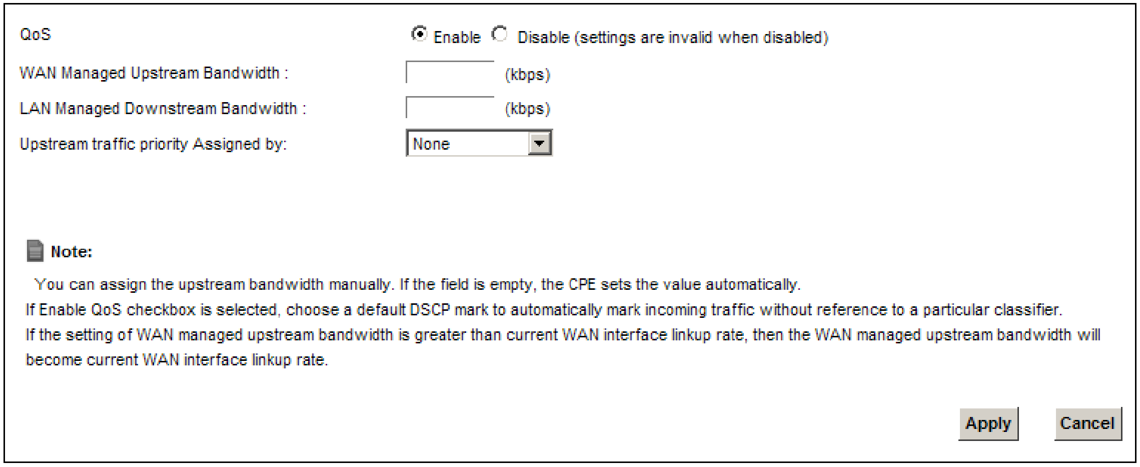
The VMG supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 10.7 on page 175 for more information on each metering algorithm.

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 163 for more information.

Figure 66 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 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.

The following table describes the labels in this screen.

Table 45 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	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. 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. 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. 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. If you leave this field blank, the VMG automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.

Table 45 Network Setting > QoS > General (continued) (continued)

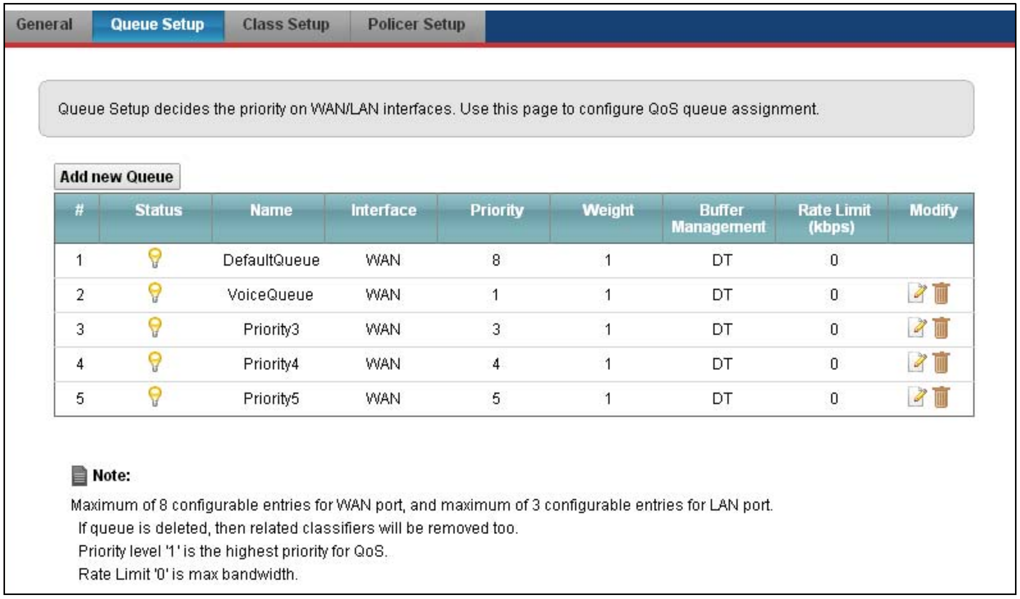
LABEL	DESCRIPTION
LAN Managed Downstream Bandwidth	Enter the amount of downstream bandwidth for the LAN interfaces (including WLAN) that you want to allocate using QoS. The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection. 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. If you leave this field blank, the VMG automatically sets this to the LAN interfaces' maximum supported connection speed.
Upstream traffic priority Assigned by	Select how the VMG assigns priorities to various upstream traffic flows. • **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 67 Network Setting > QoS > Queue Setup



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

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit (kbps)	Modify
1	💡	DefaultQueue	WAN	8	1	DT	0	
2	💡	VoiceQueue	WAN	1	1	DT	0	✎🗑
3	💡	Priority3	WAN	3	1	DT	0	✎🗑
4	💡	Priority4	WAN	4	1	DT	0	✎🗑
5	💡	Priority5	WAN	5	1	DT	0	✎🗑

Note:

Maximum of 8 configurable entries for WAN port, and maximum of 3 configurable entries for LAN port.
If queue is deleted, then related classifiers will be removed too.
Priority level '1' is the highest priority for QoS.
Rate Limit '0' is max bandwidth.

The following table describes the labels in this screen.

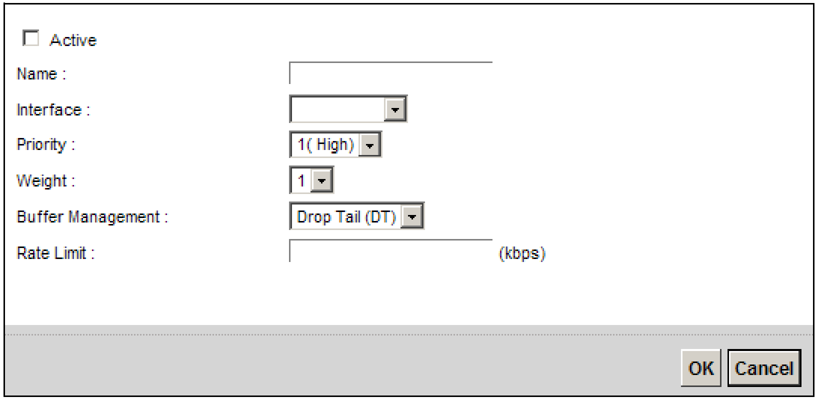
Table 46 Network Setting > QoS > Queue Setup

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 68 Queue Setup: Add



□ Active

Name :

Interface :

Priority : 1(High)

Weight : 1

Buffer Management : Drop Tail (DT)

Rate Limit : (kbps)

The following table describes the labels in this screen.

Table 47 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.

Table 47 Queue Setup: Add (continued)

LABEL	DESCRIPTION
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.

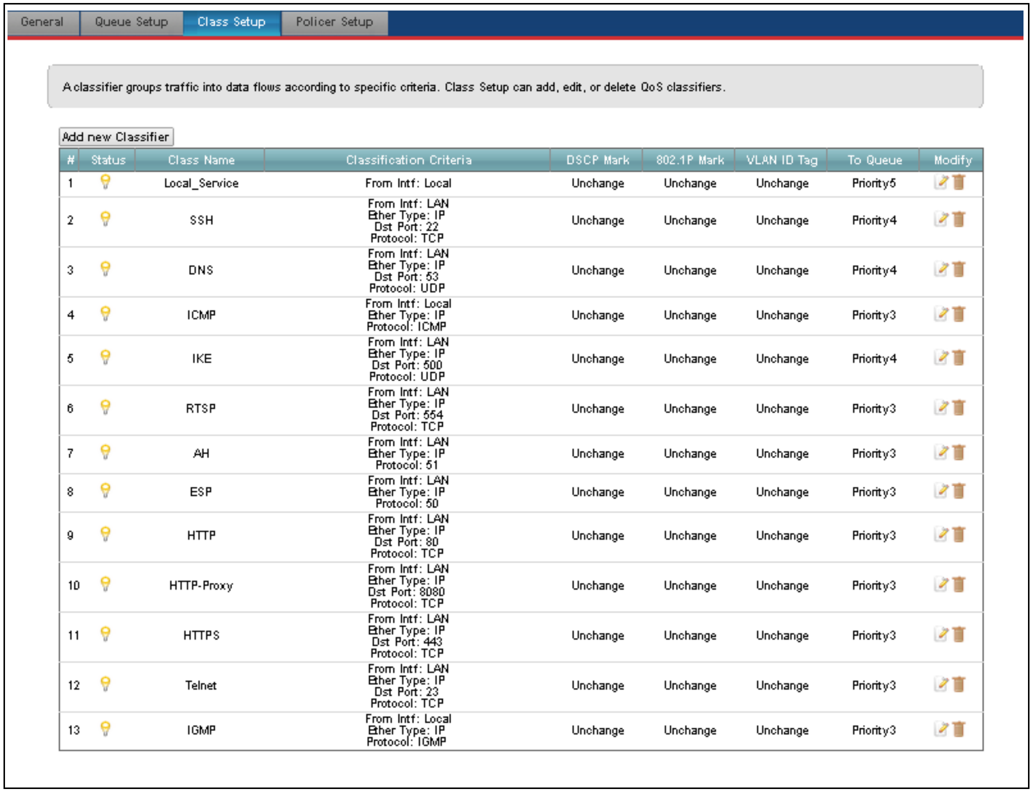
10.5 The Class Setup Screen

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

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

Figure 69 Network Setting > QoS > Class Setup



A classifier groups traffic into data flows according to specific criteria. Class Setup can add, edit, or delete QoS classifiers.

Add new Classifier

#	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
1	💡	Local_Service	From Intf: Local	Unchange	Unchange	Unchange	Priority5	✎ 🗑
2	💡	SSH	From Intf: LAN Ether Type: IP Dst Port: 22 Protocol: TCP	Unchange	Unchange	Unchange	Priority4	✎ 🗑
3	💡	DNS	From Intf: LAN Ether Type: IP Dst Port: 53 Protocol: UDP	Unchange	Unchange	Unchange	Priority4	✎ 🗑
4	💡	ICMP	From Intf: Local Ether Type: IP Protocol: ICMP	Unchange	Unchange	Unchange	Priority3	✎ 🗑
5	💡	IKE	From Intf: LAN Ether Type: IP Dst Port: 500 Protocol: UDP	Unchange	Unchange	Unchange	Priority4	✎ 🗑
6	💡	RTSP	From Intf: LAN Ether Type: IP Dst Port: 554 Protocol: TCP	Unchange	Unchange	Unchange	Priority3	✎ 🗑
7	💡	AH	From Intf: LAN Ether Type: IP Protocol: 51	Unchange	Unchange	Unchange	Priority3	✎ 🗑
8	💡	ESP	From Intf: LAN Ether Type: IP Protocol: 50	Unchange	Unchange	Unchange	Priority3	✎ 🗑
9	💡	HTTP	From Intf: LAN Ether Type: IP Dst Port: 80 Protocol: TCP	Unchange	Unchange	Unchange	Priority3	✎ 🗑
10	💡	HTTP-Proxy	From Intf: LAN Ether Type: IP Dst Port: 8080 Protocol: TCP	Unchange	Unchange	Unchange	Priority3	✎ 🗑
11	💡	HTTPS	From Intf: LAN Ether Type: IP Dst Port: 443 Protocol: TCP	Unchange	Unchange	Unchange	Priority3	✎ 🗑
12	💡	Telnet	From Intf: LAN Ether Type: IP Dst Port: 23 Protocol: TCP	Unchange	Unchange	Unchange	Priority3	✎ 🗑
13	💡	IGMP	From Intf: Local Ether Type: IP Protocol: IGMP	Unchange	Unchange	Unchange	Priority3	✎ 🗑

The following table describes the labels in this screen.

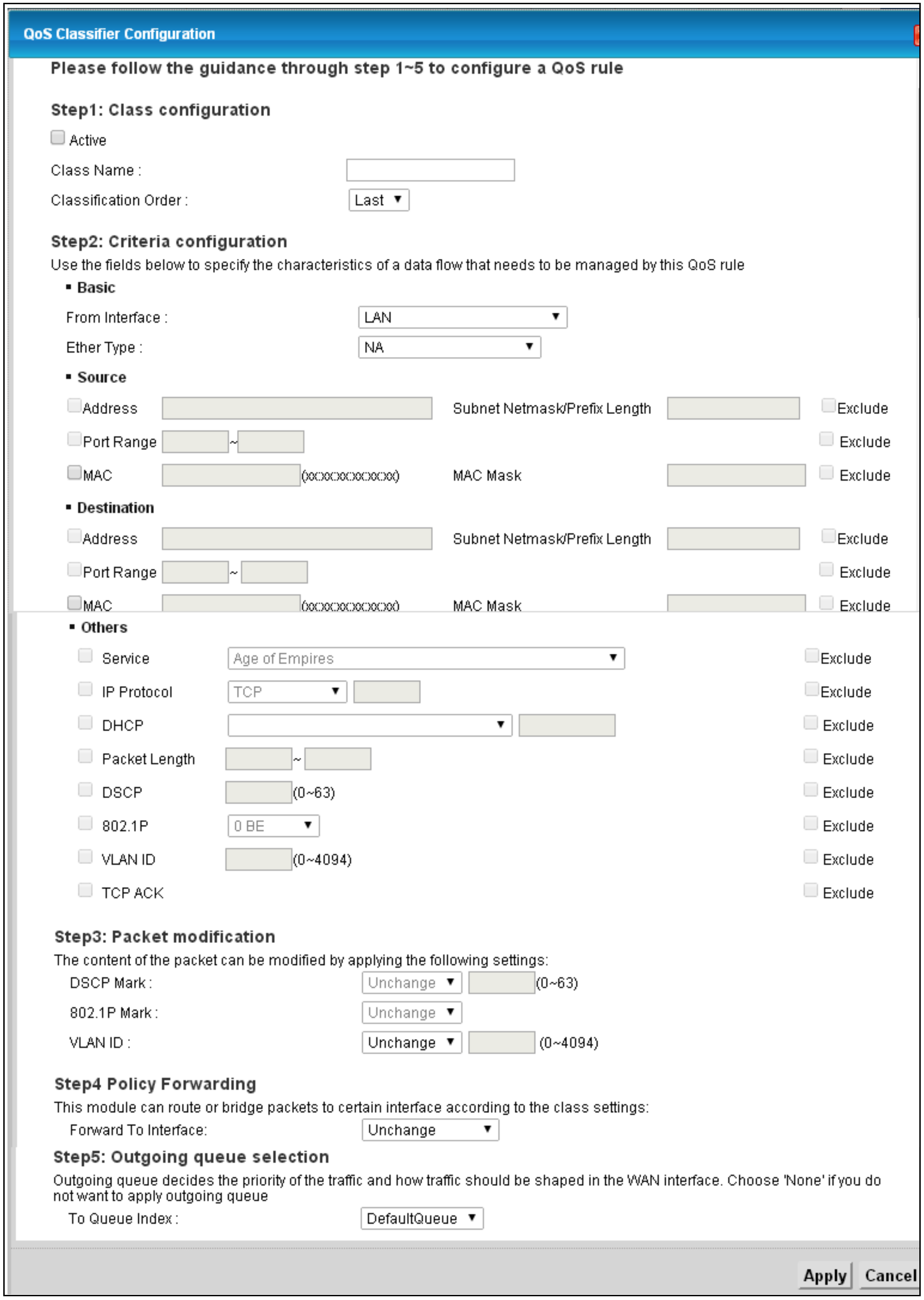
Table 48 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
#	This is the index number of the entry.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
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 Classifier** in the **Class Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 70 Class Setup: Add/Edit



QoS Classifier Configuration

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

Step1: Class configuration

□ Active

Class Name :

Classification Order : Last

Step2: Criteria configuration

Use the fields below to specify the characteristics of a data flow that needs to be managed by this QoS rule

- Basic

From Interface : LAN

Ether Type : NA

- Source

□ Address — Subnet Netmask/Prefix Length — □ Exclude

□ Port Range ~ — □ Exclude

□ MAC (xx:xx:xx:xx:xx:xx) — MAC Mask — □ Exclude

- Destination

□ Address — Subnet Netmask/Prefix Length — □ Exclude

□ Port Range ~ — □ Exclude

□ MAC (xx:xx:xx:xx:xx:xx) — MAC Mask — □ Exclude

- Others

□ Service: Age of Empires — □ Exclude

□ IP Protocol: TCP — □ Exclude

□ DHCP — □ Exclude

□ Packet Length ~ — □ Exclude

□ DSCP (0~63) — □ Exclude

□ 802.1P: 0 BE — □ 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 : Unchange (0~63)

802.1P Mark : Unchange

VLAN ID : Unchange (0~4094)

Step4 Policy Forwarding

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

Forward To Interface: Unchange

Step5: Outgoing queue selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface. Choose 'None' if you do not want to apply outgoing queue

To Queue Index : DefaultQueue

The following table describes the labels in this screen.

Table 49 Class Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select this to enable this classifier.
Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.

Table 49 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
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.
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 Netmask	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 source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	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.
Others	
Service	This field is available only when you select **IP** in the **Ether Type** field. 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.

Table 49 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. 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.
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. 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. 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.
Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. 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.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
DSCP Mark	This field is available only when you select **IP** in the **Ether Type** field. If you select **Mark**, enter a DSCP value with which the VMG replaces the DSCP field in the packets. If you select **Unchange**, the VMG keep the DSCP field in the packets.
802.1P Mark	Select a priority level with which the VMG replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the VMG keep the 802.1p priority field in the packets.
VLAN ID	If you select **Remark**, enter a VLAN ID number with which the VMG replaces the VLAN ID of the frames. If you select **Remove**, the VMG deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the VMG treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the VMG keep the VLAN ID in the packets.
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.
To Queue Index	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.

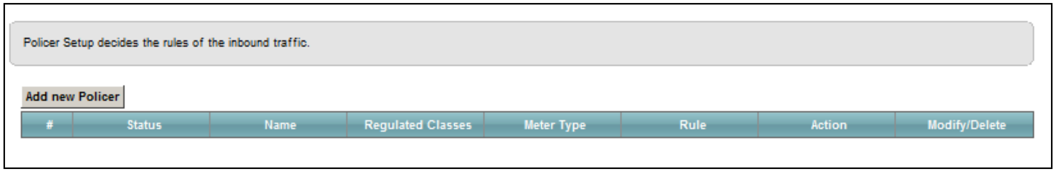
Table 49 Class Setup: Add/Edit (continued)

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

10.6 The QoS Policer Setup Screen

Use this screen to configure QoS policers that allow you to limit the transmission rate of incoming traffic. Click **Network Setting > QoS > Policer Setup**. The screen appears as shown.

Figure 71 Network Setting > QoS > Policer Setup



Policer Setup decides the rules of the inbound traffic.

The following table describes the labels in this screen.

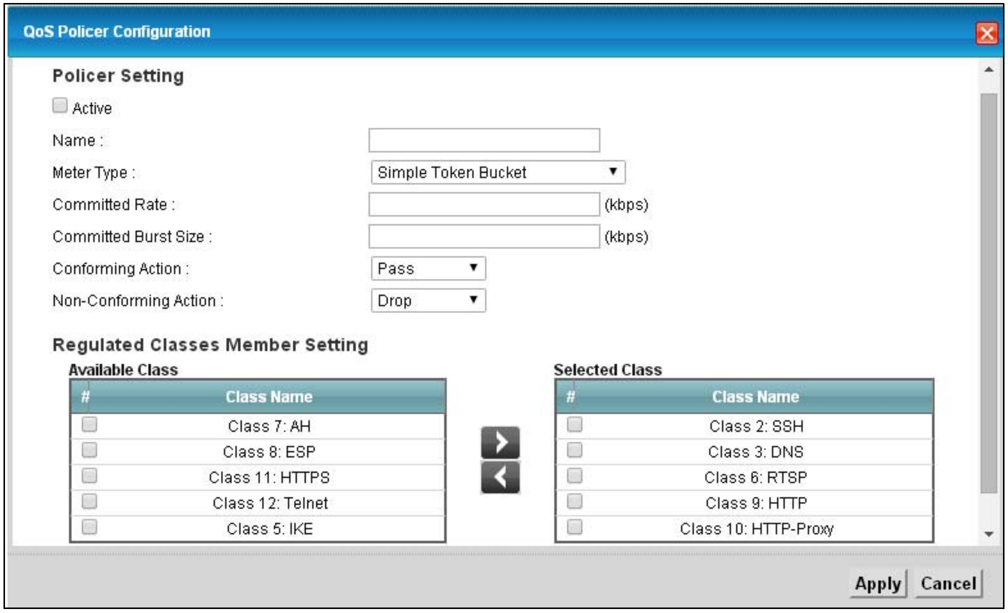
Table 50 Network Setting > QoS > Policer Setup

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

10.6.1 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 72 Policer Setup: Add/Edit



QoS Policer Configuration

Policer Setting

□ Active

Name :

Meter Type : Simple Token Bucket

Committed Rate : (kbps)

Committed Burst Size : (kbps)

Conforming Action : Pass

Non-Conforming Action : Drop

Regulated Classes Member Setting

Available Class

#	Class Name
□	Class 7: AH
□	Class 8: ESP
□	Class 11: HTTPS
□	Class 12: Telnet
□	Class 5: IKE

Selected Class

#	Class Name
□	Class 2: SSH
□	Class 3: DNS
□	Class 6: RTSP
□	Class 9: HTTP
□	Class 10: HTTP-Proxy

The following table describes the labels in this screen.

Table 51 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select the check box to activate this policer.
Name	Enter the descriptive name of this policer.
Meter Type	This shows the traffic metering algorithm used in this policer. 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 *b* bytes which is also the bucket size. 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). 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).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.

Table 51 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Conforming Action	Specify what the VMG does for packets within the committed rate and burst size (green-marked packets). • **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	Specify what the VMG does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). • **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 Selected Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. Highlight a QoS classifier in the **Available Class** box and use the **>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **<** button.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.7 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 52 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”.

Table 52 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
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 53 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.

11

Network Address Translation (NAT)

11.1 Overview

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

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 11.2 on page 182).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network (Section 11.3 on page 185).
- Use the **Port Triggering** screen to add and configure the VMG’s trigger port settings (Section 11.4 on page 187).
- Use the **DMZ** screen to configure a default server (Section 11.5 on page 189).
- Use the **ALG** screen to enable and disable the NAT and SIP (VoIP) ALG in the VMG (Section 11.6 on page 190).
- Use the **Address Mapping** screen to configure the VMG's address mapping settings (Section 11.7 on page 191).
- Use the **Sessions** screen to configure the VMG's maximum number of NAT sessions (Section 11.7 on page 191).

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 193 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.

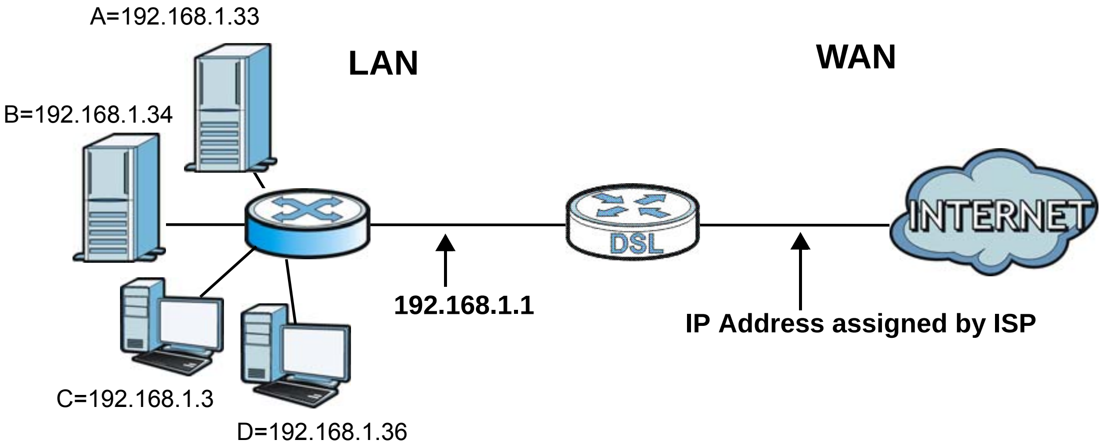
The most often used port numbers and services are shown in Appendix D on page 383. Please refer to RFC 1700 for further information about port numbers.

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.

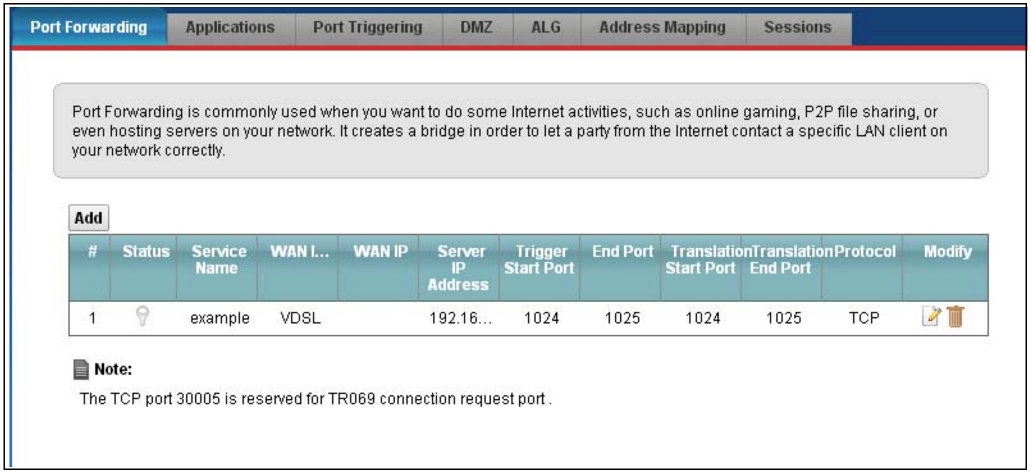
Figure 73 Multiple Servers Behind NAT Example



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

See Appendix D on page 383 for port numbers commonly used for particular services.

Figure 74 Network Setting > NAT > Port Forwarding



Port Forwarding is commonly used when you want to do some Internet activities, such as online gaming, P2P file sharing, or even hosting servers on your network. It creates a bridge in order to let a party from the Internet contact a specific LAN client on your network correctly.

#	Status	Service Name	WAN I...	WAN IP	Server IP Address	Trigger Start Port	End Port	Translation Start Port	Translation End Port	Protocol	Modify
1	💡	example	VDSL		192.16...	1024	1025	1024	1025	TCP	✎ 🗑

Note:

The TCP port 30005 is reserved for TR069 connection request port .

The following table describes the fields in this screen.

Table 54 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.

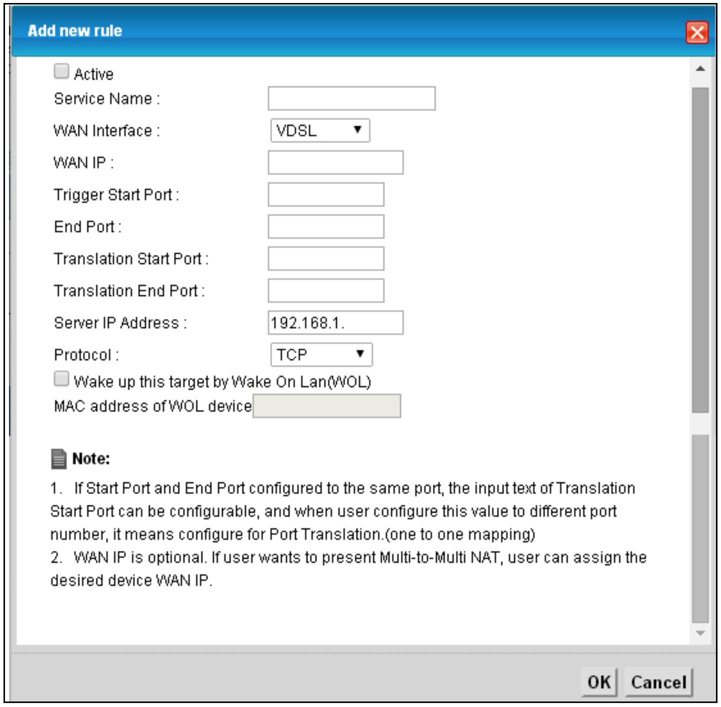
Table 54 Network Setting > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
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 75 Port Forwarding: Add/Edit



Add new rule

□ Active

Service Name :

WAN Interface : VDSL

WAN IP :

Trigger Start Port :

End Port :

Translation Start Port :

Translation End Port :

Server IP Address : 192.168.1.

Protocol : TCP

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

MAC address of WOL device

Note:

1. If Start Port and End Port configured to the same port, the input text of Translation Start Port can be configurable, and when user configure this value to different port number, it means configure for Port Translation.(one to one mapping)

2. WAN IP is optional. If user wants to present Multi-to-Multi NAT, user can assign the desired device WAN IP.

The following table describes the labels in this screen.

Table 55 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Clear the checkbox to disable the rule. Select the check box to enable it.
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.

Table 55 Port Forwarding: Add/Edit (continued)

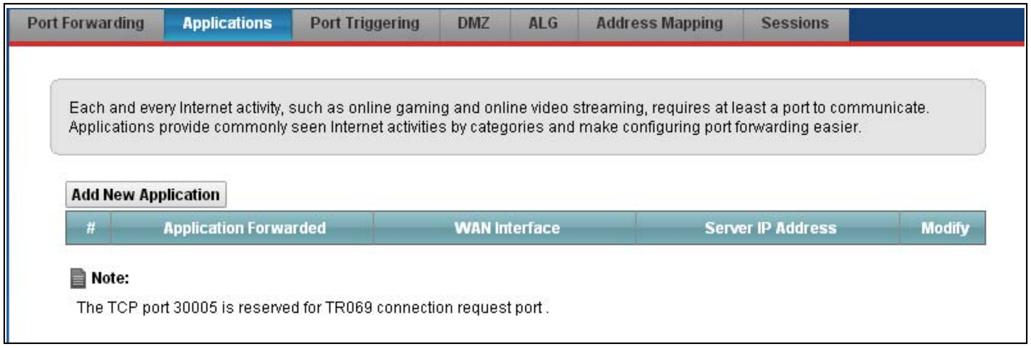
LABEL	DESCRIPTION
WAN IP	Enter the WAN IP address for which the incoming service is destined. If the packet's destination IP address doesn't match the one specified here, the port forwarding rule will not be applied.
Start Port	Enter the original destination port for the packets. To forward only one 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.
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**.
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 76 Network Setting > NAT > Applications



Each and every Internet activity, such as online gaming and online video streaming, requires at least a port to communicate. Applications provide commonly seen Internet activities by categories and make configuring port forwarding easier.

#	Application Forwarded	WAN Interface	Server IP Address	Modify

Note:

The TCP port 30005 is reserved for TR069 connection request port .

The following table describes the labels in this screen.

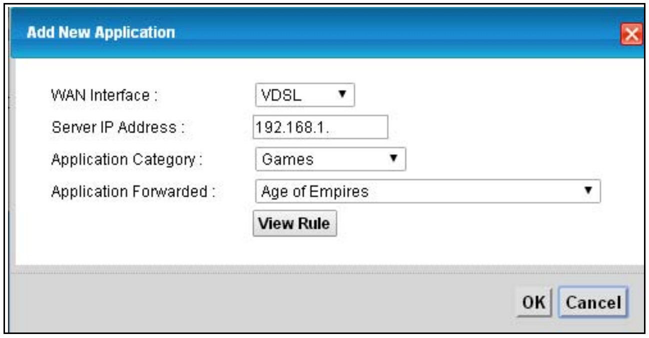
Table 56 Network Setting > NAT > Applications

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 77 Applications: Add



Add New Application

WAN Interface : VDSL

Server IP Address : 192.168.1.

Application Category : Games

Application Forwarded : Age of Empires

The following table describes the labels in this screen.

Table 57 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 Rule	Click this to display the configuration of the service that you have chosen in **Application Fowarded**.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

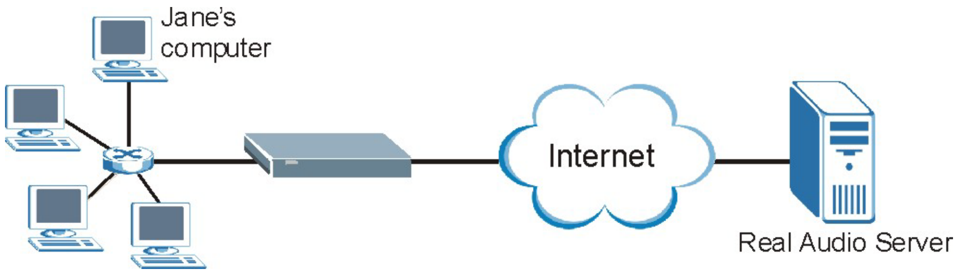
11.4 The Port Triggering Screen

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 78 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.

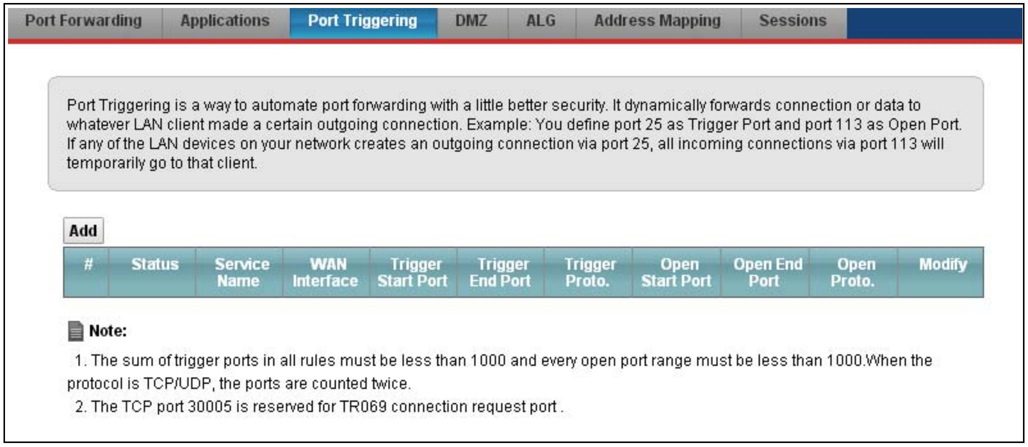
3 The Real Audio server responds using a port number ranging between 6970-7170.

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 79 Network Setting > NAT > Port Triggering



Port Triggering is a way to automate port forwarding with a little better security. It dynamically forwards connection or data to whatever LAN client made a certain outgoing connection. Example: You define port 25 as Trigger Port and port 113 as Open Port. If any of the LAN devices on your network creates an outgoing connection via port 25, all incoming connections via port 113 will temporarily go to that client.

#	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 30005 is reserved for TR069 connection request port .

The following table describes the labels in this screen.

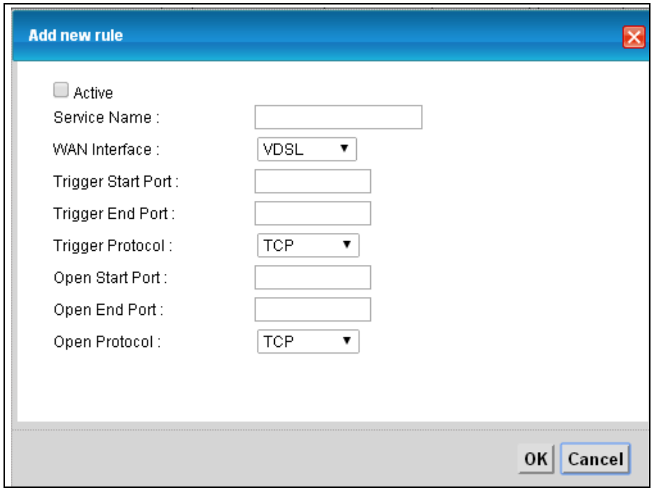
Table 58 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the VMG to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The VMG forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Proto.	This is the open transport layer protocol.
Modify	Click the **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 80 Port Triggering: Add/Edit



□ Active

Service Name :

WAN Interface : VDSL ▼

Trigger Start Port :

Trigger End Port :

Trigger Protocol : TCP ▼

Open Start Port :

Open End Port :

Open Protocol : TCP ▼

The following table describes the labels in this screen.

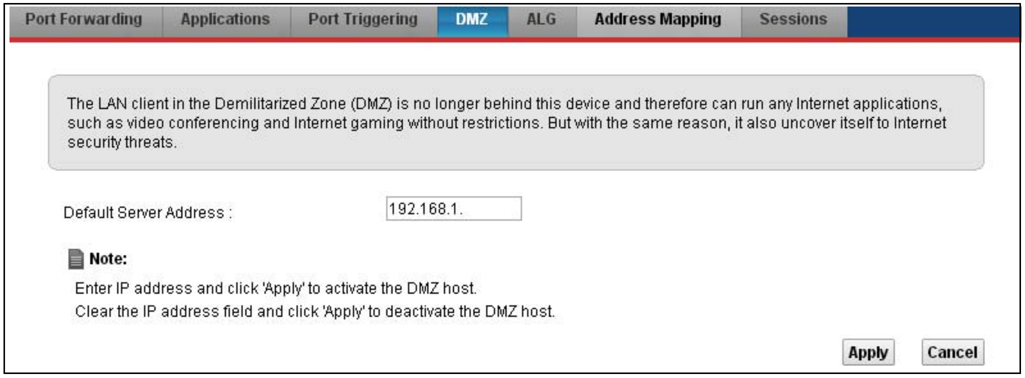
Table 59 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select the check box to enable 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.
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**, **UDP**, or **TCP/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**, **UDP**, or **TCP/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 81 Network Setting > NAT > DMZ



The LAN client in the Demilitarized Zone (DMZ) is no longer behind this device and therefore can run any Internet applications, such as video conferencing and Internet gaming without restrictions. But with the same reason, it also uncover itself to Internet security threats.

Default Server Address : 192.168.1.

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 60 Network Setting > NAT > DMZ

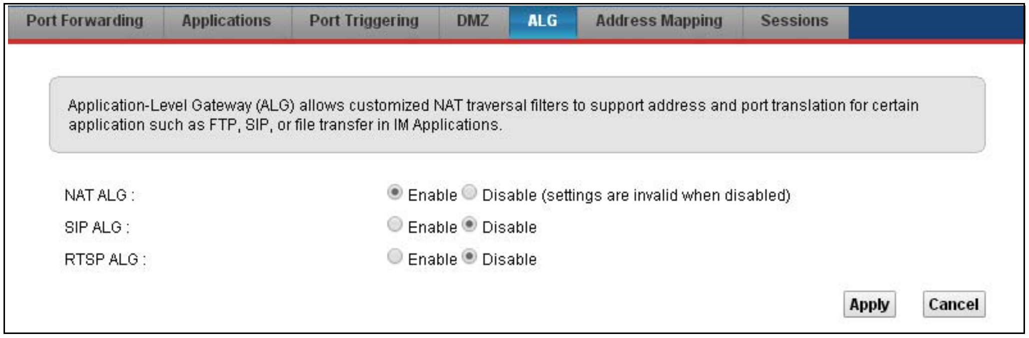
LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server Address**, the VMG discards all packets received for ports that are not specified 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 NAT and SIP (VoIP) ALG in the VMG. To access this screen, click **Network Setting > NAT > ALG**.

Figure 82 Network Setting > NAT > ALG



Application-Level Gateway (ALG) allows customized NAT traversal filters to support address and port translation for certain application such as FTP, SIP, or file transfer in IM Applications.

NAT ALG : ● Enable ○ Disable (settings are invalid when disabled)
SIP ALG : ○ Enable ● Disable
RTSP ALG : ○ Enable ● Disable

The following table describes the fields in this screen.

Table 61 Network Setting > NAT > ALG

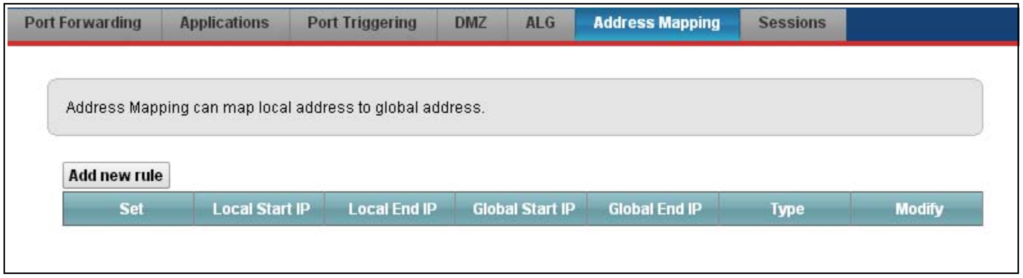
LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
RTSP ALG	Enable this 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.
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 83 Network Setting > NAT > Address Mapping



Address Mapping can map local address to global address.

Set	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify

The following table describes the fields in this screen.

Table 62 Network Setting > NAT > Address Mapping

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
Set	This is the index number of the address mapping set.
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.

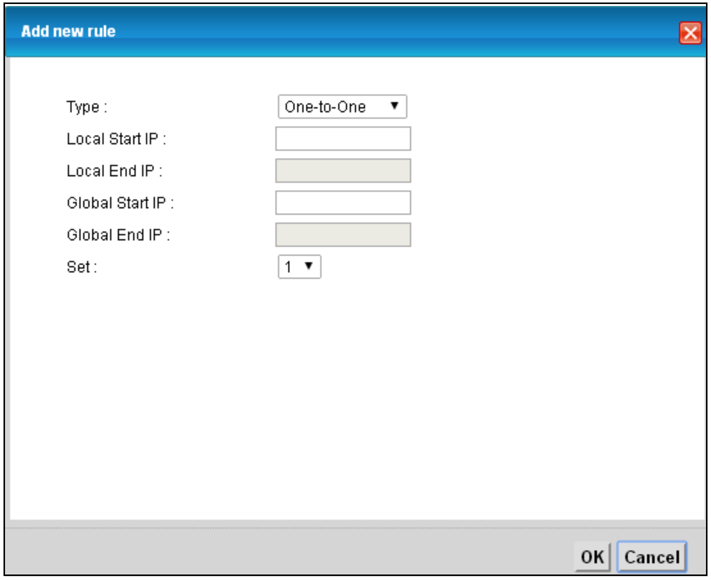
Table 62 Network Setting > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Type	This is the address mapping type. **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.
Modify	Click the **Edit** icon to go to the screen where you can edit the address mapping rule. 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.

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 84 Address Mapping: Add/Edit



Add new rule

Type :	One-to-One ▼
Local Start IP :	
Local End IP :	
Global Start IP :	
Global End IP :	
Set :	1 ▼

The following table describes the fields in this screen.

Table 63 Address Mapping: Add/Edit

LABEL	DESCRIPTION
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).

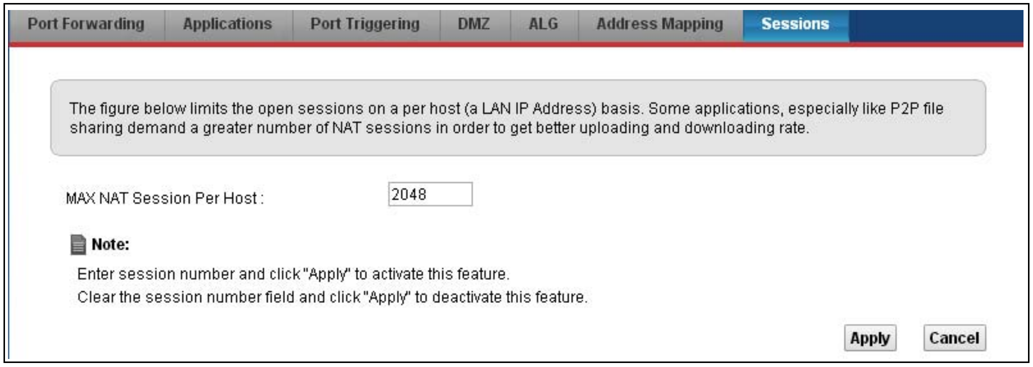
Table 63 Address Mapping: Add/Edit (continued)

LABEL	DESCRIPTION
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.
Set	Select the number of the mapping set for which you want to configure.
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 85 Network Setting > NAT > Sessions



The figure below limits the open sessions on a per host (a LAN IP Address) basis. Some applications, especially like P2P file sharing demand a greater number of NAT sessions in order to get better uploading and downloading rate.

MAX NAT Session Per Host : 2048

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 64 Network Setting > NAT > Sessions

LABEL	DESCRIPTION
WAX 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 65 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

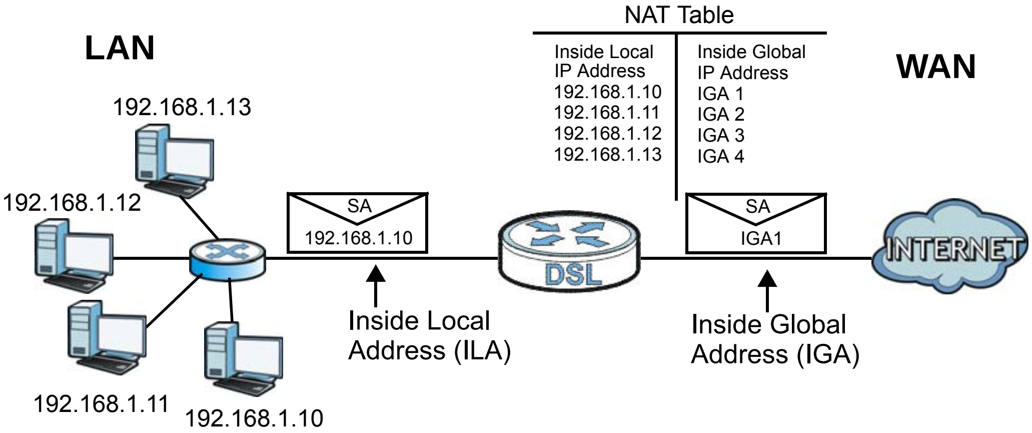
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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 86 How NAT Works



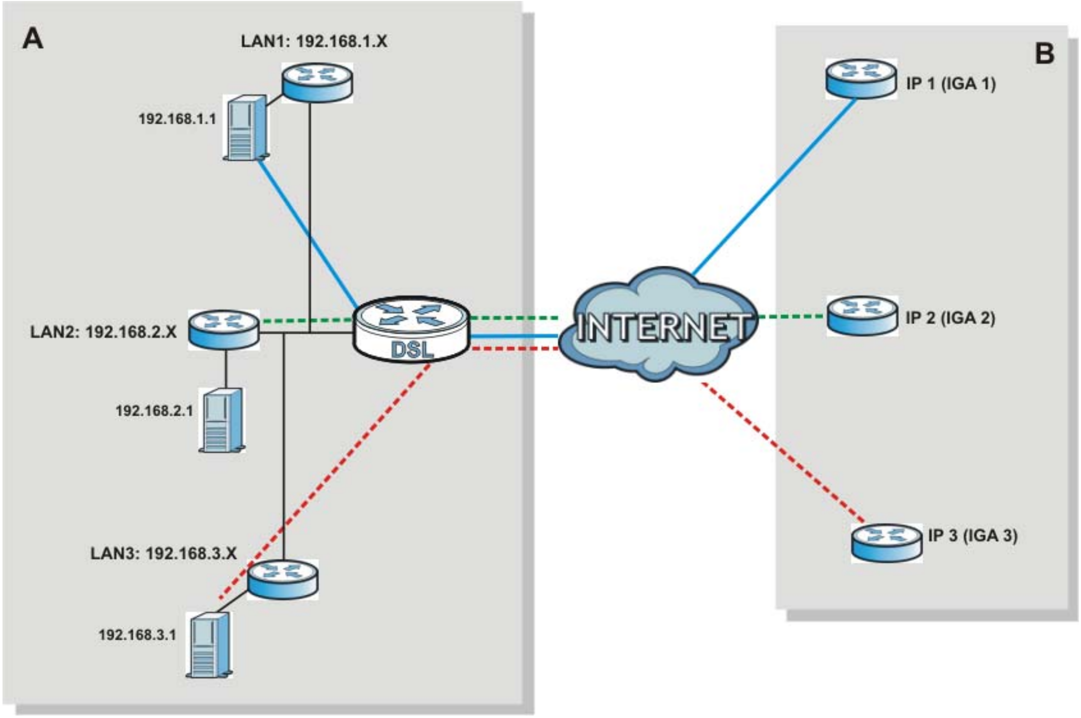
NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

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 87 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.

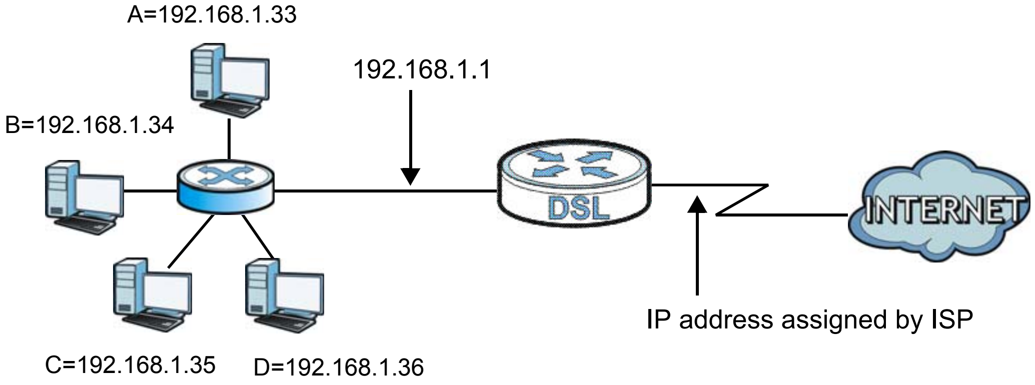
Table 66 Services and Port Numbers

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 88 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 200).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the VMG (Section 12.3 on page 201).

12.1.2 What You Need To Know

DYNDNS Wildcard

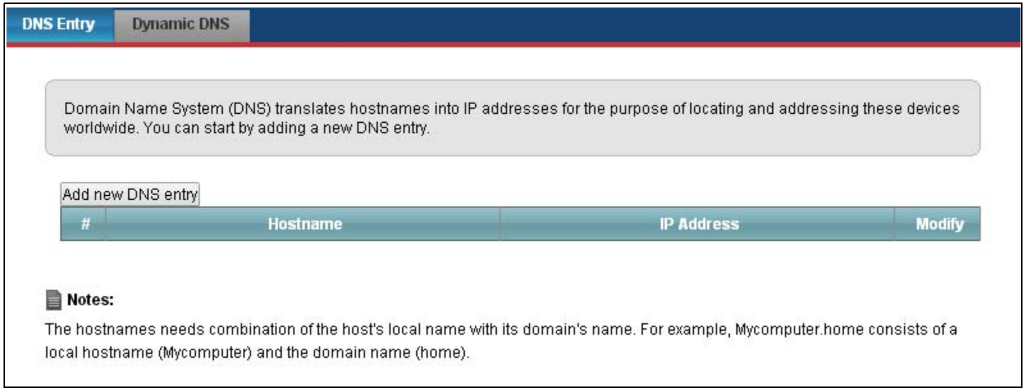
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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 89 Network Setting > DNS > DNS Entry



Domain Name System (DNS) translates hostnames into IP addresses for the purpose of locating and addressing these devices worldwide. You can start by adding a new DNS entry.

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.

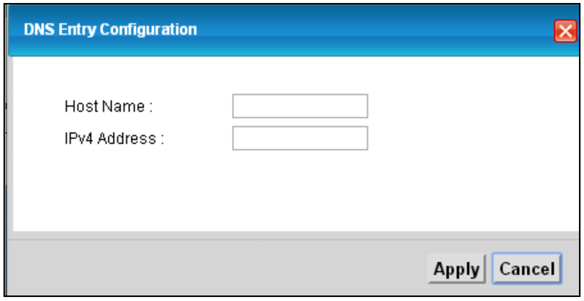
Table 67 Network Setting > DNS > DNS Entry

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 90 DNS Entry: Add/Edit



DNS Entry Configuration

Host Name :

IPv4 Address :

The following table describes the labels in this screen.

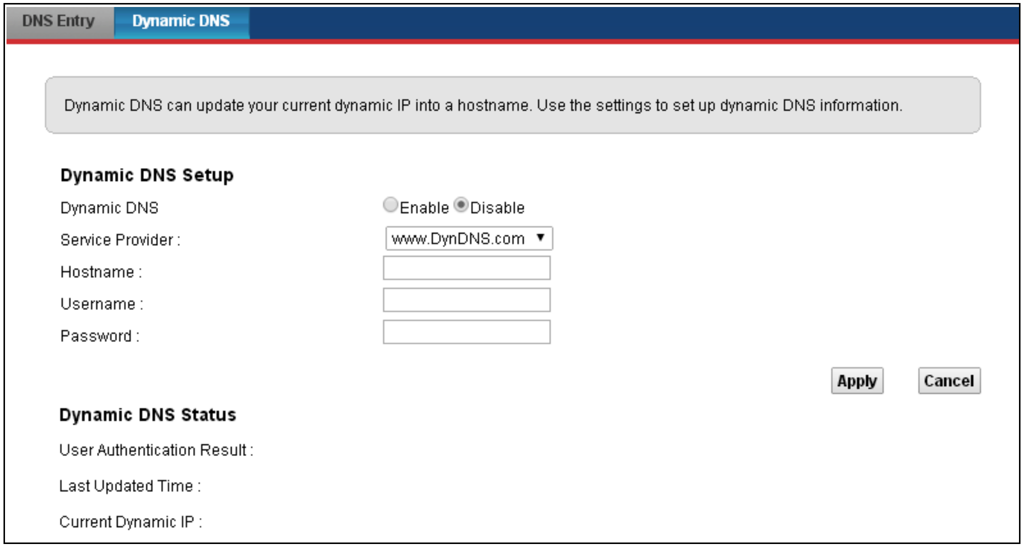
Table 68 DNS Entry: Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
IP Address	Enter the IP address of the DNS entry.
Apply	Click **Apply** 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 91 Network Setting > DNS > Dynamic DNS



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

Dynamic DNS Setup

Dynamic DNS ○ Enable ● Disable

Service Provider : www.DynDNS.com

Hostname :

Username :

Password :

Dynamic DNS Status

User Authentication Result :

Last Updated Time :

Current Dynamic IP :

The following table describes the fields in this screen.

Table 69 Network Setting > DNS > > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.

Table 69 Network Setting > DNS > > Dynamic DNS (continued)

LABEL	DESCRIPTION
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Hostname	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.
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.

13

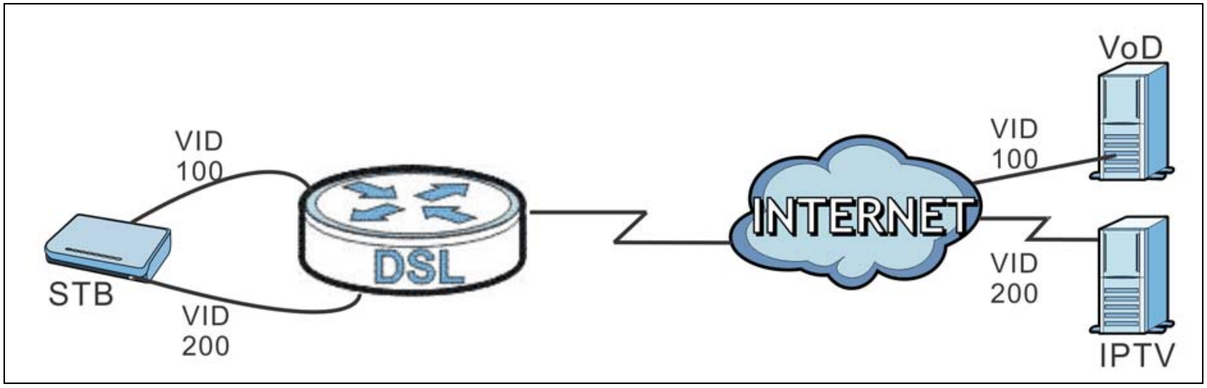
Vlan Group

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 92 VLAN Group Example



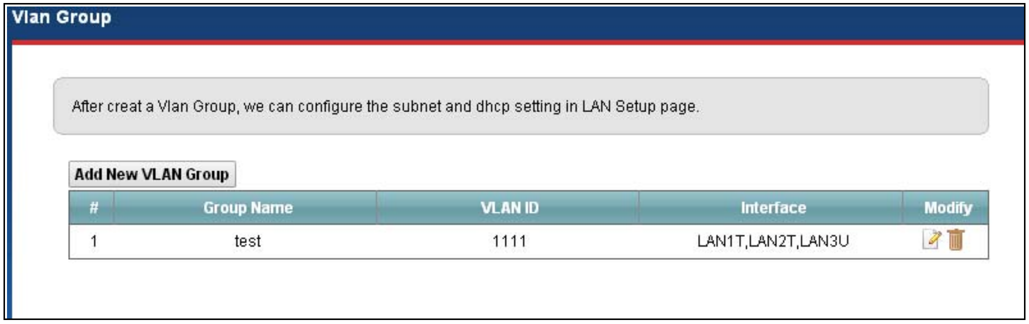
13.1.1 What You Can Do in this Chapter

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 93 Network Setting > Vlan Group



After creat a Vlan Group, we can configure the subnet and dhcp setting in LAN Setup page.

#	Group Name	VLAN ID	Interface	Modify
1	test	1111	LAN1T,LAN2T,LAN3U	

The following table describes the fields in this screen.

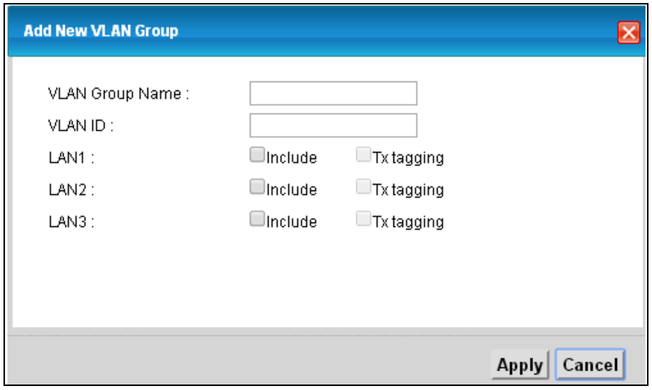
Table 70 Network Setting > Vlan Group

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 94 Add/Edit VLAN Group



Add New VLAN Group

VLAN Group Name :

VLAN ID :

LAN1 : □ Include □ Tx tagging

LAN2 : □ Include □ Tx tagging

LAN3 : □ Include □ Tx tagging

The following table describes the fields in this screen.

Table 71 Interface Group Configuration

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 **Txtagging** is selected below.
LAN	If LAN port 4 is configured as a WAN port, it will not display here. Select **Include** to add the associated LAN interface to this VLAN group. Select **Txtagging** to tag outgoing traffic from the associated LAN port with the **VLAN ID** number entered above.
Apply	Click **Apply** to save your changes back to the VMG.
Cancel	Click **Cancel** to exit this screen without saving.

14

Interface Group

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 Group** screens let you create multiple networks on the VMG (Section 14.2 on page 205).

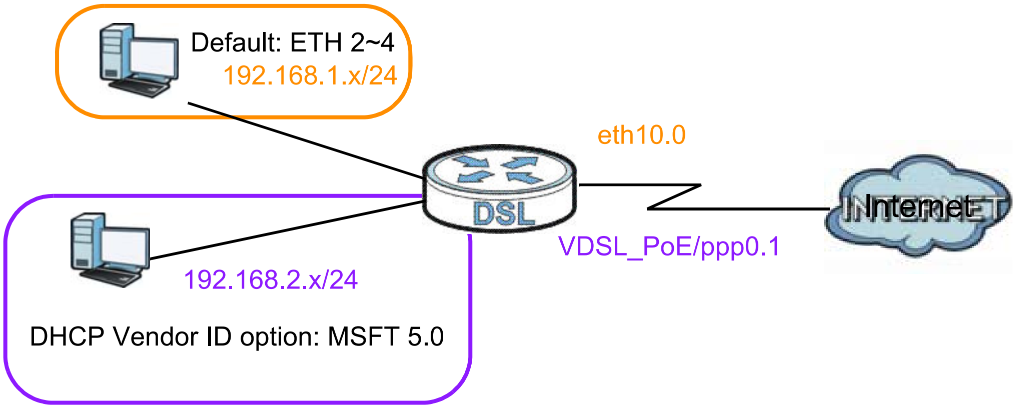
14.2 The Interface Group Screen

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 139 for more information.

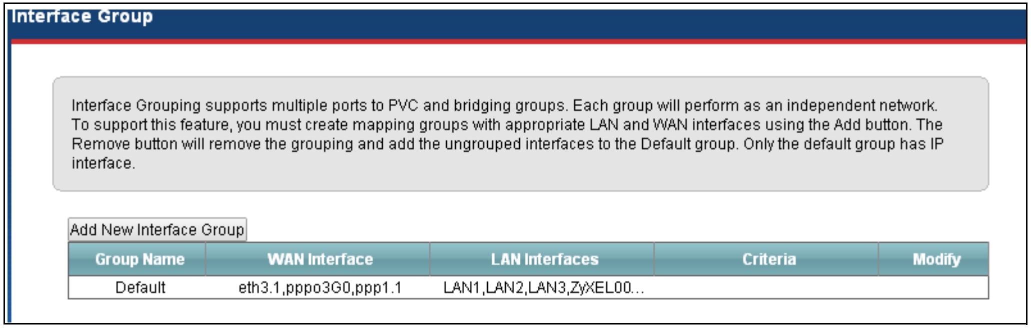
In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

Figure 95 Interface Grouping Application



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

Figure 96 Network Setting > Interface Group



Interface Group

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Add New Interface Group

Group Name	WAN Interface	LAN Interfaces	Criteria	Modify
Default	eth3.1,pppo3G0,ppp1.1	LAN1,LAN2,LAN3,ZyXEL00...		

The following table describes the fields in this screen.

Table 72 Network Setting > Interface Group

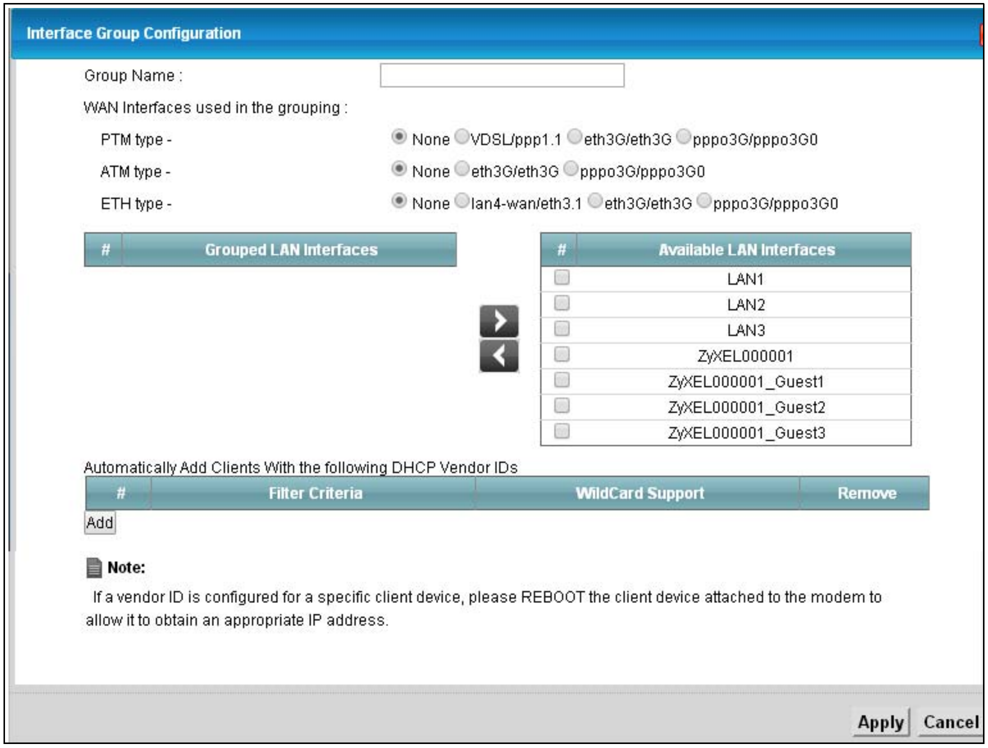
LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering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

14.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Group** 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 97 Interface Group Configuration



Interface Group Configuration

Group Name :

WAN Interfaces used in the grouping :

PTM type - ● None ○ VDSL/ppp1.1 ○ eth3G/eth3G ○ pppo3G/pppo3G0

ATM type - ● None ○ eth3G/eth3G ○ pppo3G/pppo3G0

ETH type - ● None ○ lan4-wan/eth3.1 ○ eth3G/eth3G ○ pppo3G/pppo3G0

#	Grouped LAN Interfaces

#	Available LAN Interfaces
□	LAN1
□	LAN2
□	LAN3
□	ZyXEL000001
□	ZyXEL000001_Guest1
□	ZyXEL000001_Guest2
□	ZyXEL000001_Guest3

Automatically Add Clients With the following DHCP Vendor IDs

#	Filter Criteria	WildCard Support	Remove

Add

Note:

If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

The following table describes the fields in this screen.

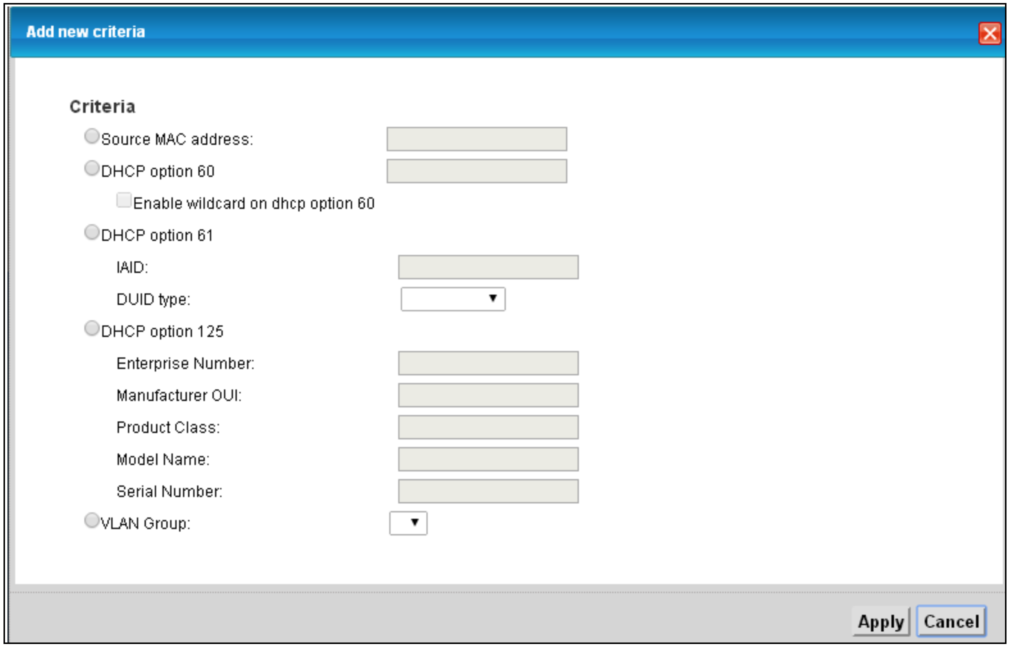
Table 73 Interface Group Configuration

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interface used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface and up to one ETH interface. Select **None** to not add a WAN interface to this group.
Grouped LAN Interfaces Available LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Grouped LAN Interfaces** list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the **Grouped LAN Interfaces**, use the right-facing arrow.
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 208 for more information.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
WildCard Support	This shows if wildcard on DHCP option 60 is enabled.
Remove	Click the **Remove** icon to delete this rule from the VMG.
Apply	Click **Apply** to save your changes back to the VMG.
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 98 Interface Grouping Criteria



Add new criteria

Criteria

○ Source MAC address:

○ DHCP option 60

□ Enable wildcard on dhcp option 60

○ DHCP option 61

IAID:

DUID type:

○ DHCP option 125

Enterprise Number:

Manufacturer OUI:

Product Class:

Model Name:

Serial Number:

○ VLAN Group:

The following table describes the fields in this screen.

Table 74 Interface Grouping Criteria

LABEL	DESCRIPTION
Source MAC Address	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 on DHCP option 60 option	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.
IAID	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DUID type	Select **DUID-LLT** (DUID Based on Link-layer Address Plus Time) to enter the hardware type, a time value and the MAC address of the device. Select **DUID-EN** (DUID Assigned by Vendor Based upon Enterprise Number) to enter the vendor’s registered enterprise number. Select **DUID-LL** (DUID Based on Link-layer Address) to enter the device’s hardware type and hardware address (MAC address) in the following fields. Select **Other** to enter any string that identifies the device in the DUID field.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.

Table 74 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.
Product Class	Enter the product class of the device.
Model Name	Enter the model name of the device.
Serial Number	Enter the serial number of the device.
Apply	Click **Apply** to save your changes back to the VMG.
Cancel	Click **Cancel** to exit this screen without saving.

15

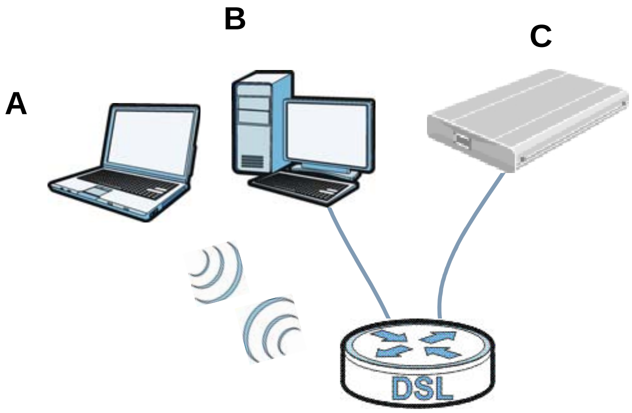
USB Service

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 99 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 213).
- Use the **Media Server** screen to enable or disable the sharing of media files (Section 15.3 on page 215).
- Use the **Printer Server** screen to enable the print server (Section 15.4 on page 216).

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).

15.1.2.2 About Printer Server

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

TCP/IP

TCP/IP (Transmission Control Protocol/ Internet Protocol) is a set of communications protocols that most of the Internet runs on.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Supported OSs

Your operating system must support TCP/IP ports for printing and be compatible with the RAW (port 9100) protocol.

The following OSs support VMG's printer sharing feature.

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.

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.

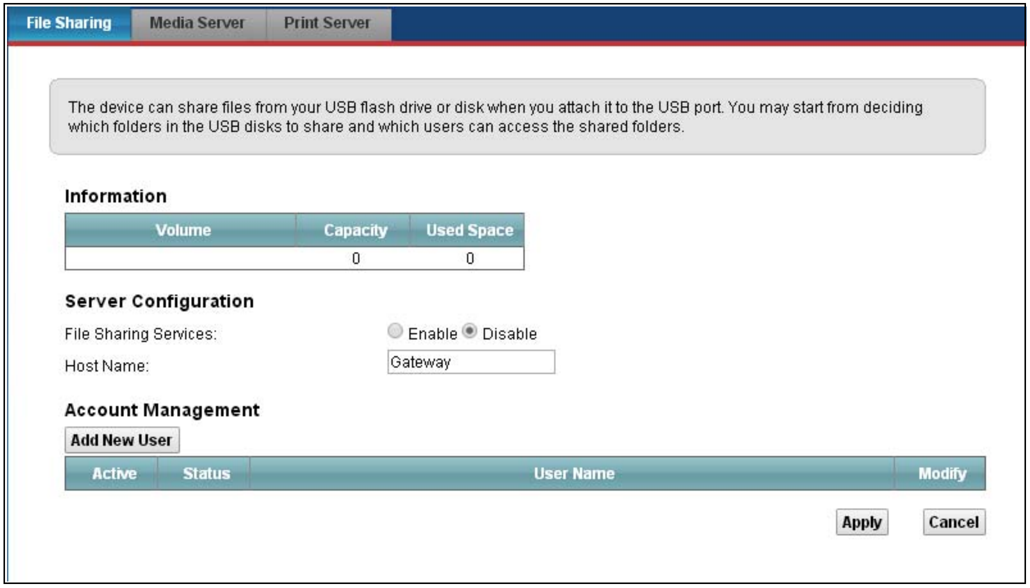
2. The VMG detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

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 100 Network Setting > USB Service > File Sharing



The device can share files from your USB flash drive or disk when you attach it to the USB port. You may start from deciding which folders in the USB disks to share and which users can access the shared folders.

Information

Volume	Capacity	Used Space
	0	0

Server Configuration

File Sharing Services: ○ Enable ● Disable

Host Name: Gateway

Account Management

Add New User

Active	Status	User Name	Modify

Apply Cancel

Each field is described in the following table.

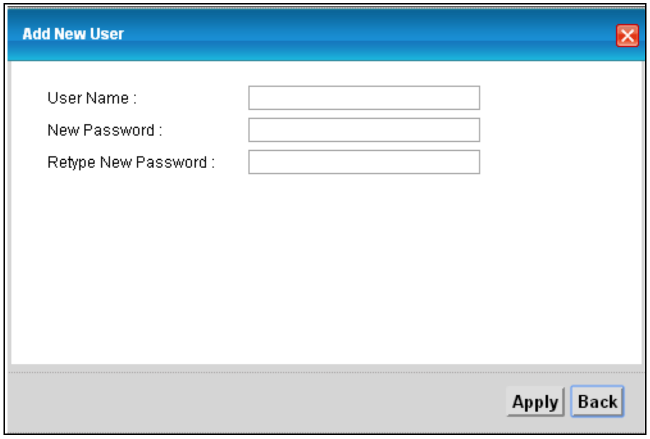
Table 75 Network Setting > USB Service > File Sharing

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.
Host Name	Enter the host name on the share.
Share Directory List	
Add New Share	Click this to create a new share for users to access through the VMG.
Active	Select this to activate the share.
Status	This field shows the status of the share. : The share is not activated. : The share is activated and shared to all users. : The share is activated and only shared to the specified users listed in the **Account Management** section below.
Share Name	This field shows the name of a folder that is shared through the VMG.
Share Path	This field shows the location of the share in the VMG.
Share Description	This field shows a short description of the share.
Modify	Click the **Edit** icon to modify the share. Click the **Delete** icon to remove the share from 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	This field shows the status of the user. : The user account is not activated for the share. : The user account is activated for the share.
User Name	This is the name of a user who is allowed to access the secured shares on the USB device.
Modify	Click the **Edit** icon to modify the user account. Click the **Delete** icon to remove the user account from the VMG.
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 101 Network Setting > USB Service > File Sharing > Add new user



Add New User

User Name :

New Password :

Retype New Password :

Each field is described in the following table.

Table 76 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 this to save your changes to the VMG.
Back	Click this to return to the previous screen.

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.

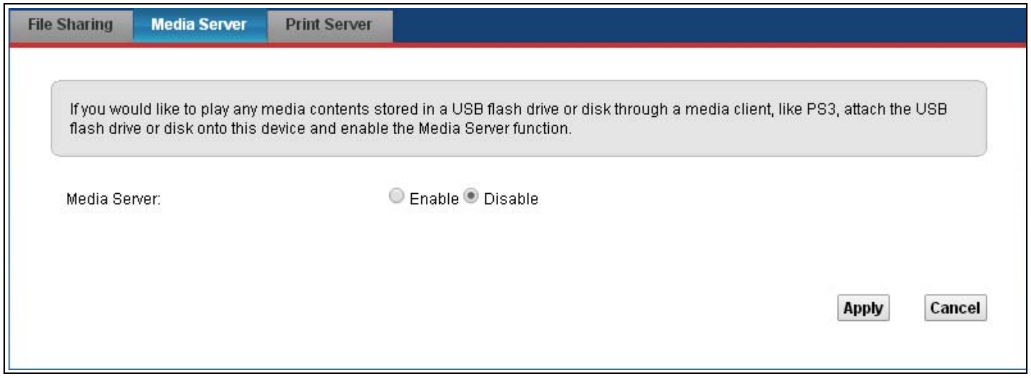
The VMG media server enables you to:

- 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 102 Network Setting > USB Service > Media Server



If you would like to play any media contents stored in a USB flash drive or disk through a media client, like PS3, attach the USB flash drive or disk onto this device and enable the Media Server function.

Media Server: ○ Enable ● Disable

The following table describes the labels in this menu.

Table 77 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.

15.4 Print Server

The VMG allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the VMG and then configuring a TCP/IP port on the computers connected to your network.

15.4.1 Before You Begin

To configure the print server you need the following:

- Your VMG must be connected to your computer and any other devices on your network. The USB printer must be connected to your VMG.
- A USB printer with the driver already installed on your computer.
- The computers on your network must have the printer software already installed before they can create a TCP/IP port for printing via the network. Follow your printer manufacturers instructions on how to install the printer software on your computer.

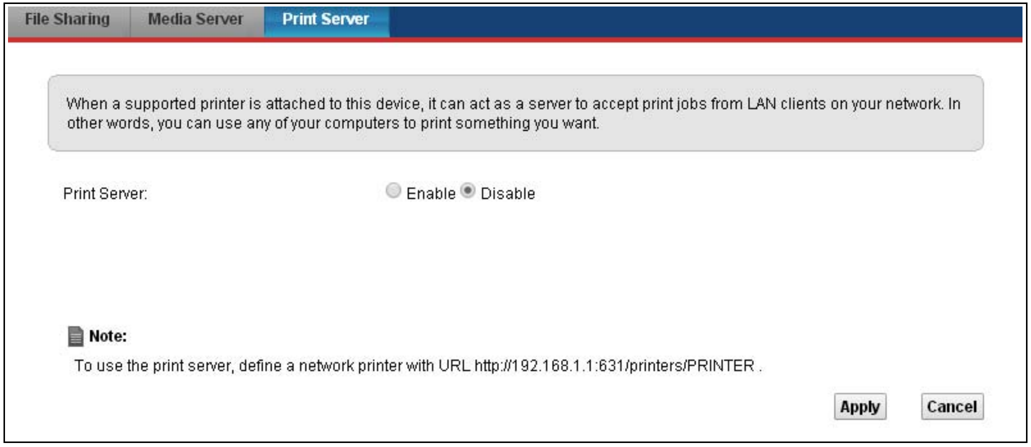
Note: Your printer’s installation instructions may ask that you connect the printer to your computer. Connect your printer to the VMG instead.

15.4.2 The Print Server Screen

Use this screen to enable or disable sharing of a USB printer via your VMG.

To access this screen, click **Network Setting > USB Service > Print Server**.

Figure 103 Network Setting > USB Service > Printer Server



When a supported printer is attached to this device, it can act as a server to accept print jobs from LAN clients on your network. In other words, you can use any of your computers to print something you want.

Print Server: ○ Enable ● Disable

Note:

To use the print server, define a network printer with URL http://192.168.1.1:631/printers/PRINTER .

The following table describes the labels in this menu.

Table 78 Network Setting > USB Service > Print Server

LABEL	DESCRIPTION
Print Server	Select **Enable** to have the VMG share a USB printer.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

Power Management

16.1 Overview

Power management allows you to turn on/off one or more interfaces and all LED lights without power off the whole system when necessary. You can configure a schedule to do so automatically or manually do it on the Web Configurator.

16.1.1 What You Can Do in this Chapter

- Use the **Power Management** screen to manually turn on/off interface(s) and/or LEDs (Section 16.2 on page 219).
- Use the **Auto Switch Off** screen to configure schedules for turning on/off interface(s) and/or LEDs automatically (Section 16.3 on page 220).

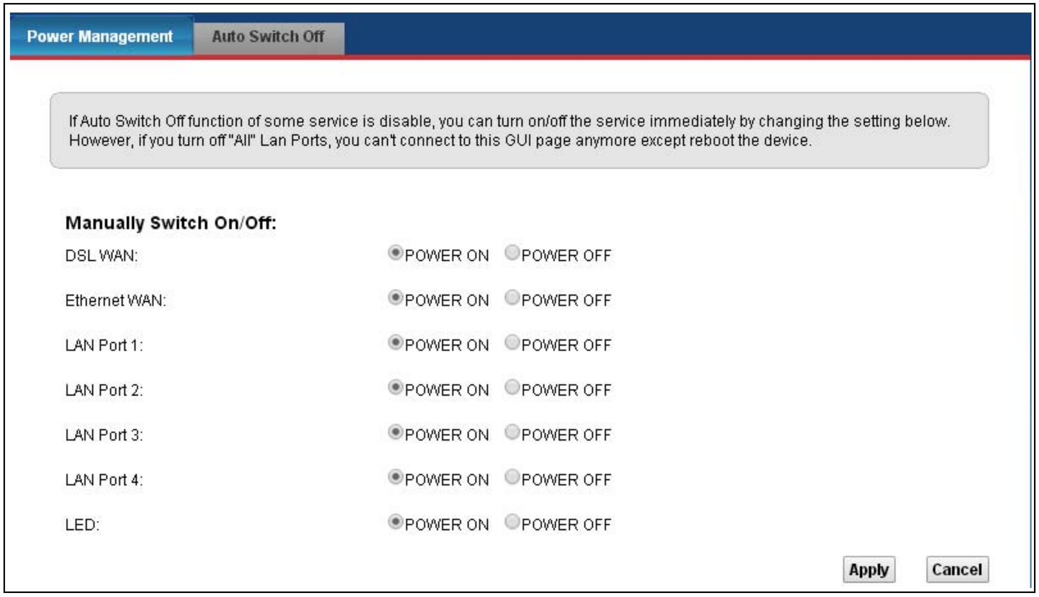
16.1.2 What You Need To Know

- These screens are only available for the “supervisor” user.
- The **Power Management** and **Auto Switch Off** screens are dependant. You can only configure the on/off switches of the same interface and LEDs in one of the two screens.

16.2 The Power Management Screen

Use this screen to manually turn on/off interface(s) or LEDs. Click **Network Setting > Power Management > Power Management**. The screen appears as shown.

Figure 104 Network Setting > Power Management



If Auto Switch Off function of some service is disable, you can turn on/off the service immediately by changing the setting below. However, if you turn off "All" Lan Ports, you can't connect to this GUI page anymore except reboot the device.

Manually Switch On/Off:

DSL WAN:	● POWER ON ○ POWER OFF
Ethernet WAN:	● POWER ON ○ POWER OFF
LAN Port 1:	● POWER ON ○ POWER OFF
LAN Port 2:	● POWER ON ○ POWER OFF
LAN Port 3:	● POWER ON ○ POWER OFF
LAN Port 4:	● POWER ON ○ POWER OFF
LED:	● POWER ON ○ POWER OFF

Each field is described in the following table.

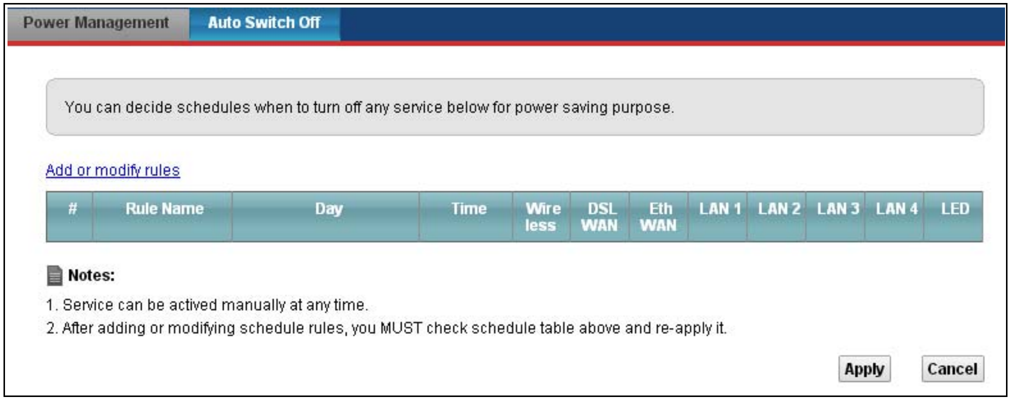
Table 79 Network Setting > Power Management

LABEL	DESCRIPTION
Manually Switch On/Off	Select **POWER ON** or **POWER OFF** to turn on/off the interface or LED lights.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

16.3 The Auto Switch Off Screen

Use this screen to view schedules to turn on or off specific interface(s) and/or all LED lights on the VMG. To access this screen, click **Network Setting > Power Management > Auto Switch Off**.

Figure 105 Network Setting > Power Managment > Auto Switch Off



You can decide schedules when to turn off any service below for power saving purpose.

#	Rule Name	Day	Time	Wireless	DSL WAN	Eth WAN	LAN 1	LAN 2	LAN 3	LAN 4	LED

Notes:

1. Service can be actived manually at any time.
2. After adding or modifying schedule rules, you MUST check schedule table above and re-apply it.

The following table describes the labels in this menu.

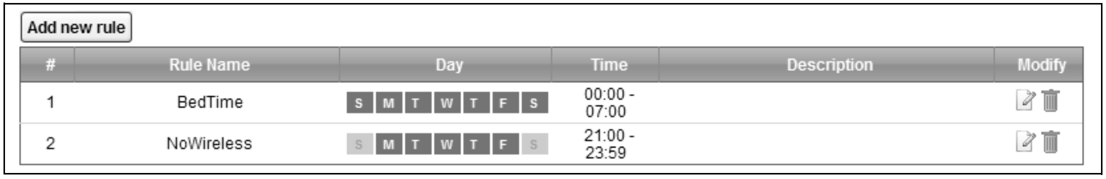
Table 80 Network Setting > Power Managment > Auto Switch OffNetwork Setting > Power Managment > Auto Switch Off

LABEL	DESCRIPTION
Add or modify rules	Click this link to create or edit a schedule.
#	This is the index number of a schedule rule.
Rule Name	This field shows the name of the schedule rule.
Day	This field shows which week days (in green) the interface(s) and/or LEDs are turned on and the days (grayed-out) they are turned off automatically.
Time	This field shows the time period the interface(s) and/or LEDs are turned on.
Wireless	This field shows whether this schedule applies to the wireless LAN interface.
DSL WAN	This field shows whether this schedule applies to the DSL WAN interface.
Eth WAN	This field shows whether this schedule applies to the Ethernet WAN interface.
LAN1~LAN4	This field shows whether this schedule applies to the corresponding LAN interface.
LED	This field shows whether this schedule applies to the LEDs.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

16.3.1 The Auto Switch Off Add or Modify Screen

Use this screen to manage the auto switch off schedules. To access this screen, click the **Add or modify rules** link in the **Network Setting > Power Management > Auto Switch Off** screen.

Figure 106 Network Setting > Power Managment > Auto Switch Off > Add or modify rules



Add new rule

#	Rule Name	Day	Time	Description	Modify
1	BedTime	S M T W T F S	00:00 - 07:00		
2	NoWireless	S M T W T F S	21:00 - 23:59		

The following table describes the labels in this menu.

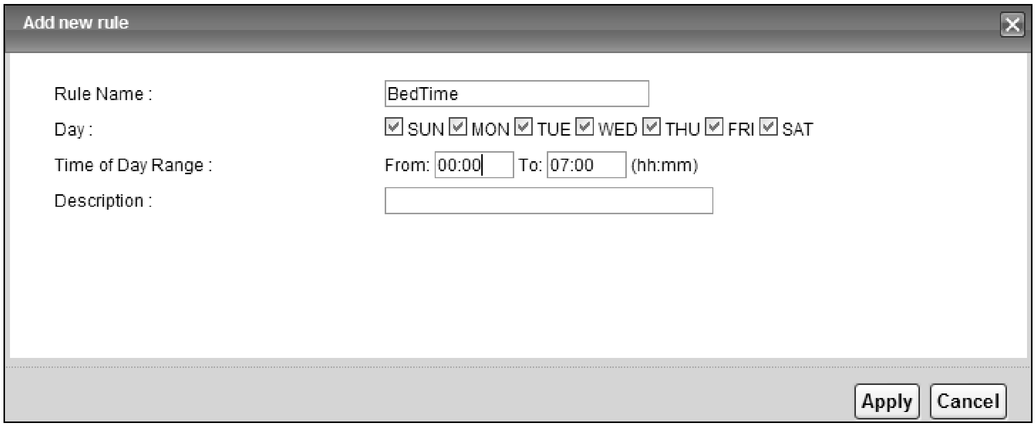
Table 81 Network Setting > Power Managment > Auto Switch Off Network Setting > Power Managment > Auto Switch Off > Add or modify rules

LABEL	DESCRIPTION
Add new rule	Click this link to create a rule.
#	This is the index number of a rule.
Rule Name	This field shows the name of the rule.
Day	This field shows the week days of the schedule (in green).
Time	This field shows the time period of the schedule.
Description	This field shows more information about this rule.
Modify	Click the **Edit** icon to modify the rule or click the **Delete** icon to remove it.

16.3.2 The Add/Edit Rule Screen

Use this screen to configure a schedule rule. To access this screen, click the **Add new rule** link or the **Edit** icon in the **Network Setting > Power Management > Auto Switch Off > Add or modify rules** screen.

Figure 107 Network Setting > Power Management > Auto Switch Off > Add or modify rules > Add new rule/Edit



Rule Name : BedTime

Day : ☑ SUN ☑ MON ☑ TUE ☑ WED ☑ THU ☑ FRI ☑ SAT

Time of Day Range : From: 00:00 To: 07:00 (hh:mm)

Description :

Each field is described in the following table.

Table 82 Network Setting > Power Management > Auto Switch Off > Add or modify rules > Add new rule/Edit>

LABEL	DESCRIPTION
Rule Name	Type up to 31 alphanumberic characters for the name of this rule.
Day	Select the week day(s) of the schedule.
Time of Day Range	Enter the **From** and **To** times (in hh:mm format) to set a time period for the schedule. You can only enter a time period between 00:00 and 23:59. To set a time period crossing over midnight, you must split the time period into two schedule rules. For example, for a time period from 10:00 PM to the next day's 8:00 AM, you can set one schedule for 22:00~23:59 and another schedule for 00:00~08:00.
Description	Enter more information for this rule here.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

Firewall

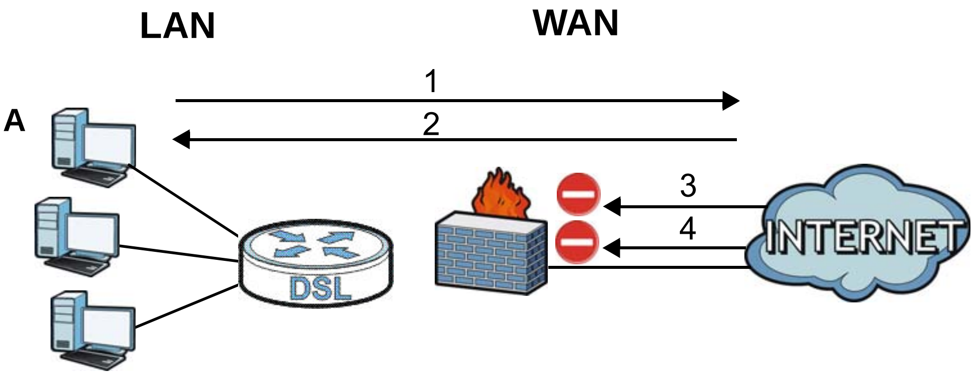
17.1 Overview

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 108 Default Firewall Action



17.1.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the VMG (Section 17.2 on page 225).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 17.3 on page 225).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 17.4 on page 228).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (.Section 17.5 on page 230).

17.1.2 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 ZyXEL Device 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

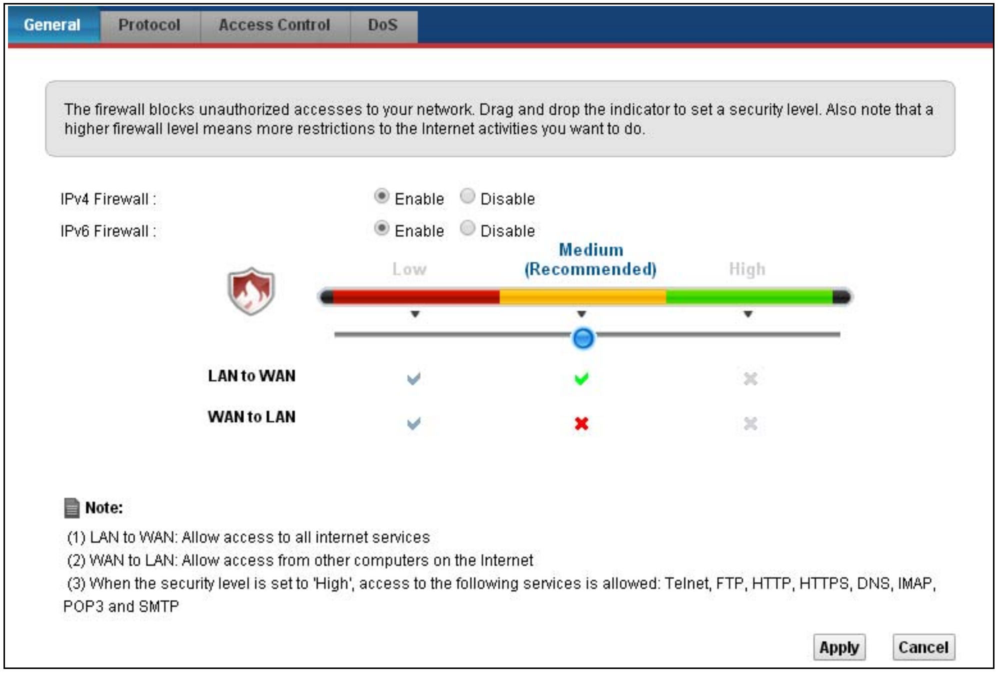
Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

17.2 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 109 Security > Firewall > General



The firewall blocks unauthorized accesses to your network. Drag and drop the indicator to set a security level. Also note that a higher firewall level means more restrictions to the Internet activities you want to do.

IPv4 Firewall : ● Enable ○ Disable

IPv6 Firewall : ● Enable ○ Disable

	Low	Medium (Recommended)	High
LAN to WAN	✓	✓	✗
WAN to LAN	✓	✗	✗

Note:

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

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

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

The following table describes the labels in this screen.

Table 83 Security > Firewall > General

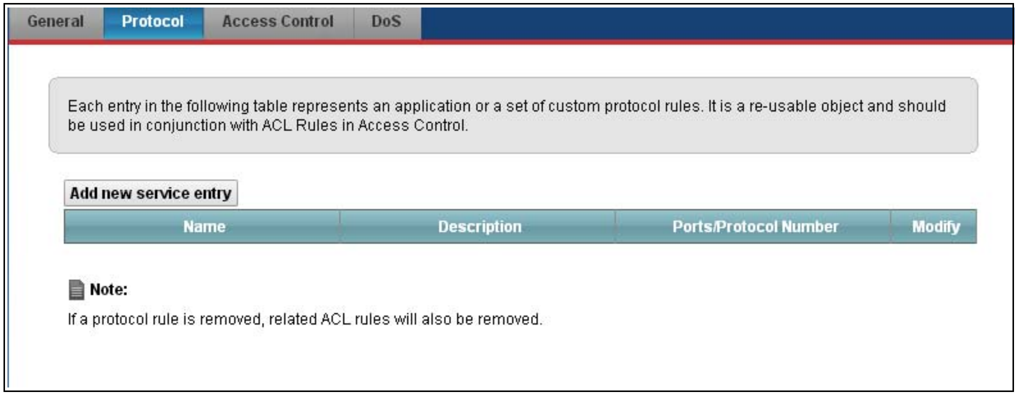
LABEL	DESCRIPTION
Firewall	Select **Enable** to activate the firewall feature on the VMG.
Easy	Select **Easy** to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select **Medium** to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select **High** to deny LAN to WAN and WAN to LAN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

17.3 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 383 for some examples.

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

Figure 110 Security > Firewall > Protocol



Each entry in the following table represents an application or a set of custom protocol rules. It is a re-usable object and should be used in conjunction with ACL Rules in Access Control.

Add new service 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.

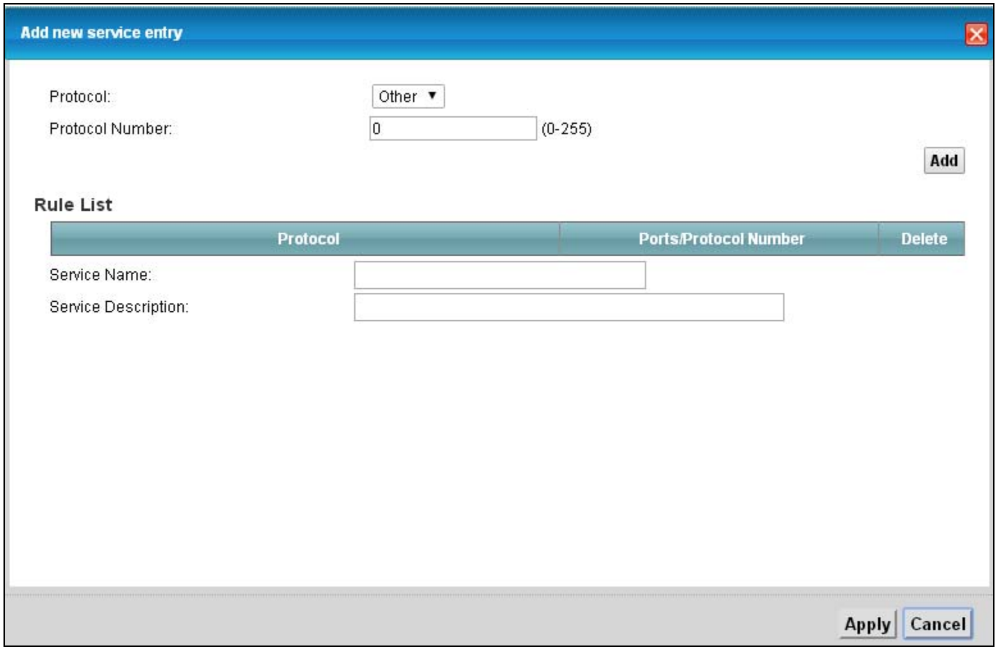
Table 84 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add new service 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.

17.3.1 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 111   Service: Add/Edit



Add new service entry

Protocol: Other ▼

Protocol Number: 0 (0-255)

Rule List

Protocol	Ports/Protocol Number	Delete

Service Name:

Service Description:

The following table describes the labels in this screen.

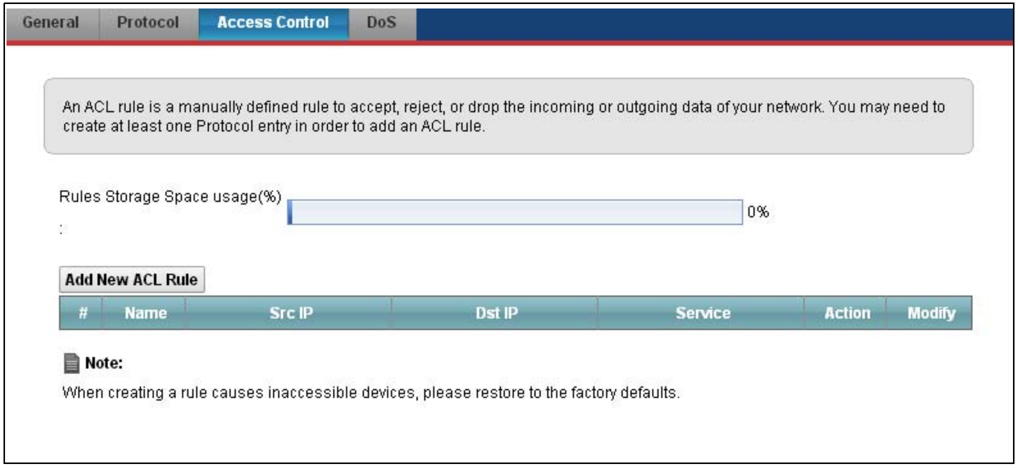
Table 85   Service: Add/Edit

LABEL	DESCRIPTION
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.
Source/ Destination Port	These fields are displayed if you select **TCP** or **UDP** as the IP port. Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. If you select **Any**, the service is applied to all ports. Type a single port number or the range of port numbers that define your customized service.
Protocol Number	This field is displayed if you select **Other** as the protocol. Enter the protocol number of your customized port.
Add	Click this to add the protocol to the **Rule List** below.
Rule List	
Protocol	This is the IP port (**TCP**, **UDP**, **ICMP**, or **Other**) that defines your customized port.
Ports/Protocol Number	For **TCP**, **UDP**, **ICMP**, or **TCP/UDP** protocol rules this shows the port number or range that defines the custom service. For other IP protocol rules this shows the protocol number.
Delete	Click the **Delete** icon to remove the rule.
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Service Description	Enter a description for your customized port.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

17.4 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 112 Security > Firewall > Access Control



An ACL rule is a manually defined rule to accept, reject, or drop the incoming or outgoing data of your network. You may need to create at least one Protocol entry in order to add an ACL rule.

Rules Storage Space usage(%) : 0%

#	Name	Src IP	Dst IP	Service	Action	Modify

Note:

When creating a rule causes inaccessible devices, please restore to the factory defaults.

The following table describes the labels in this screen.

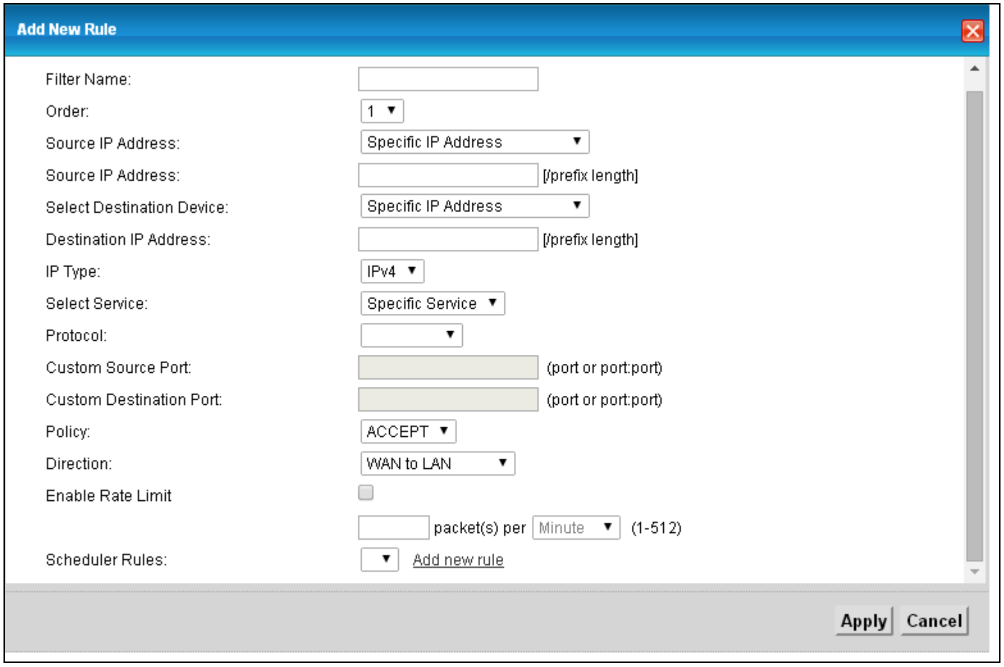
Table 86 Security > Firewall > Access Control

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.

17.4.1 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 113 Access Control: Add/Edit



Filter Name:	
Order:	1 ▼
Source IP Address:	Specific IP Address ▼
Source IP Address:	[/prefix length]
Select Destination Device:	Specific IP Address ▼
Destination IP Address:	[/prefix length]
IP Type:	IPv4 ▼
Select Service:	Specific Service ▼
Protocol:	▼
Custom Source Port:	(port or port:port)
Custom Destination Port:	(port or port:port)
Policy:	ACCEPT ▼
Direction:	WAN to LAN ▼
Enable Rate Limit	☐
	packet(s) per Minute ▼ (1-512)
Scheduler Rules:	▼ Add new rule

The following table describes the labels in this screen.

Table 87 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 destiniation 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 Protocol	Select the transport layer protocol that defines your customized port from the drop-down list box. The specific protocol rule sets you add in the **Security > Firewall > Service > Add** screen display in this list. If you want to configure a customized protocol, select **Specific Service**.
Protocol	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Choose the IP port (**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 Protocol** in **Select Protocol**. Enter a single port number or the range of port numbers of the source.

Table 87 Access Control: Add/Edit (continued)

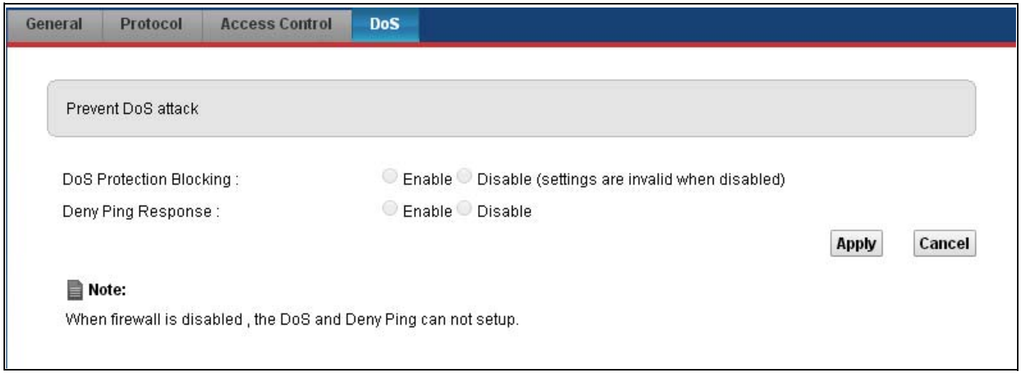
LABEL	DESCRIPTION
Custom Destination Port	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Enter a single port number or the range of port numbers of the destination.
Policy	Use the drop-down list box to select whether to discard (**DROP**), deny and send an 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 this check box 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.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

17.5 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 114 Security > Firewall > DoS



Prevent DoS attack

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

Deny Ping Response : ○ Enable ○ Disable

Note:

When firewall is disabled , the DoS and Deny Ping can not setup.

The following table describes the labels in this screen.

Table 88 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Select **Enable** to enable protection against DoS attacks.
Deny Ping Response	Select Enable to block ping request packets.

Table 88 Security > Firewall > DoS (continued)

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

18

MAC Filter

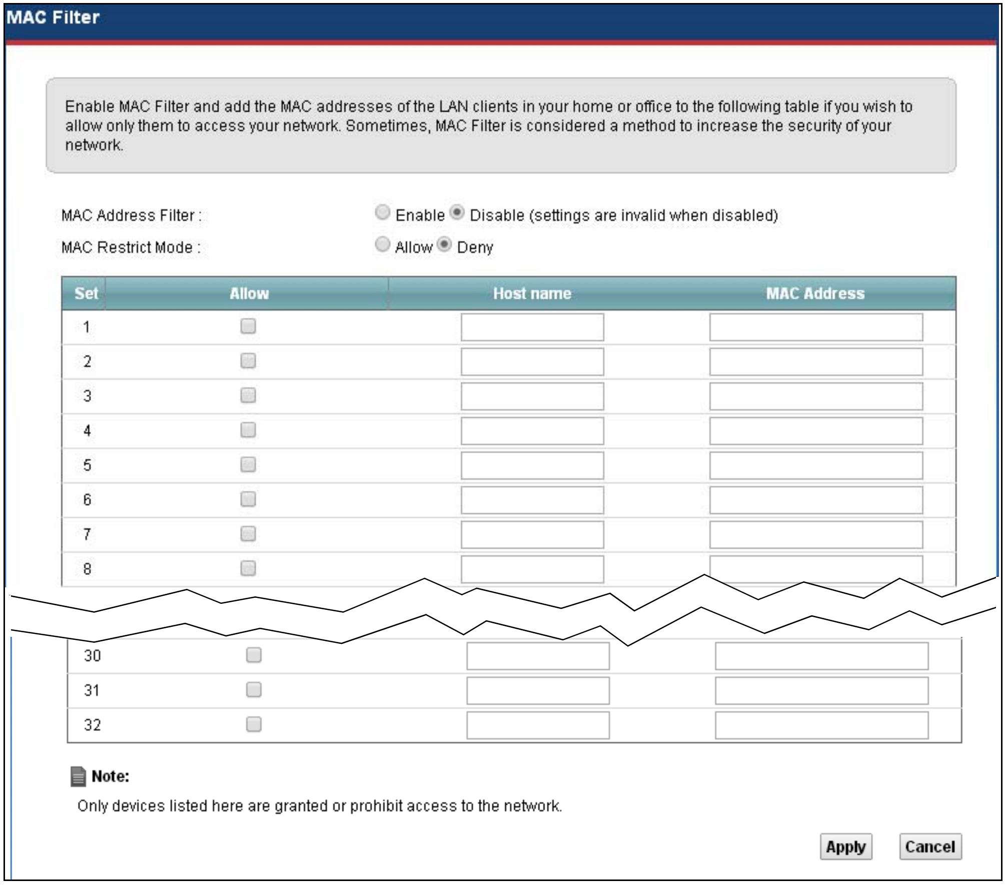
18.1 Overview

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.

18.2 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 115 Security > MAC Filter



MAC Filter

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

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

MAC Restrict Mode : ○ Allow ● Deny

Set	Allow	Host name	MAC Address
1	□		
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
8	□		
30	□		
31	□		
32	□		

Note:

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

The following table describes the labels in this screen.

Table 89 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.
Allow	Select **Allow** to enable the MAC filter rule. . The rule will not be applied if **Allow** 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.

19

Parental Control

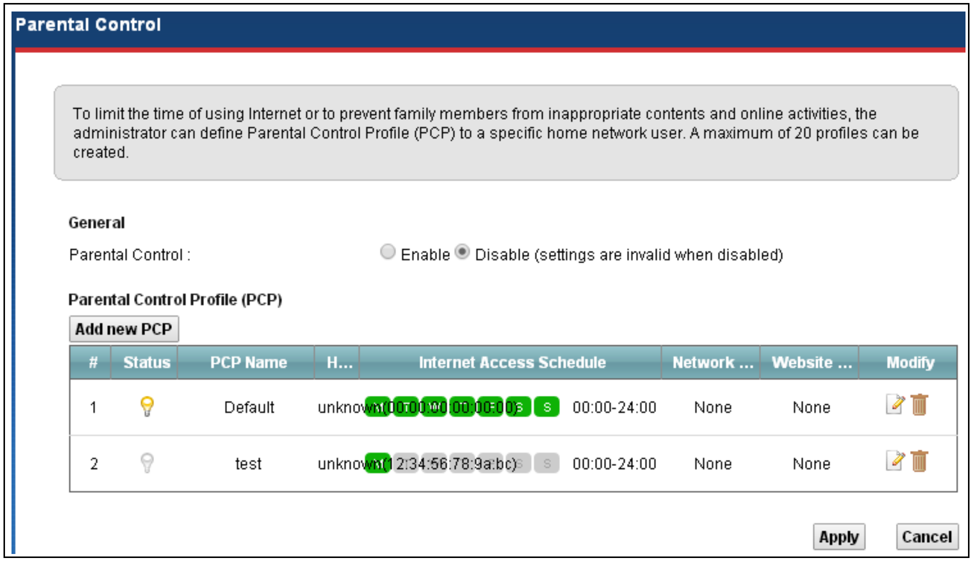
19.1 Overview

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.

19.2 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.



Parental Control

To limit the time of using Internet or to prevent family members from inappropriate contents and online activities, the administrator can define Parental Control Profile (PCP) to a specific home network user. A maximum of 20 profiles can be created.

General

Parental Control : ○ Enable ● Disable (settings are invalid when disabled)

Parental Control Profile (PCP)

#	Status	PCP Name	H...	Internet Access Schedule	Network ...	Website ...	Modify
1	💡	Default	unknown(00:00:00:00:00:00)	S 00:00-24:00	None	None	
2	💡	test	unknown(12:34:56:78:9a:bc)	S 00:00-24:00	None	None	

Figure 116 Security > Parental Control

The following table describes the fields in this screen.

Table 90 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.

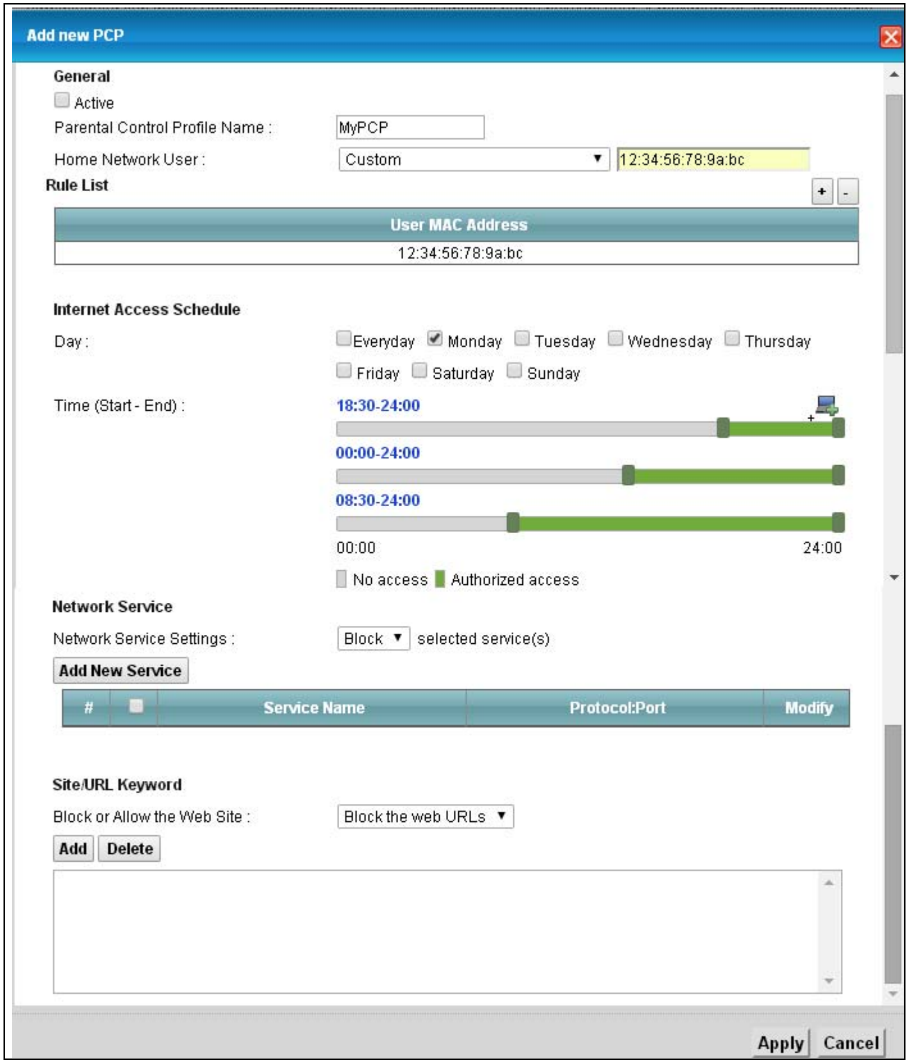
Table 90 Security > Parental Control (continued)

LABEL	DESCRIPTION
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 Block	This shows whether the website block is configured. If not, **None** will be shown.
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.

19.2.1 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 117 Parental Control Rule: Add/Edit Rule



Add new PCP

General

□ Active

Parental Control Profile Name : MyPCP

Home Network User : Custom ▾ 12:34:56:78:9a:bc

Rule List

User MAC Address
12:34:56:78:9a:bc

Internet Access Schedule

Day : □ Everyday ☑ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Time (Start - End) :

18:30-24:00

00:00-24:00

08:30-24:00

00:00 24:00

□ No access 🟩 Authorized access

Network Service

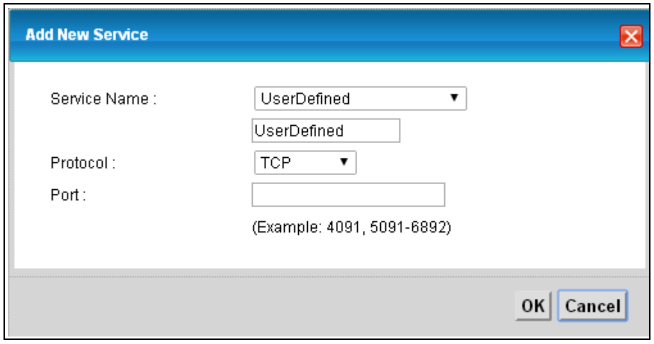
Network Service Settings : Block ▾ selected service(s)

#	□	Service Name	Protocol:Port	Modify

Site/URL Keyword

Block or Allow the Web Site : Block the web URLs ▾

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



Add New Service

Service Name : UserDefined ▾

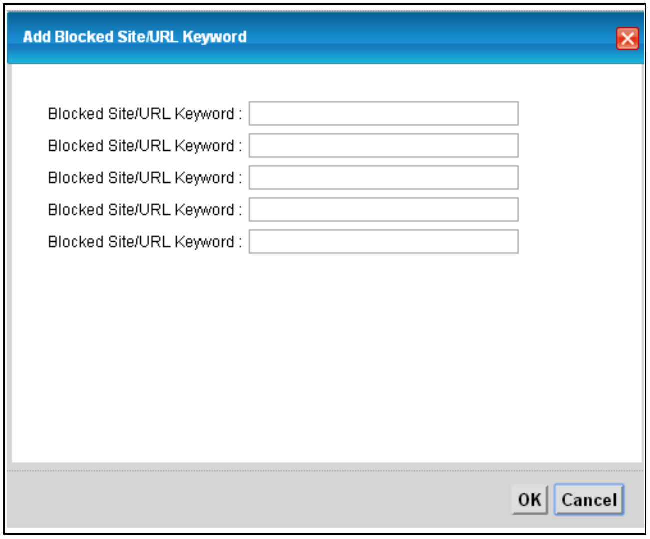
UserDefined

Protocol : TCP ▾

Port :

(Example: 4091, 5091-6892)

Figure 119 Parental Control Rule: Add/Edit Rule > Add Keyword


Add Blocked Site/URL Keyword
Blocked Site/URL Keyword :
Blocked Site/URL Keyword :
Blocked Site/URL Keyword :
Blocked Site/URL Keyword :
Blocked Site/URL Keyword :
OK
Cancel

The following table describes the fields in this screen.

Table 91 Parental Control Rule: Add/Edit

LABEL	DESCRIPTION
General	
Active	Select the checkbox to activate 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 **+** sign to enter a computer MAC address for this PCP. Up to five are allowed. Click the **-** sign 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 **+** sign above the time bar to add a new time bar. Up to three are allowed.
Authorized access	Select this to allow access for the times defined above.
No access	Select this to deny access for the times defined above.
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.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the **Service Name**, **Protocol**, and **Name** of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Service Name	This shows the name of the rule.
Protocol:Port	This shows the protocol and the port of the rule.

Table 91 Parental Control Rule: Add/Edit (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.
Blocked Site/ URL Keyword	Click **Add** to show a screen to enter the URL of web site or URL keyword to which the VMG blocks access. Click **Delete** to remove it.
Apply	Click this button to save your settings back to the VMG.
Cancel	Click **Cancel** to restore your previously saved settings.

20

Scheduler Rule

20.1 Overview

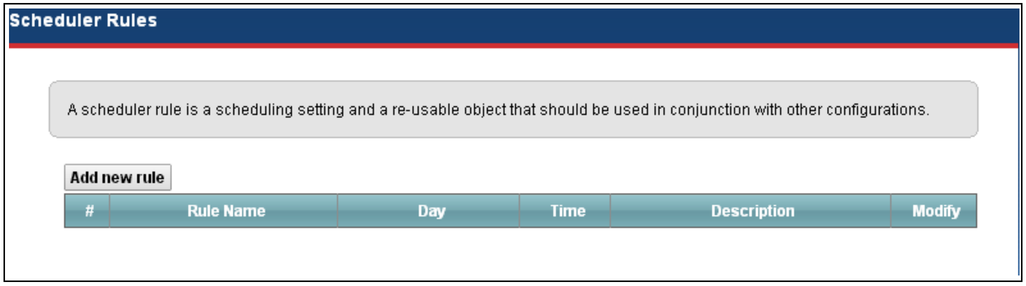
You can define time periods and days during which the VMG performs scheduled rules of certain features (such as Firewall Access Control) in the **Scheduler Rule** screen.

20.2 The Scheduler Rule Screen

Use this screen to view, add, or edit time schedule rules.

Click **Security > Scheduler Rule** to open the following screen.

Figure 120 Security > Scheduler Rule



Scheduler Rules

A scheduler rule is a scheduling setting and a re-usable object that should be used in conjunction with other configurations.

#	Rule Name	Day	Time	Description	Modify

The following table describes the fields in this screen.

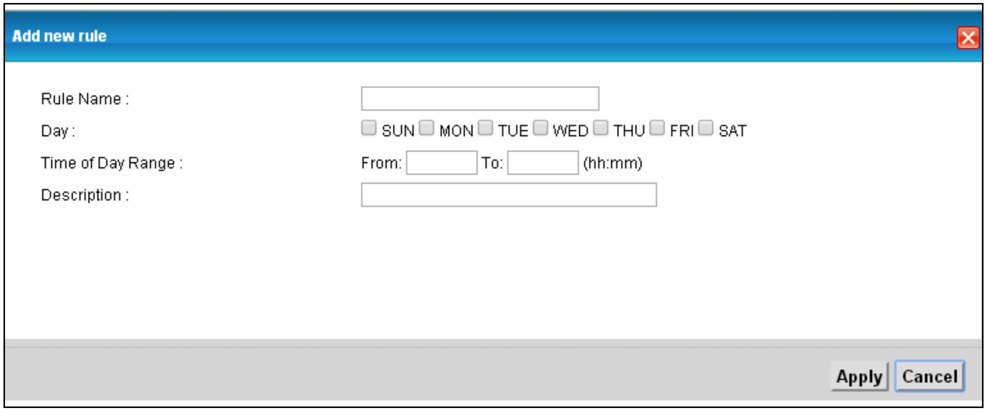
Table 92 Security > Scheduler Rule

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the day(s) on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the **Edit** icon to edit the schedule. Click the **Delete** icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

20.2.1 Add/Edit a Schedule

Click the **Add** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

Figure 121 Scheduler Rule: Add/Edit



The following table describes the fields in this screen.

Table 93 Scheduler Rule: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule.
Day	Select check boxes for the days that you want the VMG to perform this scheduler rule.
Time if Day Range	Enter the time period of each day, in 24-hour format, during which the rule will be enforced.
Description	Enter a description for this scheduler rule.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

21

Certificates

21.1 Overview

The VMG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner’s identity and public key. Certificates provide a way to exchange public keys for use in authentication.

21.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the VMG's CA-signed certificates (Section 21.4 on page 247).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the VMG (Section 21.4 on page 247).

21.2 What You Need to Know

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

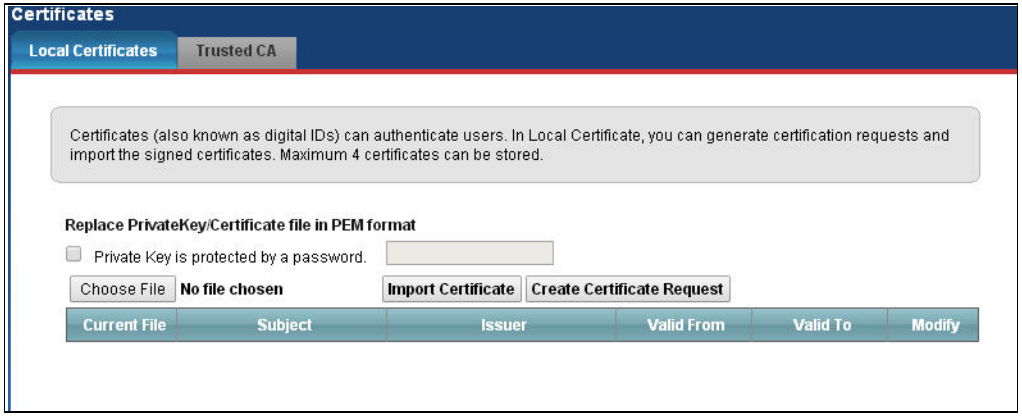
Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the VMG to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

21.3 The Local Certificates Screen

Click **Security > Certificates** to open the **Local Certificates** screen. This is the VMG’s summary list of certificates and certification requests.

Figure 122 Security > Certificates > Local Certificates



Certificates (also known as digital IDs) can authenticate users. In Local Certificate, you can generate certification requests and import the signed certificates. Maximum 4 certificates can be stored.

The following table describes the labels in this screen.

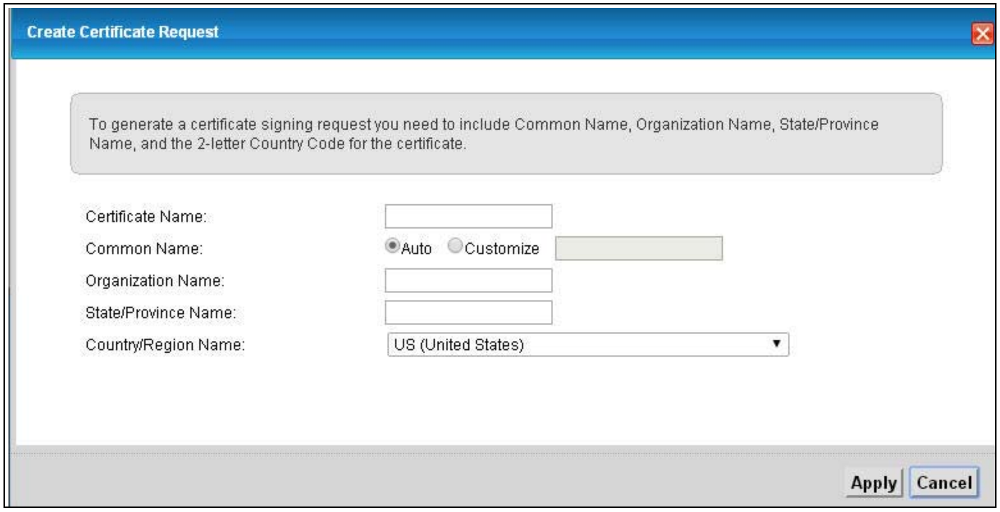
Table 94 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Private Key is protected by a password	Select the checkbox and enter the private key into the text box to store it on the VMG. The private key should not exceed 63 ASCII characters (not including spaces).
Browse...	Click this to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the VMG.
Create Certificate Request	Click this button to go to the screen where you can have the VMG generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate’s owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate’s issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

21.3.1 Create Certificate Request

Click **Security** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the VMG generate a certification request.

Figure 123 Create Certificate Request



Create Certificate Request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:	
Common Name:	● Auto ○ Customize
Organization Name:	
State/Province Name:	
Country/Region Name:	US (United States) ▼

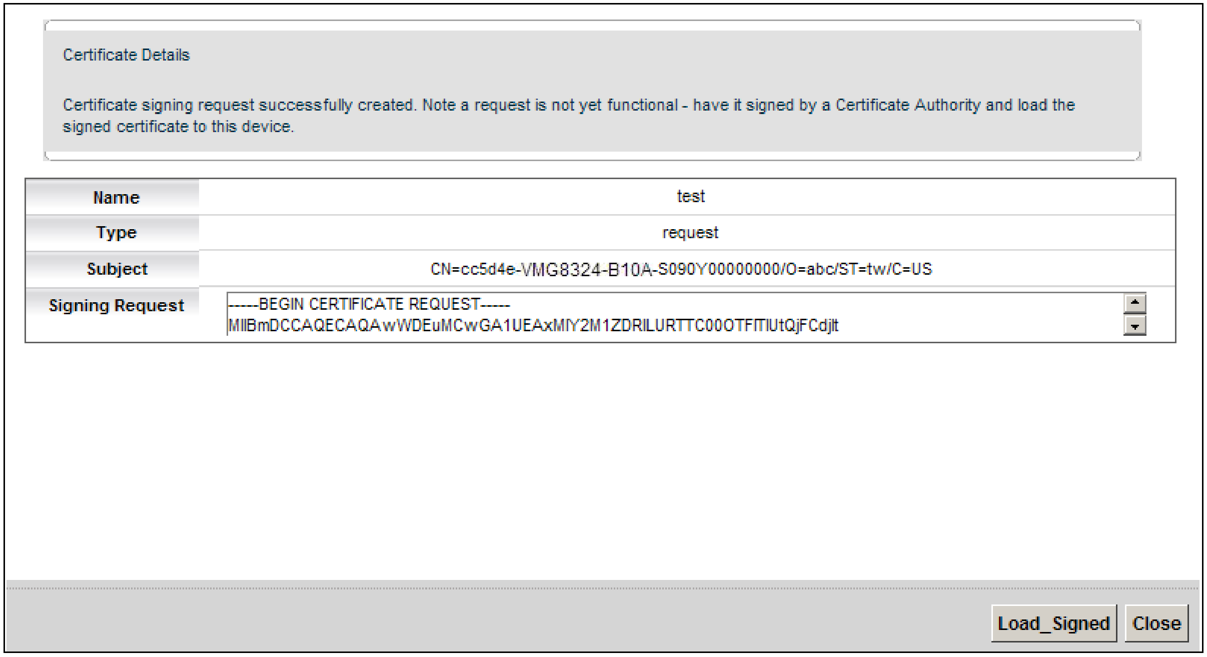
The following table describes the labels in this screen.

Table 95 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select **Auto** to have the VMG configure this field automatically. Or select **Customize** to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the VMG drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the VMG drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

After you click **Apply**, the following screen displays to notify you that you need to get the certificate request signed by a Certificate Authority. If you already have, click **Load_Signed** to import the signed certificate into the VMG. Otherwise click **Back** to return to the **Local Certificates** screen.

Figure 124 Certificate Request Created



Certificate Details

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

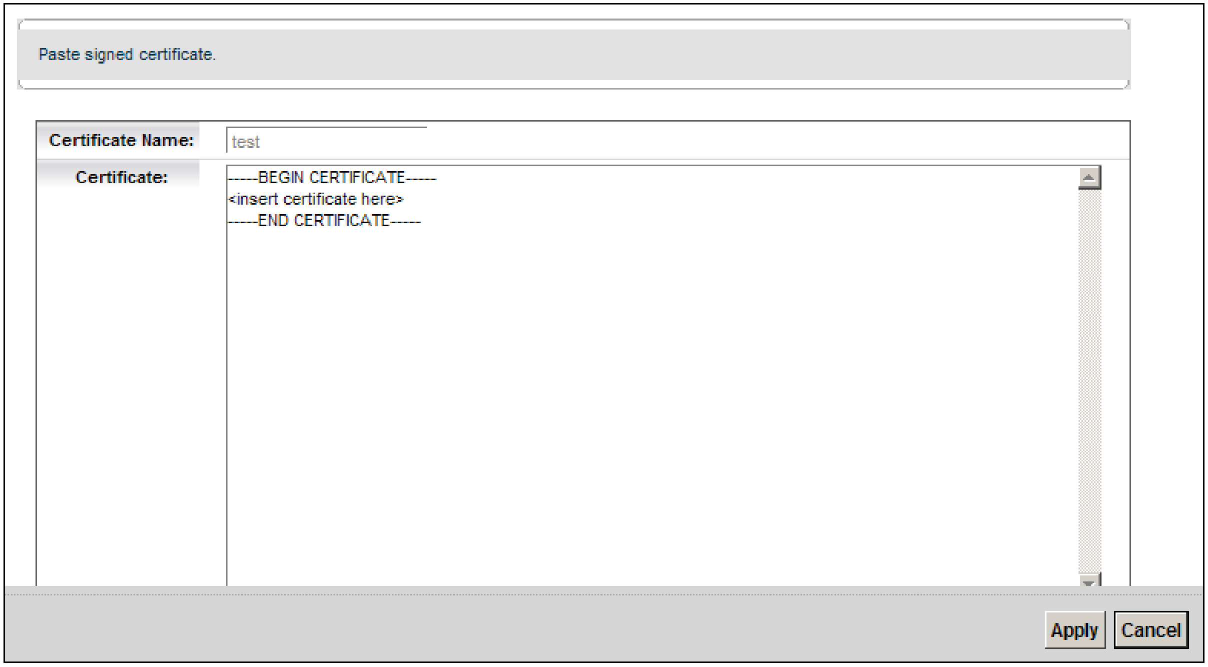
Name	test
Type	request
Subject	CN=cc5d4e-VMG8324-B10A-S090Y00000000/O=abc/ST=tw/C=US
Signing Request	-----BEGIN CERTIFICATE REQUEST----- MIIBmDCCAQECAQAwWDEuMCwGA1UEAxMlY2M1ZDRlLURTTC00OTFlTlUtQjFCdjlt

21.3.2 Load Signed Certificate

After you create a certificate request and have it signed by a Certificate Authority, in the **Local Certificates** screen click the certificate request's **Load Signed** icon to import the signed certificate into the VMG.

Note: You must remove any spaces from the certificate's filename before you can import it.

Figure 125 Load Signed Certificate



Paste signed certificate.

Certificate Name:	test
Certificate:	-----BEGIN CERTIFICATE----- <insert certificate here> -----END CERTIFICATE-----

The following table describes the labels in this screen.

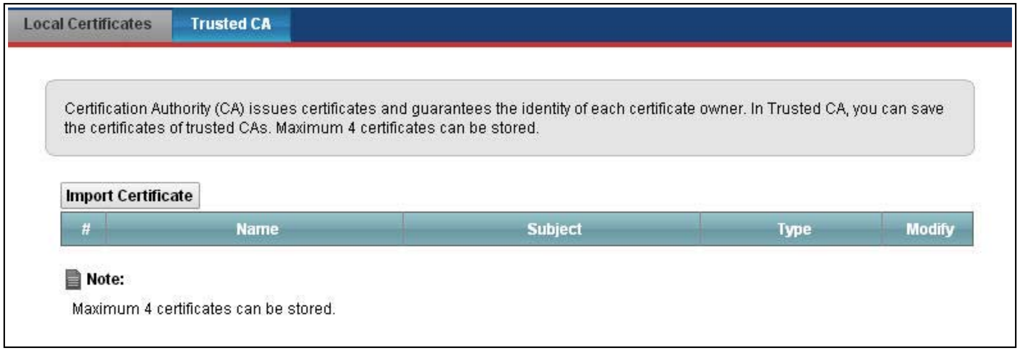
Table 96 Load Signed Certificate

LABEL	DESCRIPTION
Certificate Name	This is the name of the signed certificate.
Certificate	Copy and paste the signed certificate into the text box to store it on the VMG.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

21.4 The Trusted CA Screen

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the VMG to accept as trusted. The VMG accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 126 Security > Certificates > Trusted CA



Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. In Trusted CA, you can save the certificates of trusted CAs. Maximum 4 certificates can be stored.

#	Name	Subject	Type	Modify

Note:

Maximum 4 certificates can be stored.

The following table describes the fields in this screen.

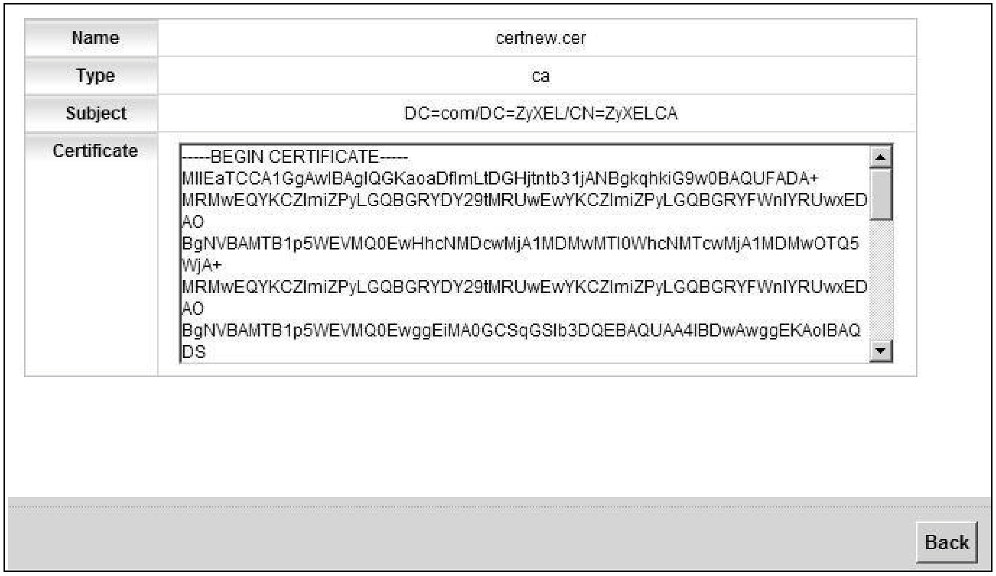
Table 97 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the VMG.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

21.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 127 Trusted CA: View



Name	certnew.cer
Type	ca
Subject	DC=com/DC=ZyXEL/CN=ZyXELCA
Certificate	

```
-----BEGIN CERTIFICATE-----
MIIEaTCCA1GgAwIBAgIQGKaoaDflmLtDGHjtntb31jANBgkqhkiG9w0BAQUFADA+
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFWnlYRUwxED
AO
BgNVBAMTB1p5WEVMQ0EwHhcNMDcwMjA1MDMwMTI0WhcNMTcwMjA1MDMwOTQ5
WjA+
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFWnlYRUwxED
AO
BgNVBAMTB1p5WEVMQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ
DS
```

The following table describes the fields in this screen.

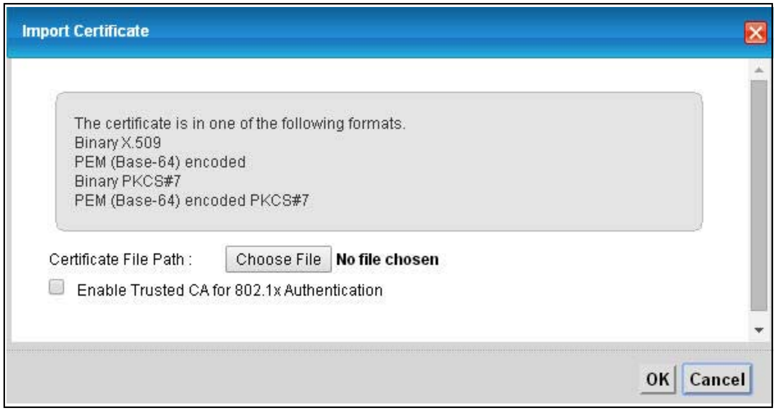
Table 98 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.

21.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The VMG trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 128 Trusted CA: Import Certificate



The certificate is in one of the following formats.
Binary X.509
PEM (Base-64) encoded
Binary PKCS#7
PEM (Base-64) encoded PKCS#7

Certificate File Path : Choose File **No file chosen**

□ Enable Trusted CA for 802.1x Authentication

The following table describes the fields in this screen.

Table 99 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the certificate you want to upload in this field or click **Browse ...** to find it.
Enable Trusted CA for 802.1x Authentication	If you select this checkbox, the trusted CA will be used for 802.1x authentication. The selected trusted CA will be displayed in the **Network Setting** > **Broadband** > **802.1x: Edit** screen.
Certificate	Copy and paste the certificate into the text box to store it on the VMG.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

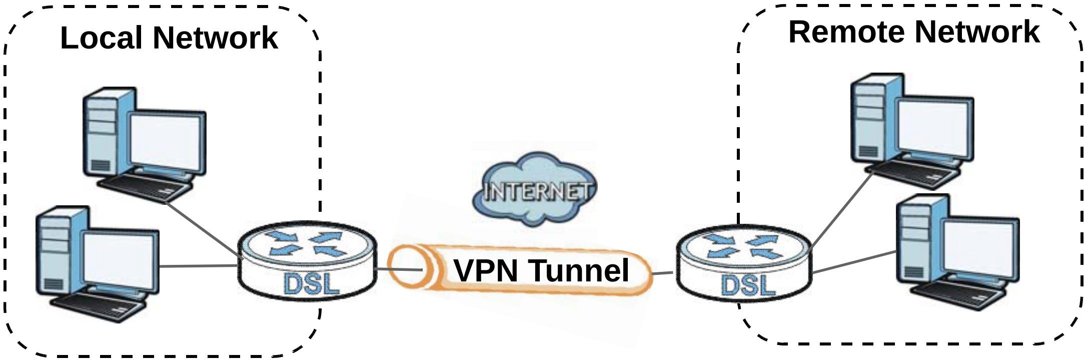
22

VPN

22.1 Overview

A virtual private network (VPN) provides secure communications over the the Internet. Internet Protocol Security (IPSec) is a standards-based VPN that provides confidentiality, data integrity, and authentication. This chapter shows you how to configure the VMG's VPN settings.

Figure 129 IPSec Fields Summary

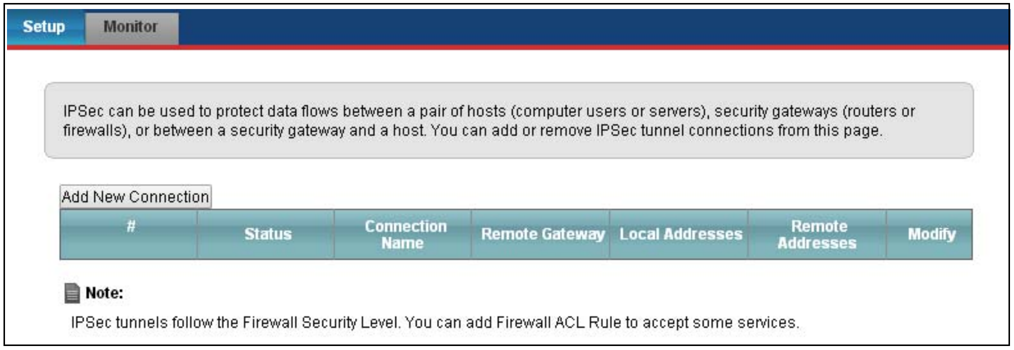


22.2 The IPSec VPN Setup Screen

Use this screen to view and manage your VPN tunnel policies. The following figure helps explain the main fields in the web configurator.

Click **Security > IPSec VPN** to open this screen as shown next.

Figure 130 Security > IPSec VPN



IPSec can be used to protect data flows between a pair of hosts (computer users or servers), security gateways (routers or firewalls), or between a security gateway and a host. You can add or remove IPSec tunnel connections from this page.

Add New Connection

#	Status	Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Modify

Note:

IPSec tunnels follow the Firewall Security Level. You can add Firewall ACL Rule to accept some services.

This screen contains the following fields:

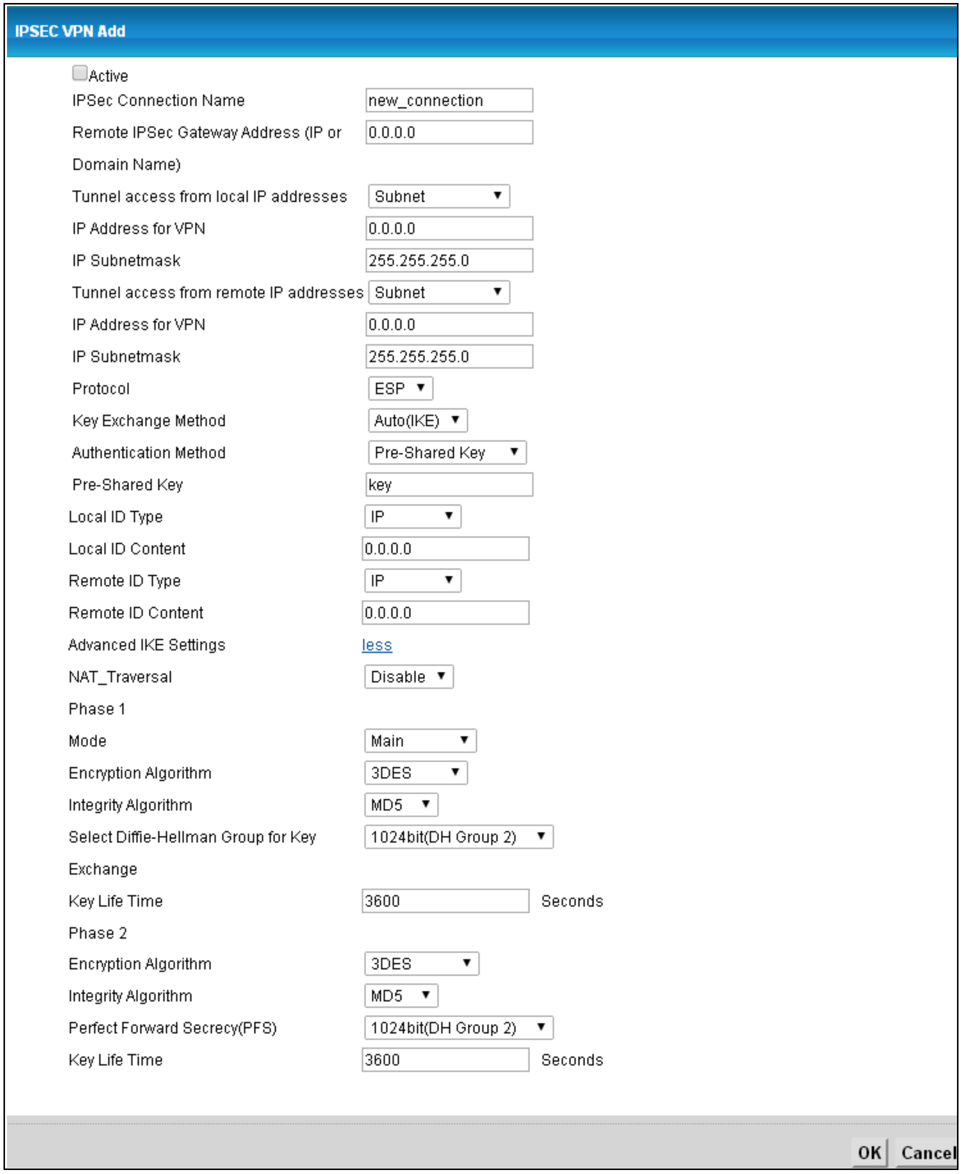
Table 100 Security > IPSec VPN

LABEL	DESCRIPTION
Add New Connection	Click this button to add an item to the list.
#	This displays the index number of an entry.
Status	This displays whether the VPN policy is enabled (**Enable**) or not (**Disable**).
Connection Name	The name of the VPN policy.
Remote Gateway	This is the IP address of the remote IPSec router in the IKE SA.
Local Addresses	This displays the IP address(es) on the LAN behind your VMG.
Remote Addresses	This displays the IP address(es) on the LAN behind the remote IPSec's router.
Modify	Click the **Edit** icon to modify the VPN policy. Click the **Delete** icon to delete the VPN policy.

22.2.1 The IPSec VPN Add/Edit Screen

Use these settings to add or edit VPN policies. Click the **Add New Connection** button in the **Security > VPN** screen to open this screen as shown next.

Figure 131 Security > IPSec VPN: Add/Edit



IPSEC VPN Add

☐ Active

IPSec Connection Name	new_connection
Remote IPSec Gateway Address (IP or Domain Name)	0.0.0.0
Tunnel access from local IP addresses	Subnet ▼
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet ▼
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Protocol	ESP ▼
Key Exchange Method	Auto(IKE) ▼
Authentication Method	Pre-Shared Key ▼
Pre-Shared Key	key
Local ID Type	IP ▼
Local ID Content	0.0.0.0
Remote ID Type	IP ▼
Remote ID Content	0.0.0.0
Advanced IKE Settings	less
NAT_Traversal	Disable ▼
Phase 1	
Mode	Main ▼
Encryption Algorithm	3DES ▼
Integrity Algorithm	MD5 ▼
Select Diffie-Hellman Group for Key Exchange	1024bit(DH Group 2) ▼
Key Life Time	3600 Seconds
Phase 2	
Encryption Algorithm	3DES ▼
Integrity Algorithm	MD5 ▼
Perfect Forward Secrecy(PFS)	1024bit(DH Group 2) ▼
Key Life Time	3600 Seconds

This screen contains the following fields:

Table 101 Security > IPSec VPN: Add/Edit

LABEL	DESCRIPTION
Active	Select this to activate this VPN policy.
IPSec Connection Name	Enter the name of the VPN policy.
Remote IPSec Gateway Address	Enter the IP address of the remote IPSec router in the IKE SA.
Tunnel access from local IP addresses	Select **Single Address** to have only one local LAN IP address use the VPN tunnel. Select **Subnet** to specify local LAN IP addresses by their subnet mask.

Table 101 Security > IPSec VPN: Add/Edit

LABEL	DESCRIPTION
IP Address for VPN	If **Single Address** is selected, enter a (static) IP address on the LAN behind your VMG. If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind your VMG. Then enter the subnet mask to identify the network address.
IP Subnetmask	If **Subnet** is selected, enter the subnet mask to identify the network address.
Tunnel access from remote IP addresses	Select **Single Address** to have only one remote LAN IP address use the VPN tunnel. Select **Subnet** to specify remote LAN IP addresses by their subnet mask.
IP Address for VPN	If **Single Address** is selected, enter a (static) IP address on the LAN behind the remote IPSec's router. If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind the remote IPSec's router. Then enter the subnet mask to identify the network address.
IP Subnetmask	If **Subnet** is selected, enter the subnet mask to identify the network address.
Protocol	Select which protocol you want to use in the IPSec SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Integraty Algorithm**. **ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption Agorithm** and **Integraty Algorithm**. Both **AH** and **ESP** increase processing requirements and latency (delay). The VMG and remote IPSec router must use the same active protocol.
Key Exchange Method	Select the key exchange method: **Auto(IKE)** - Select this to use automatic IKE key management VPN connection policy. **Manual** - Select this option to configure a VPN connection policy that uses a manual key instead of IKE key management. This may be useful if you have problems with IKE key management. Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA.
Authentication Method	Select **Pre-Shared Key** to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Select **Certificate (X.509)** to use a certificate for authentication.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself.
Local ID Type	Select **IP** to identify the VMG by its IP address. Select **E-mail** to identify this VMG by an e-mail address. Select **DNS** to identify this VMG by a domain name. Select **ASN1DN** (Abstract Syntax Notation one - Distinguished Name) to this VMG by the subject field in a certificate. This is used only with certificate-based authentication.

Table 101 Security > IPSec VPN: Add/Edit

LABEL	DESCRIPTION
Local ID Content	When you select IP in the **Local ID Type** field, type the IP address of your computer in this field. If you configure this field to 0.0.0.0 or leave it blank, the VMG automatically uses the **Pre-Shared Key** (refer to the **Pre-Shared Key** field description). It is recommended that you type an IP address other than 0.0.0.0 in this field or use the **DNS** or **E-mail** type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this VMG in this field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Remote ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **E-mail** to identify the remote IPSec router by an e-mail address. Select **DNS** to identify the remote IPSec router by a domain name. Select **ASN1DN** to identify the remote IPSec router by the subject field in a certificate. This is used only with certificate-based authentication.
Remote ID Content	The configuration of the remote content depends on the remote ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the VMG will use the address in the **Remote IPSec Gateway Address** field (refer to the **Remote IPSec Gateway Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than 0.0.0.0 or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the VMG to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
Advanced IKE Settings	Click **more** to display advanced settings. Click **less** to display basic settings only.
NAT_Traversal	Select **Enable** if you want to set up a VPN tunnel when there are NAT routers between the VMG and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router. Otherwise, select **Disable**.
Phase 1	
Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are: **Main** - this encrypts the VMG's and remote IPSec router's identities but takes more time to establish the IKE SA. **Aggressive** - this is faster but does not encrypt the identities. The VMG and the remote IPSec router must use the same negotiation mode.

Table 101 Security > IPSec VPN: Add/Edit

LABEL	DESCRIPTION
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES** - **128** - a 128-bit key with the AES encryption algorithm **AES** - **196** - a 196-bit key with the AES encryption algorithm **AES** - **256** - a 256-bit key with the AES encryption algorithm The VMG and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Integrity Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**. **SHA** is generally considered stronger than **MD5**, but it is also slower.
Select Diffie-Hellman Group for Key Exchange	Select which Diffie-Hellman key group you want to use for encryption keys. Choices for number of bits in the random number are: 768, 1024, 1536, 2048, 3072, 4096. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Key Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Phase 2	
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES** - **128** - a 128-bit key with the AES encryption algorithm **AES** - **192** - a 196-bit key with the AES encryption algorithm **AES** - **256** - a 256-bit key with the AES encryption algorithm Select **ESP_NULL** to set up a tunnel without encryption. When you select **ESP_NULL**, you do not enter an encryption key. The VMG and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Integrity Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **MD5** and **SHA1**. **SHA** is generally considered stronger than **MD5**, but it is also slower.

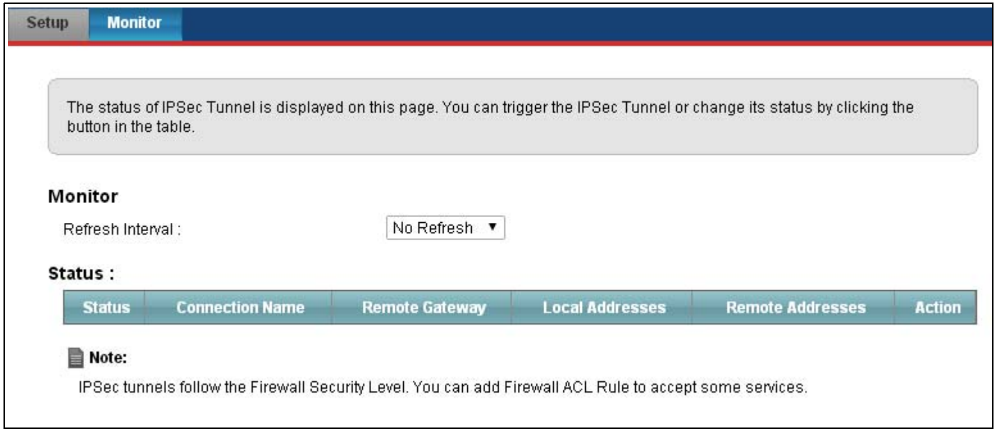
Table 101 Security > IPSec VPN: Add/Edit

LABEL	DESCRIPTION
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. Choices are: **None** - do not use any random number. **768bit(DH Group1)** - use a 768-bit random number **1024bit(DH Group2)** - use a 1024-bit random number **1536bit(DH Group5)** - use a 1536-bit random number **2048bit(DH Group14)** - use a 2048-bit random number **3072bit(DH Group15)** - use a 3072-bit random number **4096bit(DH Group16)** - use a 4096-bit random number
Key Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
The following fields are available if you select Manual in the Key Exchange Method field.	
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **EPS_NULL** - no encryption key or algorithm
Encryption Key	This field is applicable when you select an Encryption Algorithm. Enter the encryption key, which depends on the encryption algorithm. **DES** - type a unique key 16 hexadecimal characters long **3DES** - type a unique key 48 hexadecimal characters long
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are MD5, SHA1. SHA is generally considered stronger than MD5, but it is also slower.
Authentication Key	Enter the authentication key, which depends on the authentication algorithm. **MD5** - type a unique key 32 hexadecimal characters long **SHA1** - type a unique key 40 hexadecimal characters long
SPI	Type a unique SPI (Security Parameter Index) in hexadecimal characters. The SPI is used to identify the VMG during authentication. The VMG and remote IPSec router must use the same SPI.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

22.3 The IPSec VPN Monitor Screen

Use this screen to check your VPN tunnel's current status. You can also manually trigger a VPN tunnel to the remote network. Click **Security > IPSec VPN > Monitor** to open this screen as shown next.

Figure 132 Security > IPSec VPN > Monitor



The status of IPSec Tunnel is displayed on this page. You can trigger the IPSec Tunnel or change its status by clicking the button in the table.

Monitor

Refresh Interval : No Refresh ▼

Status :

Status	Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Action

Note:

IPSec tunnels follow the Firewall Security Level. You can add Firewall ACL Rule to accept some services.

This screen contains the following fields:

Table 102 Security > IPSec VPN > Monitor

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen. Select **No Refresh** to have the VMG stop updating the screen.
Status	This displays a green line between two hosts if the VPN tunnel has been established successfully. Otherwise, it displays a red line in between.
Connection Name	This displays the name of the VPN policy.
Remote Gateway	This is the IP address of the remote IPSec router in the IKE SA.
Local Addresses	This displays the IP address(es) on the LAN behind your VMG.
Remote Addresses	This displays the IP address(es) on the LAN behind the remote IPSec router.
Action	Click **Trigger** to establish a VPN connection with the remote network.

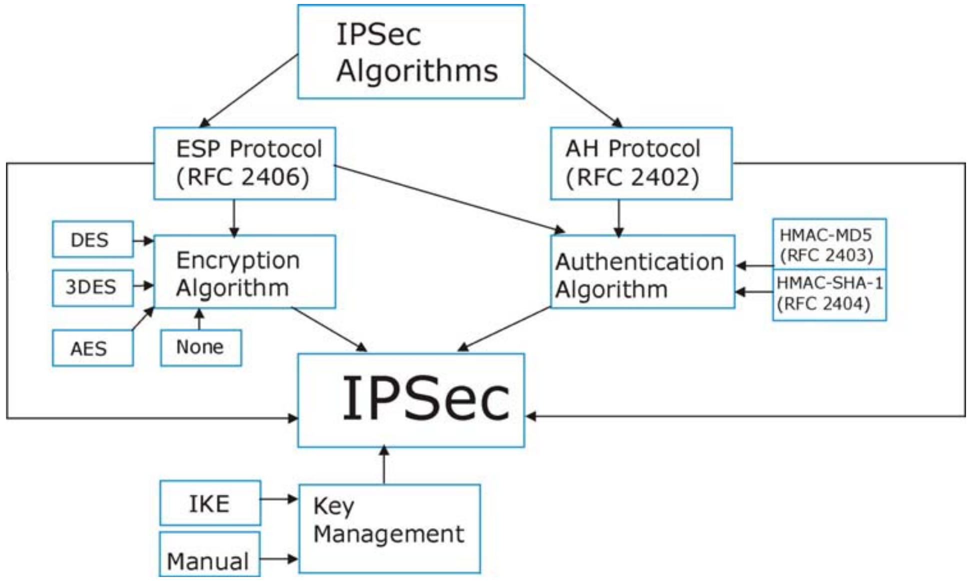
22.4 Technical Reference

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

22.4.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 133 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

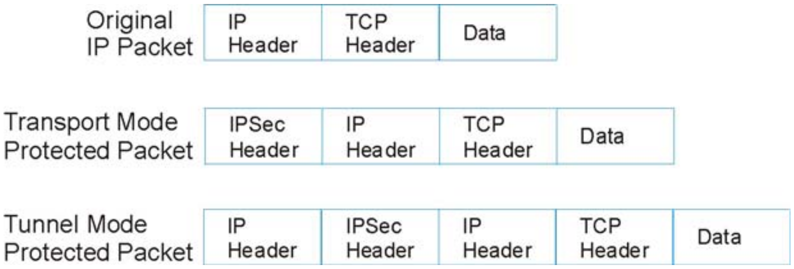
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

22.4.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the VMG supports **Tunnel** mode only.

Figure 134 Transport and Tunnel Mode IPSec Encapsulation



Original IP Packet	IP Header	TCP Header	Data		
Transport Mode Protected Packet	IPSec Header	IP Header	TCP Header	Data	
Tunnel Mode Protected Packet	IP Header	IPSec Header	IP Header	TCP Header	Data

Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

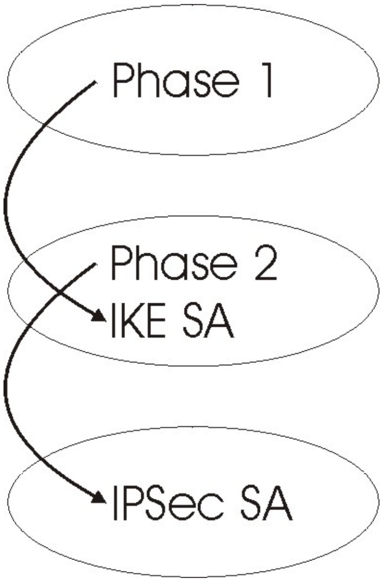
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

22.4.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 135 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The VMG automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

22.4.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).

- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

22.4.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the VMG.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 103 VPN and NAT

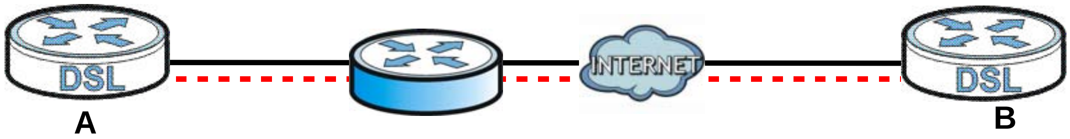
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

22.4.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the VMG’s **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 136 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In the above figure, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 104 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the VMG if you enable NAT traversal.

22.4.7 ID Type and Content

With aggressive negotiation mode (see Section 22.4.4 on page 261), the VMG identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the VMG to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the VMG does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 22.4.4 on page 261), the ID type and content are encrypted to provide identity protection. In this case the VMG can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The VMG can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section Figure 129 on page 251). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 105 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer.
DNS	Type a domain name (up to 31 characters) by which to identify this VMG.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this VMG.
	The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

22.4.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two VMGs in this example can complete negotiation and establish a VPN tunnel.

Table 106 Matching ID Type and Content Configuration Example

VMG A	VMG B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two VMGs in this example cannot complete their negotiation because VMG B’s **Local ID Type** is **IP**, but VMG A’s **Remote ID Type** is set to **E-mail**. An “ID mismatched” message displays in the IPSEC LOG.

Table 107 Mismatching ID Type and Content Configuration Example

VMG A	VMG B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2
Remote ID type: E-mail	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

22.4.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 22.4.3 on page 260 for more on IKE phases). It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

22.4.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

Voice

23.1 Overview

Use this chapter to:

- Connect an analog phone to the VMG.
- Make phone calls over the Internet, as well as the regular phone network.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

23.1.1 What You Can Do in this Chapter

These screens allow you to configure your VMG to make phone calls over the Internet and your regular phone line, and to set up the phones you connect to the VMG.

- Use the **SIP Account** screen (Section 23.3 on page 266) to set up information about your SIP account, control which SIP accounts the phones connected to the VMG use and configure audio settings such as volume levels for the phones connected to the VMG.
- Use the **SIP Service Provider** screen (Section 23.4 on page 271) to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions, and dialing plan.
- Use the **PhoneRegion** screen (Section 23.5 on page 279) to change settings that depend on the country you are in.
- Use the **Call Rule** screen (Section 23.6 on page 279) to set up shortcuts for dialing frequently-used (VoIP) phone numbers.
- Use the **Call History Summary** screen (Section 23.7 on page 280) to view the summary list of received, dialed and missed calls.
- Use the **Call History Outgoing** screen (Section 23.8 on page 281) to view detailed information for each outgoing call you made.
- Use the **Call History Incoming** screen (Section 23.9 on page 282) to view detailed information for each incoming call from someone calling you.

You don’t necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

23.1.2 What You Need to Know About VoIP

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signalling standard that lets one network device (like a computer or the VMG) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your VMG, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the VMG to use your SIP account to make calls, the VMG is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you don’t need a SIP account. It is possible for one SIP device (like the VMG) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup - figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

How to Find Out More

See Chapter 4 on page 35 for a tutorial showing how to set up these screens in an example scenario.

See Section 23.10 on page 282 for advanced technical information on SIP.

23.2 Before You Begin

- Before you can use these screens, you need to have a VoIP account already set up. If you don’t have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the VMG.

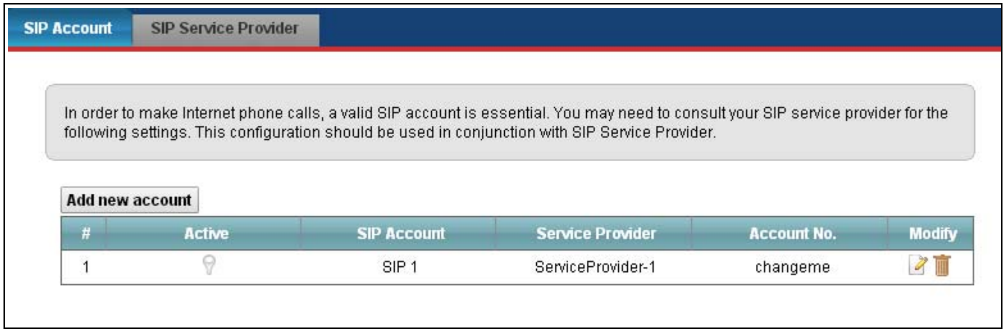
23.3 The SIP Account Screen

The VMG uses a SIP account to make outgoing VoIP calls and check if an incoming call’s destination number matches your SIP account’s SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your VMG to connect to your VoIP service provider.

See Section 23.3.1 on page 267 for how to map a SIP account to a phone port.

Use this screen to view SIP account information. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP > SIP Account**.

Figure 137 VoIP > SIP > SIP Account



In order to make Internet phone calls, a valid SIP account is essential. You may need to consult your SIP service provider for the following settings. This configuration should be used in conjunction with SIP Service Provider.

#	Active	SIP Account	Service Provider	Account No.	Modify
1	○	SIP 1	ServiceProvider-1	changeme	✎ 🗑

Each field is described in the following table.

Table 108 VoIP > SIP > SIP Account

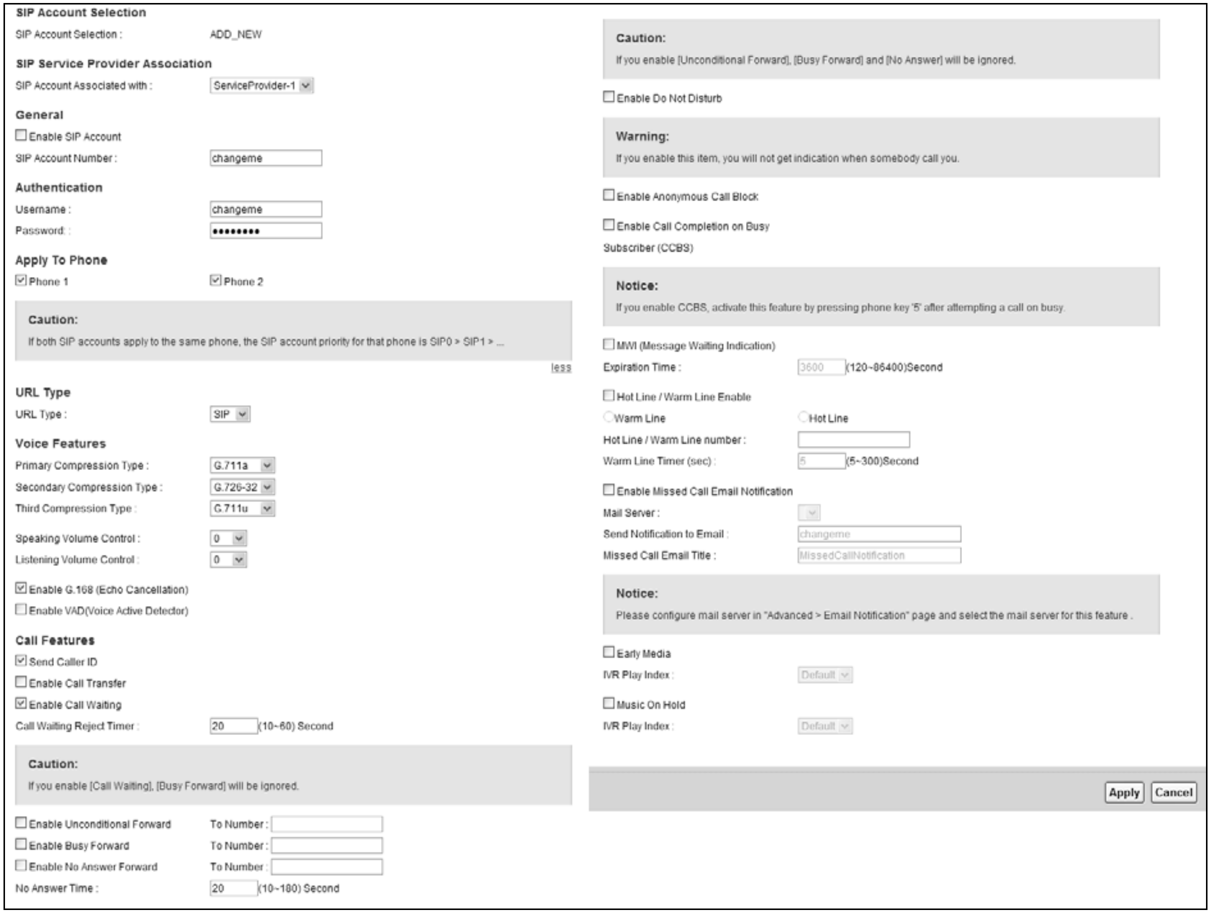
LABEL	DESCRIPTION
Add new account	Click this to configure a SIP account.
#	This is the index number of the entry.
Active	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is not activated.
SIP Account	This shows the name of the SIP account.
Service Provider	This shows the name of the SIP service provider.
Account No.	This shows the SIP number.
Modify	Click the **Edit** icon to configure the SIP account. Click the **Delete** icon to delete this SIP account from the VMG.

23.3.1 The SIP Account Add/Edit Screen

Use this screen to configure a SIP account and map it to a phone port. To access this screen, click the **Add new account** button or click the **Edit** icon of an entry in the **VoIP > SIP > SIP Account** screen.

Note: Click **more** to see all the fields in the screen. You don’t necessarily need to use all these fields to set up your account. Click **less** to see and configure only the fields needed for this feature.

Figure 138 VoIP > SIP > SIP Account > Add new accoun/Edit



SIP Account Selection

SIP Account Selection : ADD_NEW

SIP Service Provider Association

SIP Account Associated with : ServiceProvider-1

General

□ Enable SIP Account

SIP Account Number : changeme

Authentication

Username : changeme

Password: : ••••••••

Apply To Phone

☑ Phone 1 ☑ Phone 2

Caution:

If both SIP accounts apply to the same phone, the SIP account priority for that phone is SIP0 > SIP1 > ...

less

URL Type

URL Type : SIP

Voice Features

Primary Compression Type : G.711a

Secondary Compression Type : G.726-32

Third Compression Type : G.711u

Speaking Volume Control : 0

Listening Volume Control : 0

☑ Enable G.168 (Echo Cancellation)

□ Enable VAD(Voice Active Detector)

Call Features

☑ Send Caller ID

□ Enable Call Transfer

☑ Enable Call Waiting

Call Waiting Reject Timer : 20 (10~60) Second

Caution:

If you enable [Call Waiting], [Busy Forward] will be ignored.

□ Enable Unconditional Forward To Number :

□ Enable Busy Forward To Number :

□ Enable No Answer Forward To Number :

No Answer Time : 20 (10~180) Second

Caution:

If you enable [Unconditional Forward], [Busy Forward] and [No Answer] will be ignored.

□ Enable Do Not Disturb

Warning:

If you enable this item, you will not get indication when somebody call you.

□ Enable Anonymous Call Block

□ Enable Call Completion on Busy Subscriber (CCBS)

Notice:

If you enable CCBS, activate this feature by pressing phone key '5' after attempting a call on busy.

□ MWI (Message Waiting Indication)

Expiration Time : 3600 (120~86400)Second

□ Hot Line / Warm Line Enable

○ Warm Line ○ Hot Line

Hot Line / Warm Line number :

Warm Line Timer (sec) : 5 (5~300)Second

□ Enable Missed Call Email Notification

Mail Server :

Send Notification to Email : changeme

Missed Call Email Title : MissedCallNotification

Notice:

Please configure mail server in "Advanced > Email Notification" page and select the mail server for this feature .

□ Early Media

IVR Play Index : Default

□ Music On Hold

IVR Play Index : Default

Each field is described in the following table.

Table 109 VoIP > SIP > SIP Account > Add new accoun/Edit

LABEL	DESCRIPTION
SIP Account Selection	This field displays **ADD_NEW** if you are creating a new SIP account or the SIP account you are modifying.
SIP Service Provider Association	Select the SIP service provider profile to use for the SIP account you are configuring in this screen. This field is read-only when you are modifying a SIP account.
General	
Enable SIP Account	Select this if you want the VMG to use this account. Clear it if you do not want the VMG to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.

Table 109 VoIP > SIP > SIP Account > Add new accoun/Edit (continued)

LABEL	DESCRIPTION
Apply To Phone	Select a phone port on which you want to make or receive phone calls for this SIP account. If you map a phone port to more than one SIP account, there is no way to distinguish between the SIP accounts when you receive phone calls. The VMG uses the most recently registered SIP account first when you make an outgoing call. If a phone port is not mapped to a SIP account, you cannot receive or make any calls on the phone connected to this phone port.
more/less	Click **more** to display and edit more information for the SIP account. Click **less** to display and configure the basic SIP account settings.
URI Type	Select whether or not to include the SIP service domain name when the VMG sends the SIP number. **SIP** - include the SIP service domain name. **TEL** - do not include the SIP service domain name.
Voice Features	
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder/decoder (codec) that you want the VMG to use. G.711 provides high voice quality but requires more bandwidth (64 kbps). G.711 is the default codec used by phone companies and digital handsets. • **G.711a** is typically used in Europe. • **G.711u** is typically used in North America and Japan. **G.726-24** operates at **24** kbps. **G.726-32** operates at **32** kbps. **G.722** is a 7 KHz wideband voice codec that operates at 48, 56 and 64 kbps. By using a sample rate of 16 kHz, G.722 can provide higher fidelity and better audio quality than narrowband codecs like G.711, in which the voice signal is sampled at 8 KHz. The VMG must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec. Select the VMG's first choice for voice coder/decoder. Select the VMG's second choice for voice coder/decoder. Select **None** if you only want the VMG to accept the first choice. Select the VMG's third choice for voice coder/decoder. Select **None** if you only want the VMG to accept the first or second choice.
Speaking Volume Control	Select the loudness that the VMG uses for speech that it sends to the peer device. **-12** is the quietest, and **12** is the loudest.
Listening Volume Control	Select the loudness that the VMG uses for speech that it receives from the peer device. **-12** is the quietest, and **12** is the loudest.
Enable G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Enable VAD (Voice Active Detector)	Select this if the VMG should stop transmitting when you are not speaking. This reduces the bandwidth the VMG uses.
Call Features	

Table 109 VoIP > SIP > SIP Account > Add new accoun/Edit (continued)

LABEL	DESCRIPTION
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Enable Call Transfer	Select this to enable call transfer on the VMG. This allows you to transfer an incoming call (that you have answered) to another phone.
Enable Call Waiting	Select this to enable call waiting on the VMG. This allows you to place a call on hold while you answer another incoming call on the same telephone number.
Call Waiting Reject Timer	Specify a time of seconds that the VMG waits before rejecting the second call if you do not answer it.
Enable Unconditional Forward	Select this if you want the VMG to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Enable Busy Forward	Select this if you want the VMG to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Enable No Answer Forward	Select this if you want the VMG to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
No Answer Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the VMG should wait for you to answer an incoming call before it considers the call is unanswered.
Enable Do Not Disturb	Select this to set your phone to not ring when someone calls you.
Enable Anonymous Call Block	Select this if you do not want the phone to ring when someone tries to call you with caller ID deactivated.
Enable Call Completion on Busy Subscriber (CCBS)	When you make a phone call but hear a busy tone, Call Completion on Busy Subscriber (CCBS) allows you to enable auto-callback by pressing 5 and hanging up the phone. The VMG then tries to call that phone number every minute since after you hang up the phone. When the called party becomes available within the CCBS timeout period (60 minutes by default), both phones ring. • If the called party's phone rings because of CCBS but no one answers the phone after 180 seconds, you will hear a busy tone. You can enable CCBS on the called number again. • If you manually call the number on which you have enabled CCBS before the CCBS timeout period expires, the VMG disables CCBS on the called number. • If you call a second number before the first called number's CCBS timeout period expires, the VMG stops calling the first number until you finish the second call. Select this option to activate CCBS on the VMG.
MWI (Message Waiting Indication)	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
Expiration Time	Keep the default value for this field, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the VMG subscribes to the service. Before this time passes, the VMG automatically subscribes again.
Hot Line / Warm Line Enable	Select this to enable the hot line or warm line feature on the VMG.

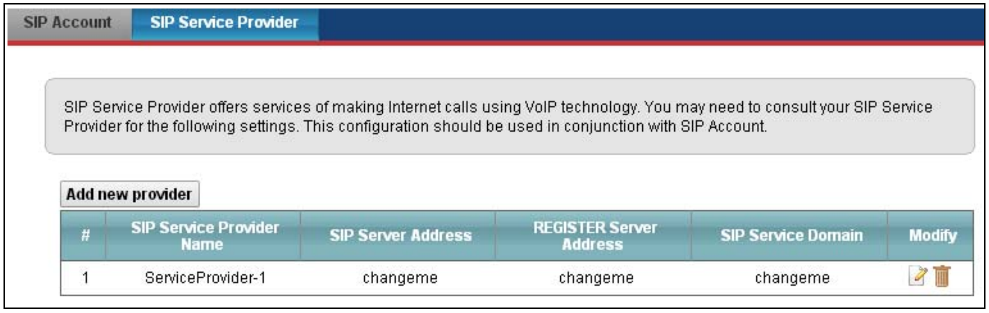
Table 109 VoIP > SIP > SIP Account > Add new accoun/Edit (continued)

LABEL	DESCRIPTION
Warm Line	Select this to have the VMG dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.
Hot Line	Select this to have the VMG dial the specified hot line number immediately when you pick up the telephone.
Hot Line / Warm Line number	Enter the number of the hot line or warm line that you want the VMG to dial.
Warm Line Timer	Enter a number of seconds that the VMG waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
Enable Missed Call Email Notification	Select this option to have the VMG e-mail you a notification when there is a missed call.
Mail Server	Select a mail server for the e-mail address specified below. If you select **None** here, e-mail notifications will not be sent via e-mail. You must have configured a mail server already in the **Email Notification** screen.
Send Notification to Email	Notifications are sent to the e-mail address specified in this field. If this field is left blank, notifications will not be sent via e-mail.
Missed Call Email Title	Type a title that you want to be in the subject line of the e-mail notifications that the VMG sends.
Early Media	Select this option if you want people to hear a customized recording when they call you.
IVR Play Index	Select the tone you want people to hear when they call you. This field is configurable only when you select **Early Media**. See Section 23.10 on page 282 for information on how to record these tones.
Music On Hold	Select this option to play a customized recording when you put people on hold.
IVR Play Index	Select the tone to play when you put someone on hold. This field is configurable only when you select **Music On Hold**. See Section 23.10 on page 282 for information on how to record these tones.
Apply	Click this to save your changes and to apply them to the VMG.
Cancel	Click this to set every field in this screen to its last-saved value.

23.4 The SIP Service Provider Screen

Use this screen to view the SIP service provider information on the VMG. Click **VoIP > SIP > SIP Service Provider** to open the following screen.

Figure 139 VoIP > SIP > SIP Service Provider



SIP Service Provider offers services of making Internet calls using VoIP technology. You may need to consult your SIP Service Provider for the following settings. This configuration should be used in conjunction with SIP Account.

#	SIP Service Provider Name	SIP Server Address	REGISTER Server Address	SIP Service Domain	Modify
1	ServiceProvider-1	changeme	changeme	changeme	✎ 🗑

Each field is described in the following table.

Table 110 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
Add new provider	
#	This is the index number of the entry.
SIP Service Provider Name	This shows the name of the SIP service provider.
SIP Server Address	This shows the IP address or domain name of the SIP server.
REGISTER Server Address	This shows the IP address or domain name of the SIP register server.
SIP Service Domain	This shows the SIP service domain name.
Modify	Click the **Edit** icon to configure the SIP service provider. Click the **Delete** icon to delete this SIP service provider from the VMG.

23.4.1 The SIP Service Provider Add/Edit Screen

A dial plan defines the dialing patterns, such as the length and range of the digits for a telephone number. It also includes country codes, access codes, area codes, local numbers, long distance numbers or international call prefixes. For example, the dial plan ([2-9]xxxxxx) does not allow a local number which begins with 1 or 0.

Without a dial plan, users have to manually enter the whole callee's number and wait for the specified dialing interval to time out or press a terminator key (usually the pound key on the phone keypad) before the VMG makes the call.

The VMG initializes a call when the dialed number matches any one of the rules in the dial plan. Dial plan rules follow these conventions:

- The collection of rules is in parentheses ().
- Rules are separated by the | (bar) symbol.
- "x" stands for a wildcard and can be any digit from 0 to 9.
- A subset of keys is in a square bracket []. Ranges are allowed.

  For example, [359] means a number matching this rule can be 3, 5 or 9. [26-8*] means a number matching this rule can be 2, 6, 7, 8 or *.

- The dot "." appended to a digit allows the digit to be ignored or repeated multiple times. Any digit (0~9, *, #) after the dot will be ignored.

  For example, (01.) means a number matching this rule can be 0, 01, 0111, 01111, and so on.
- <dialed-number:translated-number> indicates the number after the colon replaces the number before the colon in an angle bracket <>. For example,

  (<:1212> xxxxxxx) means the VMG automatically prefixes the translated-number "1212" to the number you dialed before making the call. This can be used for local calls in the US.

  (<9:> xxx xxxxxxx) means the VMG automatically removes the specified prefix "9" from the number you dialed before making the call. This is always used for making outside calls from an office.

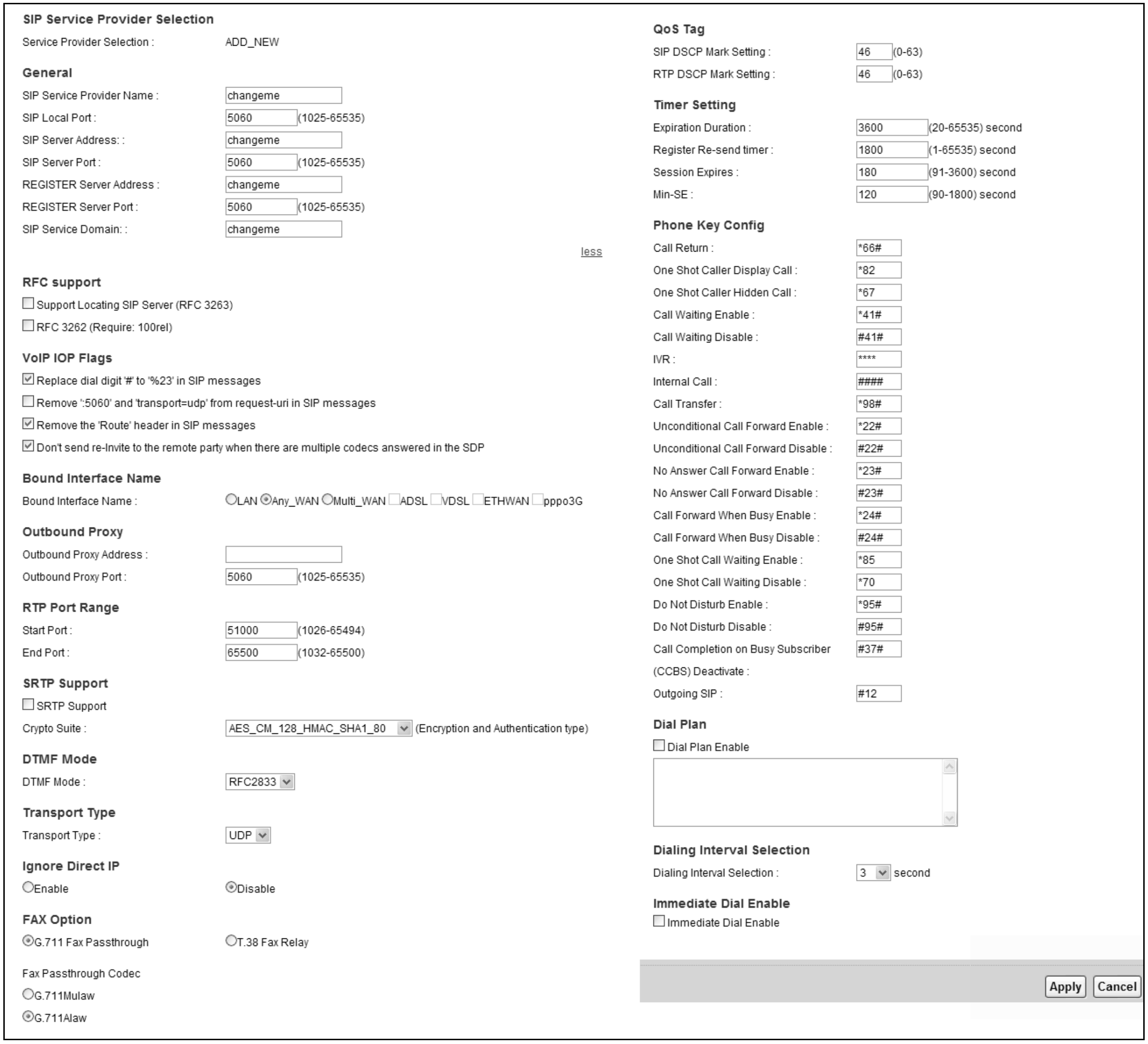
  (xx<123:456>xxxx) means the VMG automatically translates "123" to "456" in the number you dialed before making the call.
- Calls with a number followed by the exclamation mark "!" will be dropped.
- Calls with a number followed by the termination character "@" will be made immediately. Any digit (0~9, *, #) after the @ character will be ignored.

In this example dial plan (0 | [49]11 | 1 [2-9]xx xxxxxxx | 1 947 xxxxxxx !), you can dial "0" to call the local operator, call 411 or 911, or make a long distance call with an area code starting from 2 to 9 in the US. The calls with the area code 947 will be dropped.

Use the SIP Service Provider Add/Edit screen to configure a SIP service provider on the VMG. Click the **Add new provider** button or an **Edit** icon in the **VoIP > SIP > SIP Service Provider** to open the following screen.

Note: Click **more** to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click **less** to see and configure only the fields needed for this feature.

Figure 140 VoIP > SIP > SIP Service Provider > Add new provider/Edit



SIP Service Provider Selection

Service Provider Selection :	ADD_NEW

General

SIP Service Provider Name :	changeme
SIP Local Port :	5060 (1025-65535)
SIP Server Address: :	changeme
SIP Server Port :	5060 (1025-65535)
REGISTER Server Address :	changeme
REGISTER Server Port :	5060 (1025-65535)
SIP Service Domain: :	changeme

RFC support

□ Support Locating SIP Server (RFC 3263)

□ RFC 3262 (Require: 100rel)

VoIP IOP Flags

☑ Replace dial digit '#' to '%23' in SIP messages

□ Remove ':5060' and 'transport=udp' from request-uri in SIP messages

☑ Remove the 'Route' header in SIP messages

☑ Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP

Bound Interface Name

Bound Interface Name : ○LAN ●Any_WAN ○Multi_WAN □ADSL □VDSL □ETHWAN □pppo3G

Outbound Proxy

Outbound Proxy Address :	
Outbound Proxy Port :	5060 (1025-65535)

RTP Port Range

Start Port :	51000 (1026-65494)
End Port :	65500 (1032-65500)

SRTP Support

□ SRTP Support

Crypto Suite : AES_CM_128_HMAC_SHA1_80 (Encryption and Authentication type)

DTMF Mode

DTMF Mode : RFC2833

Transport Type

Transport Type : UDP

Ignore Direct IP

○Enable ●Disable

FAX Option

●G.711 Fax Passthrough ○T.38 Fax Relay

Fax Passthrough Codec

○G.711Mulaw

●G.711Alaw

QoS Tag

SIP DSCP Mark Setting :	46 (0-63)
RTP DSCP Mark Setting :	46 (0-63)

Timer Setting

Expiration Duration :	3600 (20-65535) second
Register Re-send timer :	1800 (1-65535) second
Session Expires :	180 (91-3600) second
Min-SE :	120 (90-1800) second

Phone Key Config

Call Return :	*66#
One Shot Caller Display Call :	*82
One Shot Caller Hidden Call :	*67
Call Waiting Enable :	*41#
Call Waiting Disable :	#41#
IVR :	****
Internal Call :	####
Call Transfer :	*98#
Unconditional Call Forward Enable :	*22#
Unconditional Call Forward Disable :	#22#
No Answer Call Forward Enable :	*23#
No Answer Call Forward Disable :	#23#
Call Forward When Busy Enable :	*24#
Call Forward When Busy Disable :	#24#
One Shot Call Waiting Enable :	*85
One Shot Call Waiting Disable :	*70
Do Not Disturb Enable :	*95#
Do Not Disturb Disable :	#95#
Call Completion on Busy Subscriber (CCBS) Deactivate :	#37#
Outgoing SIP :	#12

Dial Plan

□ Dial Plan Enable

Dialing Interval Selection

Dialing Interval Selection : 3 second

Immediate Dial Enable

□ Immediate Dial Enable

Each field is described in the following table.

Table 111 VoIP > SIP > SIP Service Provider > Add new provider/Edit

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen. If you change this field, the screen automatically refreshes.
General	
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the VMG's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.

Table 111 VoIP > SIP > SIP Service Provider > Add new provider/Edit (continued)

LABEL	DESCRIPTION
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
RFC Support	
Support Locating SIP Server (RFC3263)	Select this option to have the VMG use DNS procedures to resolve the SIP domain and find the SIP server's IP address, port number and supported transport protocol(s). The VMG first uses DNS Name Authority Pointer (NAPTR) records to determine the transport protocols supported by the SIP server. It then performs DNS Service (SRV) query to determine the port number for the protocol. The VMG resolves the SIP server's IP address by a standard DNS address record lookup. The **SIP Server Port** and **REGISTER Server Port** fields in the **General** section above are grayed out and not applicable and the **Transport Type** can also be set to **AUTO** if you select this option.
RFC 3262(Require: 100rel)	PRACK (RFC 3262) defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select this to have the the peer device require the option tag 100rel to send provisional responses reliably.
VoIP IOP Flags	Select the VoIP inter-operability settings you want to activate.
Replace dial digit '#' to '%23' in SIP messages	Replace a dial digit "#" with "%23" in the INVITE messages.
Remove ':5060' and 'transport=udp' from request-uri in SIP messages	Remove ":5060" and "transport=udp" from the "Request-URI" string in the REGISTER and INVITE packets.
Remove the 'Route' header in SIP messages	Remove the 'Route' header in SIP packets.
Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP	Do not send a re-Invite packet to the remote party when the remote party answers that it can support multiple codecs.
Bound Interface Name	

Table 111 VoIP > SIP > SIP Service Provider > Add new provider/Edit (continued)

LABEL	DESCRIPTION
Bound Interface Name	If you select **LAN** or **Any_WAN**, the VMG automatically activates the VoIP service when any LAN or WAN connection is up. If you select **Multi_WAN**, you also need to select two or more pre-configured WAN interfaces. The VoIP service is activated only when one of the selected WAN connections is up.
Outbound Proxy	
Outbound Proxy Address	Enter the IP address or domain name of the SIP outbound proxy server if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the VMG to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the VMG to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Outbound Proxy Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
SRTP Support	
SRTP Support	When you make a VoIP call using SIP, the Real-time Transport Protocol (RTP) is used to handle voice data transfer. The Secure Real-time Transport Protocol (SRTP) is a security profile of RTP. It is designed to provide encryption and authentication for the RTP data in both unicast and multicast applications. The VMG supports encryption using AES with a 128-bit key. To protect data integrity, SRTP uses a Hash-based Message Authentication Code (HMAC) calculation with Secure Hash Algorithm (SHA)-1 to authenticate data. HMAC SHA-1 produces a 80 or 32-bit authentication tag that is appended to the packet. Both the caller and callee should use the same algorithms to establish an SRTP session.
Crypto Suite	Select the encryption and authentication algorithm set used by the VMG to set up an SRTP media session with the peer device. Select **AES_CM_128_HMAC_SHA1_80** or **AES_CM_128_HMAC_SHA1_32** to enable both data encryption and authentication for voice data. Select **AES_CM_128_NULL** to use 128-bit data encryption but disable data authentication. Select **NULL_CIPHER_HMAC_SHA1_80** to disable encryption but require authentication using the default 80-bit tag.
DTMF Mode	
DTMF Mode	Control how the VMG handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** - send the DTMF tones in RTP packets. **PCM** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIP INFO** - send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the transport layer protocol **UDP** or **TCP** (usually UDP) used for SIP.

Table 111 VoIP > SIP > SIP Service Provider > Add new provider/Edit (continued)

LABEL	DESCRIPTION
Ignore Direct IP	Select **Enable** to have the connected CPE devices accept SIP requests only from the SIP proxy/register server specified above. SIP requests sent from other IP addresses will be ignored.
FAX Option	This field controls how the VMG handles fax messages.
G711 Fax Passthrough	Select this if the VMG should use G.711 to send fax messages. You have to also select which operating codec (**G.711Mulaw** or **G.711Alaw**) to use for encoding/decoding FAX data. The peer devices must use the same settings.
T38 Fax Relay	Select this if the VMG should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
QoS Tag	
SIP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The VMG creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The VMG creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The VMG automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the VMG waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the VMG lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the VMG lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the VMG accepts.
Phone Key Config	Enter the key combinations for certain functions of the SIP phone.
Call Return	Enter the key combinations that you can enter to place a call to the last number that called you.
One Shot Caller Display Call	Enter the key combinations that you can enter to activate caller ID for the next call only.
One Shot Caller Hidden Call	Enter the key combinations that you can enter to deactivate caller ID for the next call only.
Call Waiting Enable	Enter the key combinations that you can enter to turn on the call waiting function.
Call Waiting Disable	Enter the key combinations that you can enter to turn off the call waiting function.
IVR	Enter the key combinations that you can enter to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold). IVR stands for Interactive Voice Response.
Internal Call	Enter the key combinations that you can enter to call the phone(s) connected to the VMG.
Call Transfer	Enter the key combinations that you can enter to transfer a call to another phone.
Unconditional Call Forward Enable	Enter the key combinations that you can enter to forward all incoming calls to the phone number you specified in the **SIP > SIP Account** screen.
Unconditional Call Forward Disable	Enter the key combinations that you can enter to turn the unconditional call forward function off.

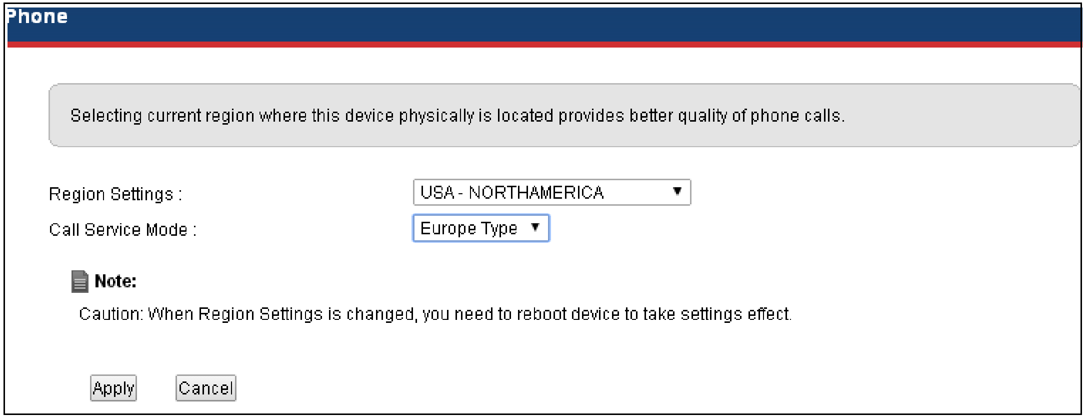
Table 111 VoIP > SIP > SIP Service Provider > Add new provider/Edit (continued)

LABEL	DESCRIPTION
No Answer Call Forward Enable	Enter the key combinations that you can enter to forward incoming calls to the phone number you specified in the **SIP > SIP Account** screen if the calls are unanswered.
No Answer Call Forward Disable	Enter the key combinations that you can enter to turn the no answer call forward function off.
Call Forward When Busy Enable	Enter the key combinations that you can enter to forward incoming calls to the phone number you specified in the **SIP > SIP Account** screen if the phone port is busy.
Call Forward When Busy Disable	Enter the key combinations that you can enter to turn the busy forward function off.
One Shot Call Waiting Enable	Enter the key combinations that you can enter to activate call waiting on the next calls.
One Shot Call Waiting Disable	Enter the key combinations that you can enter to deactivate call waiting on the next call only.
Do Not Disturb Enable	Enter the key combinations that you can enter to set your phone not to ring when someone calls you.
Do Not Disturb Disable	Enter the key combinations that you can enter to turn this function off.
Call Completion on Busy Subscriber (CCBS) Deactivate	Enter the key combinations that you can enter to disable CCBS on a call.
Outgoing SIP	Enter the key combinations that you can enter to select the SIP account that you use to make outgoing calls. If you enter #12(by default)<SIP account index number>#<the phone number you want to call>, #1201#12345678 for example, the VMG uses the first SIP account to call 12345678.
Dial Plan	
Dial Plan Enable	Select this to activate the dial plan rules you specify in the text box provided. See Section 23.5 on page 279 for how to set up a rule.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the VMG should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select **Immediate Dial Enable**, you can press the pound key (#) to tell the VMG to make the phone call immediately, regardless of this setting.
Immediate Dial Enable	
Immediate Dial Enable	Select this if you want to use the pound key (#) to tell the VMG to make the phone call immediately, instead of waiting the number of seconds you selected in the **Dialing Interval Selection** field. If you select this, dial the phone number, and then press the pound key. The VMG makes the call immediately, instead of waiting. You can still wait, if you want.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

23.5 The Phone Screen

Use this screen to maintain settings that depend on which region of the world the VMG is in. To access this screen, click **VoIP > Phone**.

Figure 141 VoIP > Phone



Phone

Selecting current region where this device physically is located provides better quality of phone calls.

Region Settings : USA - NORTHAMERICA

Call Service Mode : Europe Type

Note:

Caution: When Region Settings is changed, you need to reboot device to take settings effect.

Each field is described in the following table.

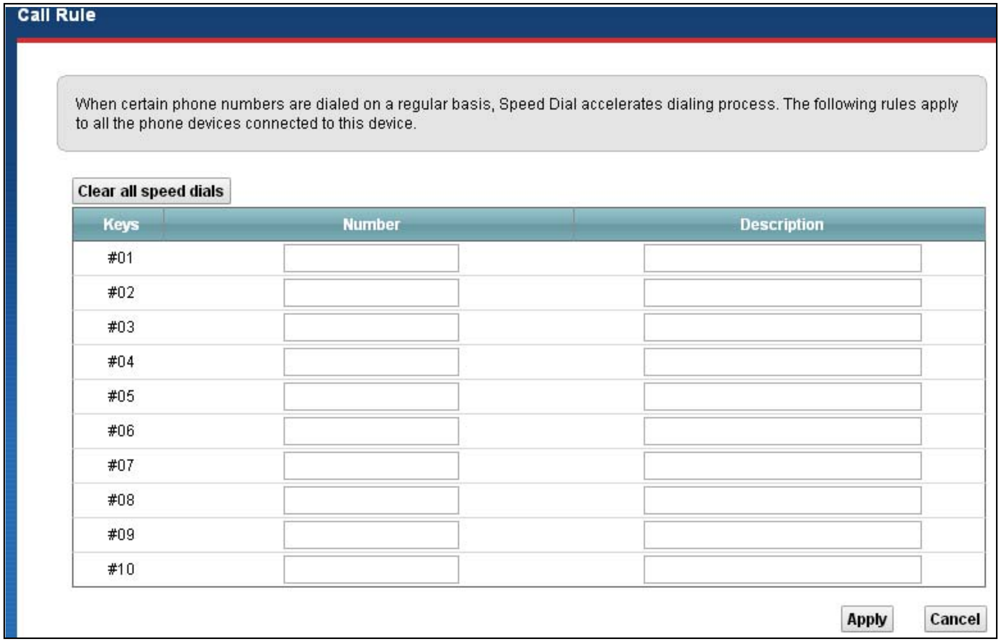
Table 112 VoIP > Phone

LABEL	DESCRIPTION
Region Settings	Select the place in which the VMG is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. **Europe Type** - use supplementary phone services in European mode **USA Type** - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the VMG.
Cancel	Click this to set every field in this screen to its last-saved value.

23.6 The Call Rule Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

Figure 142 VoIP > Call Rule



When certain phone numbers are dialed on a regular basis, Speed Dial accelerates dialing process. The following rules apply to all the phone devices connected to this device.

Keys	Number	Description
#01		
#02		
#03		
#04		
#05		
#06		
#07		
#08		
#09		
#10		

Each field is described in the following table.

Table 113 VoIP > Call Rule

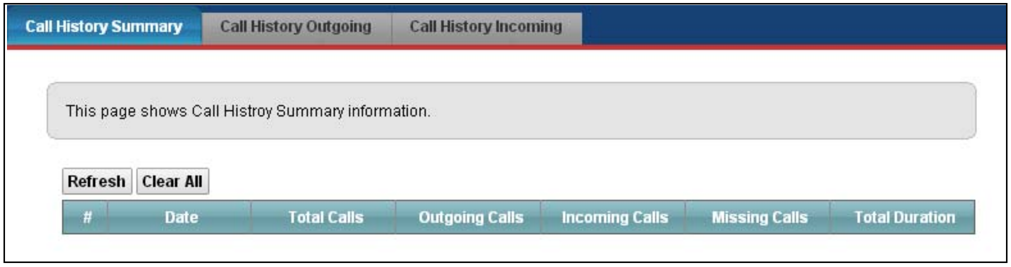
LABEL	DESCRIPTION
Clear all speed dials	Click this to erase all the speed-dial entries on this screen.
Keys	This field displays the speed-dial number you should dial to use this entry.
Number	Enter the SIP number you want the VMG to call when you dial the speed-dial number.
Description	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Apply	Click this to save your changes and to apply them to the VMG.
Cancel	Click this to set every field in this screen to its last-saved value.

23.7 The Call History Summary Screen

The VMG logs calls from or to your SIP numbers. This screen allows you to view the summary of received, dialed and missed calls.

Click **VoIP > Call History > Call History Summary**. The following screen displays.

Figure 143 VoIP > Call History > Call History Summary



This page shows Call Histroy Summary information.

#	Date	Total Calls	Outgoing Calls	Incoming Calls	Missing Calls	Total Duration

Each field is described in the following table.

Table 114 VoIP > Call History > Call History Summary

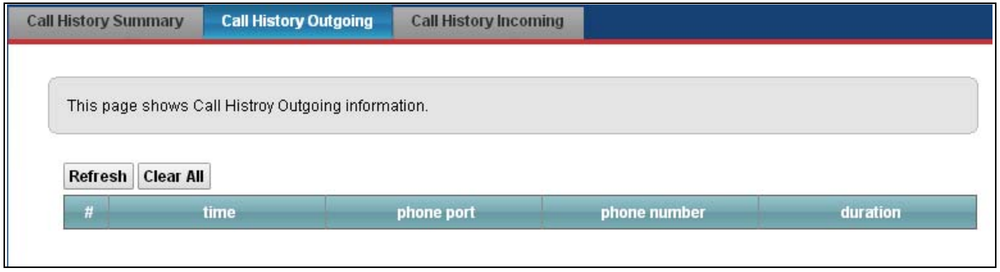
LABEL	DESCRIPTION
Refresh	Click this button to renew the call history list.
Clear All	Click this button to remove all entries from the call history list.
#	This is a read-only index number.
Date	This is the date when the calls were made.
Total Calls	This displays the total number of calls from or to your SIP numbers that day.
Outgoing Calls	This displays how many calls originated from you that day.
Incoming Calls	This displays how many calls you received that day.
Missing Calls	This displays how many incoming calls were not answered that day.
Total Duration	This displays how long all calls lasted that day.

23.8 The Call History Outgoing Calls Screen

Use this screen to see detailed information for each outgoing call you made.

Click **VoIP > Call History > Call History Outgoing**. The following screen displays.

Figure 144 VoIP > Call History > Call History Outgoing



This page shows Call Histroy Outgoing information.

#	time	phone port	phone number	duration

Each field is described in the following table.

Table 115 VoIP > Call History > Call History Outgoing

LABEL	DESCRIPTION
Refresh	Click this button to renew the dialed call list.
Clear All	Click this button to remove all entries from the dialed call list.
#	This is a read-only index number.
time	This is the date and time when the call was made.

Table 115 VoIP > Call History > Call History Outgoing

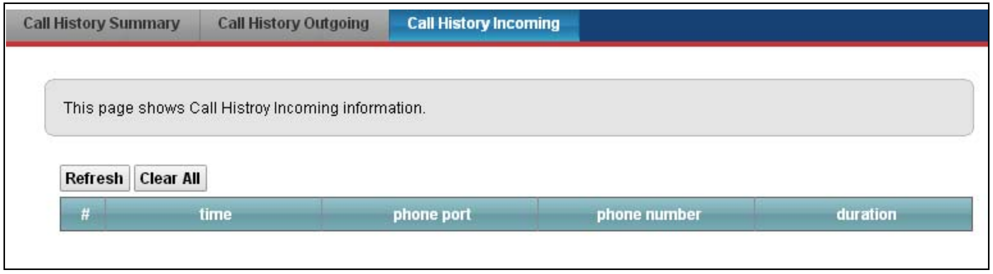
LABEL	DESCRIPTION
phone port	This is the phone port on which you made the call.
phone number	This is the SIP number you called.
duration	This displays how long the call lasted.

23.9 The Call History Incoming Calls Screen

Use this screen to see detailed information for each incoming call from someone calling you.

Click **VoIP > Call History > Call History Incoming Calls**. The following screen displays.

Figure 145 VoIP > Call History > Call History Incoming Calls



This page shows Call Histroy Incoming information.

#	time	phone port	phone number	duration

Each field is described in the following table.

Table 116 VoIP > Call History > Call History Incoming

LABEL	DESCRIPTION
Refresh	Click this button to renew the received call list.
Clear All	Click this button to remove all entries from the received call list.
#	This is a read-only index number.
time	This is the date and time when the call was made.
phone port	This is the phone port on which you received the call. **Missed** means the call was unanswered.
phone number	This is the SIP number that called you.
duration	This displays how long the call lasted.

23.10 Technical Reference

This section contains background material relevant to the **VoIP** screens.

VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

SIP Registration

Each VMG is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the VMG). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The VMG attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the VMG attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC 3261, "SIP: Session Initiation Protocol").

SIP Servers

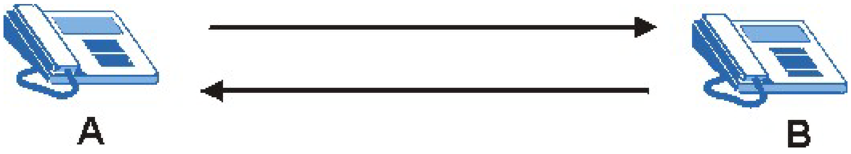
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

Figure 146 SIP User Agent



SIP Proxy Server

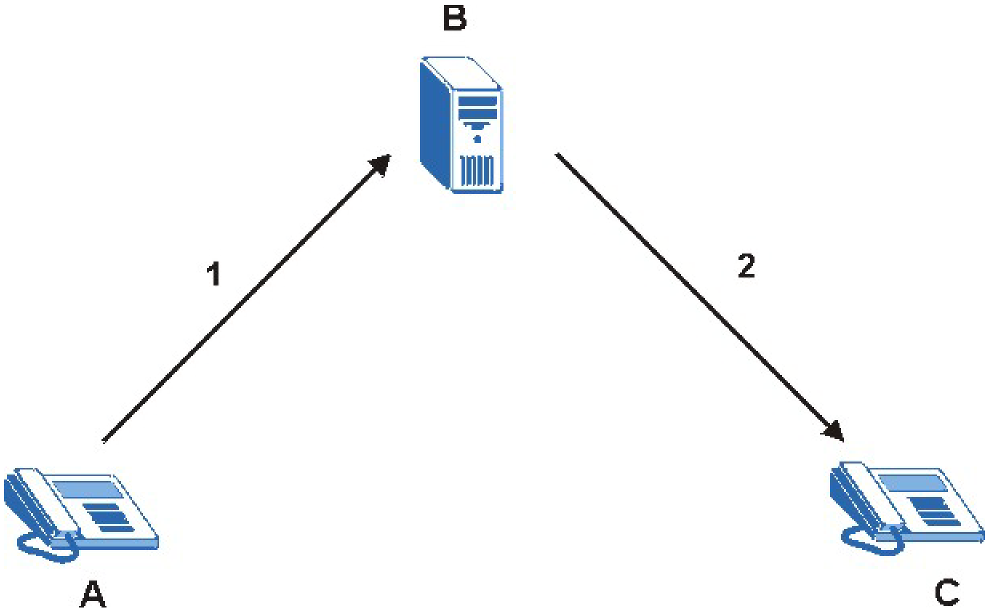
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device C.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).

2 The SIP proxy server forwards the call invitation to **C**.

Figure 147 SIP Proxy Server



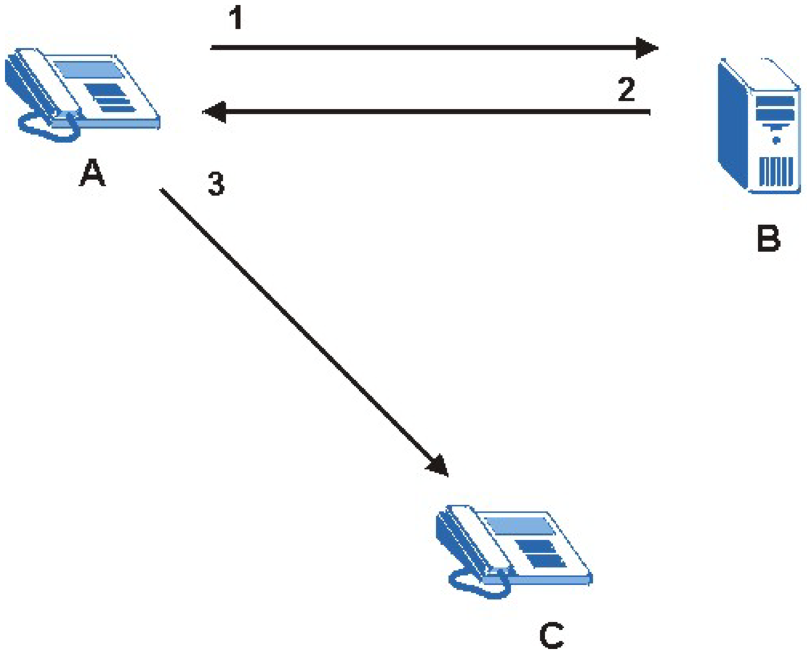
SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device **A** to call someone who is using client device **C**.

1. Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).
2. The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).
3. Client device **A** then sends the call invitation to client device **C**.

Figure 148 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 117 SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	
	5.Dialogue (voice traffic)	

Table 117 SIP Call Progression (continued)

A		B
6. BYE	→	
	←	7. OK

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

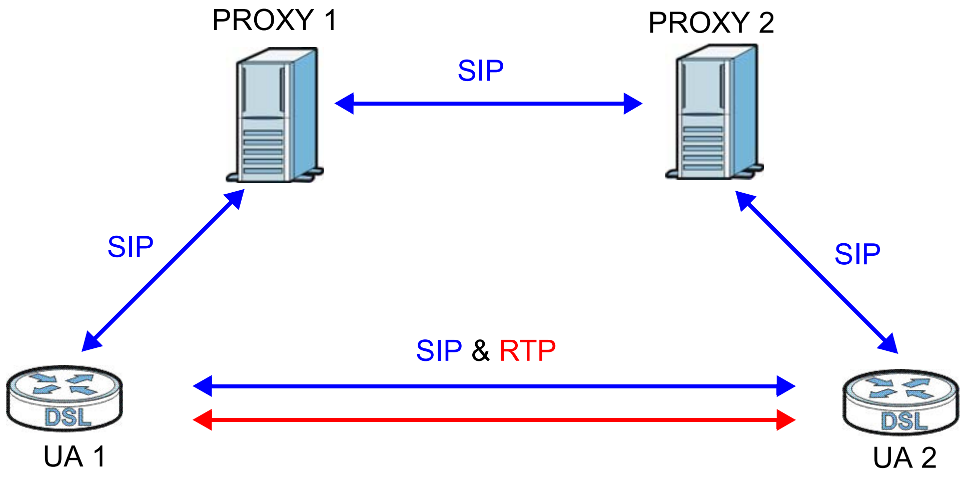
SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

Figure 149 SIP Call Through Proxy Servers



The following table shows the SIP call progression.

Table 118 SIP Call Progression

UA 1		PROXY 1		PROXY 2		UA 2
Invite	→					
		Invite	→			
	←	100 Trying		Invite	→	
			←	100 Trying		
					←	180 Ringing
			←	180 Ringing		
	←	180 Ringing				
					←	200 OK
			←	200 OK		
	←	200 OK				
ACK	→					
RTP	↔					RTP
	←					BYE
200 OK	→					

1 **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.

2 **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.

3 **Proxy 2** sends a SIP INVITE request to **User Agent 2**.

4 **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** via **Proxy 1**.

5 **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** via **Proxy 1**.

6 **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.

7 When **User Agent 2** hangs up, he sends a BYE request.

8 **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The VMG supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.

- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the VMG reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

Comfort Noise Generation

When using VAD, the VMG generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the VMG. The VMG allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 119 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	900 seconds for all custom tones combined
Maximum Time per Individual Tone	180 seconds
Total Number of Tones Recordable	5 You can record up to 5 different custom tones but the total time must be 900 seconds or less.

Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1 Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1101~1105 on your phone followed by the "#" key.

3 Play your desired music or voice recording into the receiver's mouthpiece. Press the "#" key.

4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Listening to Custom Tones

Do the following to listen to a custom tone:

1 Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1201~1208 followed by the "#" key to listen to the tone.

3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Deleting Custom Tones

Do the following to delete a custom tone:

1 Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1301~1308 followed by the "#" key to delete the tone of your choice. Press 14 followed by the "#" key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

23.10.1 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the VMG) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

DiffServ

DiffServ 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 (DSCP) 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.[3]

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) 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.

Figure 150 DiffServ: Differentiated Service Field

DSCP	Unused
(6-bit)	(2-bit)

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 priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

23.10.2 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The VMG supports the following services:

- Call Return
- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb
- IVR
- Call Completion
- CCBS
- Outgoing SIP

[3] The VMG does not support DiffServ at the time of writing.

Note: To take full advantage of the supplementary phone services available through the VMG's phone ports, you may need to subscribe to the services from your VoIP service provider.

23.10.2.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the VMG.

You can invoke all the supplementary services by using the flash key.

23.10.2.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 120 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.

  Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then “2”.

European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1 Press the flash key to put the caller on hold.

2 When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call.

3 After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1 When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.

2 Dial a phone number directly to make another call.

3 When the second call is answered, press the flash key and press “3” to create a three-way conversation.

4 Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

23.10.2.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 121 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

USA Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call (to party B).
3. When party B answers the second call, press the flash key to create a three-way conversation.

4 Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.

6 If you want to go back to the three-way conversation, press the flash key again.

7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

23.10.2.4 Phone Functions Summary

The following table shows the key combinations you can enter on your phone’s keypad to use certain features.

Table 122 Phone Functions Summary

ACTION	FUNCTION	DESCRIPTION
*98#	Call transfer	Transfer a call to another phone. See Section 23.10.2.2 on page 292 (Europe type) and Section 23.10.2.3 on page 293 (USA type).
*66#	Call return	Place a call to the last person who called you.
*95#	Enable Do Not Disturb	Use these to set your phone not to ring when someone calls you, or to turn this function off.
#95#	Disable Do Not Disturb	
*41#	Enable Call Waiting	Use these to allow you to put a call on hold when you are answering another, or to turn this function off.
#41#	Disable Call Waiting	
****	IVR	Use these to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold).
####	Internal Call	Call the phone(s) connected to the VMG.
*82	One Shot Caller Display Call	Activate or deactivate caller ID for the next call only.
*67	One Shot Caller Hidden Call	

Log

24.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the VMG log and then display the logs or have the VMG send them to an administrator (as e-mail) or to a syslog server.

24.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs (Section 24.2 on page 298).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 24.3 on page 299).

24.1.2 What You Need To Know

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

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 123 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.

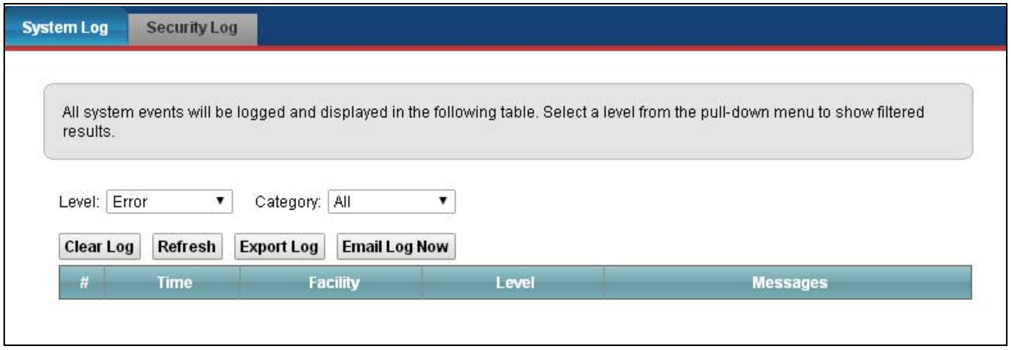
Table 123 Syslog Severity Levels

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

24.2 The System Log Screen

Use the **System Log** screen to see the system logs. Click **System Monitor > Log** to open the **System Log** screen.

Figure 151 System Monitor > Log > System Log



All system events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

Level: Error

Category: All

The following table describes the fields in this screen.

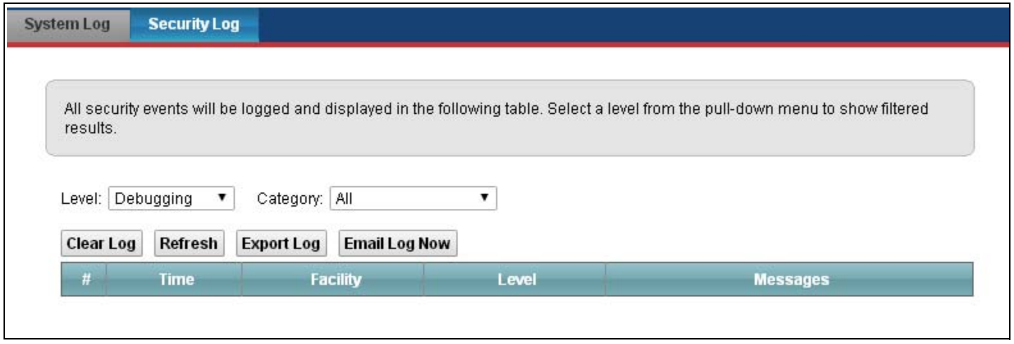
Table 124 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the VMG searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Logs Setting** screen.
System Log	
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

24.3 The Security Log Screen

Use the **Security Log** screen to see the security-related logs for the categories that you select. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 152 System Monitor > Log > Security Log



All security events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

Level: Debugging Category: All

The following table describes the fields in this screen.

Table 125 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the VMG searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Logs Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

Traffic Status

25.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

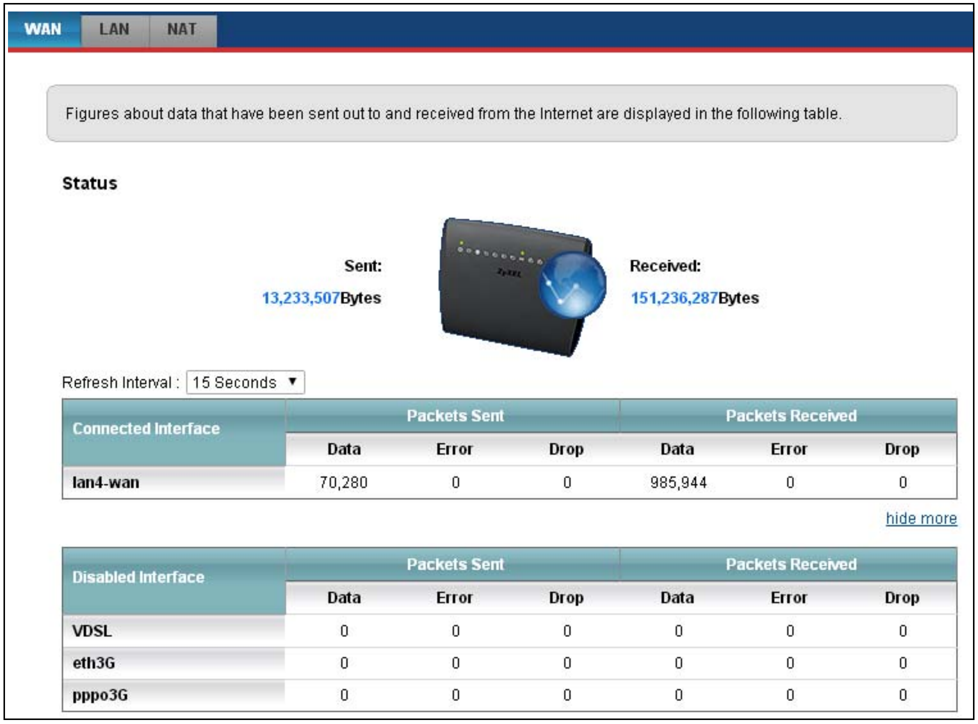
25.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 25.2 on page 301).
- Use the **LAN** screen to view the LAN traffic statistics (Section 25.3 on page 302).
- Use the **NAT** screen to view the NAT status of the VMG's client(s) (Section 25.4 on page 303)

25.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figure in this screen shows the number of bytes received and sent on the VMG.

Figure 153 System Monitor > Traffic Status > WAN



Figures about data that have been sent out to and received from the Internet are displayed in the following table.

Status

Sent: 13,233,507Bytes

Received: 151,236,287Bytes

Refresh Interval : 15 Seconds ▼

Connected Interface	Packets Sent			Packets Received		
	Data	Error	Drop	Data	Error	Drop
lan4-wan	70,280	0	0	985,944	0	0

hide more

Disabled Interface	Packets Sent			Packets Received		
	Data	Error	Drop	Data	Error	Drop
VDSL	0	0	0	0	0	0
eth3G	0	0	0	0	0	0
pppo3G	0	0	0	0	0	0

The following table describes the fields in this screen.

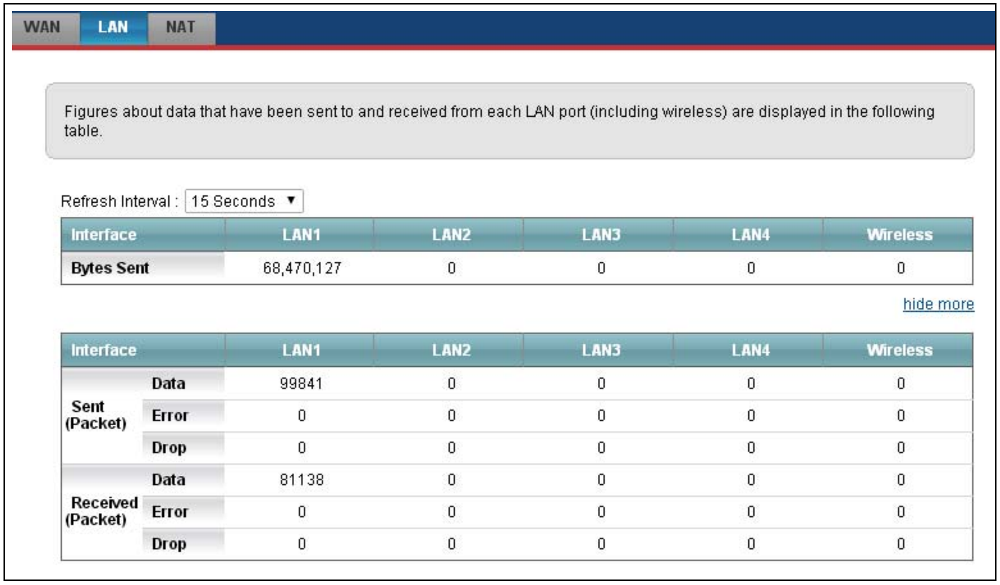
Table 126 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
more...hide more	Click **more...** to show more information. Click **hide more** to hide them.
Disabled Interface	This shows the name of the WAN interface that is currently disconnected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

25.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figure in this screen shows the interface that is currently connected on the VMG.

Figure 154 System Monitor > Traffic Status > LAN



Figures about data that have been sent to and received from each LAN port (including wireless) are displayed in the following table.

Refresh Interval : 15 Seconds ▼

Interface	LAN1	LAN2	LAN3	LAN4	Wireless
Bytes Sent	68,470,127	0	0	0	0

Interface		LAN1	LAN2	LAN3	LAN4	Wireless
Sent (Packet)	Data	99841	0	0	0	0
	Error	0	0	0	0	0
	Drop	0	0	0	0	0
Received (Packet)	Data	81138	0	0	0	0
	Error	0	0	0	0	0
	Drop	0	0	0	0	0

The following table describes the fields in this screen.

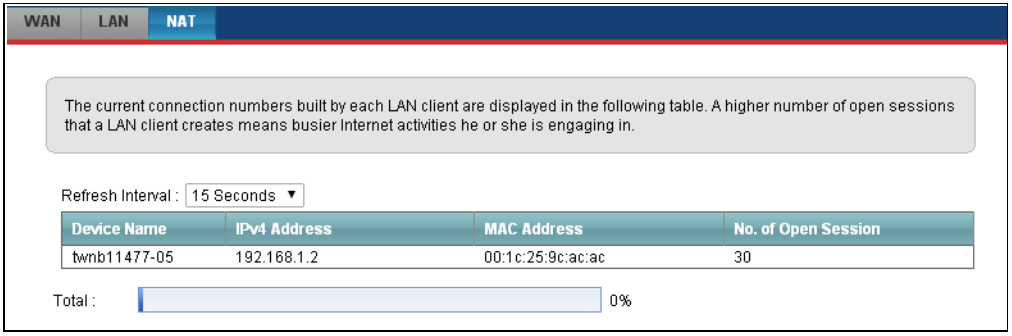
Table 127 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
more...hide more	Click **more...** to show more information. Click **hide more** to hide them.
Interface	This shows the LAN or WLAN interface.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

25.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. The figure in this screen shows the NAT session statistics for hosts currently connected on the VMG.

Figure 155 System Monitor > Traffic Status > NAT



The current connection numbers built by each LAN client are displayed in the following table. A higher number of open sessions that a LAN client creates means busier Internet activities he or she is engaging in.

Refresh Interval : 15 Seconds

Device Name	IPv4 Address	MAC Address	No. of Open Session
twnb11477-05	192.168.1.2	00:1c:25:9c:ac:ac	30

Total : 0%

The following table describes the fields in this screen.

Table 128 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the VMG to update this screen.
Device Name	This displays the name of the connected host.
IP Address	This displays the IP address of the connected host.
MAC Address	This displays the MAC address of the connected host.
No. of Open Session	This displays the number of NAT sessions currently opened for the connected host.
Total	This displays what percentage of NAT sessions the VMG can support is currently being used by all connected hosts.

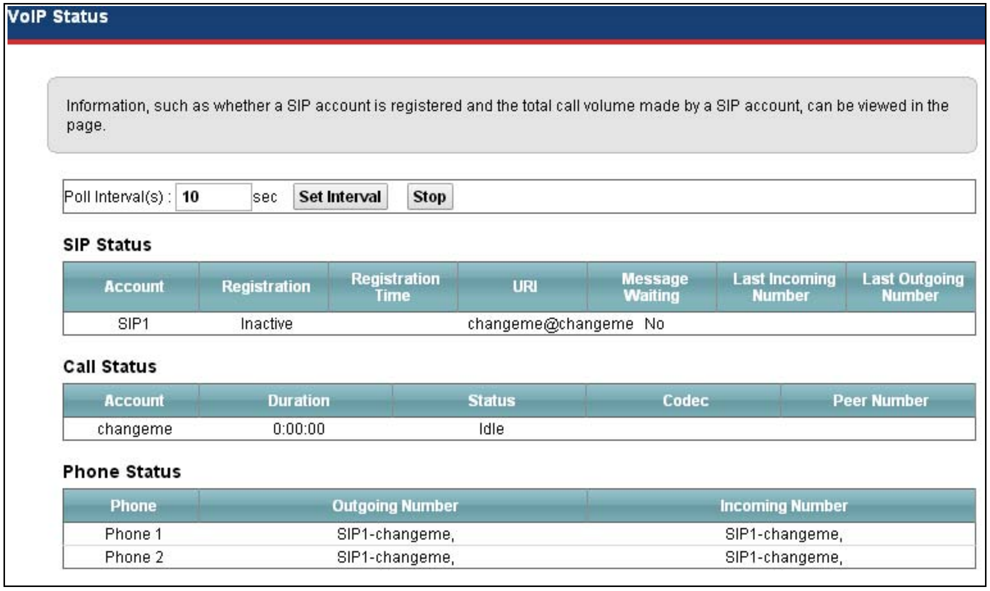
26

VoIP Status

26.1 The VoIP Status Screen

Click **System Monitor > VoIP Status** to open the following screen. You can view the VoIP registration, current call status and phone numbers in this screen.

Figure 156 System Monitor > VoIP Status



VoIP Status

Information, such as whether a SIP account is registered and the total call volume made by a SIP account, can be viewed in the page.

Poll Interval(s) : 10 sec Set Interval Stop

SIP Status

Account	Registration	Registration Time	URI	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP1	Inactive		changeme@changeme	No		

Call Status

Account	Duration	Status	Codec	Peer Number
changeme	0:00:00	Idle		

Phone Status

Phone	Outgoing Number	Incoming Number
Phone 1	SIP1-changeme,	SIP1-changeme,
Phone 2	SIP1-changeme,	SIP1-changeme,

The following table describes the fields in this screen.

Table 129 System Monitor > VoIP Status

LABEL	DESCRIPTION
Poll Interval(s)	Enter the number of seconds the VMG needs to wait before updating this screen and then click **Set Interval**. Click **Stop** to have the VMG stop updating this screen.
SIP Status	
Account	This column displays each SIP account in the VMG.
Registration	This field displays the current registration status of the SIP account. You can change this in the **Status** screen. **Registered** - The SIP account is registered with a SIP server. **Not Registered** - The last time the VMG tried to register the SIP account with the SIP server, the attempt failed. The VMG automatically tries to register the SIP account when you turn on the VMG or when you activate it. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Account**.

Table 129 System Monitor > VoIP Status (continued)

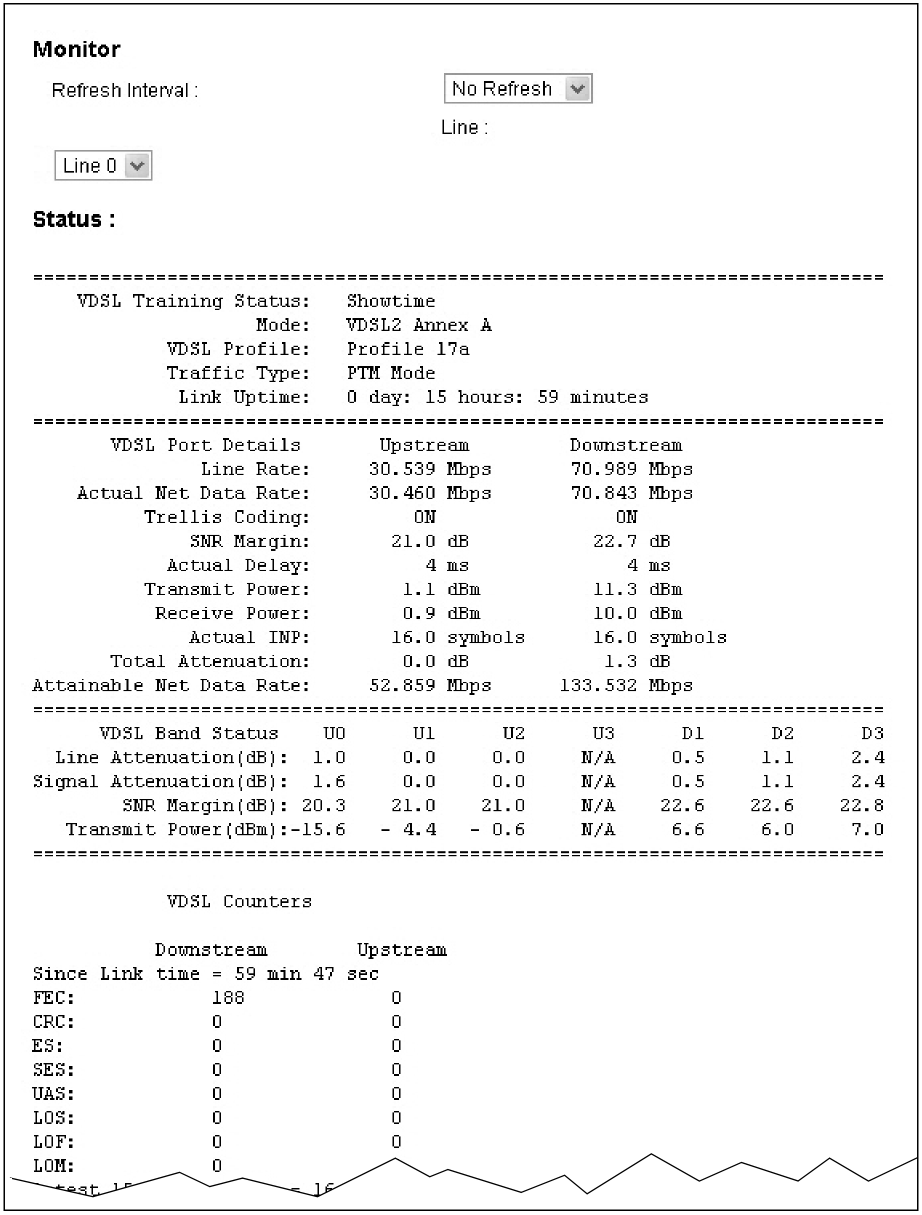
LABEL	DESCRIPTION
Registration Time	This field displays the last time the VMG successfully registered the SIP account. The field is blank if the VMG has never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP > SIP** screens.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the VMG.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** - There are no current VoIP calls, incoming calls or outgoing calls being made. **Dial** - The callee’s phone is ringing. **Ring** - The phone is ringing for an incoming VoIP call. **Process** - There is a VoIP call in progress. **DISC** - The callee’s line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Phone	This field displays the name of a phone port on the VMG.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.

xDSL Statistics

27.1 The xDSL Statistics Screen

Use this screen to view detailed DSL statistics. Click **System Monitor > xDSL Statistics** to open the following screen.

Figure 157 System Monitor > xDSL Statistics



Monitor

Refresh Interval : No Refresh

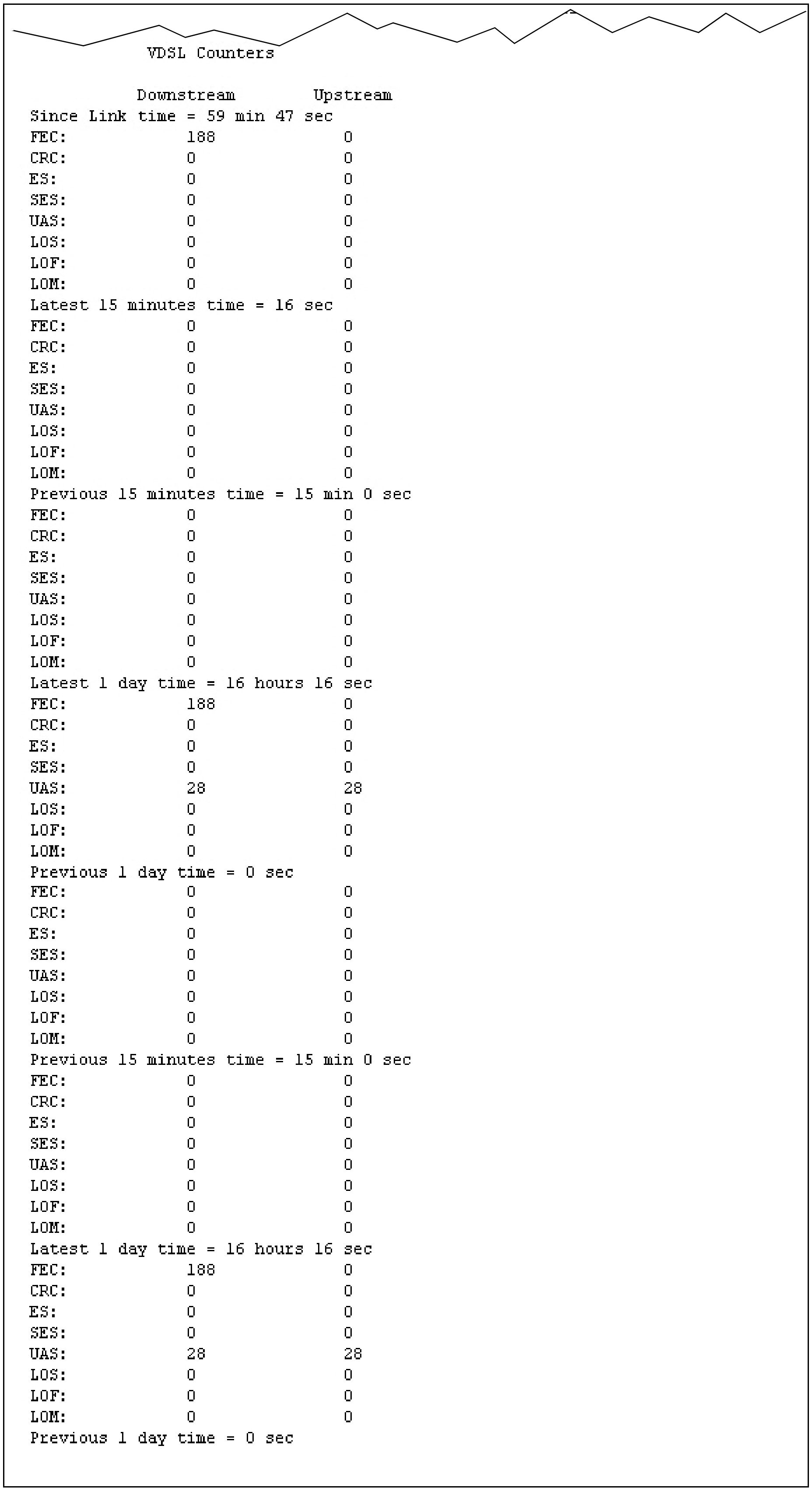
Line : Line 0

Status :

```
============================================================================
    VDSL Training Status:   Showtime
                    Mode:   VDSL2 Annex A
            VDSL Profile:   Profile 17a
            Traffic Type:   PTM Mode
             Link Uptime:   0 day: 15 hours: 59 minutes
============================================================================
       VDSL Port Details       Upstream         Downstream
               Line Rate:     30.539 Mbps       70.989 Mbps
    Actual Net Data Rate:     30.460 Mbps       70.843 Mbps
          Trellis Coding:         ON                ON
              SNR Margin:       21.0 dB           22.7 dB
            Actual Delay:          4 ms              4 ms
          Transmit Power:        1.1 dBm          11.3 dBm
           Receive Power:        0.9 dBm          10.0 dBm
              Actual INP:       16.0 symbols      16.0 symbols
       Total Attenuation:        0.0 dB            1.3 dB
Attainable Net Data Rate:     52.859 Mbps      133.532 Mbps
============================================================================
      VDSL Band Status    U0      U1      U2      U3      D1      D2      D3
  Line Attenuation(dB):  1.0     0.0     0.0     N/A     0.5     1.1     2.4
Signal Attenuation(dB):  1.6     0.0     0.0     N/A     0.5     1.1     2.4
        SNR Margin(dB): 20.3    21.0    21.0     N/A    22.6    22.6    22.8
   Transmit Power(dBm):-15.6   - 4.4   - 0.6     N/A     6.6     6.0     7.0
============================================================================


            VDSL Counters

           Downstream        Upstream
Since Link time = 59 min 47 sec
FEC:            188             0
CRC:            0               0
ES:             0               0
SES:            0               0
UAS:            0               0
LOS:            0               0
LOF:            0               0
LOM:            0
```



```
           VDSL Counters

          Downstream        Upstream
Since Link time = 59 min 47 sec
FEC:           188            0
CRC:           0              0
ES:            0              0
SES:           0              0
UAS:           0              0
LOS:           0              0
LOF:           0              0
LOM:           0              0
Latest 15 minutes time = 16 sec
FEC:           0              0
CRC:           0              0
ES:            0              0
SES:           0              0
UAS:           0              0
LOS:           0              0
LOF:           0              0
LOM:           0              0
Previous 15 minutes time = 15 min 0 sec
FEC:           0              0
CRC:           0              0
ES:            0              0
SES:           0              0
UAS:           0              0
LOS:           0              0
LOF:           0              0
LOM:           0              0
Latest 1 day time = 16 hours 16 sec
FEC:           188            0
CRC:           0              0
ES:            0              0
SES:           0              0
UAS:           28             28
LOS:           0              0
LOF:           0              0
LOM:           0              0
Previous 1 day time = 0 sec
FEC:           0              0
CRC:           0              0
ES:            0              0
SES:           0              0
UAS:           0              0
LOS:           0              0
LOF:           0              0
LOM:           0              0
Previous 15 minutes time = 15 min 0 sec
FEC:           0              0
CRC:           0              0
ES:            0              0
SES:           0              0
UAS:           0              0
LOS:           0              0
LOF:           0              0
LOM:           0              0
Latest 1 day time = 16 hours 16 sec
FEC:           188            0
CRC:           0              0
ES:            0              0
SES:           0              0
UAS:           28             28
LOS:           0              0
LOF:           0              0
LOM:           0              0
Previous 1 day time = 0 sec
```

The following table describes the labels in this screen.

Table 130 Status > xDSL Statistics

LABEL	DESCRIPTION
Refresh Interval	Select the time interval for refreshing statistics.
Line	Select which DSL line's statistics you want to display.
xDSL Training Status	This displays the current state of setting up the DSL connection.
Mode	This displays the ITU standard used for this connection.
Traffic Type	This displays the type of traffic the DSL port is sending and receiving. **Inactive** displays if the DSL port is not currently sending or receiving traffic.
Link Uptime	This displays how long the port has been running (or connected) since the last time it was started.
xDSL Port Details	
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Line Rate	These are the data transfer rates at which the port is sending and receiving data.
Actual Net Data Rate	These are the rates at which the port is sending and receiving the payload data without transport layer protocol headers and traffic.
Trellis Coding	This displays whether or not the port is using Trellis coding for traffic it is sending and receiving. Trellis coding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable.
SNR Margin	This is the upstream and downstream Signal-to-Noise Ratio margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the system still being able to meet its transmission targets.
Actual Delay	This is the upstream and downstream interleave delay. It is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed.
Transmit Power	This is the upstream and downstream far end actual aggregate transmit power (in dBm). Upstream is how much power the port is using to transmit to the service provider. Downstream is how much port the service provider is using to transmit to the port.
Receive Power	Upstream is how much power the service provider is receiving from the port. Downstream is how much power the port is receiving from the service provider.
Actual INP	Sudden spikes in the line's level of external noise (impulse noise) can cause errors and result in lost packets. This could especially impact the quality of multimedia traffic such as voice or video. Impulse noise protection (INP) provides a buffer to allow for correction of errors caused by error correction to deal with this. The number of DMT (Discrete Multi-Tone) symbols shows the level of impulse noise protection for the upstream and downstream traffic. A higher symbol value provides higher error correction capability, but it causes overhead and higher delay which may increase error rates in received multimedia data.
Total Attenuation	This is the upstream and downstream line attenuation, measured in decibels (dB). This attenuation is the difference between the power transmitted at the near-end and the power received at the far-end. Attenuation is affected by the channel characteristics (wire gauge, quality, condition and length of the physical line).
Attainable Net Data Rate	These are the highest theoretically possible transfer rates at which the port could send and receive payload data without transport layer protocol headers and traffic.
xDSL Counters	

Table 130 Status > xDSL Statistics (continued)

LABEL	DESCRIPTION
Downstream	These are the statistics for the traffic direction coming into the port from the service provider.
Upstream	These are the statistics for the traffic direction going out from the port to the service provider.
FEC	This is the number of Far End Corrected blocks.
CRC	This is the number of Cyclic Redundancy Checks.
ES	This is the number of Errored Seconds meaning the number of seconds containing at least one errored block or at least one defect.
SES	This is the number of Severely Errored Seconds meaning the number of seconds containing 30% or more errored blocks or at least one defect. This is a subset of ES.
UAS	This is the number of UnAvailable Seconds.
LOS	This is the number of Loss Of Signal seconds.
LOF	This is the number of Loss Of Frame seconds.
LOM	This is the number of Loss of Margin seconds.

28

3G Statistics

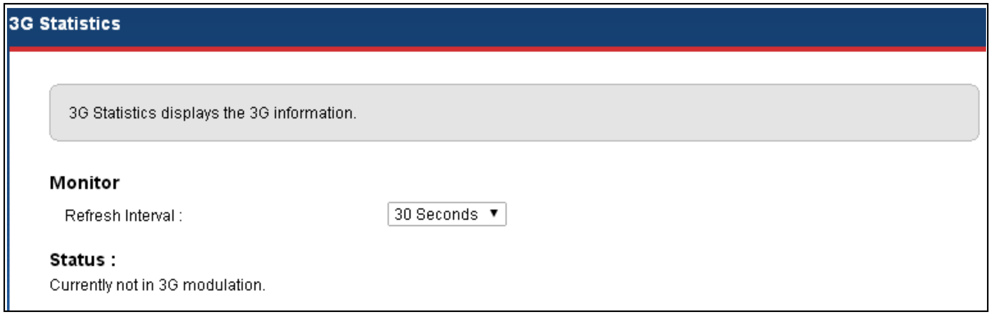
28.1 Overview

Use the **3G Statistics** screens to look at 3G Internet connection status.

28.2 The 3G Statistics Screen

To open this screen, click **System Monitor > 3G Statistics**. The 3G status is available on this screen only when you insert a compatible 3G dongle in a USB port on the VMG.

Figure 158 System Monitor > 3G Statistics



3G Statistics

3G Statistics displays the 3G information.

Monitor

Refresh Interval : 30 Seconds

Status :

Currently not in 3G modulation.

The following table describes the labels in this screen.

Table 131 System Monitor > 3G Statistics

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Device to update this screen. Select **No Refresh** to stop refreshing.
3G Status	This field displays the status of the 3G Internet connection. This field can display: **GSM** - Global System for Mobile Communications, 2G **GPRS** - General Packet Radio Service, 2.5G **EDGE** - Enhanced Data rates for GSM Evolution, 2.75G **WCDMA** - Wideband Code Division Multiple Access, 3G **HSDPA** - High-Speed Downlink Packet Access, 3.5G **HSUPA** - High-Speed Uplink Packet Access, 3.75G **HSPA** - HSDPA+HSUPA, 3.75G
Service Provider	This field displays the name of the service provider.
Signal Strength	This field displays the strength of the signal in dBm.

Table 131 System Monitor > 3G Statistics (continued)

LABEL	DESCRIPTION
Connection Uptime	This field displays the time the connection has been up.
3G Card Manufacturer	This field displays the manufacturer of the 3G card.
3G Card Model	This field displays the model name of the 3G card.
3G Card F/W Version	This field displays the firmware version of the 3G card.
SIM Card IMSI	The International Mobile Subscriber Identity or IMSI is a unique identification number associated with all cellular networks. This number is provisioned in the SIM card.

29

User Account

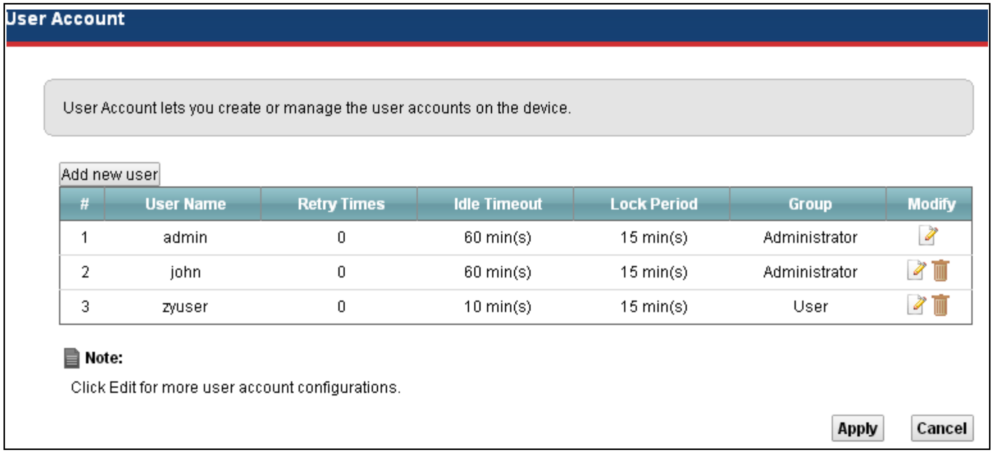
29.1 Overview

A user account is the In the **Users Account** screen, you can change the password of the “admin” user account that you used to log in the VMG.

29.2 The User Account Screen

Click **Maintenance > User Account** to open the following screen.

Figure 159 Maintenance > User Account



User Account

User Account lets you create or manage the user accounts on the device.

Add new user

#	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	admin	0	60 min(s)	15 min(s)	Administrator	
2	john	0	60 min(s)	15 min(s)	Administrator	
3	zyuser	0	10 min(s)	15 min(s)	User	

Note:

Click Edit for more user account configurations.

Apply Cancel

The following table describes the labels in this screen.

Table 132 Maintenance > User Account

LABEL	DESCRIPTION
#	This is the index number
User Name	This field displays the name of the account used to log into the VMG web configurator.
Retry Times	This field displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This field displays the the length of inactive time before the VMG will automatically log the user out of the web configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	This field displays whether this user has **Administrator** or **User** privleges.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.

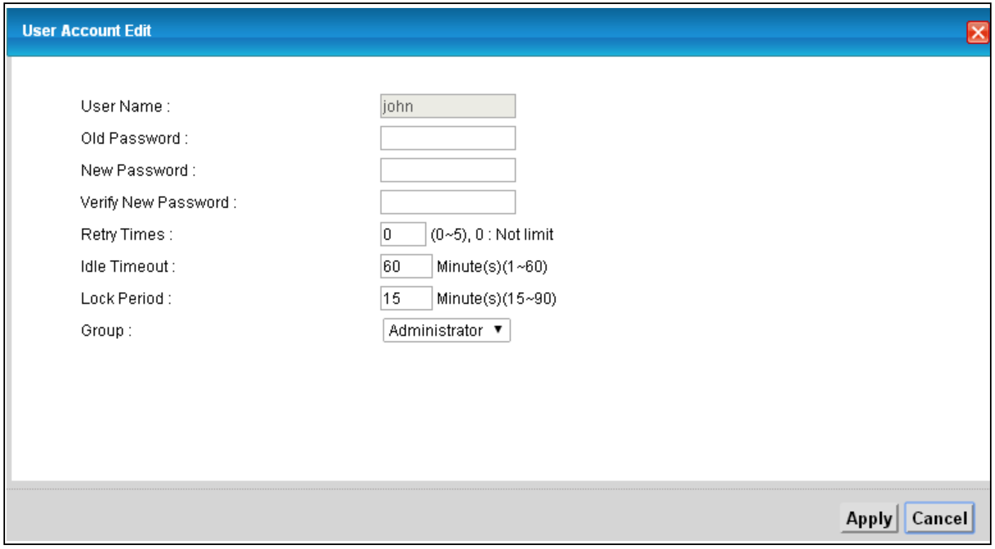
Table 132 Maintenance > User Account (continued) (continued)

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

29.2.1 The User Account Add/Edit Screen

Click Add new user or the Edit icom of an existign account in the **Maintenance > User Account** to open the following screen.

Figure 160 Maintenance > User Account >Add/Edit



User Name : john

Old Password :

New Password :

Verify New Password :

Retry Times : 0 (0~5), 0 : Not limit

Idle Timeout : 60 Minute(s)(1~60)

Lock Period : 15 Minute(s)(15~90)

Group : Administrator

The following table describes the labels in this screen.

Table 133 Maintenance > User Account

LABEL	DESCRIPTION
User Name	Enter a new name for the This field displays the name of an existing account.
Old Password	Type the default password or the existing password used to access the VMG web configurator.
New Password	Type your new system password (up to 256 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the VMG.
Verify Password	Type the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the VMG will automatically log the user out of the web configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number if consecutive wrong passwords have been entered as defined in **Retry Times**.
Group	Specify whether this user will have **Administrator** or **User** privleges.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

30

Remote Management

30.1 Overview

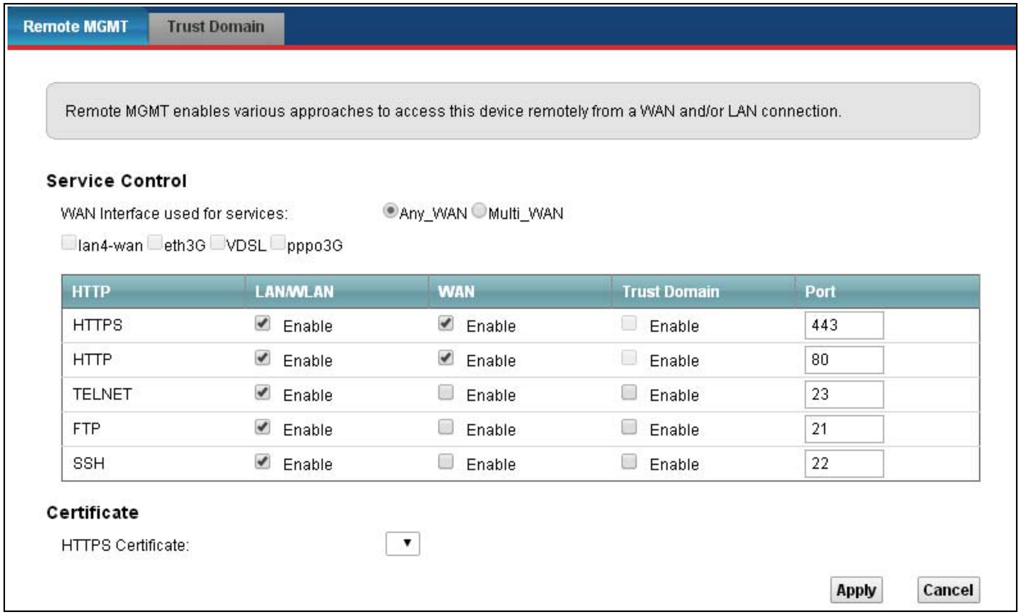
Remote management controls through which interface(s), which services can access the Device.

Note: The VMG is managed using the Web Configurator.

30.2 The Remote MGMT Screen

Use this screen to configure through which interface(s), which services can access the Device. You can also specify the port numbers the services must use to connect to the Device. Click **Maintenance > Remote MGMT** to open the following screen.

Figure 161 Maintenance > Remote MGMT



Remote MGMT enables various approaches to access this device remotely from a WAN and/or LAN connection.

Service Control

WAN Interface used for services: ● Any_WAN ○ Multi_WAN

□ lan4-wan □ eth3G □ VDSL □ pppo3G

HTTP	LAN/WLAN	WAN	Trust Domain	Port
HTTPS	☑ Enable	☑ Enable	□ Enable	443
HTTP	☑ Enable	☑ Enable	□ Enable	80
TELNET	☑ Enable	□ Enable	□ Enable	23
FTP	☑ Enable	□ Enable	□ Enable	21
SSH	☑ Enable	□ Enable	□ Enable	22

Certificate

HTTPS Certificate: ▼

The following table describes the fields in this screen.

Table 134 Maintenance > Remote MGMT

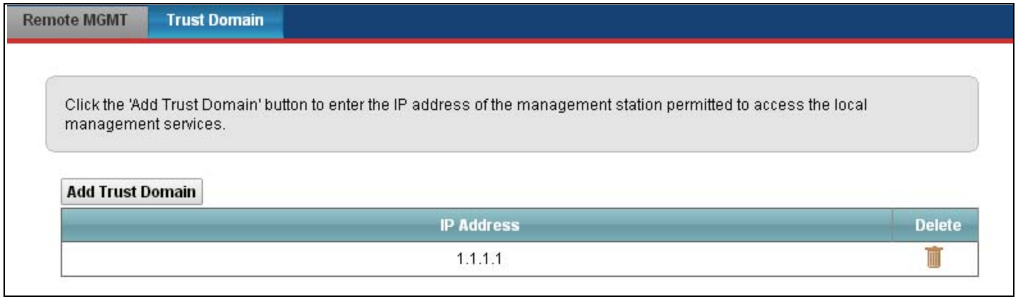
LABEL	DESCRIPTION
WAN Interface used for services	Select **Any WAN** to have the VMG automatically activate the remote management service when any WAN connection is up. Select **Multi WAN** and then select one or more WAN connections to have the VMG activate the remote management service when the selected WAN connections are up.
HTTP	This is the service you may use to access the VMG.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the VMG from the LAN/WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the VMG from all WAN connections.
Trust Domain	If you only want certain WAN connections to have access to to the VMG using the corresponding services, then clear **WAN**, select **Trust Domain** and configure the allowed IP address(es) in the **Trust Domain** screen.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Certificate	
HTTPS Certificate	Select a certificate the HTTPS server (the VMG) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **Certificates** screen.
Apply	Click **Apply** to save your changes back to the VMG.
Cancel	Click **Cancel** to restore your previously saved settings.

30.3 The Trust Domain Screen

Use this screen to view a list of public IP addresses which are allowed to access the VMG through the services configured in the **Maintenance > Remote MGMT** screen. Click **Maintenance > Remote MGMT > Turst Domain** to open the following screen.

Note: If this list is empty, all public IP addresses can access the VMG from the WAN through the specified services.

Figure 162 Maintenance > Remote MGMT > Trust Domain



Click the 'Add Trust Domain' button to enter the IP address of the management station permitted to access the local management services.

IP Address	Delete
1.1.1.1	🗑

The following table describes the fields in this screen.

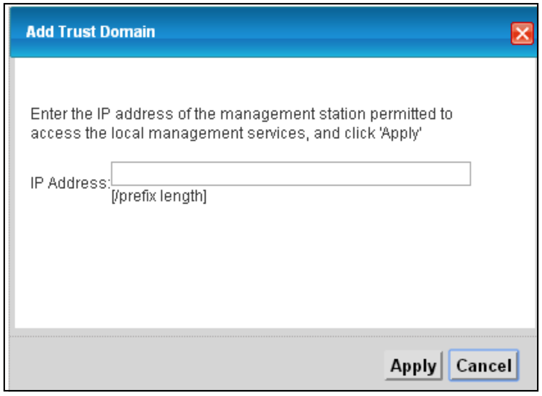
Table 135 Maintenance > Remote MGMT > Trust Domain

LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IPv4 Address	This field shows a trusted host IP address.
Delete	Click the **Delete** icon to remove the trust IP address.

30.4 The Add Trust Domain Screen

Use this screen to configure a public IP address which is allowed to access the VMG. Click the **Add Trust Domain** button in the **Maintenance > Remote MGMT > Turst Domain** screen to open the following screen.

Figure 163 Maintenance > Remote MGMT > Trust Domain > Add Trust Domain



Enter the IP address of the management station permitted to access the local management services, and click 'Apply'

IP Address: [/prefix length]

The following table describes the fields in this screen.

Table 136 Maintenance > Remote MGMT > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IPv4 Address	Enter a public IPv4 IP address which is allowed to access the service on the VMG from the WAN.
Apply	Click **Apply** to save your changes back to the VMG.
Cancel	Click **Cancel** to restore your previously saved settings.

31

TR-069 Client

31.1 Overview

This chapter explains how to configure the VMG's TR-069 auto-configuration settings.

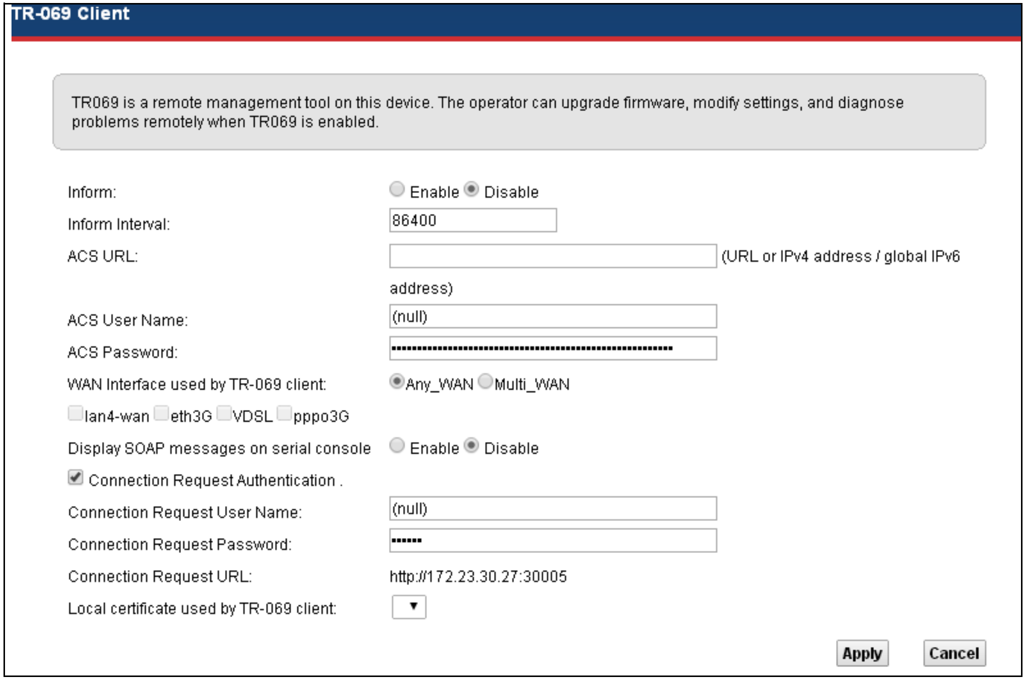
31.2 The TR-069 Client Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your VMG, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the VMG, modify settings, perform firmware upgrades as well as monitor and diagnose the VMG. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Maintenance > TR-069 Client** to open the following screen. Use this screen to configure your VMG to be managed by an ACS.

Figure 164 Maintenance > TR-069 Client



TR-069 Client

TR069 is a remote management tool on this device. The operator can upgrade firmware, modify settings, and diagnose problems remotely when TR069 is enabled.

Inform: ○ Enable ● Disable

Inform Interval: 86400

ACS URL: (URL or IPv4 address / global IPv6 address)

ACS User Name: (null)

ACS Password: ••

WAN Interface used by TR-069 client: ● Any_WAN ○ Multi_WAN

□ lan4-wan □ eth3G □ VDSL □ pppo3G

Display SOAP messages on serial console ○ Enable ● Disable

☑ Connection Request Authentication .

Connection Request User Name: (null)

Connection Request Password: ••••••

Connection Request URL: http://172.23.30.27:30005

Local certificate used by TR-069 client: ▼

The following table describes the fields in this screen.

Table 137 Maintenance > TR-069 Client

LABEL	DESCRIPTION
Inform	Select **Enable** for the VMG to send periodic inform via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the VMG sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select **Any_WAN**, the VMG automatically passes the TR-069 traffic when any WAN connection is up. If you select **Multi_WAN**, you also need to select two or more pre-configured WAN interfaces. The VMG automatically passes the TR-069 traffic when one of the selected WAN connections is up.
Display SOAP messages on serial console	Select **Enable** to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the VMG, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the VMG, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the VMG.
Local certificate used by TR-069 client	You can choose a local certificate used by TR-069 client. The local certificate should be imported in the **Security** > **Certificates** > **Local Certificates** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

32

TR-064

32.1 Overview

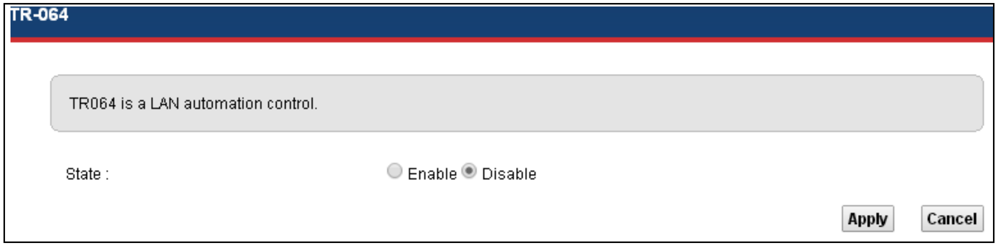
This chapter explains how to configure the VMG's TR-064 auto-configuration settings.

32.2 The TR-064 Screen

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

Click **Maintenance > TR-064** to open the following screen.

Figure 165 Maintenance > TR-064



TR-064

TR064 is a LAN automation control.

State : ○ Enable ● Disable

The following table describes the fields in this screen.

Table 138 Maintenance > TR-064

LABEL	DESCRIPTION
State	Select **Enable** to activate management via TR-064 on the LAN.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

33

SNMP

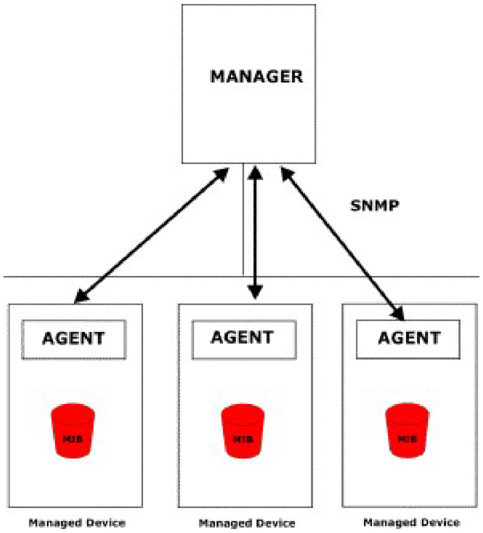
33.1 Overview

This chapter explains how to configure the SNMP settings on the VMG.

33.2 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your VMG supports SNMP agent functionality, which allows a manager station to manage and monitor the VMG through the network. The VMG supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 166 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the VMG). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

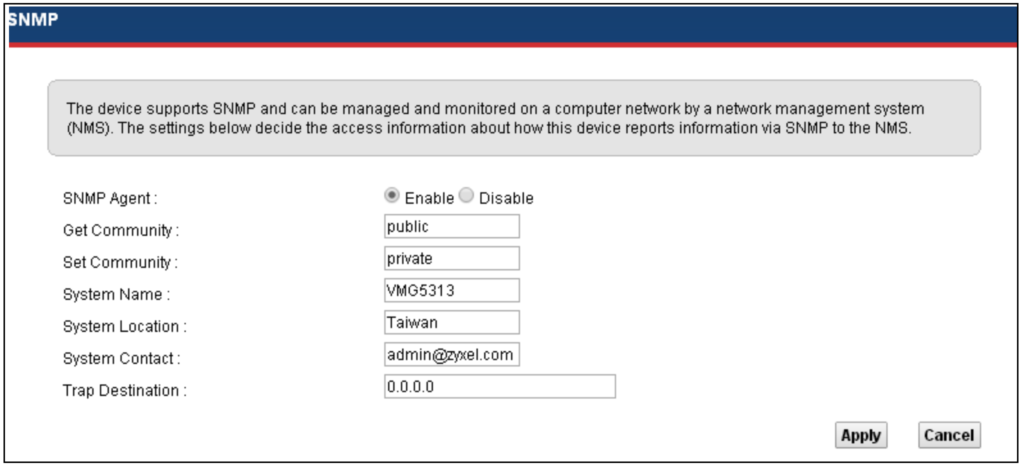
The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Click **Maintenance > SNMP** to open the following screen. Use this screen to configure the VMG SNMP settings.

Figure 167 Maintenance > SNMP



SNMP

The device supports SNMP and can be managed and monitored on a computer network by a network management system (NMS). The settings below decide the access information about how this device reports information via SNMP to the NMS.

SNMP Agent : ● Enable ○ Disable
Get Community : public
Set Community : private
System Name : VMG5313
System Location : Taiwan
System Contact : admin@zyxel.com
Trap Destination : 0.0.0.0

The following table describes the fields in this screen.

Table 139 Maintenance > SNMP

LABEL	DESCRIPTION
SNMP Agent	Select **Enable** to let the VMG act as an SNMP agent, which allows a manager station to manage and monitor the Device through the network. Select **Disable** to turn this feature off.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.
System Contact	Enter the SNMP system contact.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click this to save your changes back to the VMG.
Cancel	Click this to restore your previously saved settings.

34

Time Settings

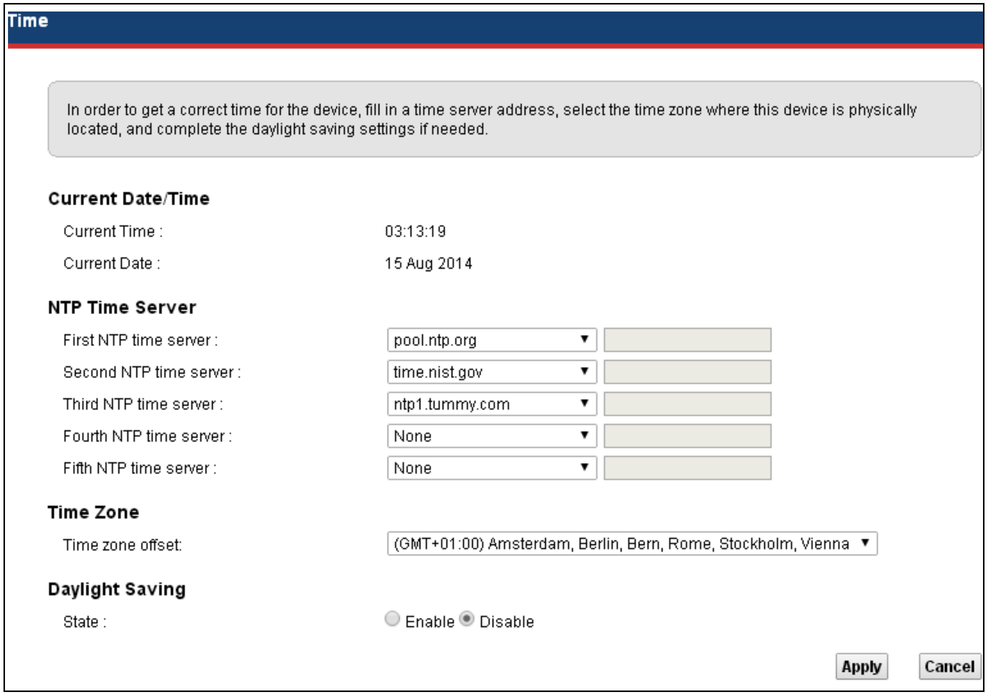
34.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

34.2 The Time Screen

To change your VMG's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the VMG's time based on your local time zone.

Figure 168 Maintenance > Time



Time

In order to get a correct time for the device, fill in a time server address, select the time zone where this device is physically located, and complete the daylight saving settings if needed.

Current Date/Time

Current Time : 03:13:19

Current Date : 15 Aug 2014

NTP Time Server

First NTP time server : pool.ntp.org

Second NTP time server : time.nist.gov

Third NTP time server : ntp1.tummy.com

Fourth NTP time server : None

Fifth NTP time server : None

Time Zone

Time zone offset: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Daylight Saving

State : ○ Enable ● Disable

The following table describes the fields in this screen.

Table 140 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your VMG. Each time you reload this page, the VMG synchronizes the time with the time server.

Table 140 Maintenance > Time (continued)

LABEL	DESCRIPTION
Current Date	This field displays the date of your VMG. Each time you reload this page, the VMG synchronizes the date with the time server.
NTP Time Server	
First ~ Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
State	Select **Enable** if you use Daylight Saving Time.
Start rule:	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday** and the month to **March**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Hour** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday**, and the month to **October**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

E-mail Notification

35.1 Overview

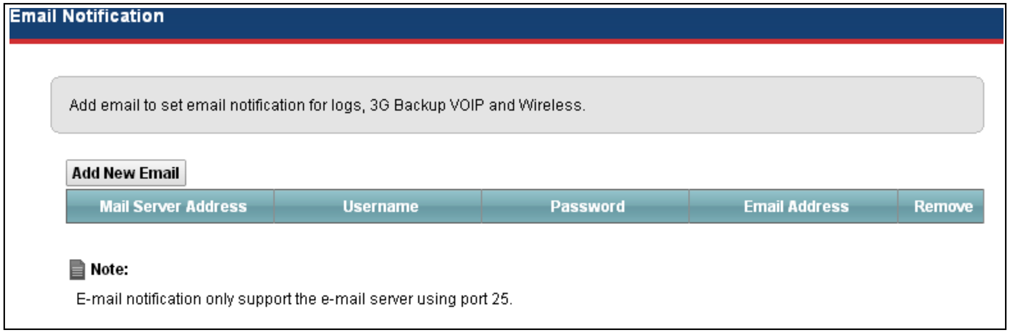
A mail server is an application or a computer that runs such an application to receive, forward and deliver e-mail messages.

To have the VMG send reports, logs or notifications via e-mail, you must specify an e-mail server and the e-mail addresses of the sender and receiver.

35.2 The Email Notification Screen

Click **Maintenance > Email Notification** to open the **Email Notification** screen. Use this screen to view, remove and add mail server information on the VMG.

Figure 169 Maintenance > Email Notification



Email Notification

Add email to set email notification for logs, 3G Backup VOIP and Wireless.

Mail Server Address	Username	Password	Email Address	Remove

Note:

E-mail notification only support the e-mail server using port 25.

The following table describes the labels in this screen.

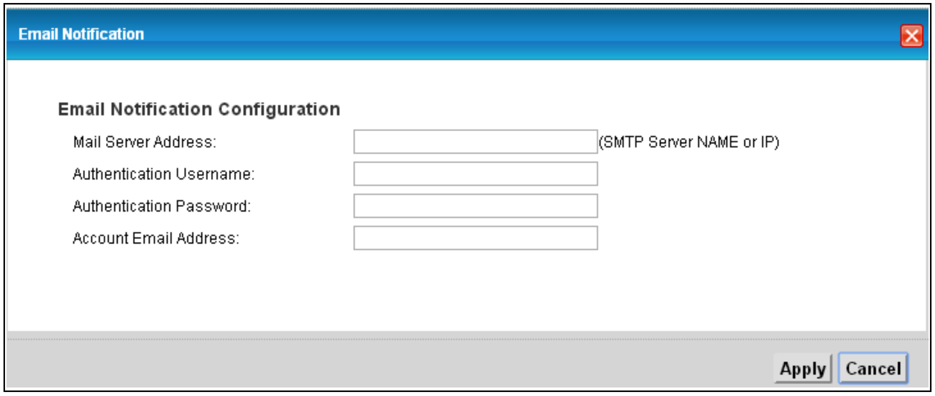
Table 141 Maintenance > Email Notification

LABEL	DESCRIPTION
Add New Email	Click this button to create a new entry.
Mail Server Address	This field displays the server name or the IP address of the mail server.
Username	This field displays the user name of the sender’s mail account.
Password	This field displays the password of the sender’s mail account.
Email Address	This field displays the e-mail address that you want to be in the from/sender line of the e-mail that the VMG sends.
Delete	Click this button to delete the selected entry(ies).

35.2.1 Email Notification Edit

Click the **Add** button in the **Email Notification** screen. Use this screen to configure the required information for sending e-mail via a mail server.

Figure 170 Email Notification > Add


Email Notification

Email Notification Configuration

Mail Server Address: (SMTP Server NAME or IP)

Authentication Username:

Authentication Password:

Account Email Address:

The following table describes the labels in this screen.

Table 142 Email Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Account Email Address** field. If this field is left blank, reports, logs or notifications will not be sent via e-mail.
Authentication Username	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the **Account Email Address** field.
Authentication Password	Enter the password associated with the user name above.
Account Email Address	Enter the e-mail address that you want to be in the from/sender line of the e-mail notification that the VMG sends. If you activate SSL/TLS authentication, the e-mail address must be able to be authenticated by the mail server as well.
Apply	Click this button to save your changes and return to the previous screen.
Cancel	Click this button to begin configuring this screen afresh.

Log Setting

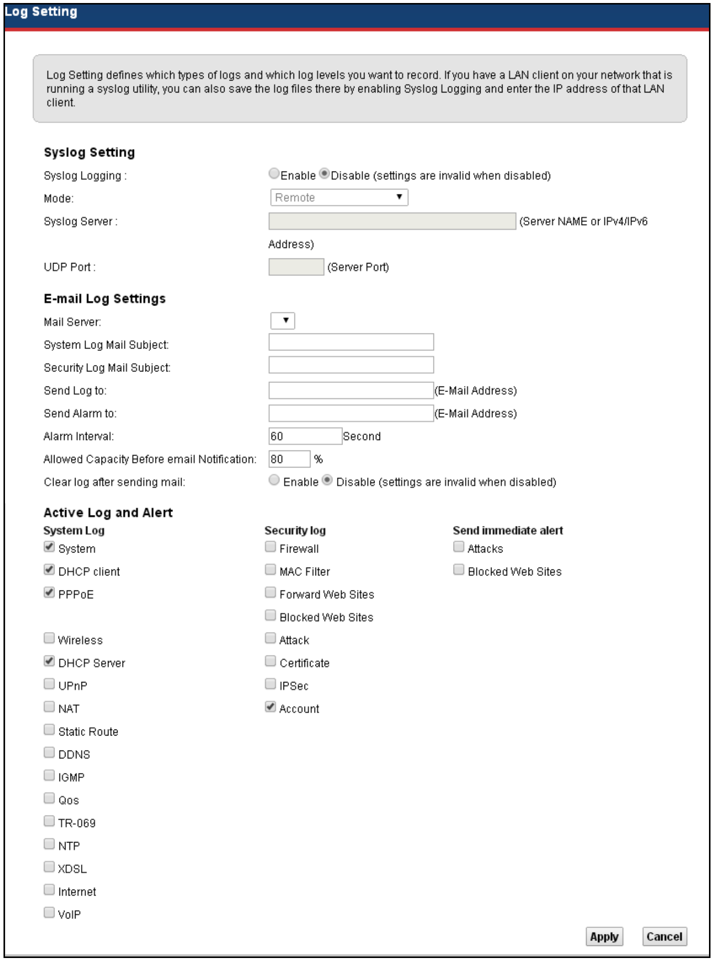
36.1 Overview

You can configure where the VMG sends logs and which logs and/or immediate alerts the VMG records in the **Logs Setting** screen.

36.2 The Log Settings Screen

To change your VMG's log settings, click **Maintenance > Logs Setting**. The screen appears as shown.

Figure 171 Maintenance > Logs Setting



Log Setting

Log Setting defines which types of logs and which log levels you want to record. If you have a LAN client on your network that is running a syslog utility, you can also save the log files there by enabling Syslog Logging and enter the IP address of that LAN client.

Syslog Setting

Syslog Logging : ○ Enable ● Disable (settings are invalid when disabled)

Mode: Remote

Syslog Server : (Server NAME or IPv4/IPv6 Address)

UDP Port : (Server Port)

E-mail Log Settings

Mail Server:

System Log Mail Subject:

Security Log Mail Subject:

Send Log to: (E-Mail Address)

Send Alarm to: (E-Mail Address)

Alarm Interval: 60 Second

Allowed Capacity Before email Notification: 80 %

Clear log after sending mail: ○ Enable ● Disable (settings are invalid when disabled)

Active Log and Alert

System Log	Security log	Send immediate alert
☑ System	□ Firewall	□ Attacks
☑ DHCP client	□ MAC Filter	□ Blocked Web Sites
☑ PPPoE	□ Forward Web Sites	
	□ Blocked Web Sites	
□ Wireless	□ Attack	
☑ DHCP Server	□ Certificate	
□ UPnP	□ IPSec	
□ NAT	☑ Account	
□ Static Route		
□ DDNS		
□ IGMP		
□ Qos		
□ TR-069		
□ NTP		
□ XDSL		
□ Internet		
□ VoIP		

The following table describes the fields in this screen.

Table 143 Maintenance > Logs Setting

LABEL	DESCRIPTION
Syslog Setting	
Syslog Logging	The VMG sends a log to an external syslog server. Select **Enable** to enable syslog logging.
Mode	Select the syslog destination from the drop-down list box. If you select **Remote**, the log(s) will be sent to a remote syslog server. If you select **Local File**, the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select **Local File and Remote**.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the VMG sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log e-mail message that the VMG sends.
Send Log to	The VMG sends logs to the e-mail address specified in this field. If this field is left blank, the VMG does not send logs via E-mail.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Alarm Interval	Specify how often the alarm should be updated.
Allowed Capacity Before Email	Set what percent of the VMG's log storage space can be filled before the VMG sends a log e-mail.
Clear log after sending mail	Select this to delete all the logs after the VMG sends an E-mail of the logs.
Active Log and Alert	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Send immediate alert	Select log categories for which you want the VMG to send E-mail alerts immediately.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

36.2.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.

- "End of Log" message shows that a complete log has been sent.

Figure 172 E-mail Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
………………………………..{snip}………………………………..
………………………………..{snip}………………………………..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |

End of Firewall Log
```

37

Firmware Upgrade

37.1 Overview

This chapter explains how to upload new firmware to your VMG. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

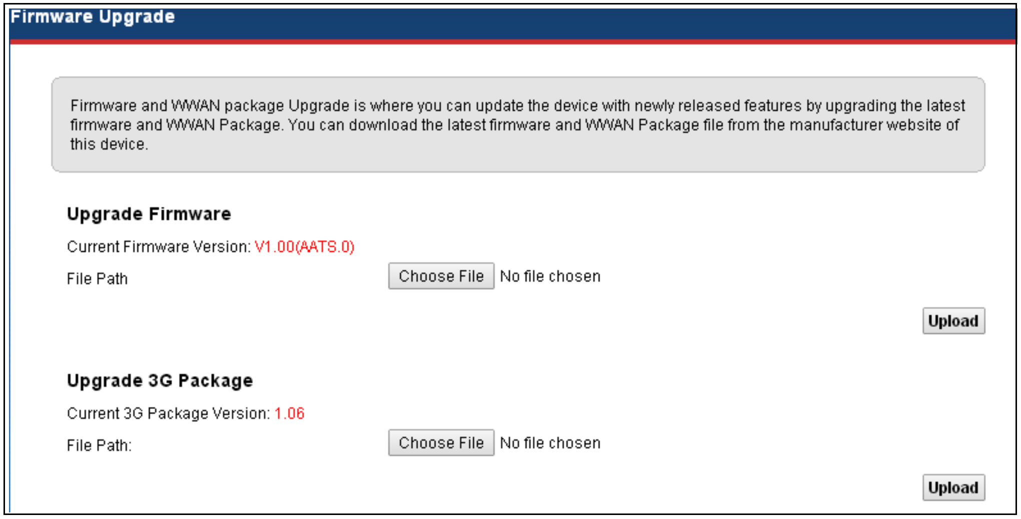
Only use firmware for your device's specific model. Refer to the label on the bottom of your VMG.

37.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the VMG while firmware upload is in progress!

Figure 173 Maintenance > Firmware Upgrade



Firmware Upgrade

Firmware and WWAN package Upgrade is where you can update the device with newly released features by upgrading the latest firmware and WWAN Package. You can download the latest firmware and WWAN Package file from the manufacturer website of this device.

Upgrade Firmware

Current Firmware Version: V1.00(AATS.0)

File Path: Choose File No file chosen

Upload

Upgrade 3G Package

Current 3G Package Version: 1.06

File Path: Choose File No file chosen

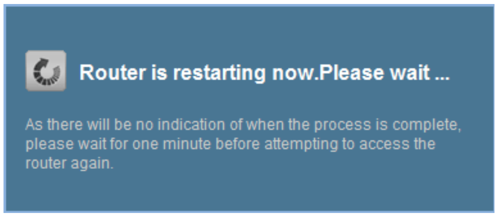
Upload

The following table describes the labels in this screen. After you see the firmware updating screen, wait two minutes before logging into the VMG again.

Table 144 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.
Upgrade 3G Package	
Current 3G Package Version	This is the present 3G Package version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

Figure 174 Firmware Uploading

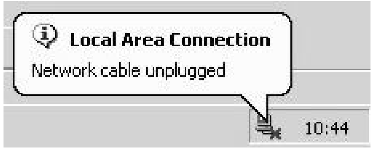


Router is restarting now.Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

The VMG automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 175 Network Temporarily Disconnected



Local Area Connection

Network cable unplugged

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 176 Error Message

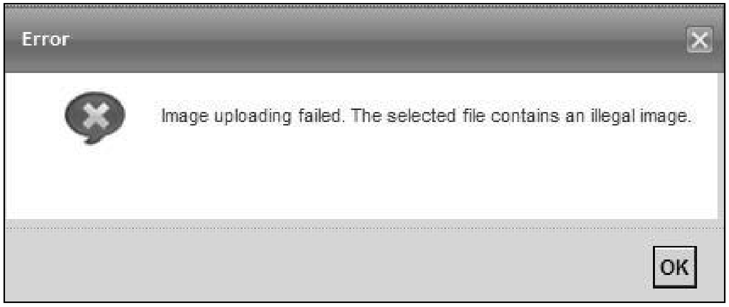


Image uploading failed. The selected file contains an illegal image.

Configuration

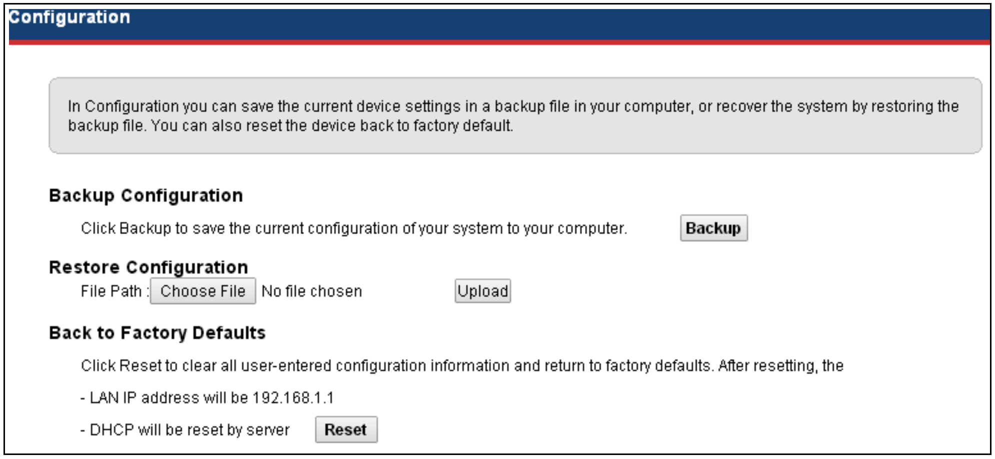
38.1 Overview

The **Configuration** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

38.2 The Configuration Screen

Click **Maintenance > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 177 Maintenance > Configuration



Configuration

In Configuration you can save the current device settings in a backup file in your computer, or recover the system by restoring the backup file. You can also reset the device back to factory default.

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

File Path : No file chosen

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- LAN IP address will be 192.168.1.1

- DHCP will be reset by server

Backup Configuration

Backup Configuration allows you to back up (save) the VMG's current configuration to a file on your computer. Once your VMG is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the VMG's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your VMG.

Table 145 Restore Configuration

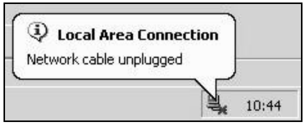
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do not turn off the VMG while configuration file upload is in progress.

After the VMG configuration has been restored successfully, the login screen appears. Login again to restart the VMG.

The VMG automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 178 Network Temporarily Disconnected

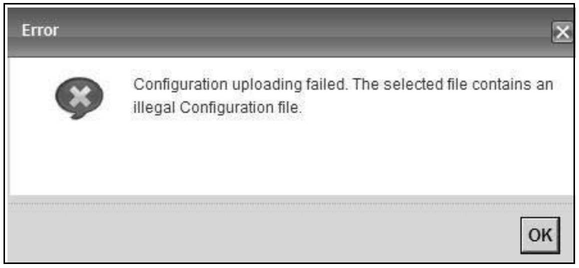


Local Area Connection
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix B on page 371 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 179 Configuration Upload Error



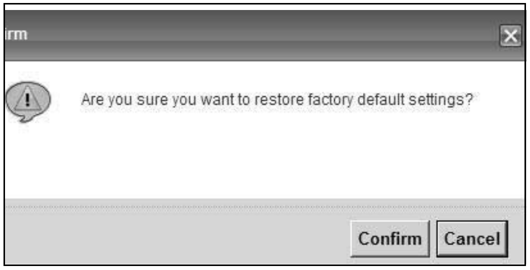
Error

Configuration uploading failed. The selected file contains an illegal Configuration file.

Reset to Factory Defaults

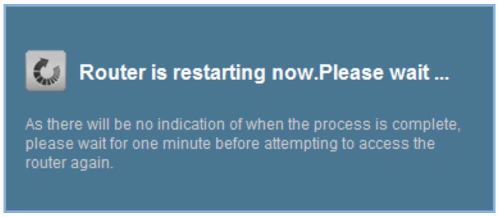
Click the **Reset** button to clear all user-entered configuration information and return the VMG to its factory defaults. The following warning screen appears.

Figure 180 Reset Warning Message



Are you sure you want to restore factory default settings?

Figure 181 Reset In Process Message



Router is restarting now.Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

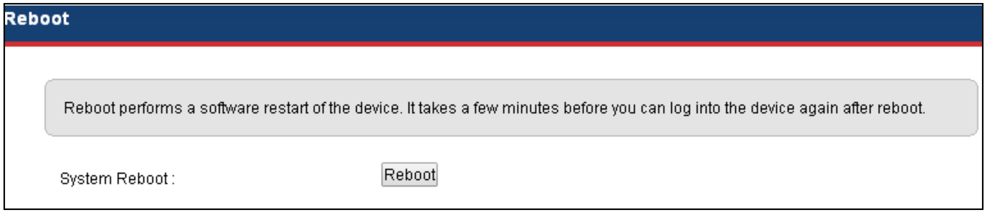
You can also press the **RESET** button on the rear panel to reset the factory defaults of your VMG. Refer to Section 1.7 on page 21 for more information on the **RESET** button.

38.3 The Reboot Screen

System restart allows you to reboot the VMG remotely without turning the power off. You may need to do this if the VMG hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the VMG reboot. This does not affect the VMG's configuration.

Figure 182 Maintenance > Reboot



Reboot

Reboot performs a software restart of the device. It takes a few minutes before you can log into the device again after reboot.

System Reboot :

39

Diagnostic

39.1 Overview

The **Diagnostic** screens display information to help you identify problems with the VMG.

The route between a CO VDSL switch and one of its CPE may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

39.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you ping an IP address or trace the route packets take to a host (Section 39.3 on page 341).
- The **802.1ag** screen lets you perform CFM actions (Section 39.5 on page 342).
- The **OAM Ping** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. (Section 39.5 on page 342).

39.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

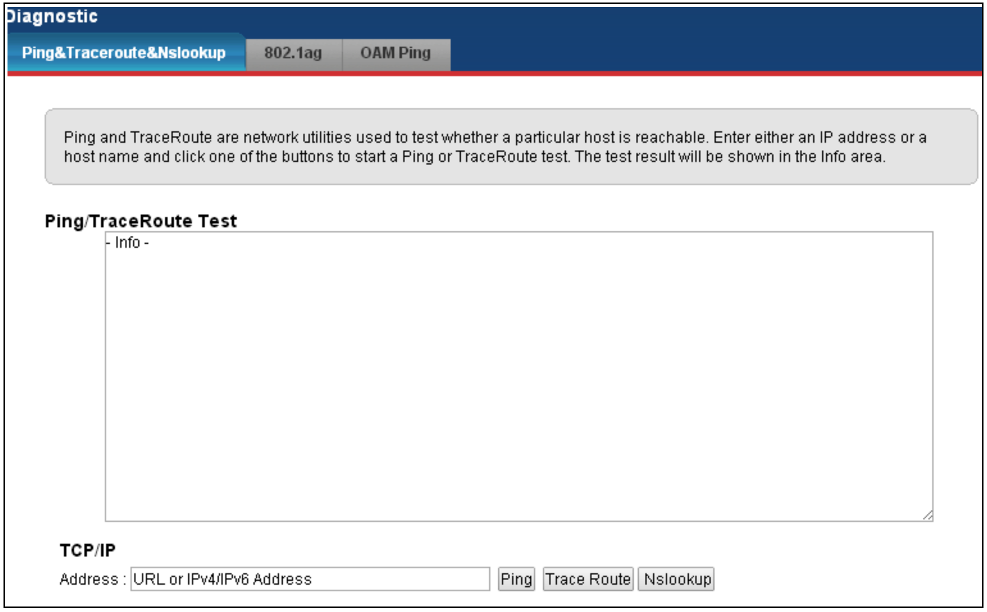
CFM provides two tests to discover connectivity faults.

- Loopback test - checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test - provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

39.3 Ping & TraceRoute & NsLookup

Use this screen to ping, traceroute, or nslookup an IP address. Click **Maintenance > Diagnostic > Ping&TraceRoute&NsLookup** to open the screen shown next.

Figure 183 Maintenance > Diagnostic > Ping &TraceRoute&NsLookup



Ping and TraceRoute are network utilities used to test whether a particular host is reachable. Enter either an IP address or a host name and click one of the buttons to start a Ping or TraceRoute test. The test result will be shown in the Info area.

Ping/TraceRoute Test

- Info -

TCP/IP

Address : URL or IPv4/IPv6 Address

The following table describes the fields in this screen.

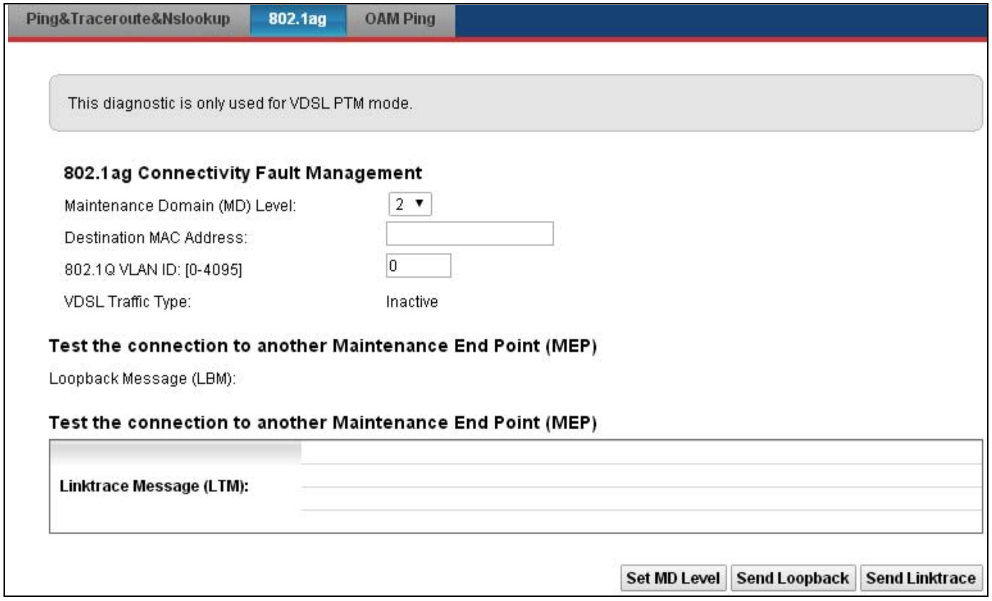
Table 146 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

LABEL	DESCRIPTION
URL or IP Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IP address that you entered.
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified computer.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

39.4 802.1ag

Click **Maintenance > Diagnostic** > **8.2.1ag** to open the following screen. Use this screen to perform CFM actions.

Figure 184 Maintenance > Diagnostic > 802.1ag



This diagnostic is only used for VDSL PTM mode.

802.1ag Connectivity Fault Management

Maintenance Domain (MD) Level: 2

Destination MAC Address:

802.1Q VLAN ID: [0-4095] 0

VDSL Traffic Type: Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM):

Test the connection to another Maintenance End Point (MEP)

Linktrace Message (LTM):

The following table describes the fields in this screen.

Table 147 Maintenance > Diagnostic > 802.1ag

LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
Maintenance Domain (MD) Level	Select a level (0-7) under which you want to create an MA.
Destination MAC Address	Enter the target device’s MAC address to which the VMG performs a CFM loopback test.
802.1Q VLAN ID	Type a VLAN ID (0-4095) for this MA.
VDSL Traffic Type	This shows whether the VDSL traffic is activated.
Loopback Message (LBM)	This shows how many Loop Back Messages (LBMs) are sent and if there is any inorder or outorder Loop Back Response (LBR) received from a remote MEP.
Linktrace Message (LTM)	This shows the destination MAC address in the Link Trace Response (LTR).
Set MD Level	Click this button to configure the MD (Maintenance Domain) level.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

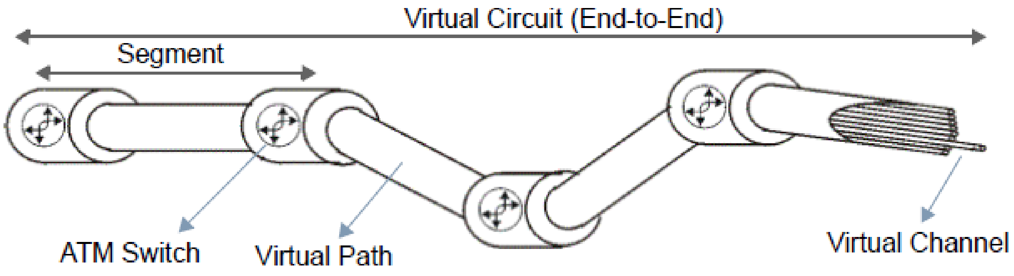
39.5 OAM Ping

Click **Maintenance > Diagnostic > OAM Ping** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The VMG sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the VMG. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

Virtual Channel (VC)	Logical connections between ATM devices
Virtual Path (VP)	A bundle of virtual channels
Virtual Circuits	A series of virtual paths between circuit end points

Figure 185 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefinded Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

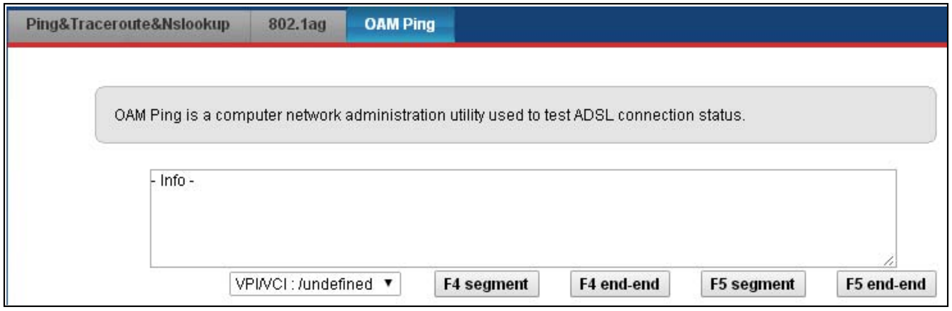
- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the VMG is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 186 Maintenance > Diagnostic > OAM Ping



OAM Ping is a computer network administration utility used to test ADSL connection status.

- Info -

The following table describes the fields in this screen.

Table 148 Maintenance > Diagnostic > OAM Ping

LABEL	DESCRIPTION
	Select a PVC on which you want to perform the loopback test.
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

40

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- VMG Access and Login
- Internet Access
- Wireless Internet Access
- USB Device Connection
- UPnP

40.1 Power, Hardware Connections, and LEDs

The VMG does not turn on. None of the LEDs turn on.

1. Make sure the VMG is turned on.
2. Make sure you are using the power adaptor or cord included with the VMG.
3. Make sure the power adaptor or cord is connected to the VMG and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the VMG off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.6 on page 20.
2. Check the hardware connections.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the VMG off and on.

5 If the problem continues, contact the vendor.

40.2 VMG Access and Login

I forgot the IP address for the VMG.

1 The default LAN IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the VMG by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the VMG (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.7 on page 21.

I forgot the password.

1 See the cover page for the default login names and associated passwords.

2 If those do not work, you have to reset the device to its factory defaults. See Section 1.7 on page 21.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 8.2 on page 141), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the VMG.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.6 on page 20.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix D on page 399.

4 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance > Remote MGMT**).

5 Reset the device to its factory defaults, and try to access the VMG with the default IP address. See Section 1.7 on page 21.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the VMG using another service, such as Telnet. If you can access the VMG, check the remote management settings and firewall rules to find out why the VMG does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the VMG.

1 Make sure you have entered the password correctly. See the cover page for the default login names and associated passwords. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the VMG. Log out of the VMG in the other session, or ask the person who is logged in to log out.

3 Turn the VMG off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 40.1 on page 345.

I cannot Telnet to the VMG.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

40.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 1.6 on page 20.
2. Make sure you entered your ISP account information correctly in the **Network Setting > Broadband** screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure that you enabled the wireless LAN in the VMG and your wireless client and that the wireless settings in the wireless client are the same as the settings in the VMG.
4. Disconnect all the cables from your device and reconnect them.
5. If the problem continues, contact your ISP.

I cannot access the Internet through a DSL connection.

1. Make sure you have the **DSL WAN** port connected to a telephone jack (or the DSL or modem jack on a splitter if you have one).
2. Make sure you configured a proper DSL WAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.
3. Check that the LAN interface you are connected to is in the same interface group as the DSL connection (**Network Setting > Interface Group**).
4. If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a second DSL connection.

ADSL and VDSL connections cannot work at the same time. You can only use one type of DSL connection, either ADSL or VDSL connection at one time.

I cannot connect to the Internet using an Ethernet connection.

1. The DSL connection has priority. If the DSL connection is up, then the Ethernet connection will be down.

2 Make sure you have the Ethernet WAN port connected to a MODEM or Router.

3 Make sure you converted LAN port number four as WAN. Click **Enable** in **Network Setting** > **Broadband** > **Ethernet WAN** screen.

4 Make sure you configured a proper EthernetWAN interface (**Network Setting > Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.

5 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting > Interface Group**).

6 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **LAN** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a 3G connection.

1 The DSL and Ethernet connections have priority in that order. If the DSL or Ethernet connection is up, then the 3G connection will be down.

2 Make sure you have connected a compatible 3G dongle to the USB port.

3 Make sure you have configured **Network Setting > Broadband > 3G Backup** correctly.

Check that the VMG is within range of a 3G base station.I cannot access the VMG anymore. I had access to the VMG, but my connection is not available anymore.

1 Your session with the VMG may have expired. Try logging into the VMG again.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and Section 1.6 on page 20.

3 Turn the VMG off and on.

4 If the problem continues, contact your vendor.

40.4 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.

- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

40.5 USB Device Connection

The VMG fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the VMG.
3. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
4. Re-connect your USB device to the VMG.

40.6 UPnP

When using UPnP and the VMG reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the VMG’s LAN port or from your computer.

2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

3

PART III
Appendices

Appendices contain general information. Some information may not apply to your device.

A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

Regional websites are listed below

See also *http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml*

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Asia

China

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- ZyXEL Kazakhstan

- http://www.zyxel.kz

Korea

- ZyXEL Korea Corp.
- http://www.zyxel.kr

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philipines

- ZyXEL Philippines
- http://www.zyxel.com.ph

Singapore

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Thailand

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Belarus

- ZyXEL BY
- http://www.zyxel.by

Belgium

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/

Bulgaria

- ZyXEL България
- http://www.zyxel.com/bg/bg/

Czech

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- ZyXEL Communications A/S
- http://www.zyxel.dk

Estonia

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

Finland

- ZyXEL Communications
- http://www.zyxel.fi

France

- ZyXEL France
- http://www.zyxel.fr

Germany

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Hungary

- ZyXEL Hungary & SEE
- http://www.zyxel.hu

Latvia

- ZyXEL Latvia

- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- ZyXEL Benelux
- http://www.zyxel.nl

Norway

- ZyXEL Communications
- http://www.zyxel.no

Poland

- ZyXEL Communications Poland
- http://www.zyxel.pl

Romania

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

Russia

- ZyXEL Russia
- http://www.zyxel.ru

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- ZyXEL Spain
- http://www.zyxel.es

Sweden

- ZyXEL Communications
- http://www.zyxel.se

Switzerland

- Studerus AG

- http://www.zyxel.ch/

Turkey

- ZyXEL Turkey A.S.
- http://www.zyxel.com.tr

UK

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- ZyXEL Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Ecuador

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Egypt

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

Middle East

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- http://www.us.zyxel.com/

Oceania

Australia

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

Wireless LANs

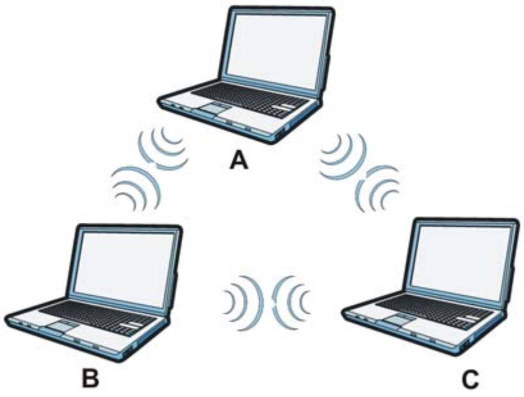
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 187 Peer-to-Peer Communication in an Ad-hoc Network

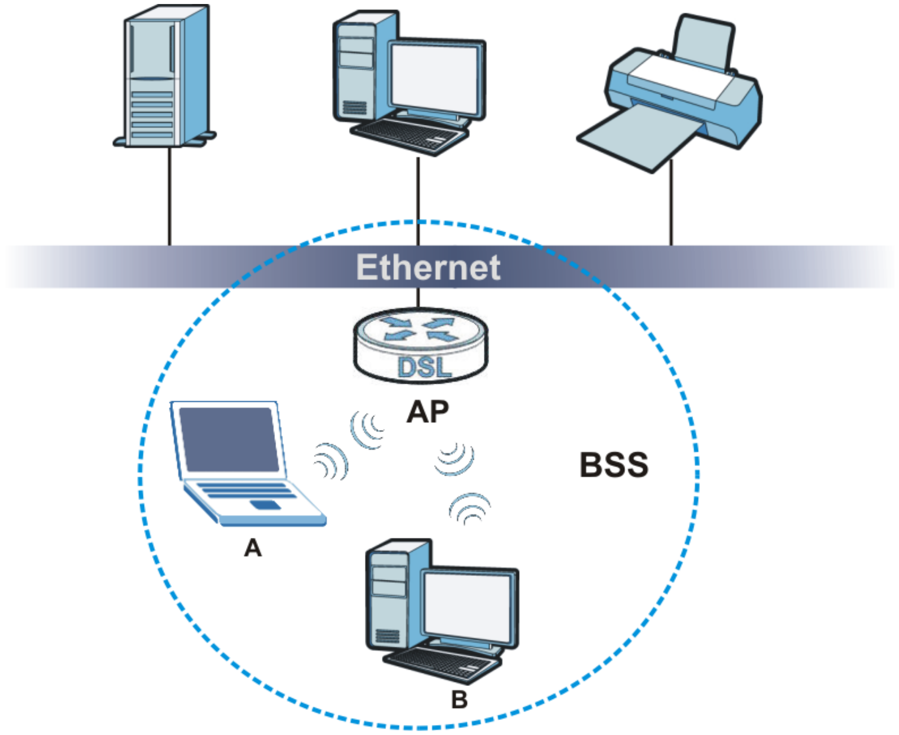


BSS

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

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

Figure 188 Basic Service Set



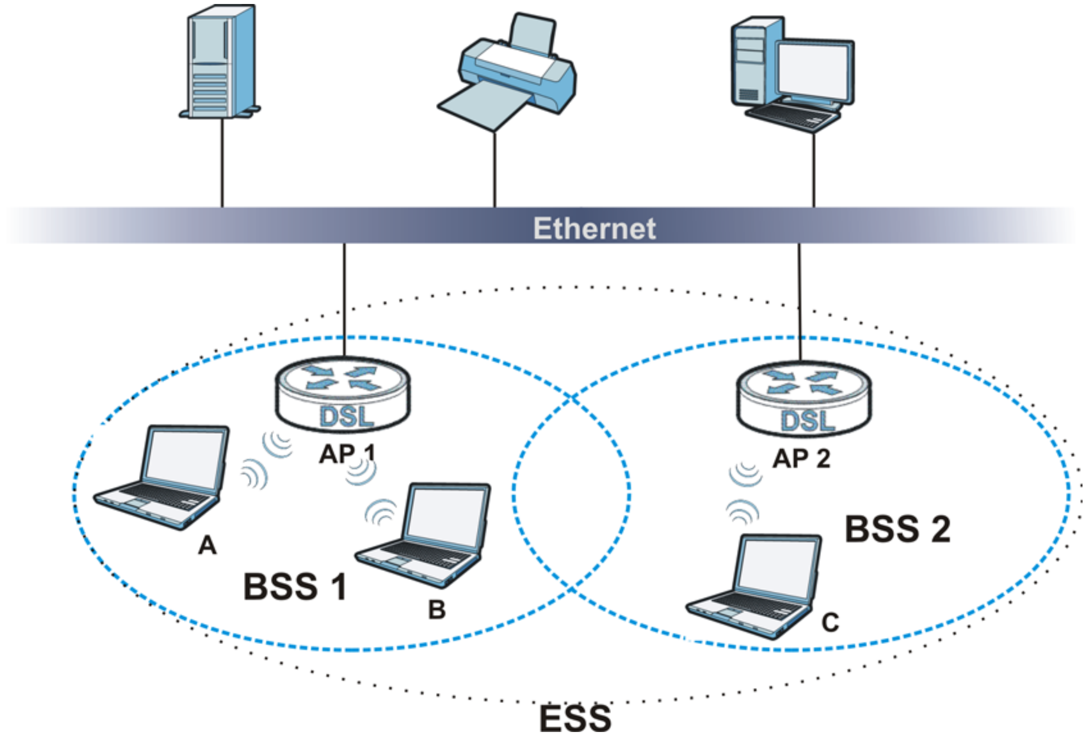
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 189 Infrastructure WLAN



Channel

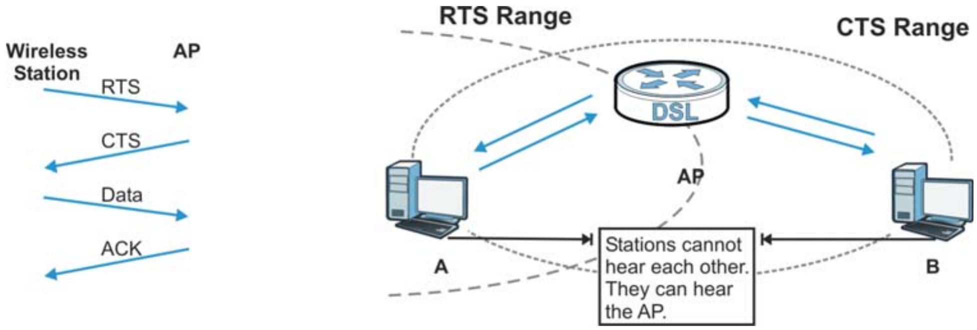
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 190 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 149 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the VMG are data encryption, wireless client authentication, restricting access by device MAC address and hiding the VMG identity.

The following figure shows the relative effectiveness of these wireless security methods available on your VMG.

Table 150 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the VMG and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.

- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 151 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use

WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

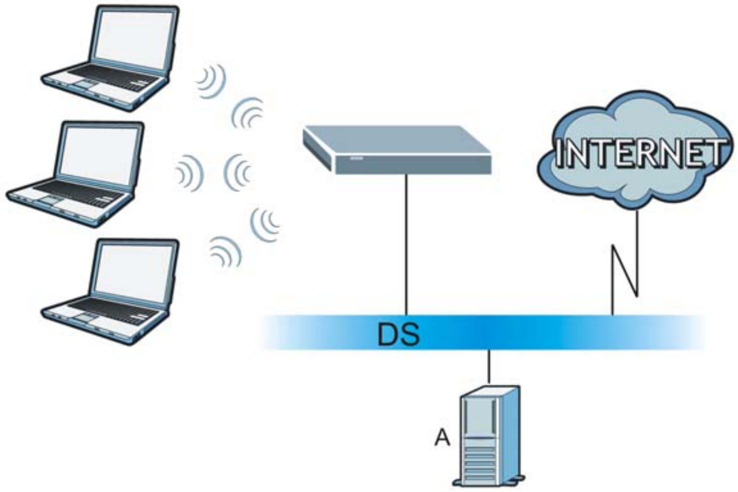
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 191 WPA(2) with RADIUS Application Example

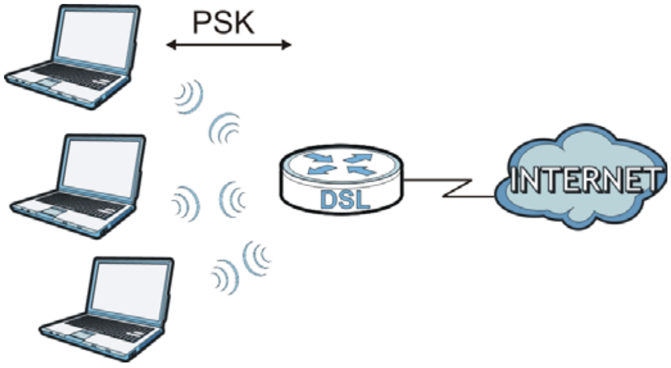


WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
4. The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 192 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 152 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna’s coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately

2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

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

Prefix and Prefix Length

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

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

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

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a “private IP address” in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 153 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to “0.0.0.0” in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 154 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 155 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0

Table 155 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

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

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

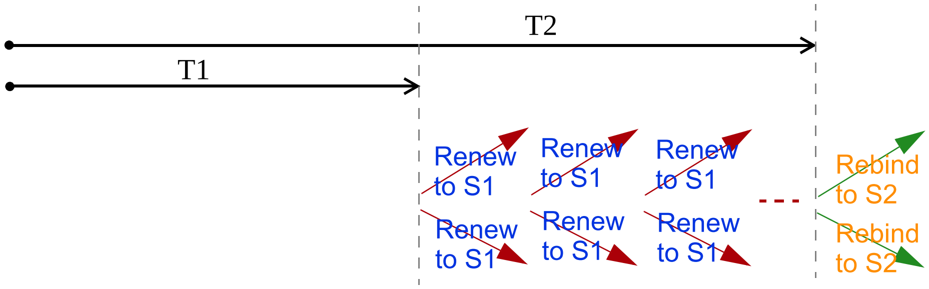
The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

MAC	00	: 13	: 49	: 12	: 34	: 56		
EUI-64	02	: 13	: 49	: FF	: FE	: 12	: 34	: 56

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The VMG uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the VMG passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor’s reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor’s link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being “reachable” means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.

- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The VMG maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the VMG configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the VMG also sends out a neighbor solicitation message. When the VMG receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the VMG uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The VMG creates an entry in the default router list cache if the router can be used as a default router.

When the VMG needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the VMG uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the VMG determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the VMG looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the VMG cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . : 10.1.1.254
```

IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

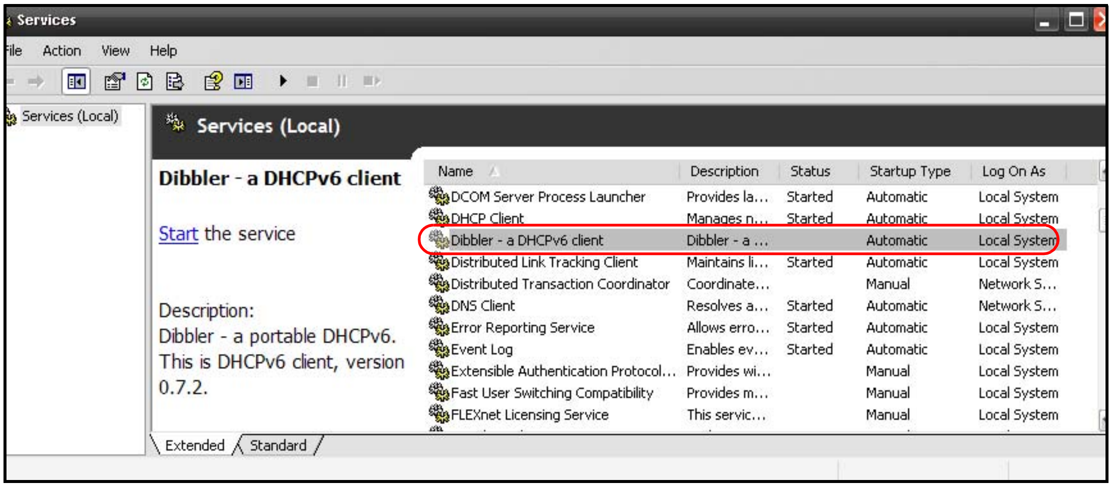
This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

1 Install Dibbler and select the DHCPv6 client option on your computer.

2 After the installation is complete, select **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.

3 Select **Start** > **Control Panel** > **Administrative Tools** > **Services**.

4 Double click **Dibbler - a DHCPv6 client**.



Services (Local)

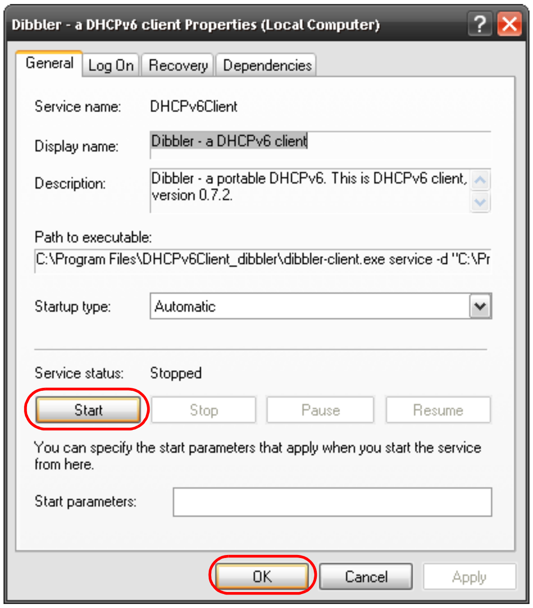
Dibbler - a DHCPv6 client

Start the service

Description:
Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Name	Description	Status	Startup Type	Log On As
DCOM Server Process Launcher	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System
Dibbler - a DHCPv6 client	Dibbler - a ...		Automatic	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...		Manual	Network S...
DNS Client	Resolves a...	Started	Automatic	Network S...
Error Reporting Service	Allows erro...	Started	Automatic	Local System
Event Log	Enables ev...	Started	Automatic	Local System
Extensible Authentication Protocol...	Provides wi...		Manual	Local System
Fast User Switching Compatibility	Provides m...		Manual	Local System
FLEXnet Licensing Service	This servic...		Manual	Local System

5 Click **Start** and then **OK**.



Service name: DHCPv6Client

Display name: Dibbler - a DHCPv6 client

Description: Dibbler - a portable DHCPv6. This is DHCPv6 client, version 0.7.2.

Path to executable:
C:\Program Files\DHCPv6Client_dibbler\dibbler-client.exe service -d "C:\Pr

Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

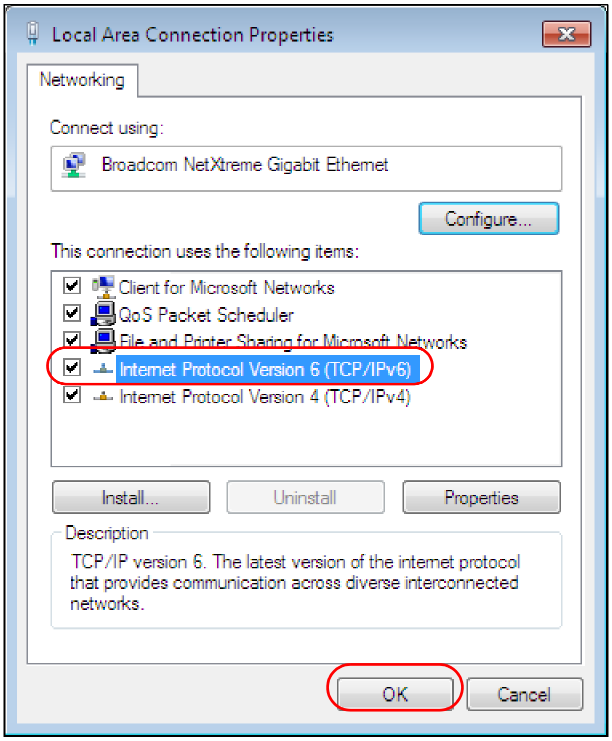
Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

1 Select **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.

3 Click **OK** to save the change.


Local Area Connection Properties
Networking
Connect using:
Broadcom NetXtreme Gigabit Ethernet
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
Install...
Uninstall
Properties
Description
OK
Cancel

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

4 Click **Close** to exit the **Local Area Connection Status** screen.

5 Select **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

D

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
    - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
    - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 156 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.

Table 156 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.

Table 156 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

The following information applies if you use the product within Canada area.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. If you cannot find it there, contact your vendor or ZyXEL Technical Support at support@zyxel.com.tw.

To obtain the source code covered under those Licenses, please contact your vendor or ZyXEL Technical Support at support@zyxel.com.tw

CE

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.

- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index