COMTREND CORPORATION

VG-8050

Wireless Router - Access Point

User Manual

Version 1.4, October 2014

Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.comtrend.com

Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix A.

Copyright

NOTE: This document is subject to change without notice.

Technical support

If you find the product to be inoperable or malfunctioning, please contact a technical support engineer for immediate service by email at INT-support@comtrend.com

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/

Protect Our Environment

This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.

Table of Contents

Chapter 1 Introduction

The VG-8050 is an 802.11n 2.4GHz compliant VoIP Gateway. It employs a 10/100/1000 Base-T Gigabit Ethernet port for WAN, four 10/100/1000 Base-T Gigabit Ethernet ports for LAN, one FXS port, one 2.4GHz WiFi On-Off/WPS button, and an integrated 802.11n 2.4GHz (2T2R) for WLAN Access Point (AP), which is backward compatible with 802.11b/g; therefore VG-8050 allows both wired LAN connectivity and wireless connectivity. It is also capable of facilitating predictable, real-time, toll-quality voice over the Internet.

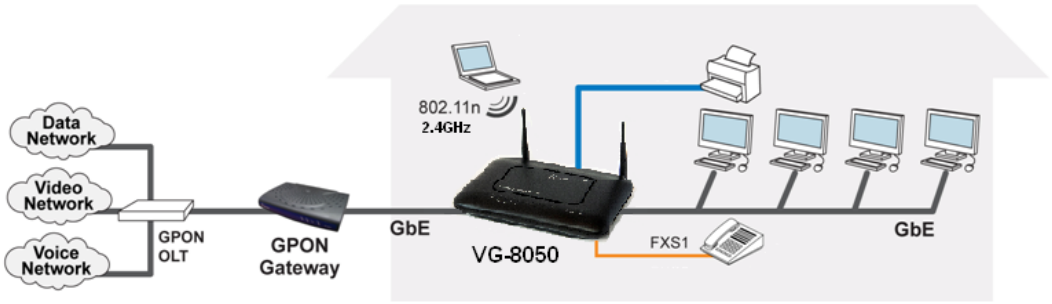
VG-8050 connects to ADSL or GPON (Gigabit-Capable Passive Optical Network) modem for providing VoIP services. It supports state-of-the-art security features such as WPA data encryption, Firewall & VPN pass through and is designed for both residential and business applications that require wireless and wired connectivity. VG-8050 is also designed with TR-068 compliant color panel and LED indicators for easy installation and user-friendliness.

1.1 Features

- UPnP
- Integrated 802.11n 2.4GHz AP (Backward compatible with 802.11g/b)
- WPA/WPA2 and 802.1x
- WMM
- RADIUS client
- IP filtering
- Static route routing functions
- Dynamic IP assignment
- Parental Control
- IGMP Proxy
- DHCP Server/Client
- DHCP Server/Client
- DNS Relay
- Supports remote administration
- Configuration backup and restoration
- FTP/TFTP server
- Supports QoS (Quality of Service) for voice
- Supports caller ID display and restriction
- Supports call hold, call waiting, call forwarding, call transfer, 3-way conference
- Supports Direct number dialing
- Supports T.38/ TR-069

1.2 Application

The following diagram depicts the application of the VG-8050.



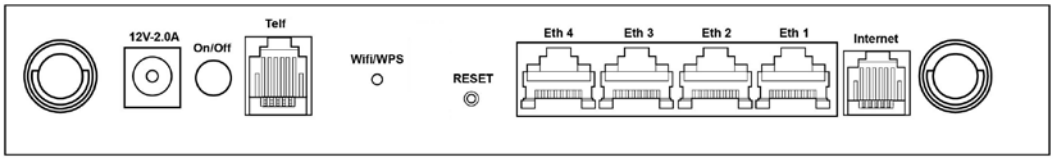
Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

BACK PANEL

The figure below shows the back panel of the device.



Power ON
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section 2.2 LED Indicators).

Caution 1:	If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely. Then power it on again. If the problem persists, contact technical support.
Caution 2:	Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

Telf
For VoIP service, connect telephone(s) to these ports with RJ11 cable.

Reset Button
Restore the default parameters of the device by pressing the Reset button during 5 seconds. The device will reboot. After the device has rebooted successfully, the front panel should display as expected (see section 2.2 LED Indicators).

NOTE:	If pressed down for more than 20 seconds, the VG-8050 will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

LAN PORTS
Use 1000-BASE-T RJ-45 cables to connect up to four network devices to a Gigabit LAN, or 10/100BASE-T RJ-45 cables for slower networks. As these ports are auto-sensing MDI/X, either straight-through or crossover cable can be used.

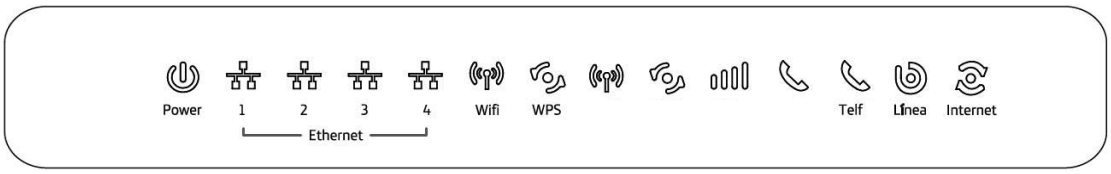
Internet
This port has the same features as the LAN ports described above with additional Ethernet WAN functionality.

WiFi / WPS Button

This button is used to enable/disable WiFi and WPS.
If pushed for 2 seconds it will enable/disable the wireless functionality.
If pushed for 5 seconds or longer, it will activate the WPS functionality.

2.2 LED Indicators

The front panel LED indicators are shown below and explained in the following table. This information can be used to check the status of the device and its connections.



LED	*Color*	*Mode*	*Description*
POWER	Green	On	Power on
	Red	Blinking 2Hz Red	Failure Power On Self Test
		Off	Power off
Ethernet 1x~4x	Green	On	Ethernet connection is available
		Blink	LAN activity present (traffic in either direction)
		Off	Ethernet connection is not available
WiFi	Green	On	WiFi connection is available
		Blink	Negotiation or traffic on line
		Off	WiFi connection is not available
WPS	Green	On (120 sec)	WPS window enabled
		Blink	WPS negotiation on going
		Off	WPS enabled but WPS window inactive
	Red	Solid Red (20 sec)	Problems on WPS Registration
Telf1	Green	Blinking	Negotiation or VoIP traffic presence.
		Solid	VoIP configuration OK, ATA has been registered in proxy SIP
		Quick blinking	Tx/Rx traffic on line
		Off	No VoIP configuration

	Red	Solid	VoIP configuration error, ATA can't register in proxy SIP
Línea	Green	On	Line up
		Off	WAN cable disconnected
Internet	Green	Blink	PPP/DHCP negotiation
		Solid	PPP/DHCP Up
		Quick Blinking	Tx/Rx traffic on line
		Off	No Internet connection (WAN cable disconnected or PPP interface deleted)
	Red	Solid Red	Authentication failed

NOTE:	During a FW Upgrade both the POWER and Internet LEDs will blink at 2Hz (Green Color). This blinking will indicate that the Flash memory is being overwritten. After the FW upgrade the router will reboot automatically.

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 5.0 and later).

3.1 Default Settings

The factory default settings of this device are summarized below.

- ☐ LAN IP address: 192.168.1.1
- ☐ LAN subnet mask: 255.255.255.0
- ☐ Administrative access (username: **1234** , password: **1234**)
- ☐ WLAN access: **enabled**

Technical Note

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button during 5 seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

3.2 IP Configuration

DHCP MODE

When the VG-8050 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

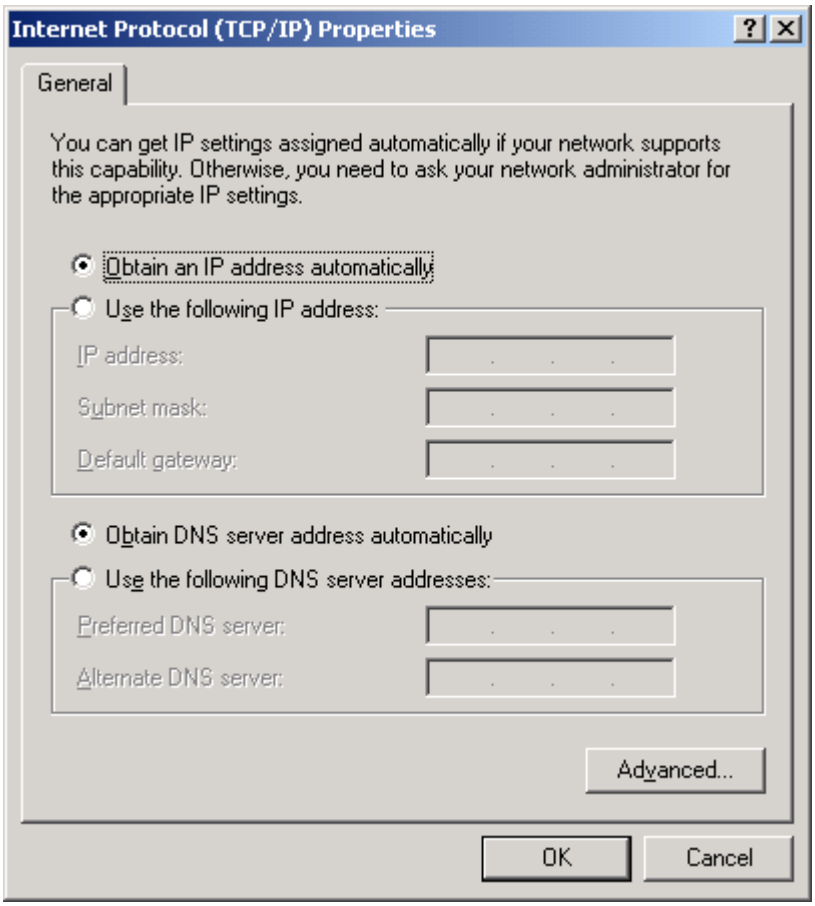
To obtain an IP address from the DCHP server, follow the steps provided below.

NOTE:	The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Select Obtain an IP address automatically as shown below.



STEP 4: Click **OK** to submit these settings.

If you experience difficulty with DHCP mode, you can try static IP mode instead.

STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

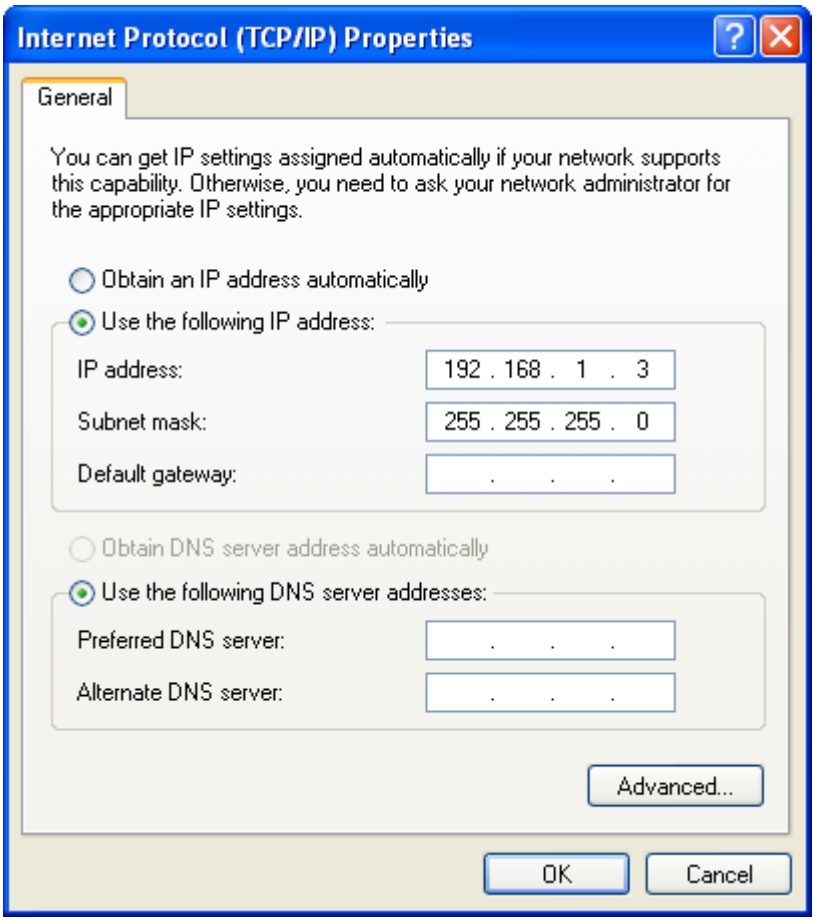
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

NOTE:	The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.



STEP 4: Click **OK** to submit these settings.

3.3 Login Procedure

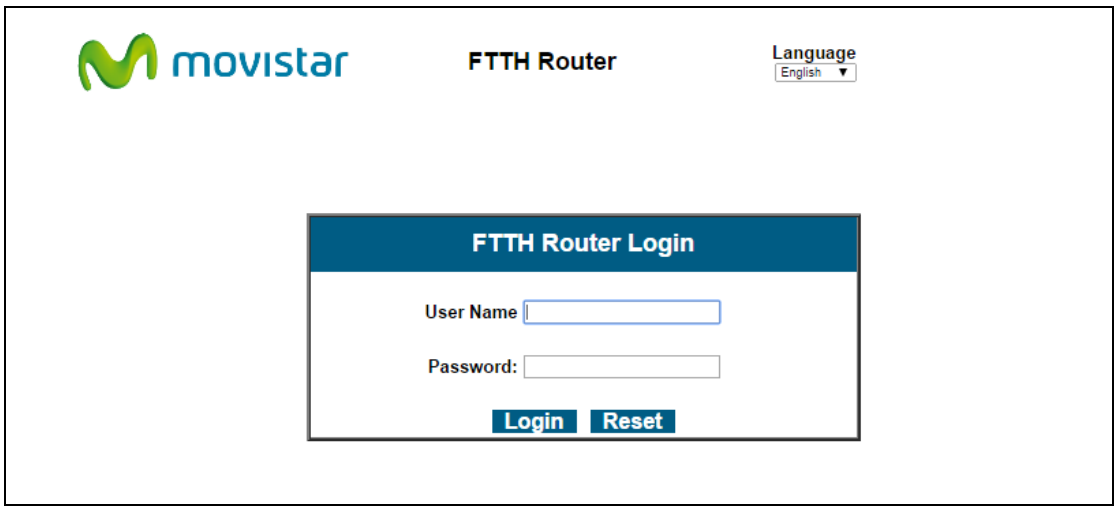
Perform the following steps to login to the web user interface.

NOTE:	The default settings can be found in section 3.1.

STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.1, type http://192.168.1.1.

NOTE:	For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the IP address shown on the Device Information screen and login with remote username and password.

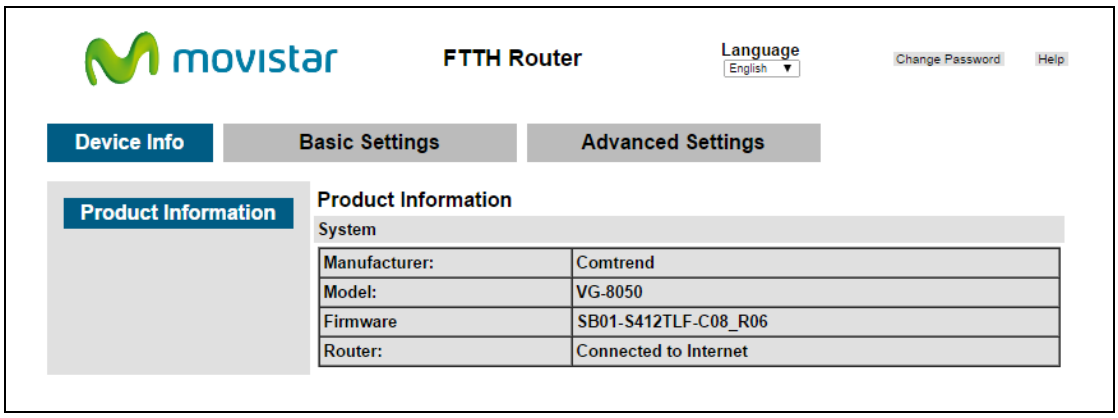
STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.



Click **Login** (or **Acceso**) to continue.

NOTE:	The login password can be changed later (see section 4.1.7)

STEP 3: After successfully logging in for the first time, you will reach this screen.

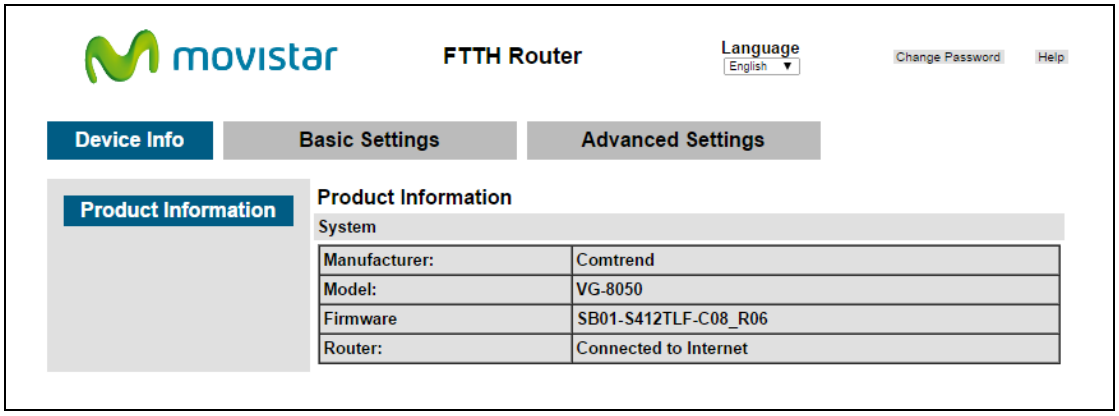


Chapter 4 Basic User Interface

The Basic Web User Interface is divided into 3 navigation tabs (Device Info, Basic Settings, Advanced Settings). By selecting each of these tabs it opens a submenu with more selections.

Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

The Product Information screen will display at startup.



This screen shows the manufacturer, hardware model, software version and IP settings and other related information.

There are 2 languages available for the Basic User Interface (Spanish and English), to change between languages simply click on the drop down **Language** (or **Idioma**) and select the language you prefer.

4.1 Basic Settings

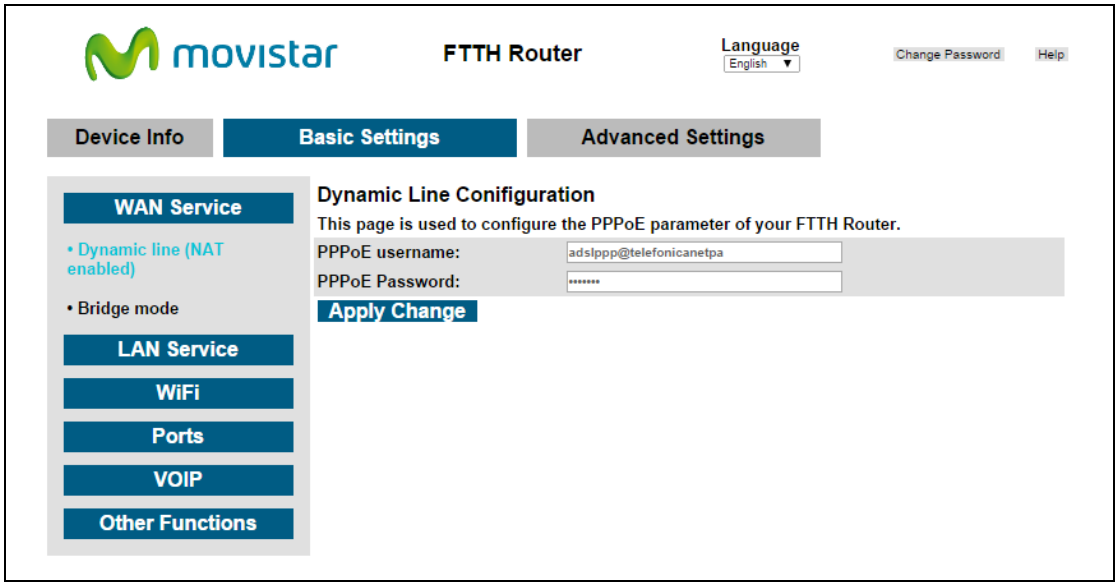
By clicking on the tab ‘Basic Settings’ you’ll be able to configure the different common settings of your network.

These settings are divided into different categories on the left side of the window.

4.1.1 WAN Service

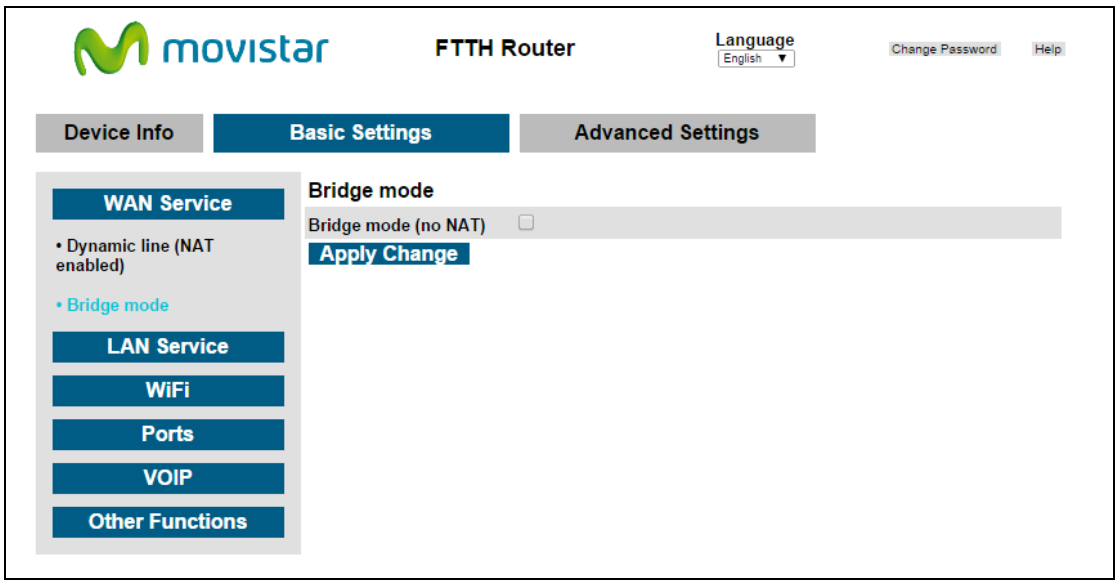
This option will allow you to set the PPP configuration or, on the contrary to disable the WAN PPP client in order to use an external client/router (Bridge mode)

By clicking on “Dynamic line (NAT enabled)” the following menu will appear:



There you can set a different PPP username and password. To set the new values press on ‘Apply Change’.

By clicking on “Bridge mode” the following menu will appear:

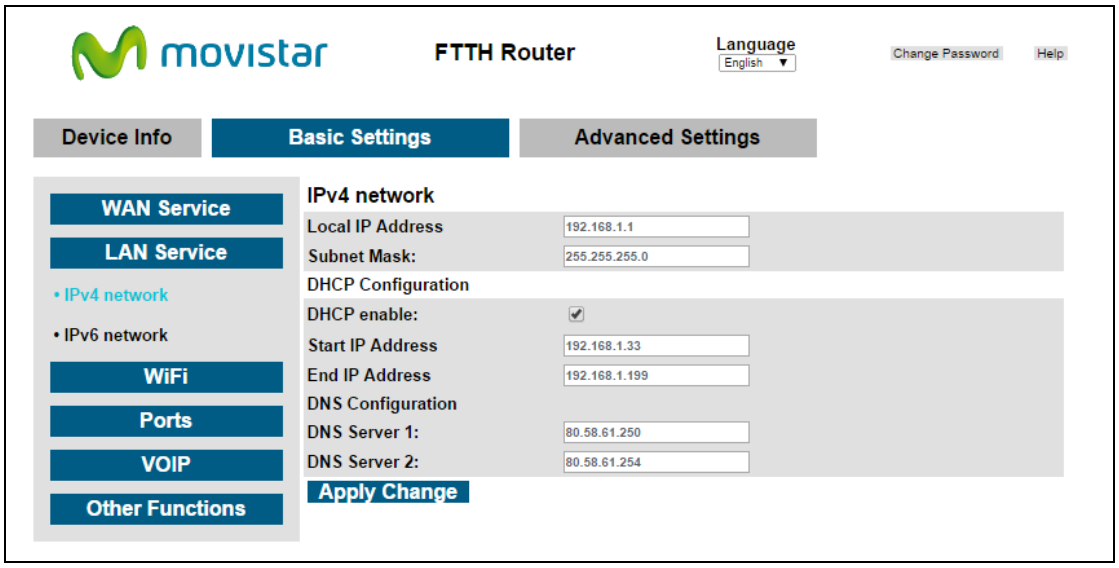


To disable the PPP client to be able to connect an external client or an external Router mark the option “Bridge mode (no NAT)” and press ‘Apply Changes’.

4.1.2 LAN Service

This menu allows changing the local IP address, modify the DHCP server range or configure the IPv6 LAN network.

By clicking on “IPv4 network” the following LAN IP options will be configurable:



In this menu you’ll be able to configure the following parameters:

IP Address: Input the IP address for the LAN port.

Subnet Mask: Input the subnet mask for the LAN port.

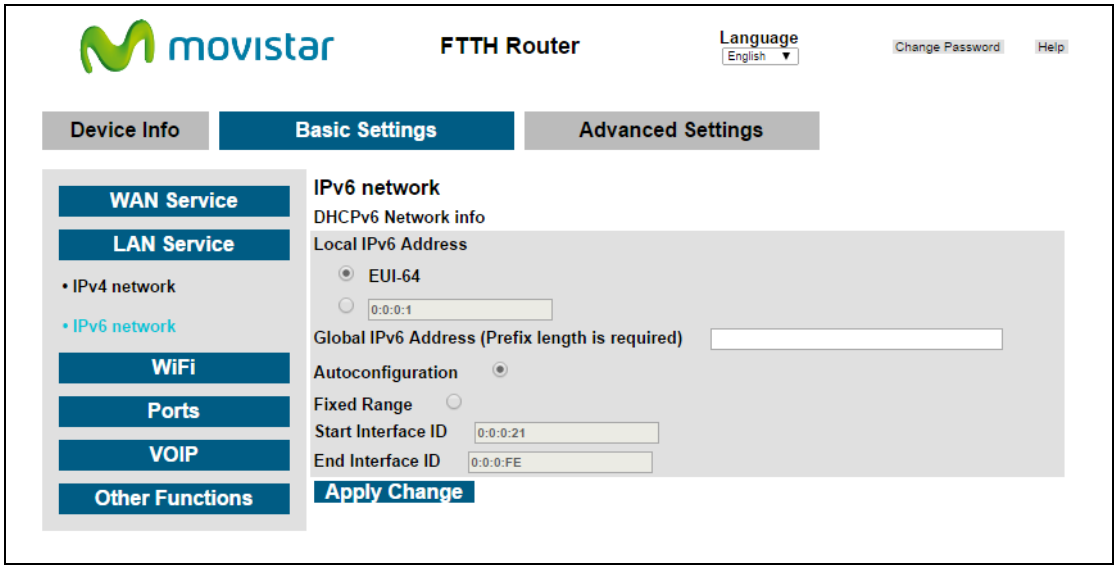
DHCP Configuration: To enable DHCP, select **Enable DHCP** and enter Start and End IP addresses. This setting configures the router to

automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

DNS Server 1: The Primary DNS server which is delivered to the LAN site hosts via DHCP protocol.

DNS Server 2: The Secondary DNS server which is delivered to the LAN site hosts via DHCP protocol.

To configure the LAN IPv6 network you need to click on “IPv6 network”:



Local IPv6 Address Configuration

Heading	Description
EUI-64	Use EUI-64 algorithm to calculate link-local address from MAC address
User Setting	Use the Interface Identifier field to define a link-local address

Global IPv6 Address Configuration

Heading	Description
Interface Address (prefix length is required):	Configure static LAN IPv6 address and subnet prefix length

DHCPv6 Configuration

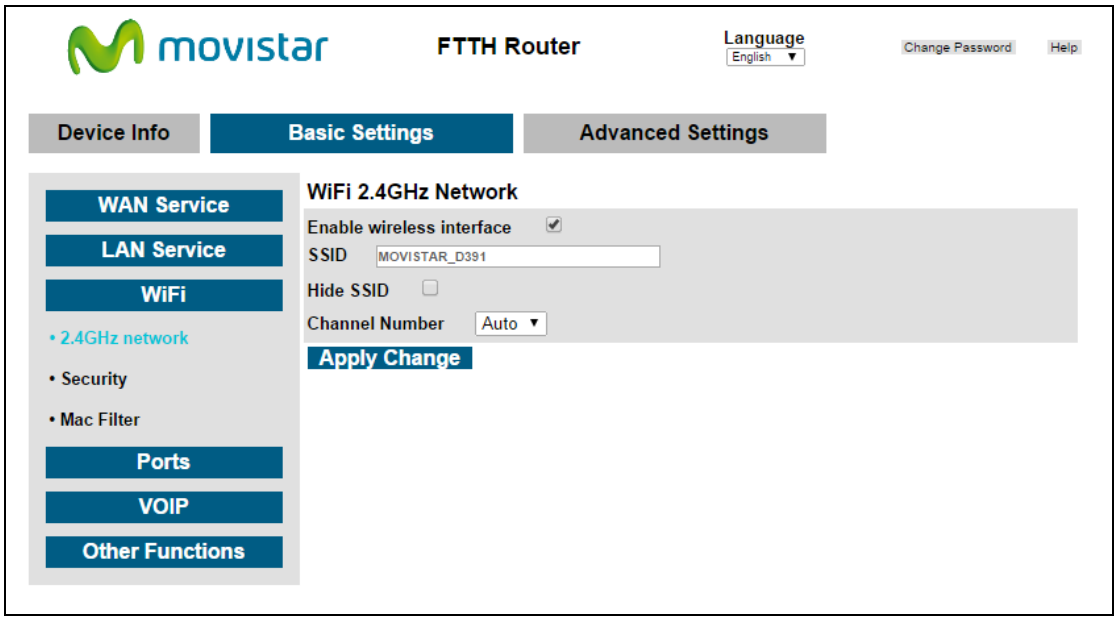
Heading	Description
Autoconfiguration	Use stateless configuration
Fixed Range	Use stateful configuration
Start interface ID:	Start of interface ID to be assigned to dhcpv6 client
End interface ID:	End of interface ID to be assigned to dhcpv6 client

4.1.3 WiFi

This option allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the access to your wireless network based on the physical addresses of the clients.

The WiFi option is divided in 3 simple menus:

"2.4GHz network":



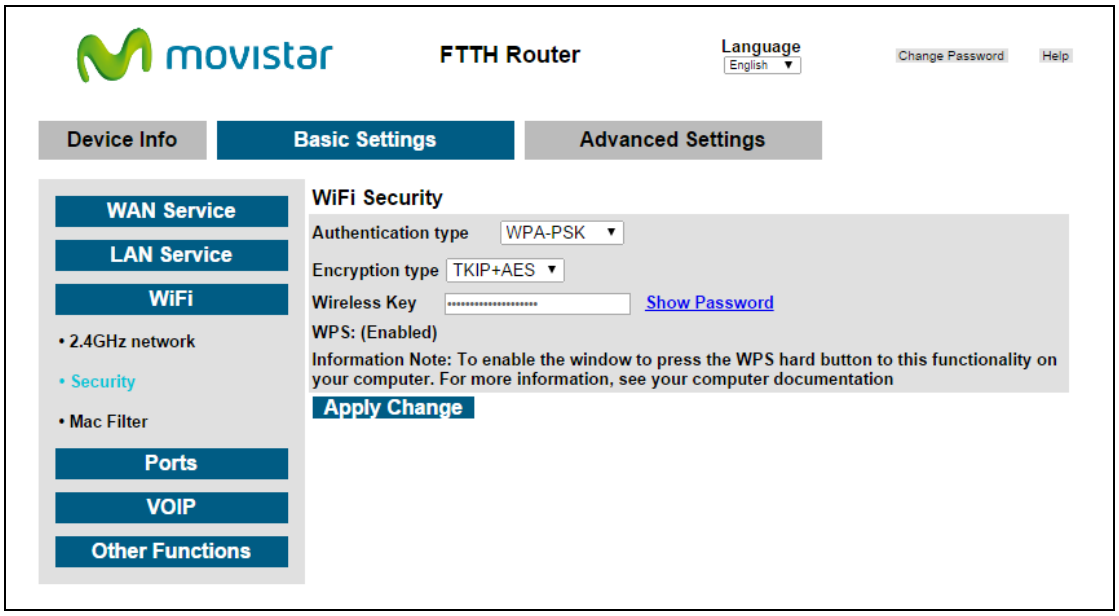
Consult the table below for descriptions of these options.

Option	Description
Enable wireless interface	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, the wireless network is enabled.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
Hide SSID	Select Hide SSID to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open **Network Connections** from the **start** Menu and select **View Available Network Connections**. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Channel number	Select in the drop down the channel number you wish to use for your wireless network. If you have no preference you can select 'Auto' and the router will automatically select the best channel.

Click **Apply Change** to implement new configuration settings.

"Security":

The following screen appears when the menu “Security” is selected. The options shown here allow you to configure security features of the wireless LAN interface.



WiFi Security

Here the authentication/encryption type and security key can be configured.

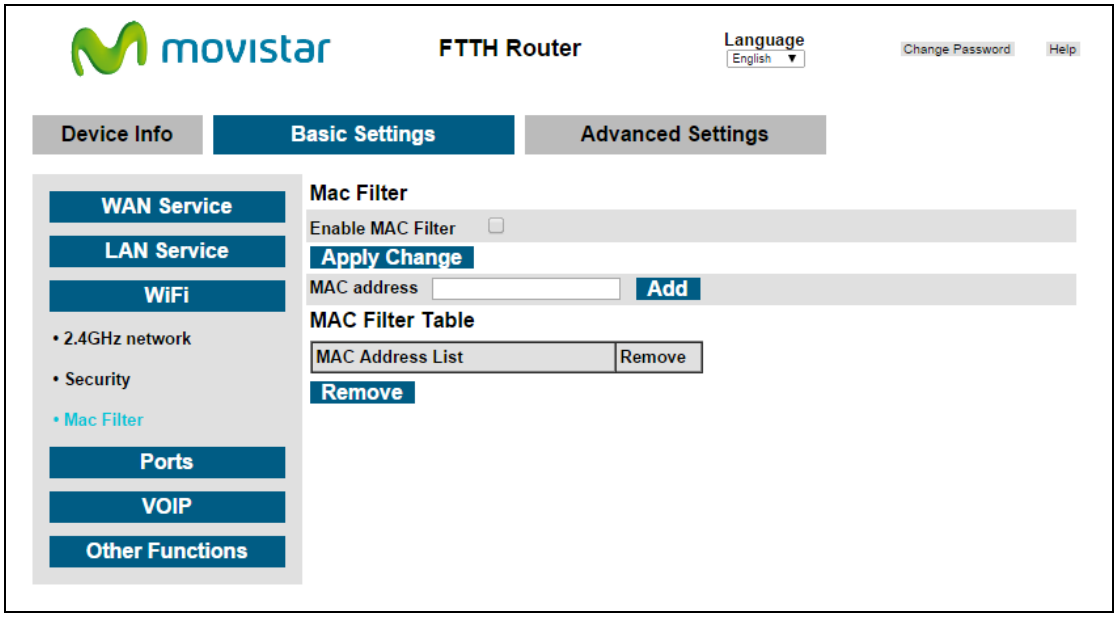
Authentication Type
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to OPEN, then no authentication is provided. On the contrary other authentication methods can be configurable (from less to stronger security): WEP: This is actually Open authentication with WEP encryption (128 bits). By selecting WEP you only need to enter the security key you want to use in your network (remember it must be 13 ASCII characters or 26 hex digits). WPA-PSK: Here you can select the encryption level (see next row). Just enter the security key you want to use in your network (remember it must greater or equal to 8 ASCII characters). WPA2-PSK: This is the strongest authentication level nowadays. Here you can select the encryption level (see next row). Just enter the security key you want to use in your network (remember it must greater or equal to 8 ASCII characters).
Encryption type
This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. This drop down only is available when WPA-PSK or WPA2-PSK authentication types are selected. You can set which encryption TKIP, AES or both (TKIP+AES) will be used for the communication. TKIP is less secure than AES (recommended).

Wireless Key
Enter the required security key.

Click **Apply Change** to implement new configuration settings.

"Mac Filter":

This page is used to set allowed MAC addresses, and click the associated button for each interface to enable/disable the MAC address control.
The current MAC control status is shown on the associated buttons.



Option	Description
Enable MAC Filter	A checkbox ☑ that enables or disables the MAC Filter. When selected, only the listed MAC address will be able to access the device.

Click **Apply Change** to apply the new MAC Filter configuration.

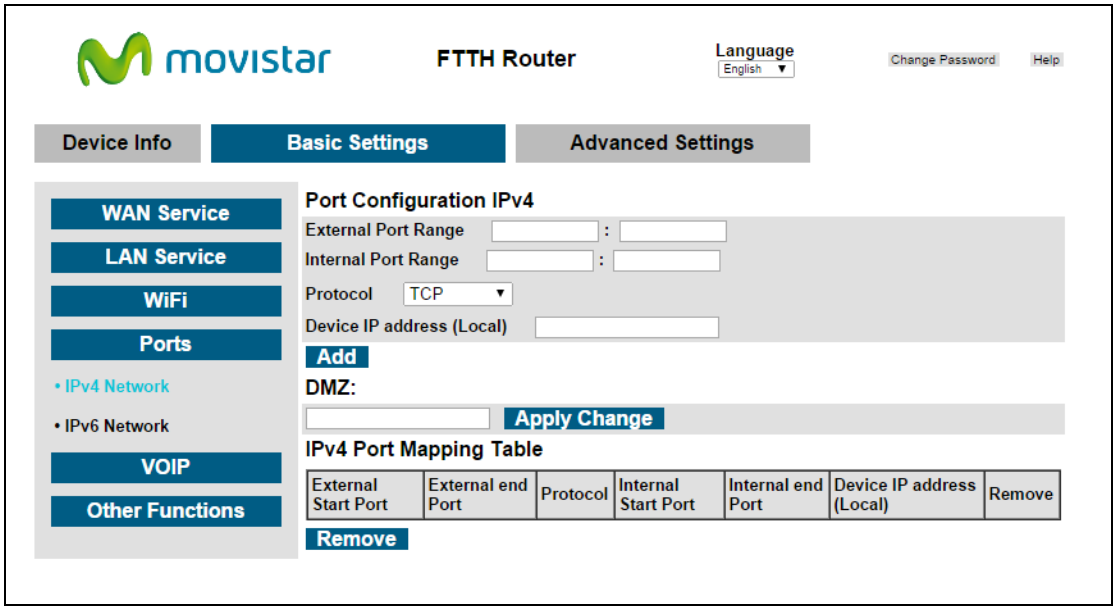
To Add a new MAC address in the list just enter the physical address of the desired device (format *XX:XX:XX:XX:XX:XX*) and press the button **Add**.

To remove one MAC address from the list select the checkbox ☑ associated to that address and press the button **Remove**.

4.1.4 Ports

Ports menu allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the Internal server with private IP addresses on the LAN side.

A maximum of 32 entries can be configured.



To open a IPv4 port(s) (also known as add a Virtual Server) you need to fill the following items shown in the table below.

Field / Header	**Description**
External Port Range	Enter the starting external port number and the ending external port number. This port is reserved in the public IP address for one specific service. The external port range cannot be repeated in any other entry.
Internal Port Range	Enter the starting internal port number and the ending internal port number. This port is reserved in the private IP address specified in the field “Device IP address”. The external port range cannot be repeated in the same private machine.
Protocol	TCP, TCP/UDP, or UDP.
Server IP Address	Enter the IP address for the server.

Finally, press the button **Add** to create the Virtual Server entry.

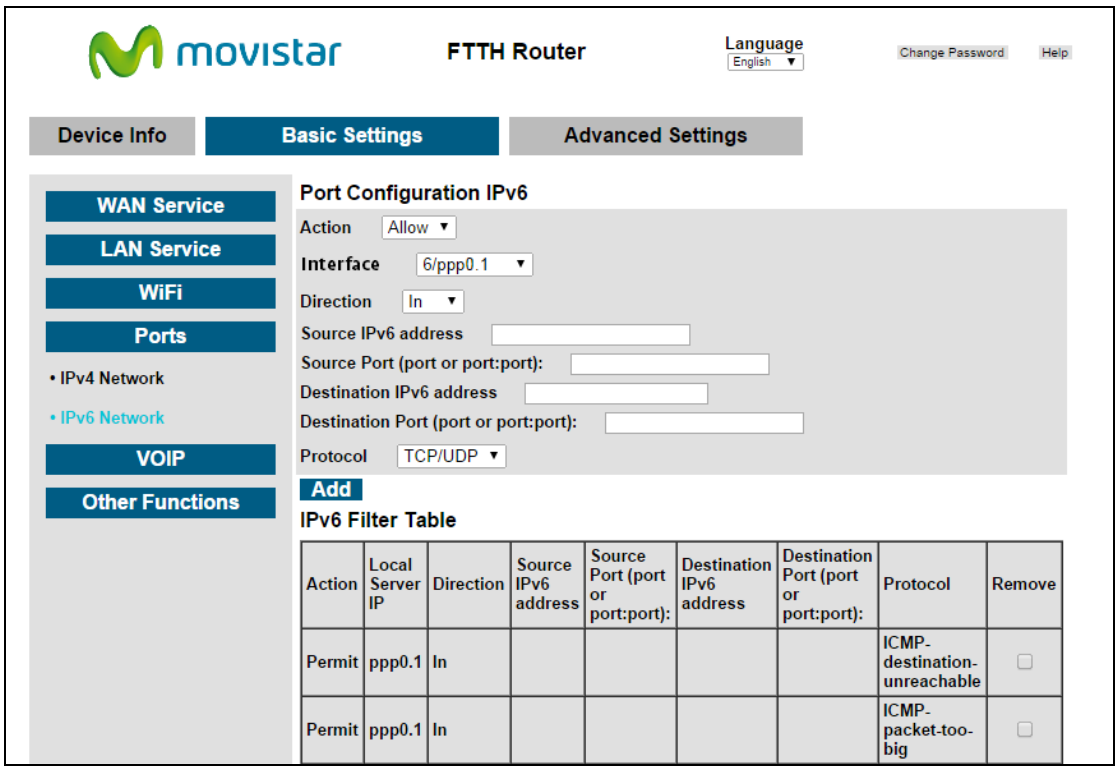
With the **DMZ option**, the router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

To **Activate** the DMZ host, enter the DMZ host IP address and click **Apply Change**.

To **Deactivate** the DMZ host, clear the IP address field and click **Apply Change**.

Finally, to remove one Virtual Server entry from the list select the checkbox ☑ associated to that Virtual Server and press the button **Remove**.

If you want to apply a similar configuration for IPv6 network (your ISP has enabled the IPv6 access) you can configure the remote access to your servers in the LAN by clicking on the menu “IPv6 network”:



Similar to the IPv4 network you need to fill the following items shown in the table below.

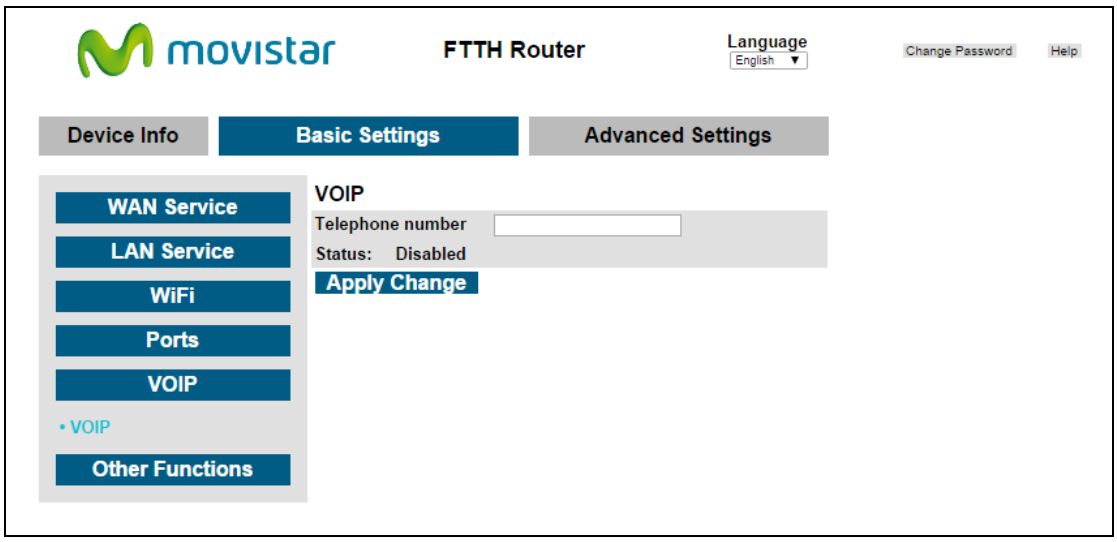
Field	Description
Action	This is to choose to allow or deny the packets that match the criteria.
Interface	Select the correct WAN interface from the drop down list.
Direction	Chose between incoming traffic (In) or outgoing traffic (out).
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.
Protocol	TCP, TCP/UDP, UDP, or ICMP.

Finally, press the button **Add** to create the IPv6 filtering entry.

4.1.5 VoIP

This menu configures the SIP voice service.

After clicking on “VOIP” the following menu will appear:



To enable your VoIP service you only need to enter the telephone number in the corresponding field.

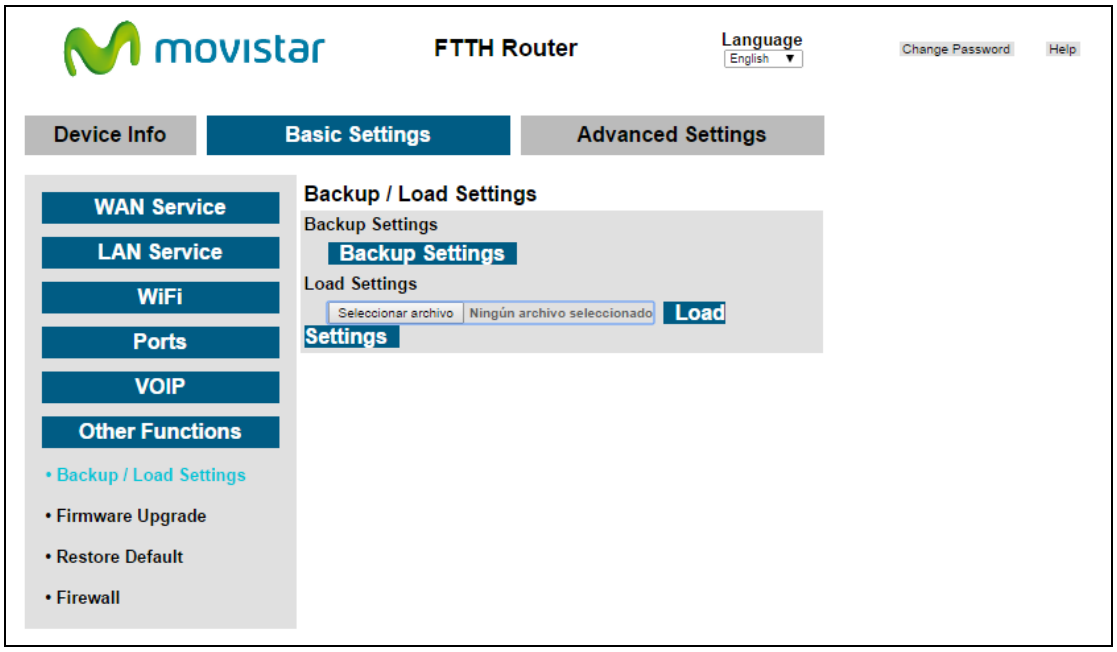
Click **Apply Change** to apply the new phone number.

At that moment the VoIP service will start and the phone LED indicator will show the service status (for further info see paragraph *2.2 LED indicators*)

4.1.6 Other functions

This menu has the following maintenance functions and processes:

Backup / Load Settings:



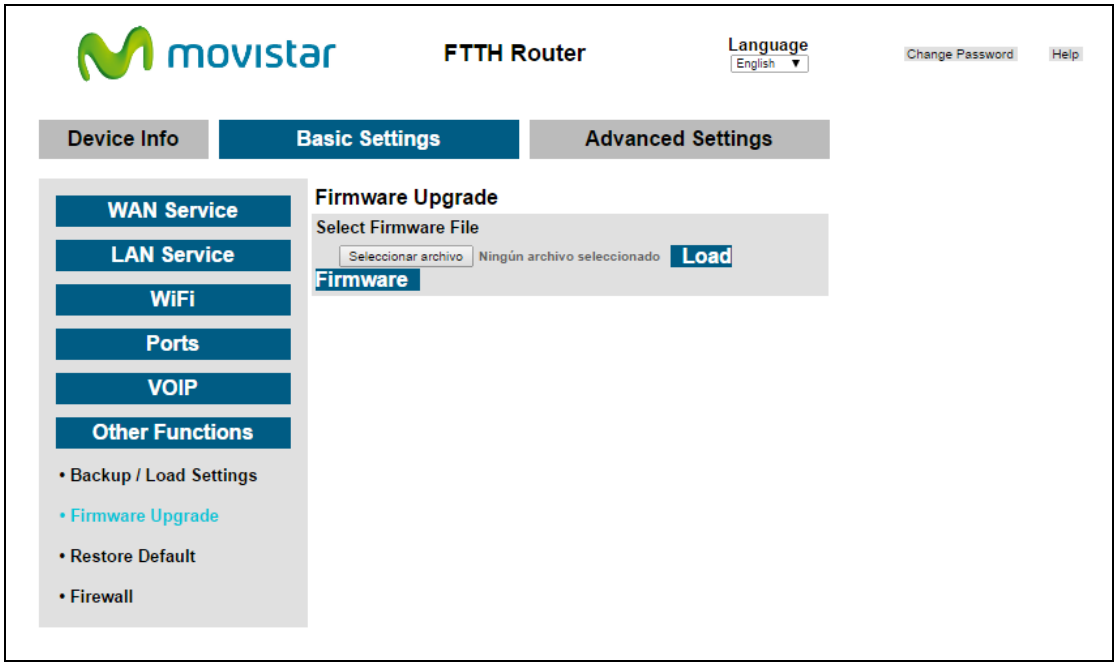
To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for a location of the backup file. This file can later be used to

recover settings on the **Load Settings** option, as described below.

To recover the configuration file previously saved using **Backup Settings** press **Browse…** to search for the file, then click **Load Settings** to recover settings (the router will reboot).

Backup/Load Settings:

This option allows for firmware upgrades from a locally stored file.



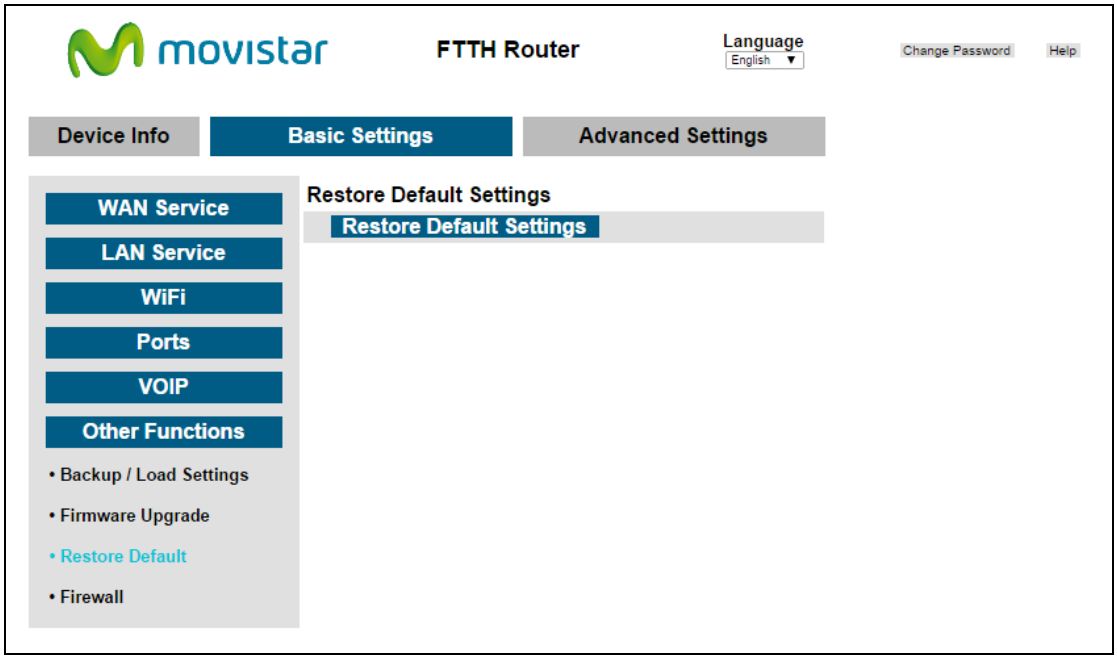
STEP 1: Obtain an updated software image file from your ISP.

STEP 2: Enter the path and filename of the firmware image file by clicking the **Browse** button to locate the image file.

STEP 3: Click the **Load Firmware** button once to upload and install the file.

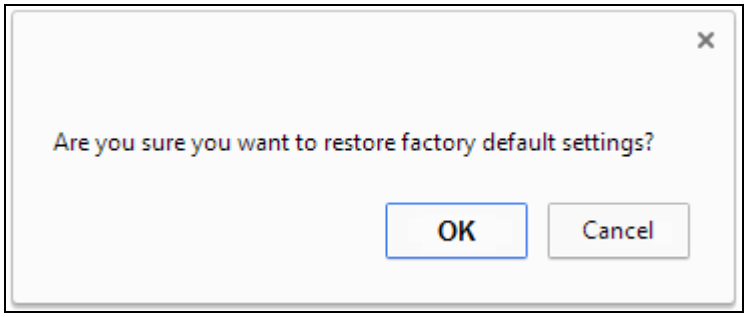
NOTE:	The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** at the top of the Device Info screen with the firmware version installed, to confirm the installation was successful.

Restore Default:

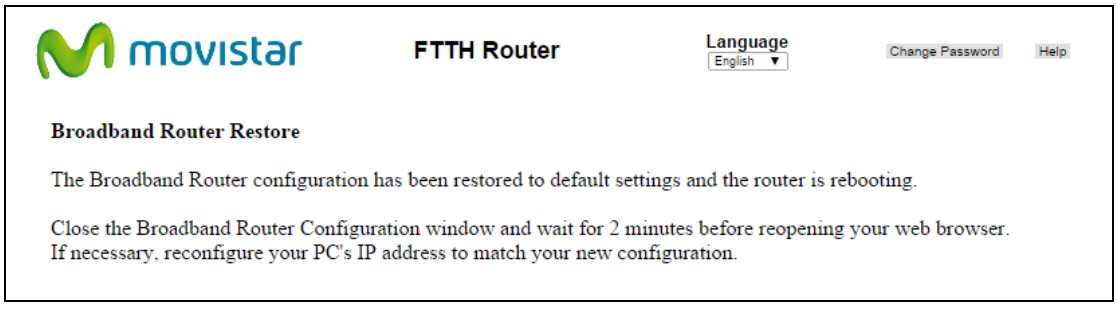


Click **Restore Default Settings** to restore factory default settings.

A warning window will appear:



Press OK and the following screen appears.

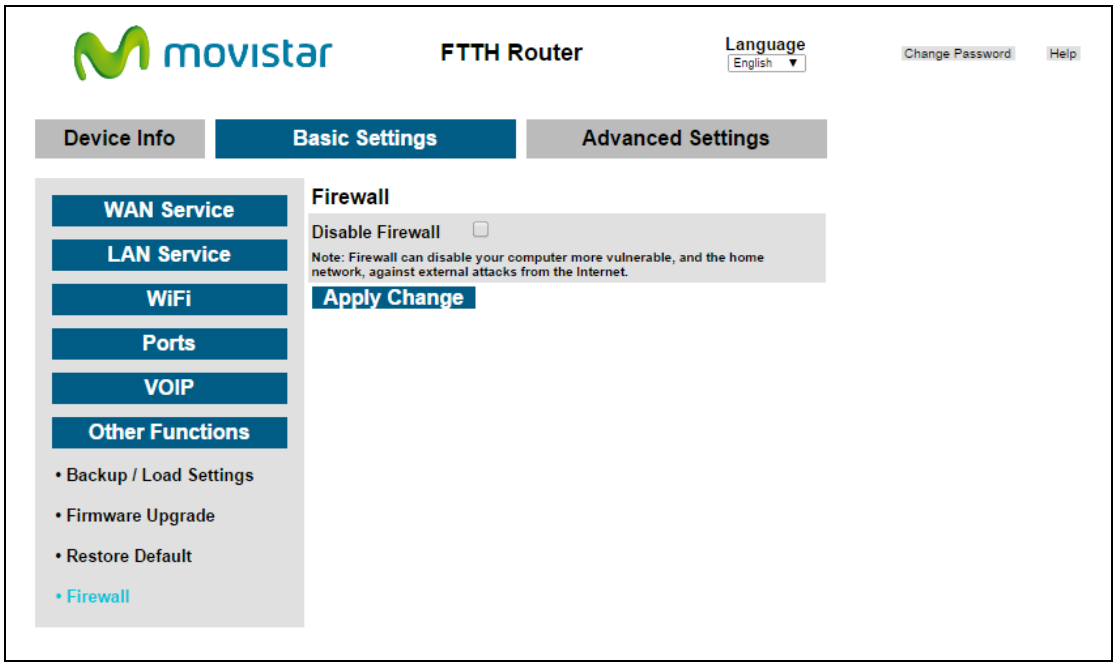


Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

NOTE:	This entry has the same effect as the **Reset** button located in the back panel of the router. The VG-8050 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for 5 seconds, the boot loader will erase the configuration data saved in flash memory.

Firewall:

Firewall menu only offers one option:



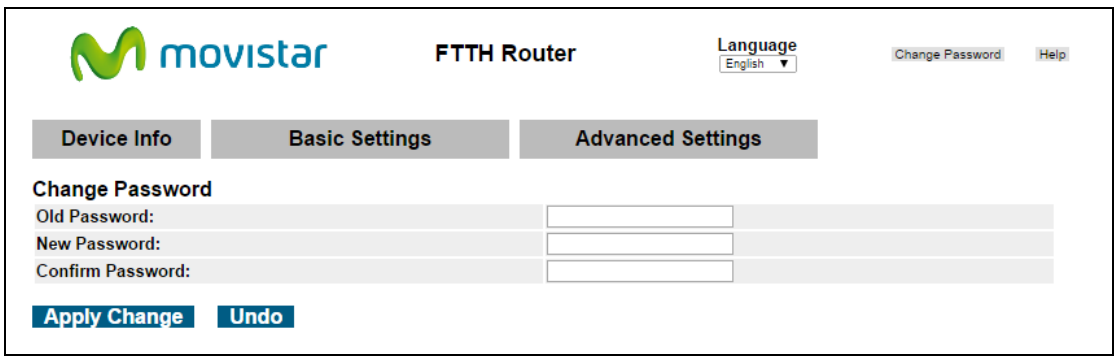
By clicking on the checkbox ☑ "Disable Firewall" and pressing the button **Apply Change** all the rules of filtering (IN/OUT) and Firewall capabilities will be disabled.

To restore the FW capabilities simply uncheck the "Disable Firewall" option and press **Apply Change.**

4.1.7 Password change

On the top-right part of the basic user interface there is the option to change the administrator password. To do so click on the button Change Password and the following screen will be shown.

Remember that the access to the VG-8050 is controlled by only one user account '1234'.



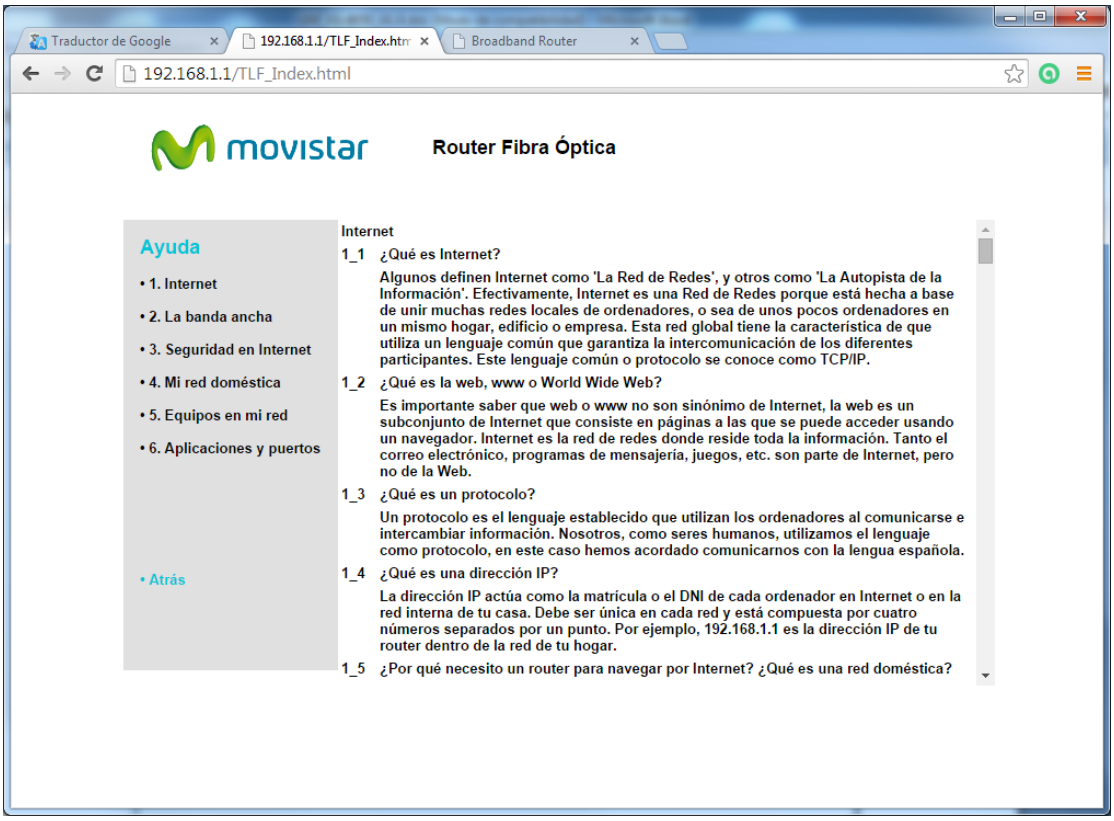
Enter the old password (by default '1234') and the new one twice. Click **Apply Change** to set the new password (you may need to re-authenticate with the new

credentials).

NOTE: Passwords must be 16 characters or less.

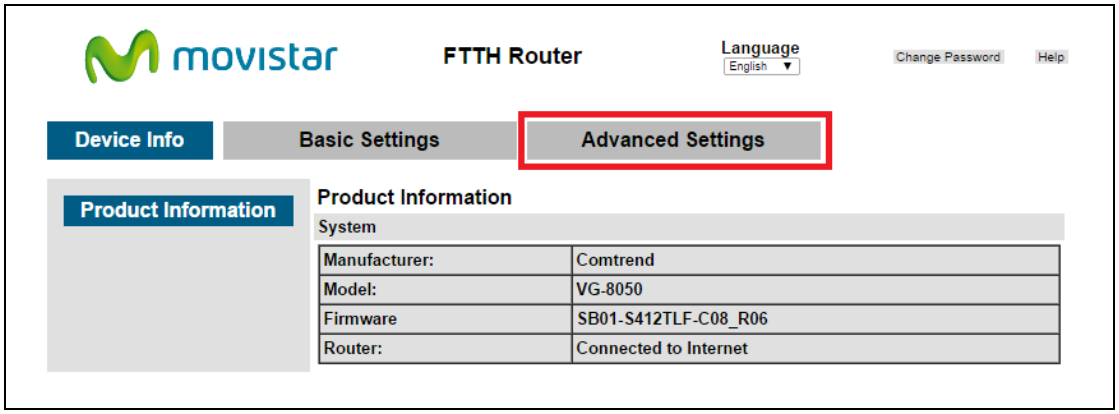
4.1.8 Help

The help menu is located to the top-right part of the basic user interface. By clicking on the **Help** button you will reach a new Window with basic contents that may help you to understand some capabilities of the router:

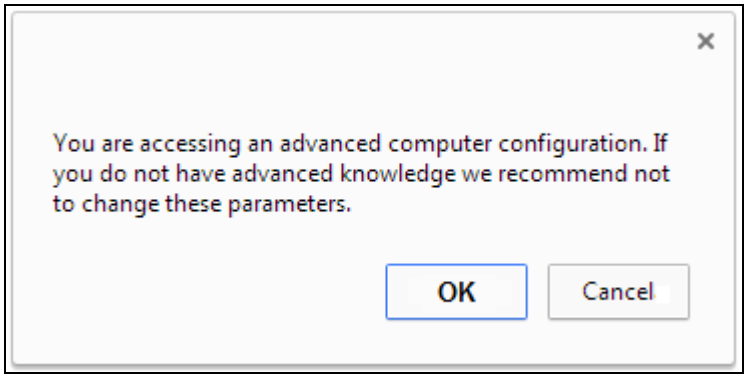


Chapter 5 Advanced User Interface

To access to the **Advanced User Interface** you need first login the device (see chapter '3.3. Login procedure'). In the Basic User Interface press on the option 'Advanced Settings' as shown below:



The following warning window will appear indicating you're accessing to an advanced configuration menu:



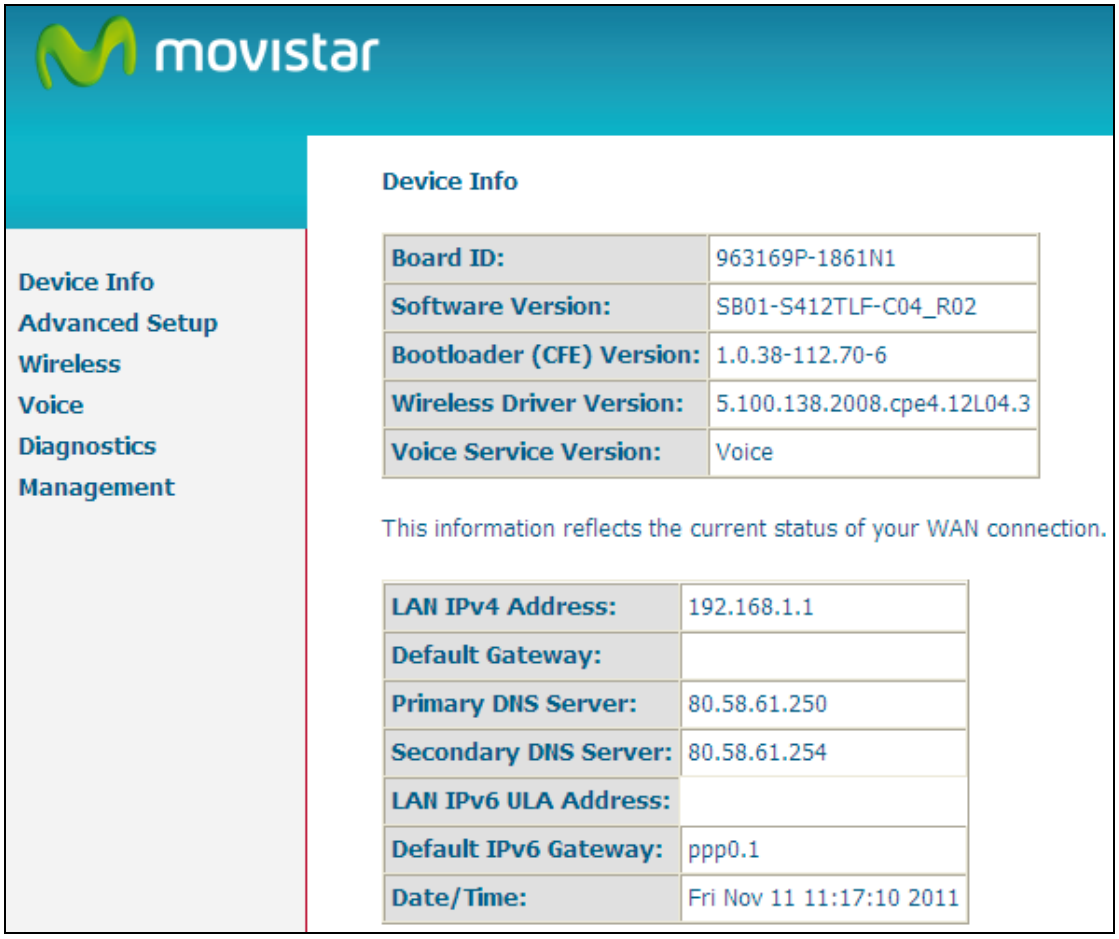
Accept that Window and your browser will be redirected to the Advanced User Interface.

The web user interface is divided into two windowpanes, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

NOTE:	The menu items shown are based upon the configured connection(s) and user account privileges. For example, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

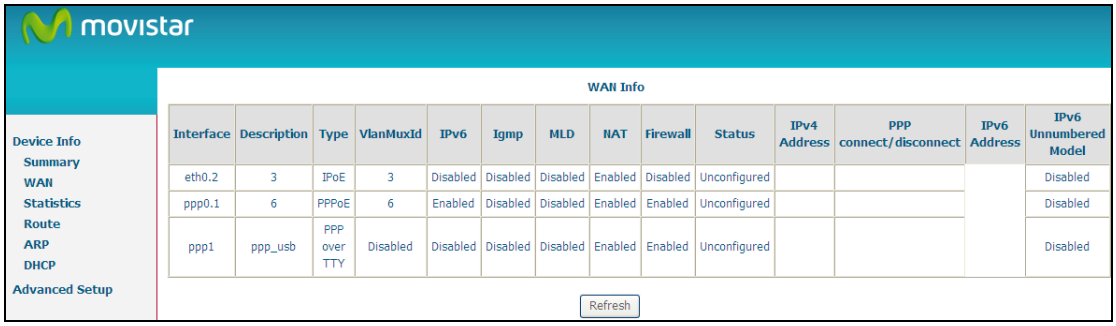
The Device Info Summary screen will display at startup.



This screen shows hardware, software, IP settings and other related information.

5.1 WAN

Select WAN from the Device Info submenu to display the configured PVC(s).



Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
VlanMuxId	Shows 802.1Q VLAN ID
IPv6	Shows if IPv6 is enabled on this interface or not.
IGMP	Shows Internet Group Management Protocol (IGMP) status
MLD	Shows Multicast Listener Discovery (MLD) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the status of Firewall
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address
PPP connect/disconnect	Shows the PPP connection status
IPv6 Address	Shows WAN IPv6 address
IPv6 Unnumbered Model	Shows if unnumbered model is used or not; Only ppp interfaces can use this model and in this model, only IPv6 link-local address is used on the interface.

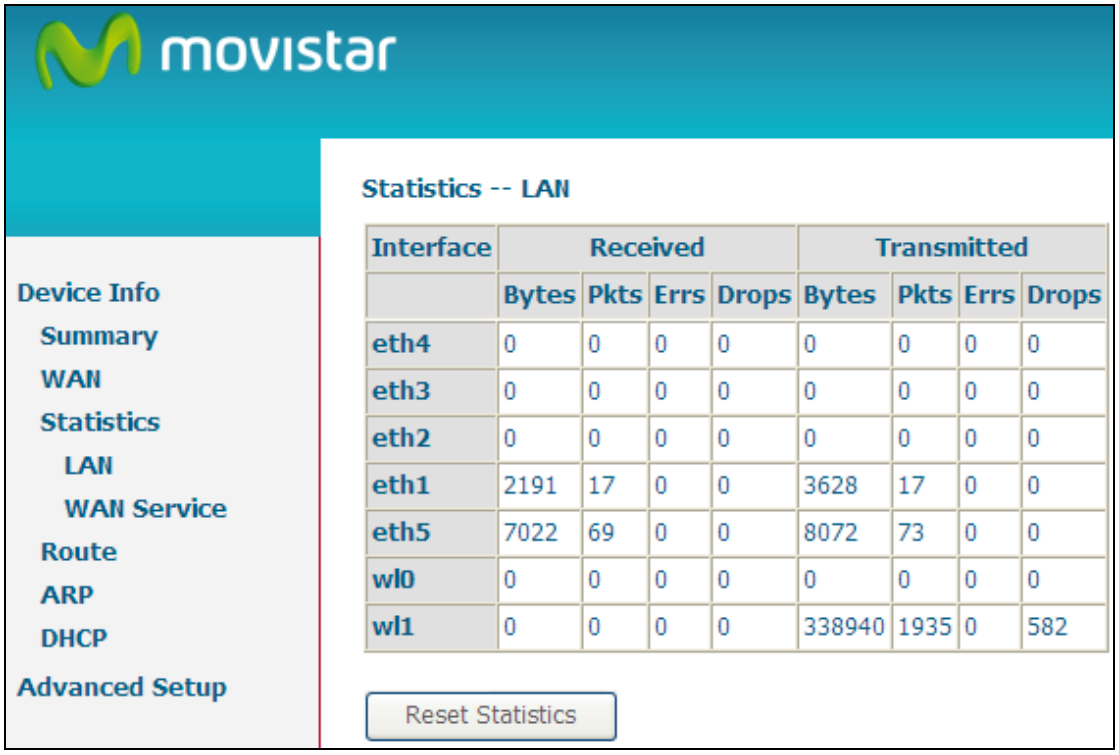
5.2 Statistics

This selection provides LAN, WAN, ATM and DSL statistics.

NOTE:	These screens are updated automatically every 15 seconds. Click **Reset Statistics** to perform a manual update of these statistics.

5.2.1 LAN Statistics

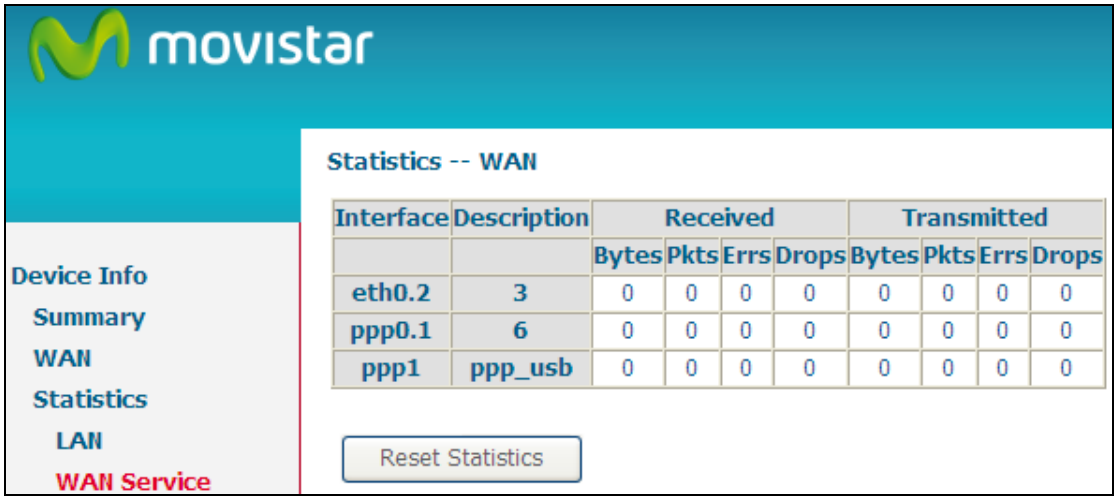
This screen shows data traffic statistics for each LAN interface.



Heading		Description
Interface		LAN interface(s)
Received/Transmitted:	- Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

5.2.2 WAN Service

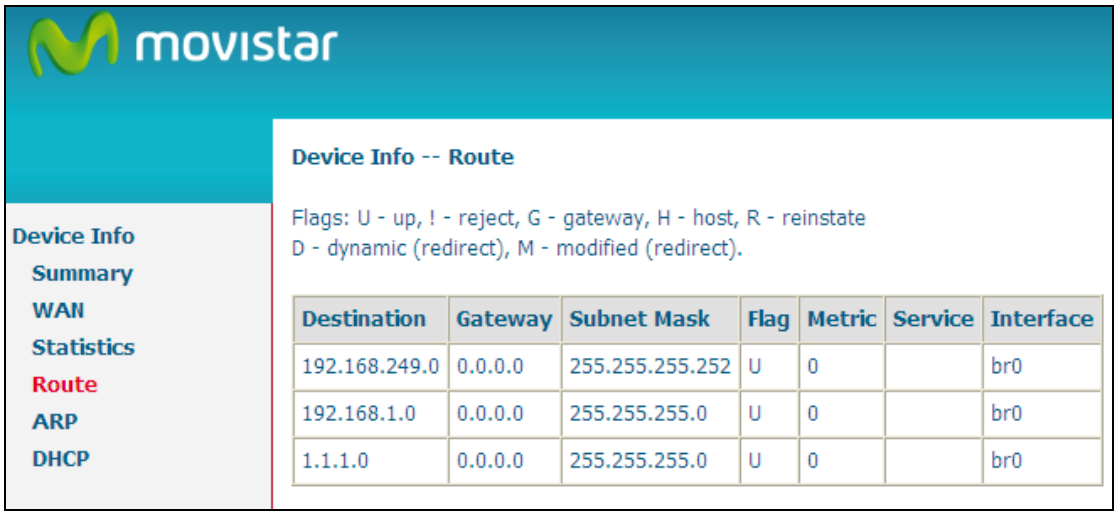
This screen shows data traffic statistics for each WAN interface.



Heading	Description
Interface	WAN interfaces
Description	WAN service label
Received/Transmitted - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

5.3 Route

Choose **Route** to display the routes that the VG-8050 has found.



Field	Description
Destination	Destination network or destination host
Gateway	Next hub IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the WAN connection label
Interface	Shows connection interfaces

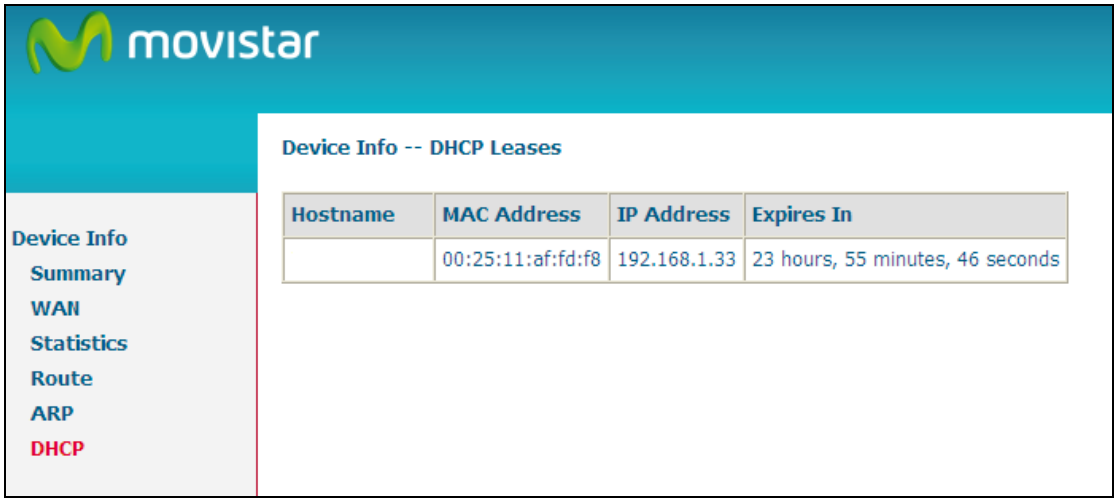
5.4 ARP

Click **ARP** to display the ARP information.

Field	Description
IP address	Shows IP address of host pc
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

5.5 DHCP

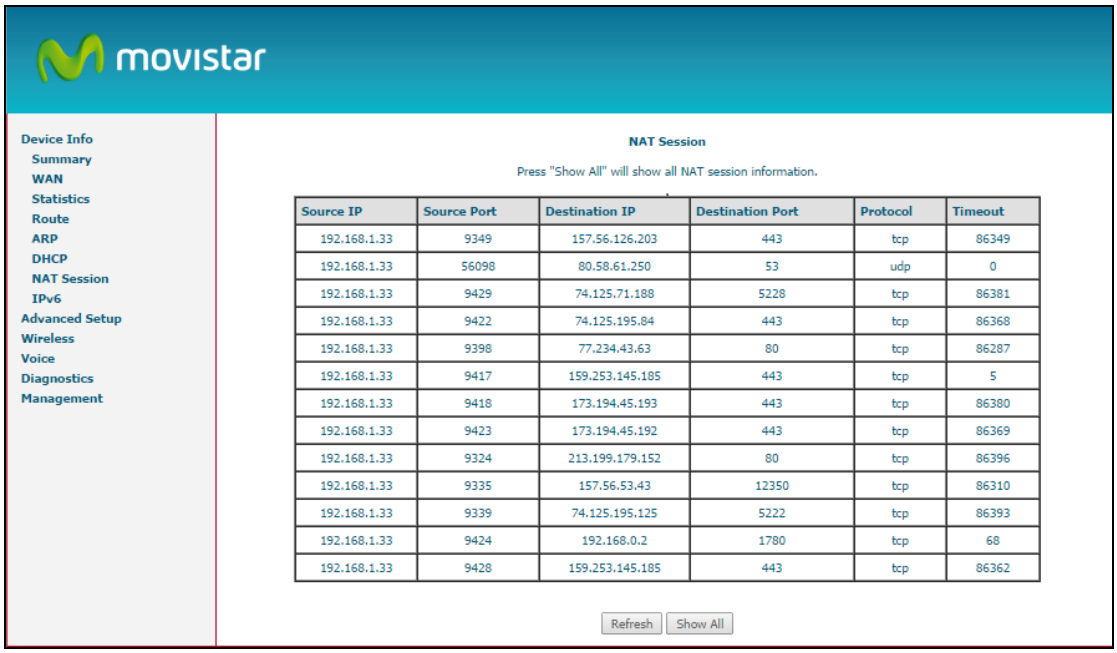
Click **DHCP** to display all DHCP Leases.



Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP Address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

5.6 NAT Session

Click on **NAT Session** to show the current most significant connections:



Click on **Show All** to show all the connections that the router is managing.

5.7 IPv6

If your environment support IPv6 protocol this menu will show all the IPv6 clients that are share the same link (similar to ARP for IPv4)

Field	Description
IPv6 address	Shows IPv6 address of host pc
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

Chapter 6 Advanced Setup

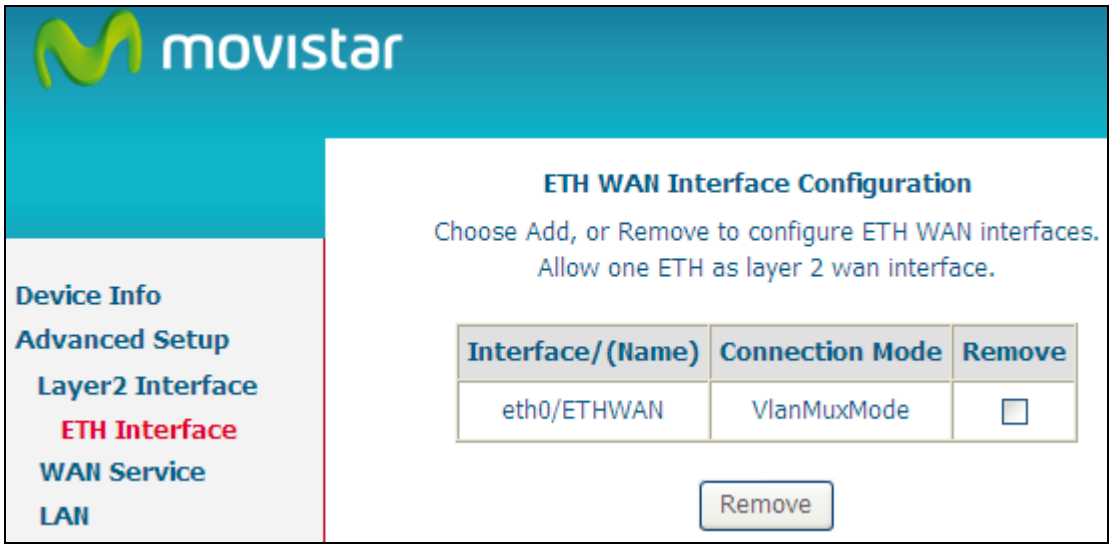
The Advanced menu provides access to the Advanced options discussed below.

6.1 Layer 2 Interface

The ETH WAN interface screen is described here.

6.1.1 ETH Interface

This screen displays the Ethernet WAN Interface configuration.

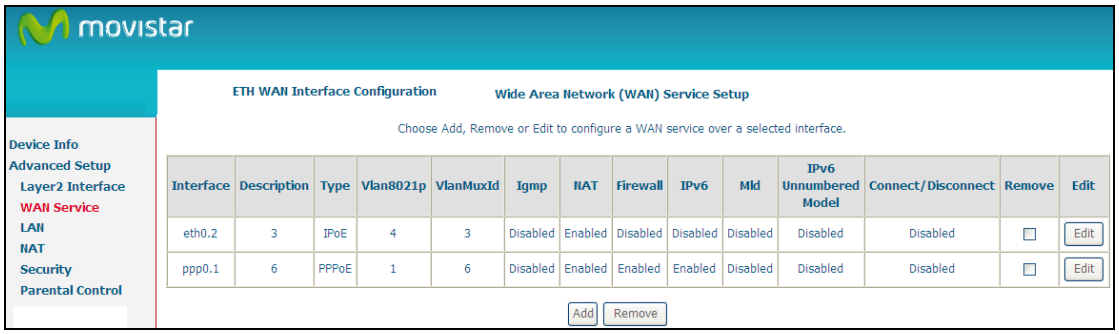


Click **Add** to create a new connection (see Appendix G). To remove a connection, select its Remove column radio button and click **remove.**

Heading	Description
Interface/(Name)	Ethernet WAN Interface.
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface. MSC Mode – Multiple Services over one interface.
Remove	Select interfaces to remove

6.2 WAN Service

This screen allows for the configuration of WAN interfaces.



Click the **Add** button to create a new connection. For connections on ATM or ETH WAN interfaces see Appendix G.

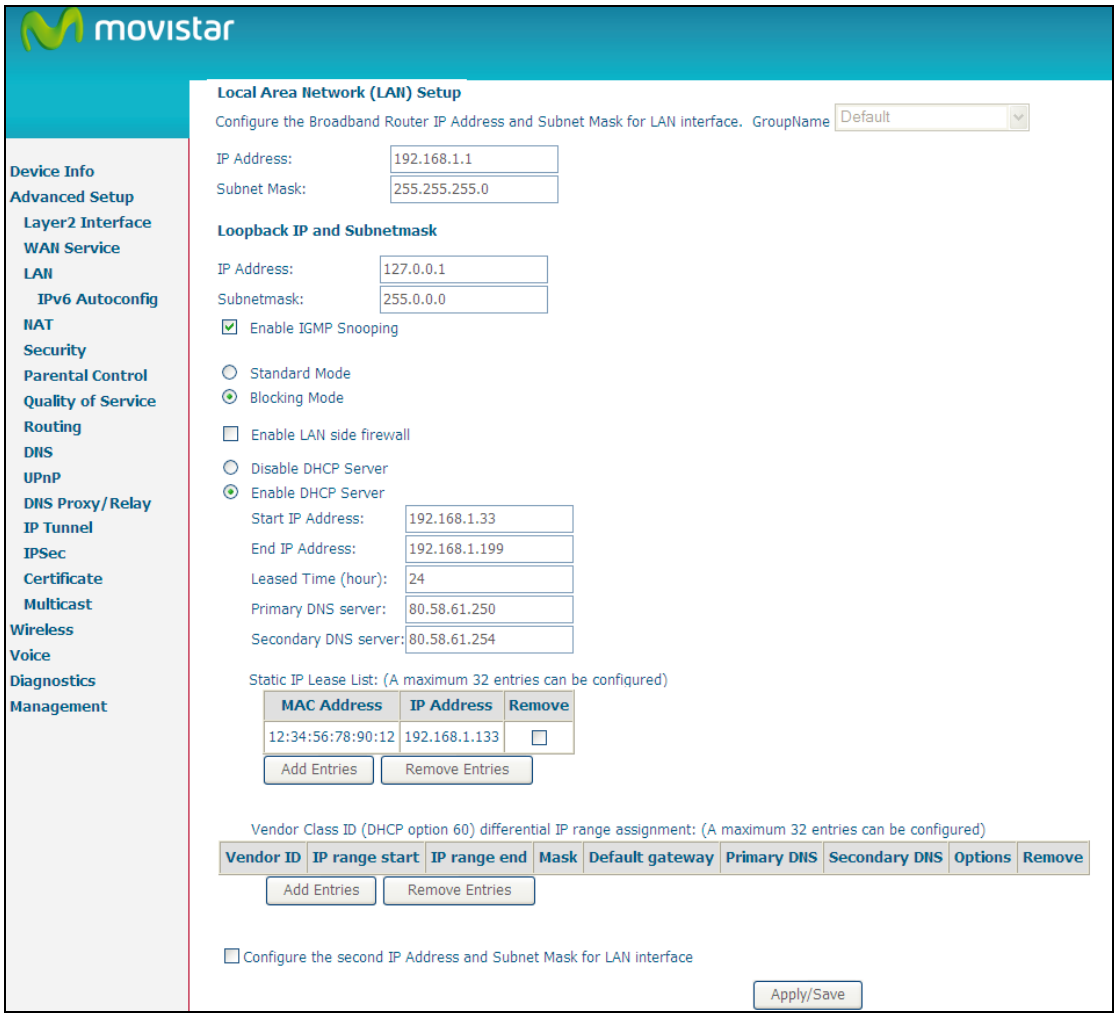
ETH and ATM service connections cannot coexist. In Default Mode, up to 8 WAN connections can be configured; while VLAN Mux and MSC Connection Modes support up to 16 WAN connections.

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
ConnId	Connection ID
IGMP	Shows Internet Group Management Protocol (IGMP) status
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
IPv6	Shows if IPv6 is enabled on this interface or not
MLD	Shows Multicast Listener Discovery (MLD) status
IPv6 Unnumbered Model	Shows if the unnumbered model is used or not; Only ppp interfaces can use this model and in this model, only IPv6 link-local address is used on the interface
Connect/Disconnect	Shows the connection status
Remove	Select interfaces to remove

To remove a connection, select its Remove column radio button and click **Remove.**

6.3 LAN

From this screen, LAN interface settings can be configured.



Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

1st LAN INTERFACE

IP Address: Input the IP address for the LAN port.

Subnet Mask: Input the subnet mask for the LAN port.

Loopback IP and Subnetmask

IP Address: Input the loopback IP address for the LAN port.

Subnetmask: Input the loopback subnet mask for the LAN port.

Enable IGMP Snooping: **Enable by ticking the checkbox ☑.**

Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

Enable LAN side firewall: Enable by ticking the checkbox ☑.

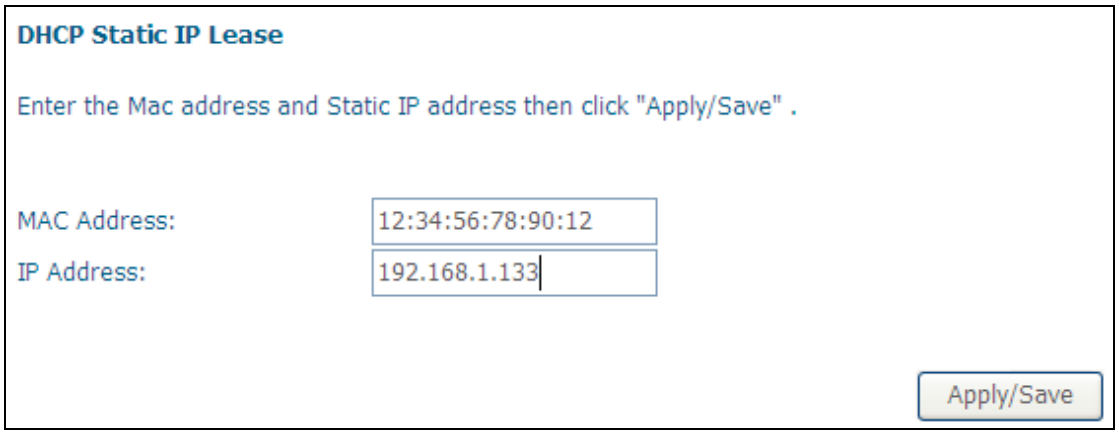
DHCP Server: To enable DHCP, select **Enable DHCP server** and enter Start and End IP addresses and the Leased Time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

Primary DNS server: The Primary DNS server which is delivered to the LAN site hosts via DHCP protocol.

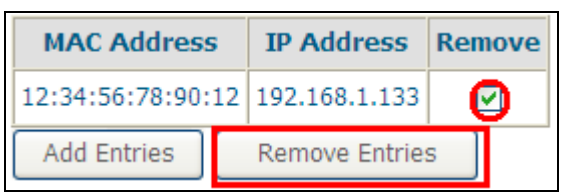
Secondary DNS server: The Secondary DNS server which is delivered to the LAN site hosts via DHCP protocol.

Static IP Lease List: A maximum 32 entries can be configured.

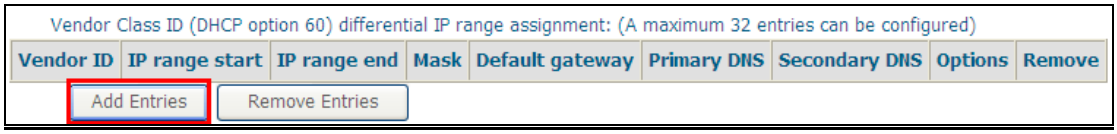
To add an entry, enter MAC address and Static IP and then click **Save/Apply**.



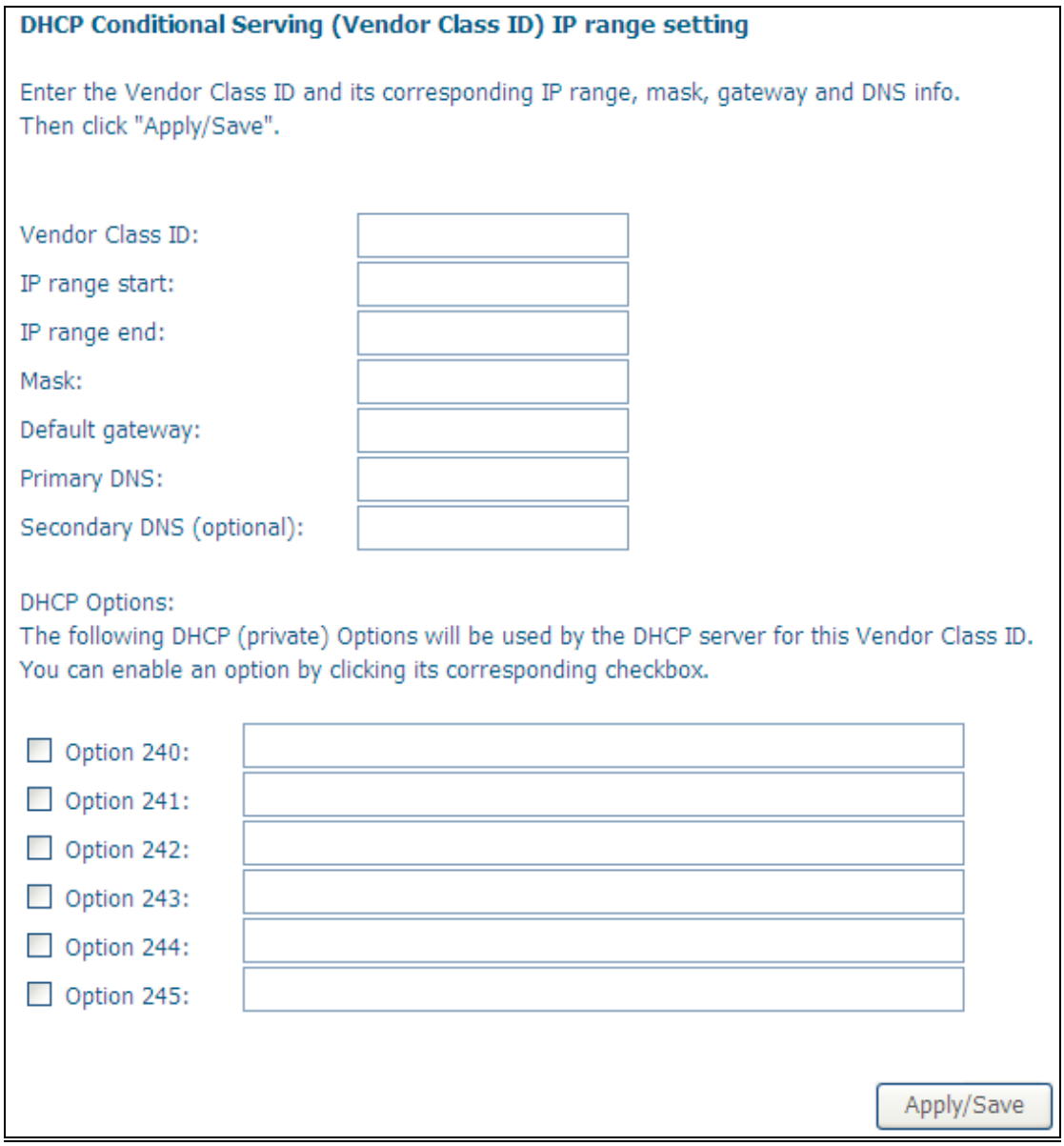
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove Entries** button, as shown below.



Vendor Class ID



Click the Add Entries to display the following:



Heading	Description
Vendor Class ID	It denotes the vendor of the LAN site hosts which would be recognized via option 60 of DHCP protocol.
IP range start	If the Vendor Class ID is recognized and matched, a new DHCP lease pool can be created. This table is the start of the pool.

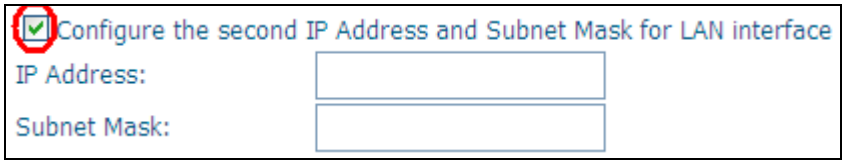
Heading	Description
IP range end	If the Vendor Class ID is recognized and matched, a new DHCP lease pool can be created. This table is the end of the pool.
Mask	If the Vendor Class ID is recognized and matched, a new DHCP lease pool can be created. This table is the subnet mask of the pool.
Default gateway	If the Vendor Class ID is recognized and matched, a new default gateway could be assigned via this field.
Primary DNS	If the Vendor Class ID is recognized and matched, a new Primary DNS server could be assigned via this field.
Secondary DNS (optional):	If the Vendor Class ID is recognized and matched, a new Secondary DNS server could be assigned via this field.

DHCP Options

If the Vendor Class ID is recognized and matched, a set of string based DHCP options could be assigned to the client for customization purposes. The options are mostly used by Set-top-box.

2ND LAN INTERFACE

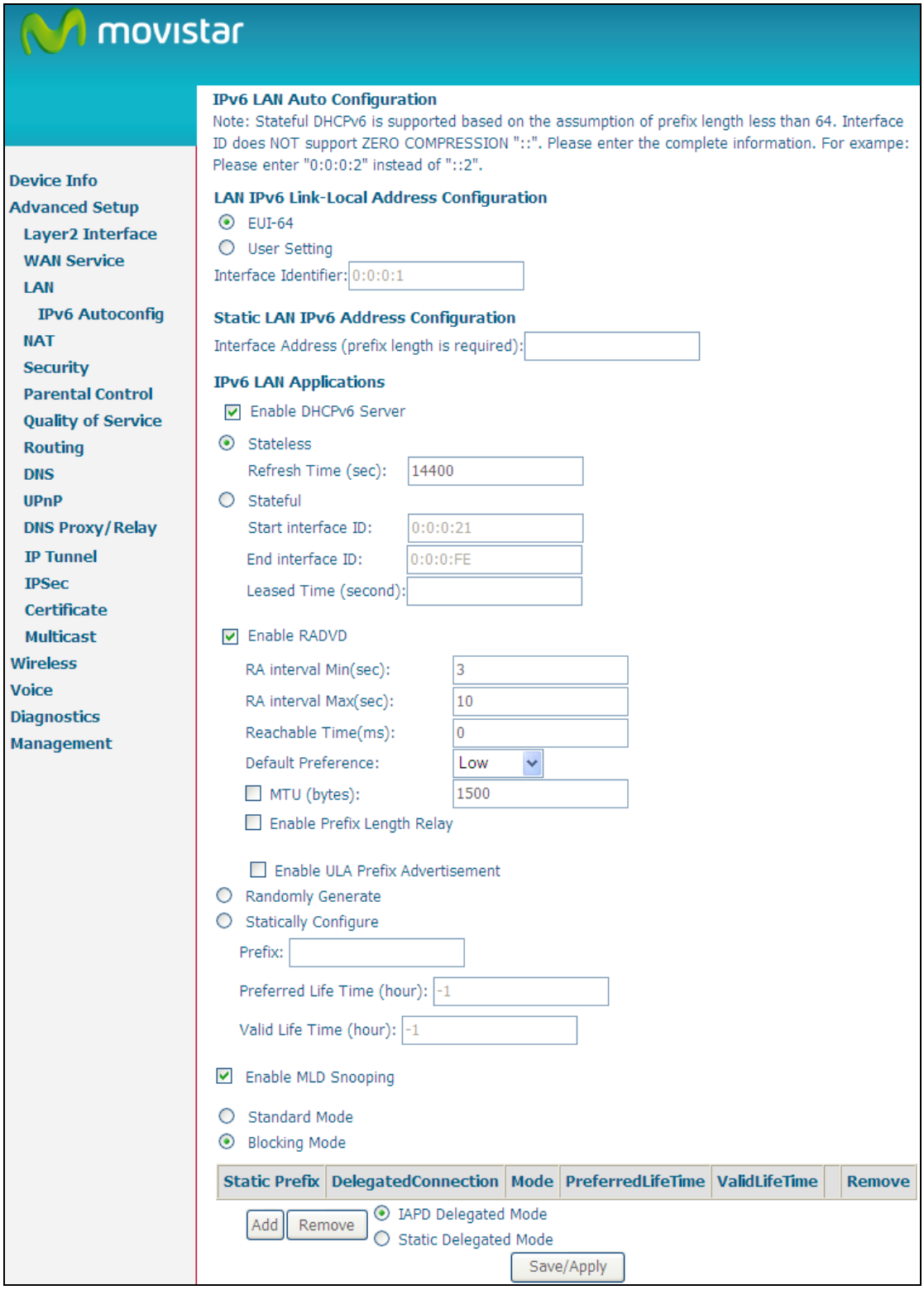
To configure a secondary IP address, tick the checkbox ☑ outlined (in RED) below.



IP Address: Enter the secondary IP address for the LAN port.

Subnet Mask: Enter the secondary subnet mask for the LAN port.

6.3.1 IPv6 Autoconfig



LAN IPv6 Link-Local Address Configuration

Heading	Description
EUI-64	Use EUI-64 algorithm to calculate link-local address from MAC address
User Setting	Use the Interface Identifier field to define a link-local address

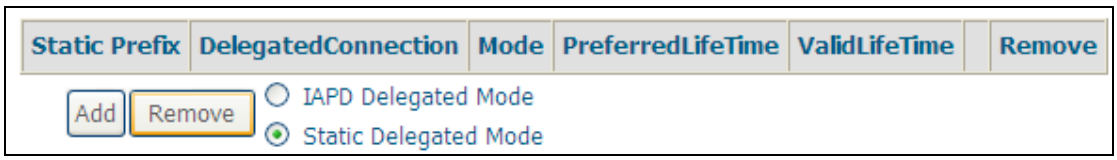
Static LAN IPv6 Address Configuration

Heading	Description
Interface Address (prefix length is required):	Configure static LAN IPv6 address and subnet prefix length

IPv6 LAN Applications

Heading	Description
Stateless	Use stateless configuration
Refresh Time (sec):	The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6
Stateful	Use stateful configuration
Start interface ID:	Start of interface ID to be assigned to dhcpv6 client
End interface ID:	End of interface ID to be assigned to dhcpv6 client
Leased Time (Second):	Lease time for dhcpv6 client to use the assigned IP address

Heading	Description
Enable RADVD	Enable use of router advertisement daemon
RA interval Min(sec):	Minimum time to send router advertisement
RA interval Max(sec):	Maximum time to send router advertisement
Reachable Time(ms):	The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation
Default Preference:	Preference level associated with the default router
MTU (bytes):	MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value
Enable Prefix Length Relay	Use prefix length receive from WAN interface
Enable ULA Prefix Advertisement	It is to enable announcing the unique local address.
Enable MLD Snooping	Enable/disable IPv6 multicast forward to LAN ports
Standard Mode	Forwarding un-known multicast to all ports
Blocking Mode	Blocking un-known multicast to all ports



To manually set a Static Prefix for LAN side hosts it is possible by creating an entry in the Static Prefix table with desired prefix and relative parameters.

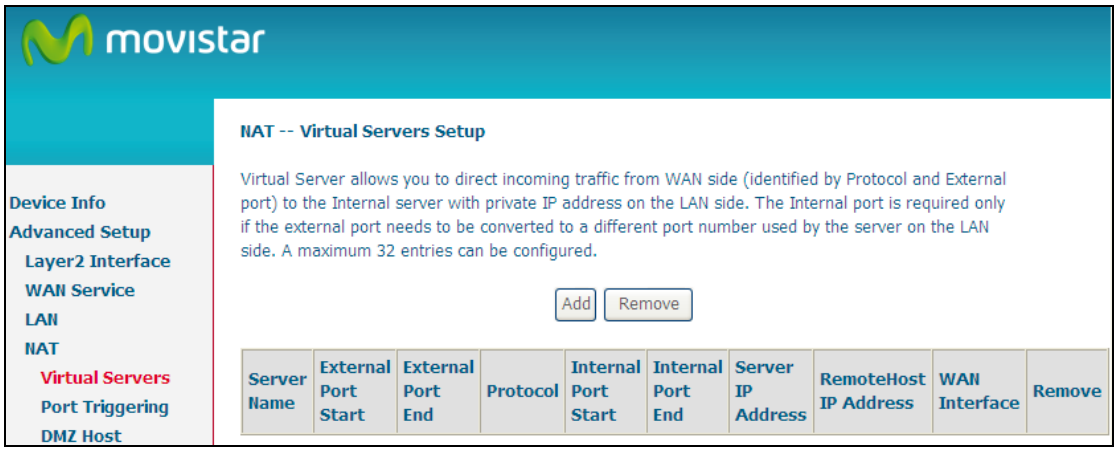
If Static=1 for example, then the prefixes set in the Static Prefx table would be used for LAN side hosts to generate an IPv6 address. Furthermore if IAPD=1, then the WAN side prefix delegation would be used for LAN side hosts to generate an IPv6 address.

6.4 NAT

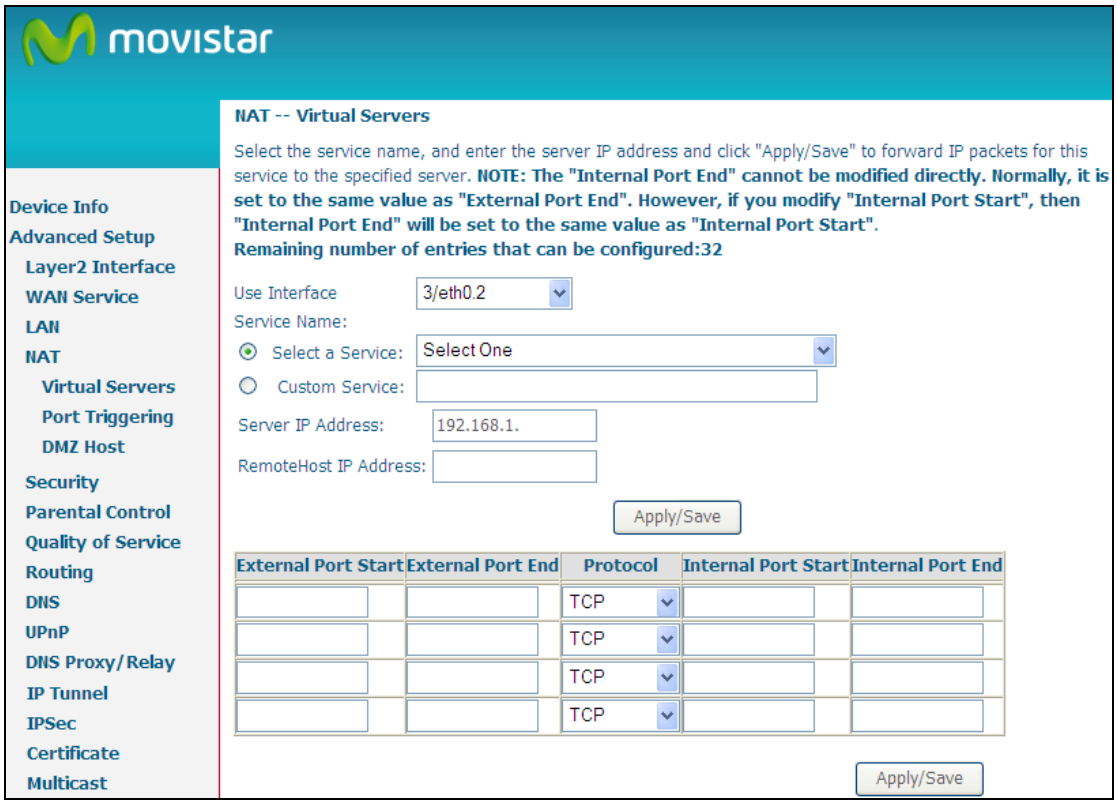
To display this option, NAT must be enabled in at least one PVC shown on the Advanced Setup - WAN screen. *NAT is not an available option in Bridge mode*.

6.4.1 Virtual Servers

Virtual Servers allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the Internal server with private IP addresses on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.
A maximum of 32 entries can be configured.



To add a Virtual Server, click **Add**. The following will be displayed.

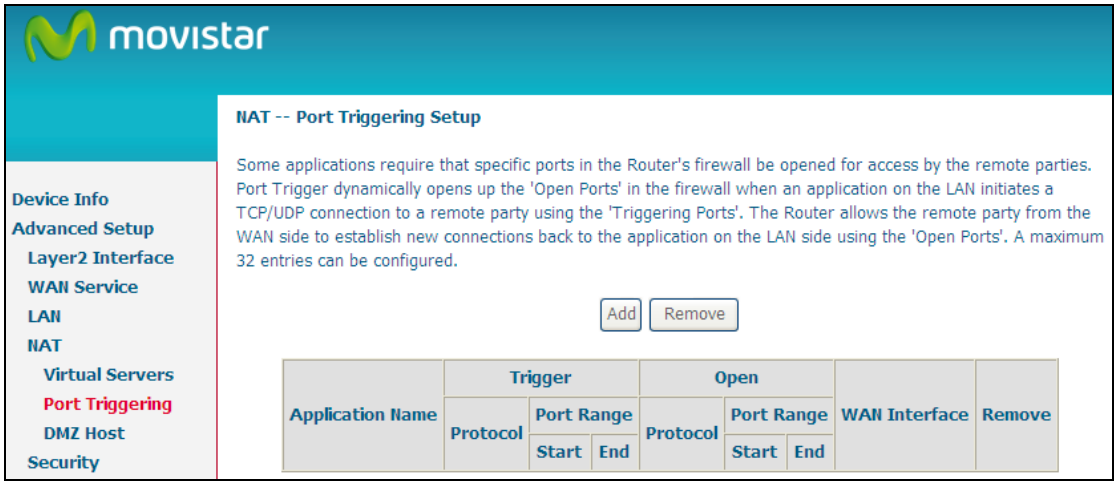


Consult the table below for field and header descriptions.

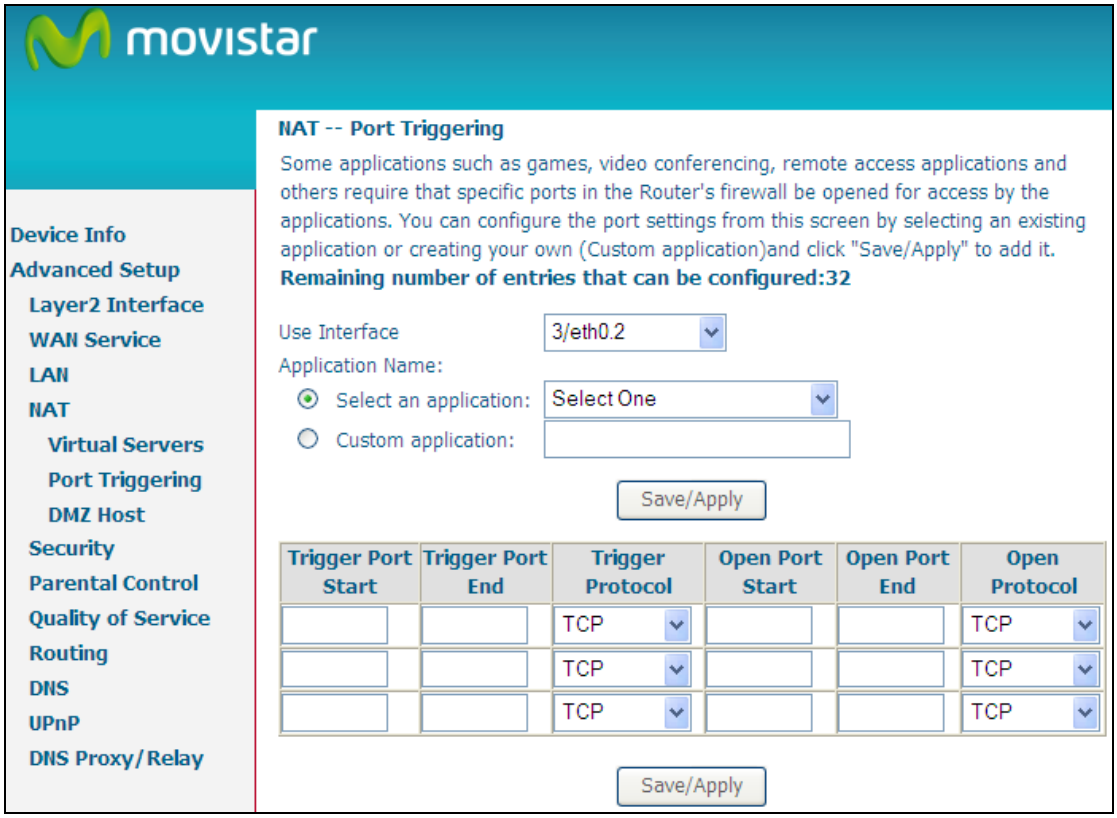
Field/Header	Description
Use Interface	Select the WAN interface from the drop-down box.
Select a Service **Or** Custom Service	User should select the service from the list. **Or** User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
RemoteHost IP Address	The only remote host that is allowed to use this virtual server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

6.4.2 Port Triggering

Some applications require that specific ports in the firewall be opened for access by the remote parties. Port Triggers dynamically 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.



To add a Trigger Port, click **Add**. The following will be displayed.

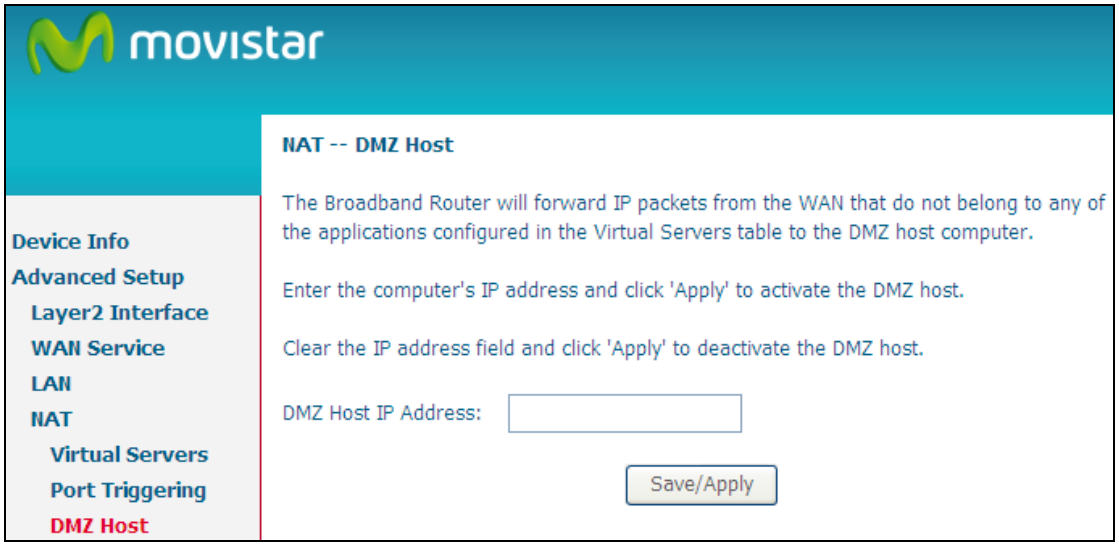


Consult the table below for field and header descriptions.

Field / Header	Description
Use Interface	Select the WAN interface from the drop-down box.
Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP, or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP, or UDP.

6.4.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



To **Activate** the DMZ host, enter the DMZ host IP address and click **Save / Apply**.

To **Deactivate** the DMZ host, clear the IP address field and click **Save / Apply**.

6.5 Security

To display this function, you must enable the firewall feature in WAN Setup.
For detailed descriptions, with examples, please consult Appendix A.

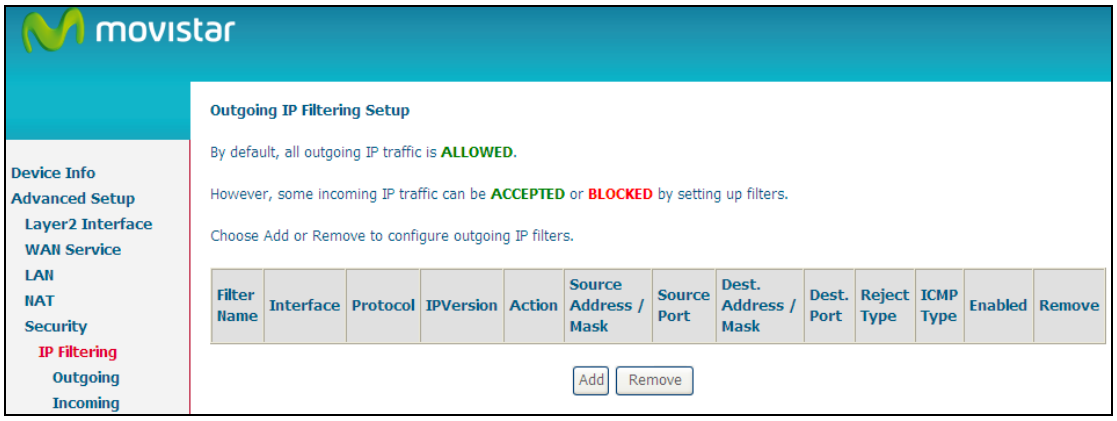
6.5.1 IP Filtering

This screen sets filter rules that limit IP traffic (Outgoing/Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

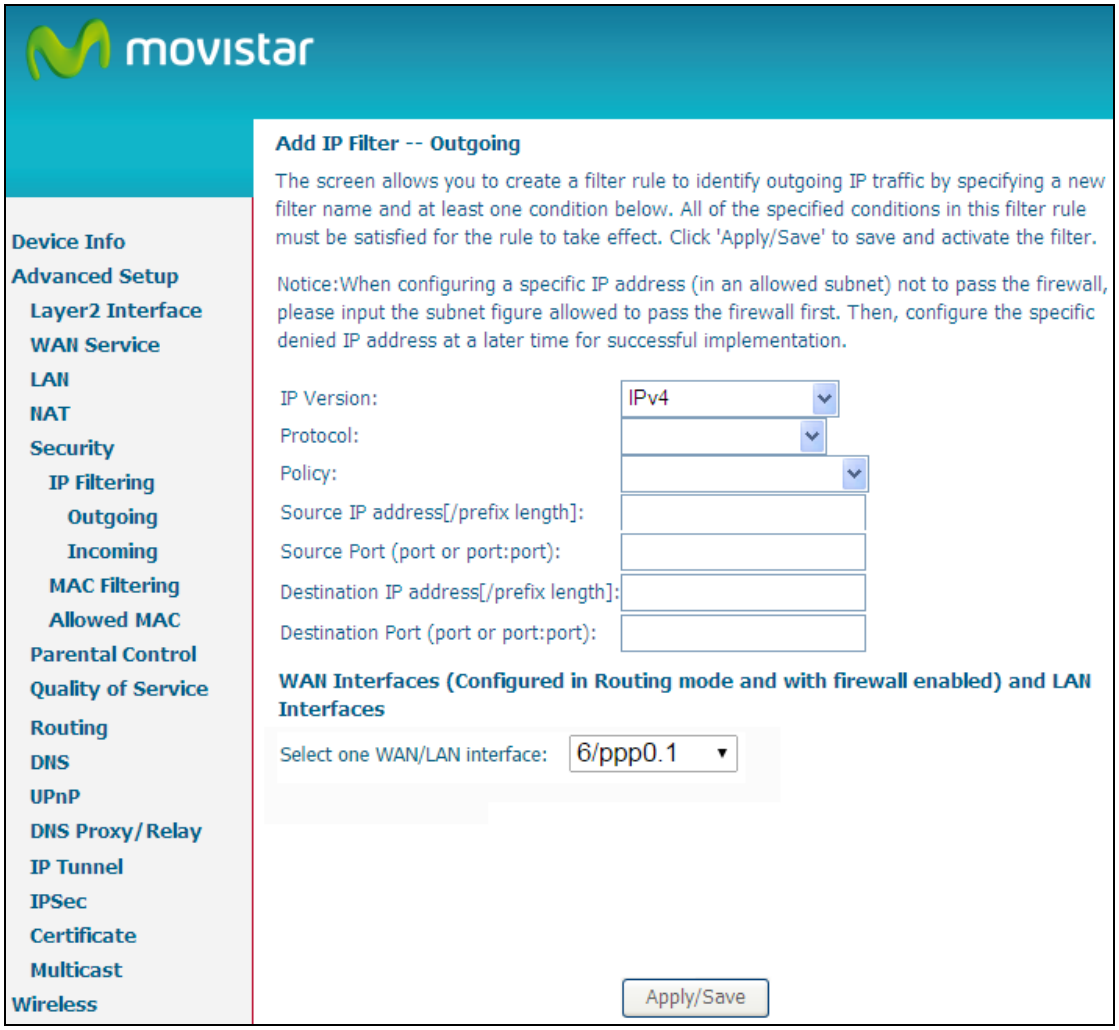
NOTE:	This function is not available when in bridge mode. Instead, see MAC Filtering which performs a similar function.

OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.



To add a filter (to block some outgoing IP traffic), click the **Add** button.
On the following screen, enter your filter criteria and then click **Apply/Save**.

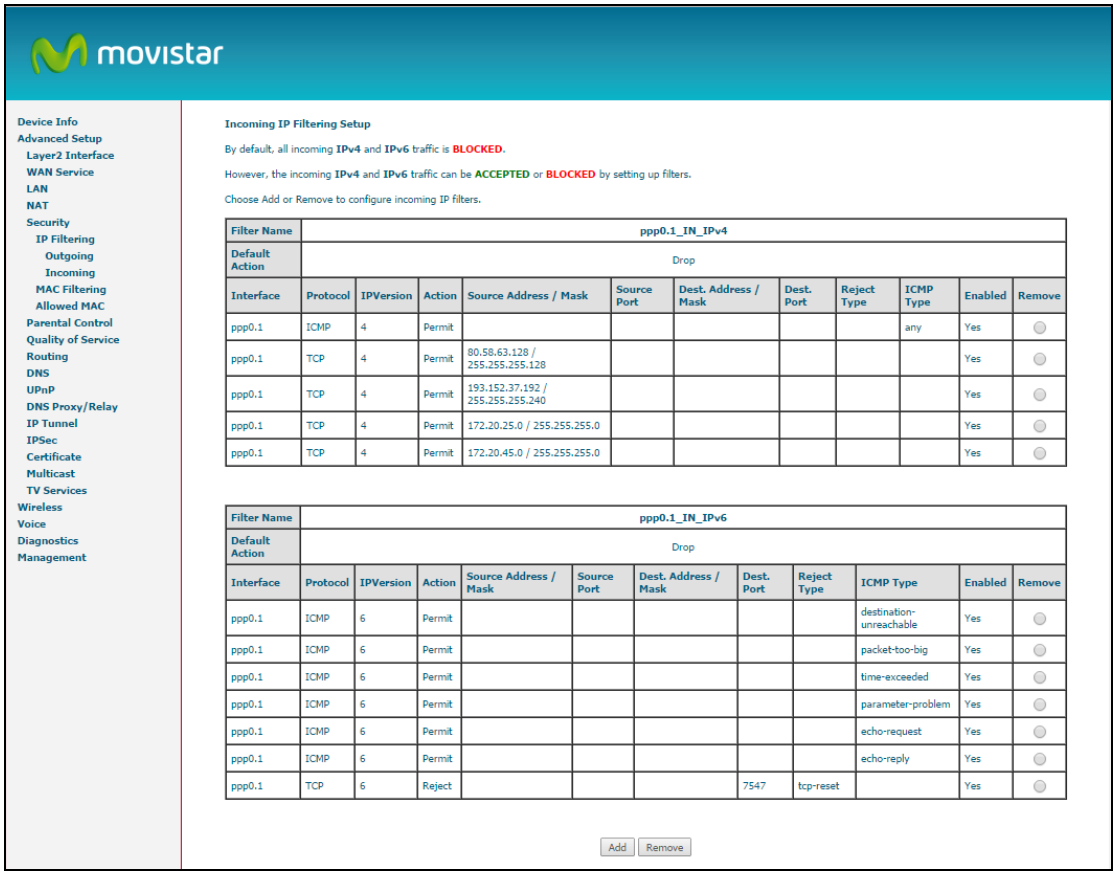


Consult the table below for field descriptions.

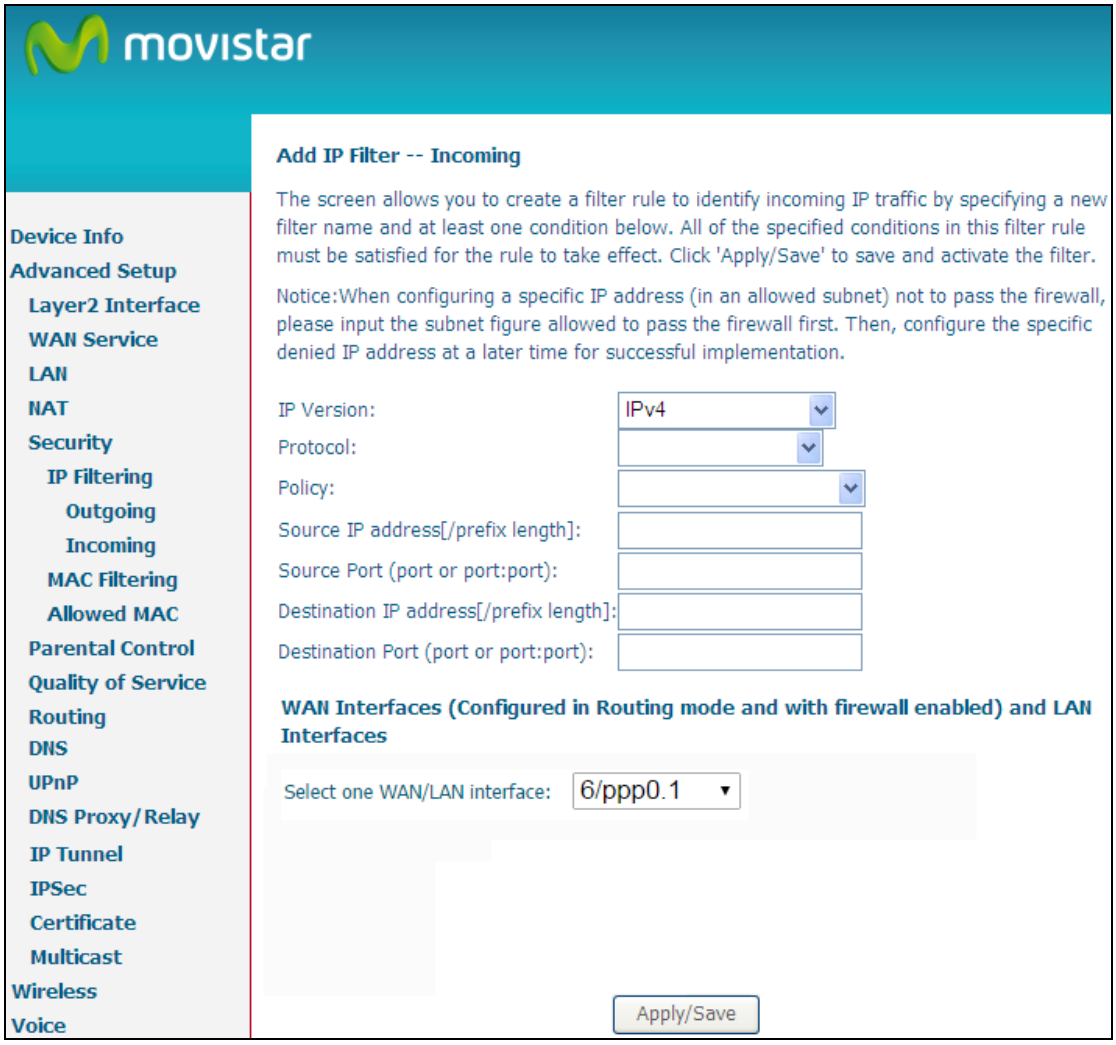
Field	Description
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Policy	This is to choose to allow or deny the packets that match the criteria.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.



To add a filter (to allow incoming IP traffic), click the **Add** button.
On the following screen, enter your filter criteria and then click **Apply/Save**.



Consult the table below for field descriptions.

Field	Description
IP Version	IPv4 selected by default.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Policy	This is to choose to allow or deny the packets that match the criteria.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

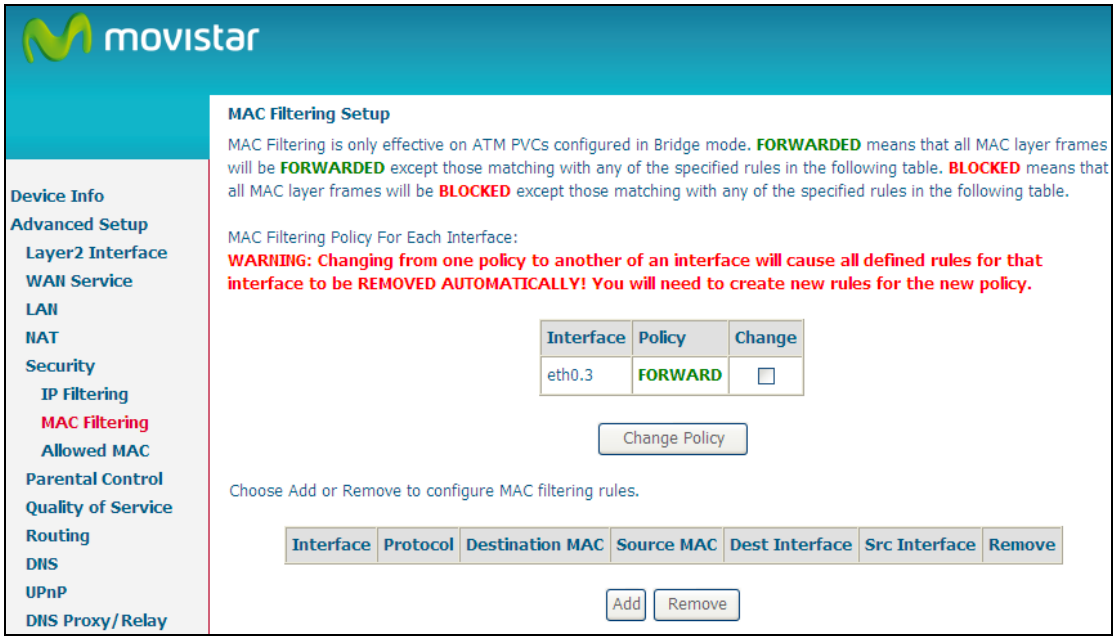
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.

6.5.2 MAC Filtering

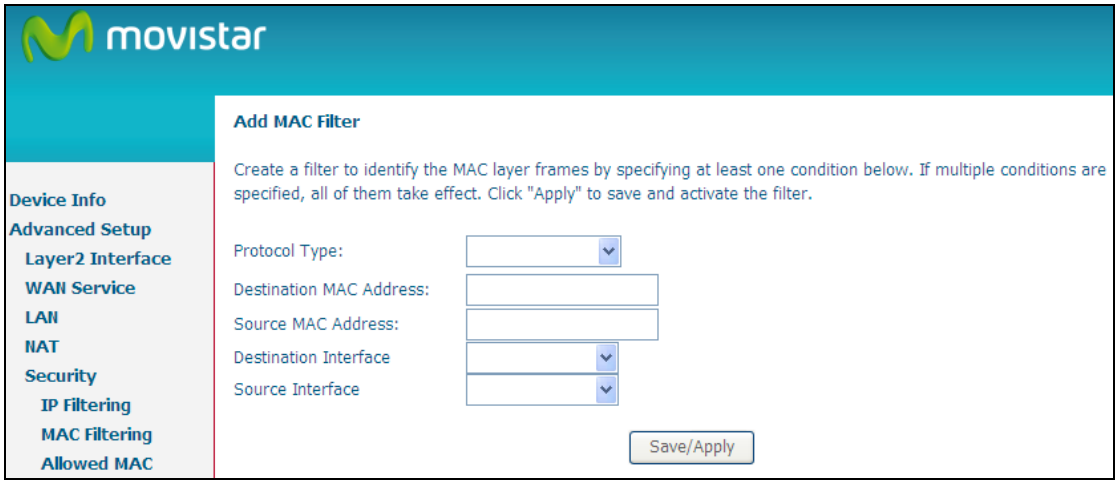
NOTE:	This option is only available in bridge mode. Other modes use IP Filtering to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the VG-8050 can be set according to the following procedure.

The MAC Filtering Global Policy is defined as follows. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the MAC filter rules. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the MAC filter rules. The default MAC Filtering Global policy is **FORWARDED**. It can be changed by clicking the **Change Policy** button.



Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met. Click **Save / Apply** to save and activate the filter rule.

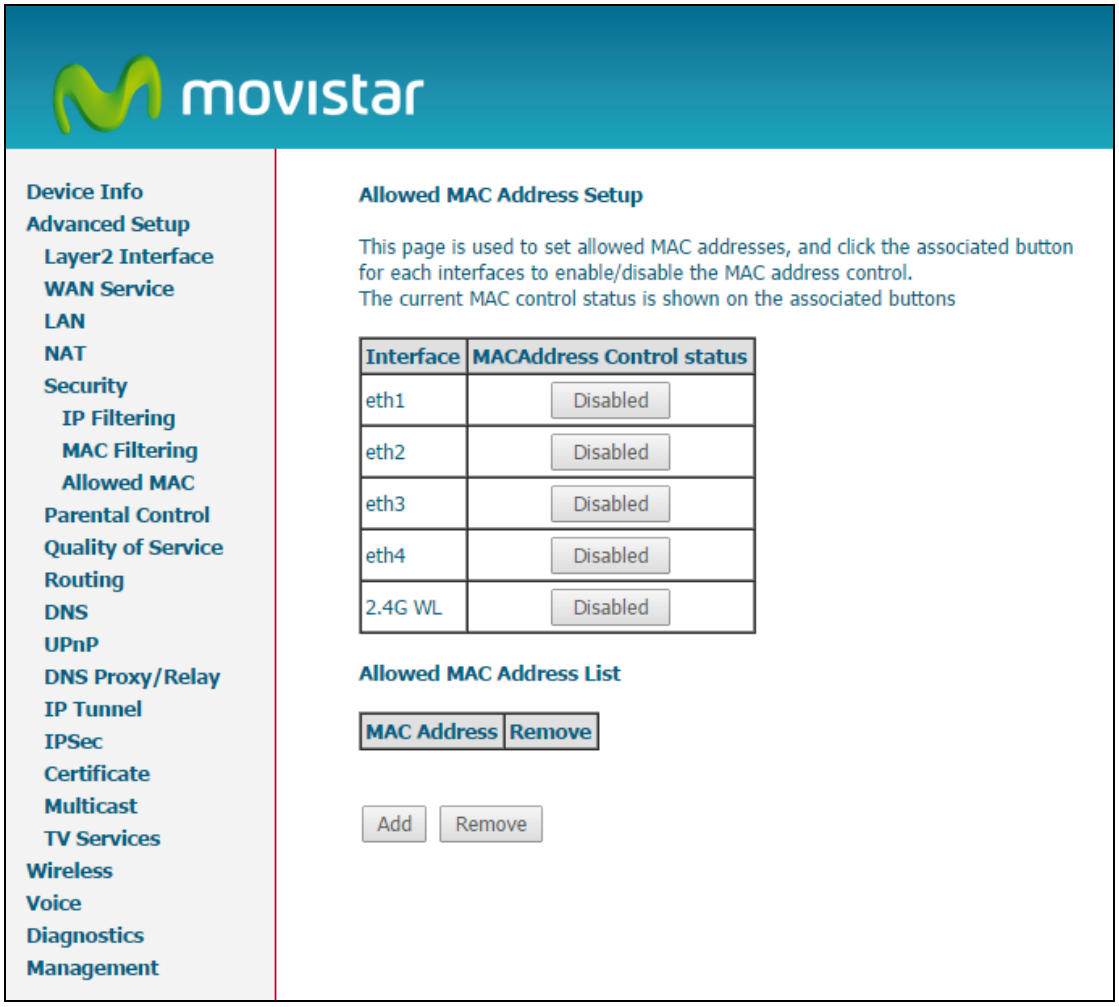


Consult the table below for detailed field descriptions.

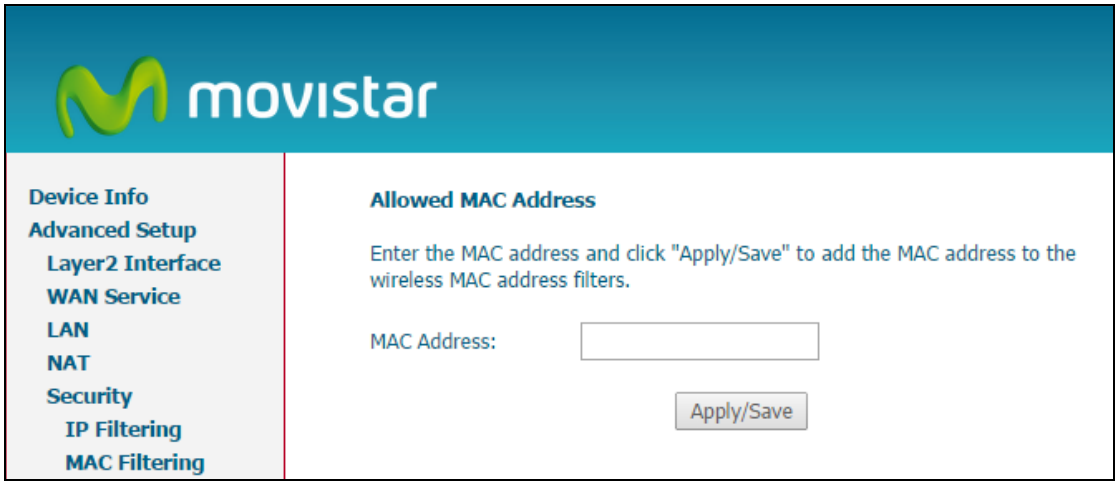
Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Source/Destination Interfaces	Applies the filter to selected WAN interfaces.

6.5.3 Allowed MAC

This page is used to set allowed MAC addresses, and click the associated button for each interface to enable/disable the MAC address control.
The current MAC control status is shown on the associated buttons.



After clicking the **Add** button, the following screen appears.
Input the MAC address in the box provided, and click **Apply/Save**.


movistar
Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
NAT
Security
IP Filtering
MAC Filtering
Allowed MAC Address
Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.
MAC Address:
Apply/Save

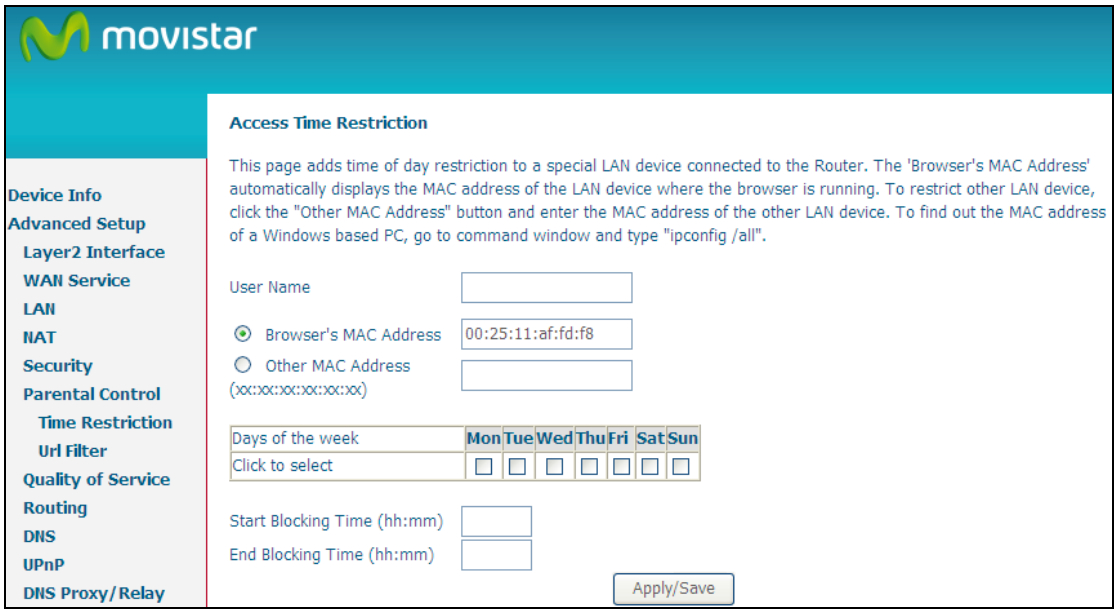
6.6 Parental Control

This selection provides WAN access control functionality.

6.6.1 Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 9.4, so that the scheduled times match your local time.

Click **Add** to display the following screen.

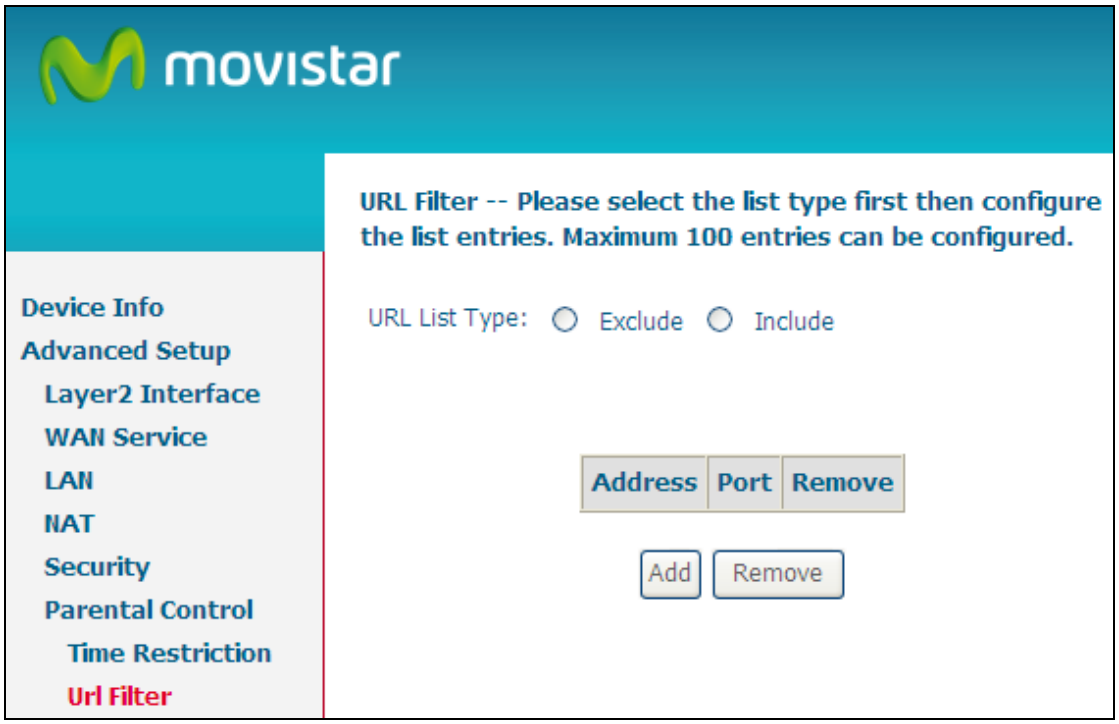


See below for field descriptions. Click **Save/Apply** to add a time restriction.

User Name: A user-defined label for this restriction.
Browser's MAC Address: MAC address of the PC running the browser.
Other MAC Address: MAC address of another LAN device.
Days of the Week: The days the restrictions apply.
Start Blocking Time: The time the restrictions start.
End Blocking Time: The time the restrictions end.

6.6.2 URL Filter

This screen allows for the creation of a filter rule for access rights to websites based on their URL address and port number.

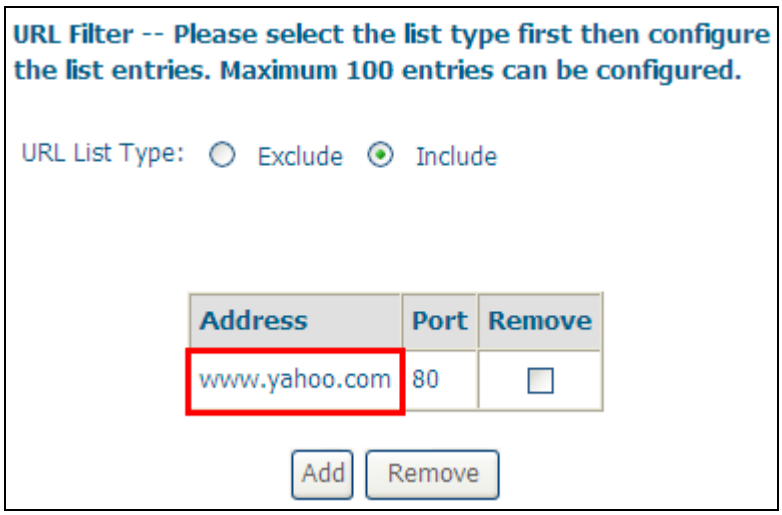


Tick the **Exclude** radio button to deny access to the websites listed.

Tick the **Include** radio button to restrict access to only those listed websites.

Click **Add** to display the following screen.

Select the list type first, then input the URL address and port number then click **Save / Apply** to add the entry to the URL filter. URL Addresses begin with “www”, as shown in this example.



A maximum of 100 entries can be added to the URL Filter list.

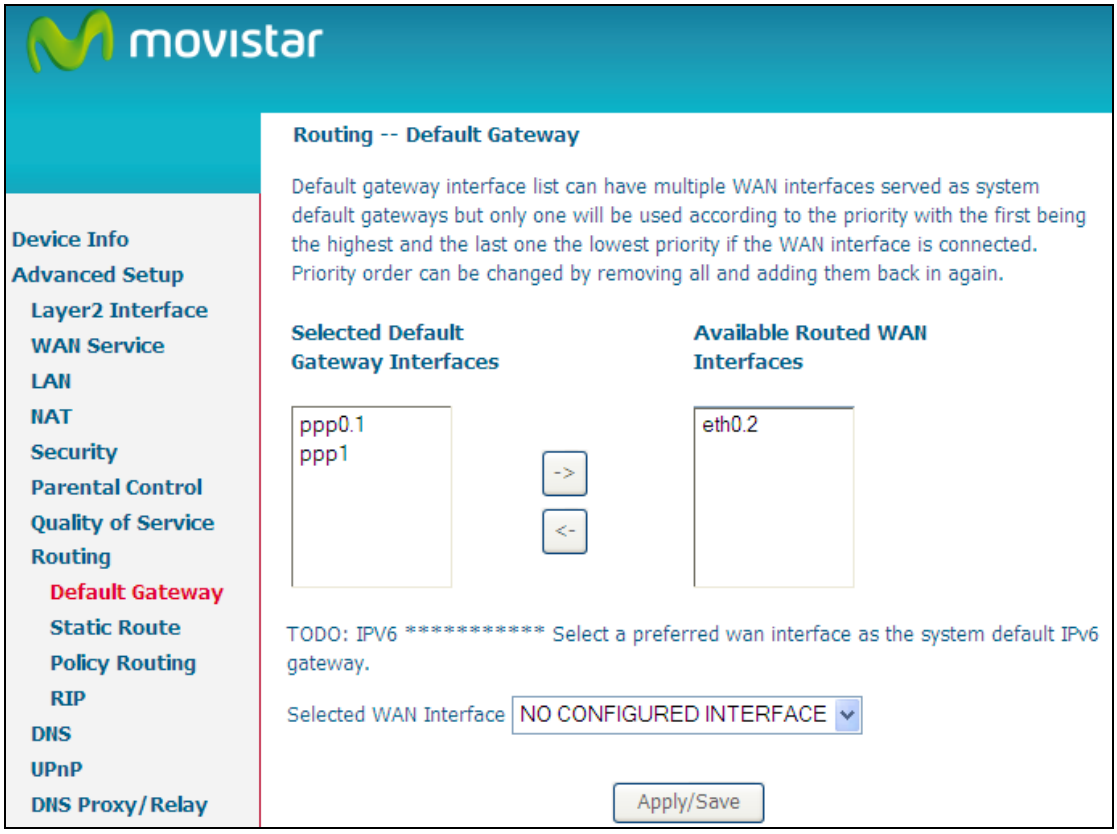
6.7 Routing

This option allows for **Default Gateway, Static Route, Policy Routing, and IPv6 Static Route** configuration.

NOTE:	In bridge mode, the **RIP** screen is hidden while the **Default Gateway** and **Static Route** configuration screens are shown but ineffective.

6.7.1 Default Gateway

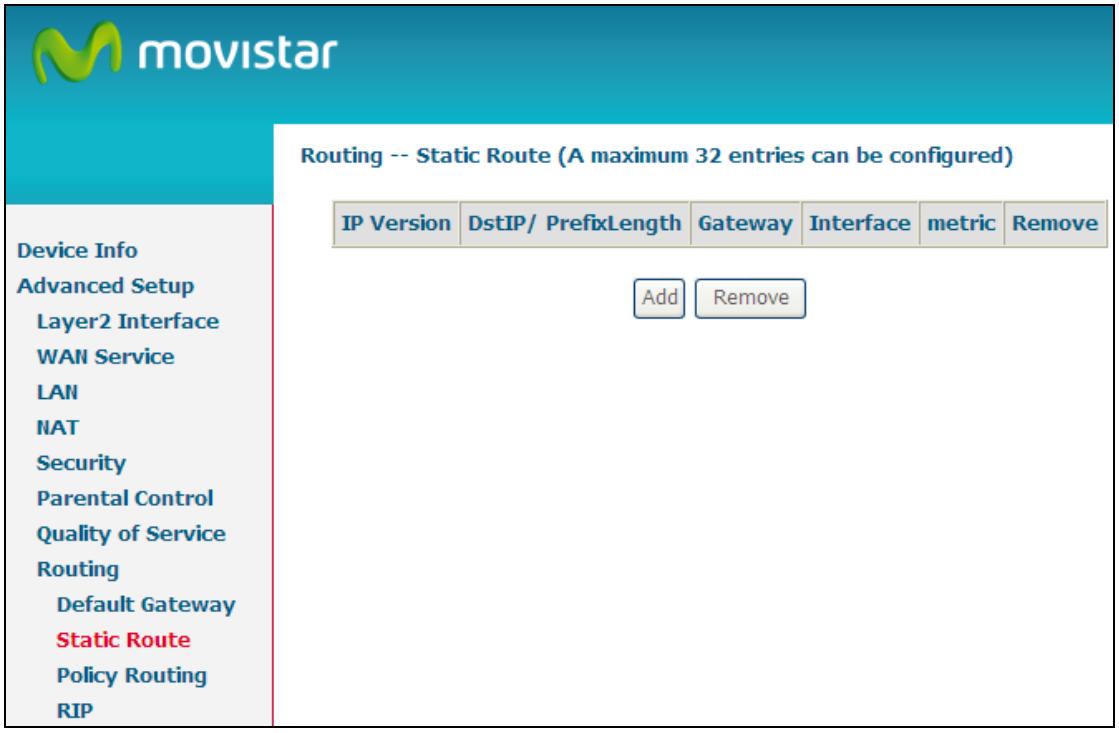
Select a WAN Interface as the default gateway and click **Save / Apply**.



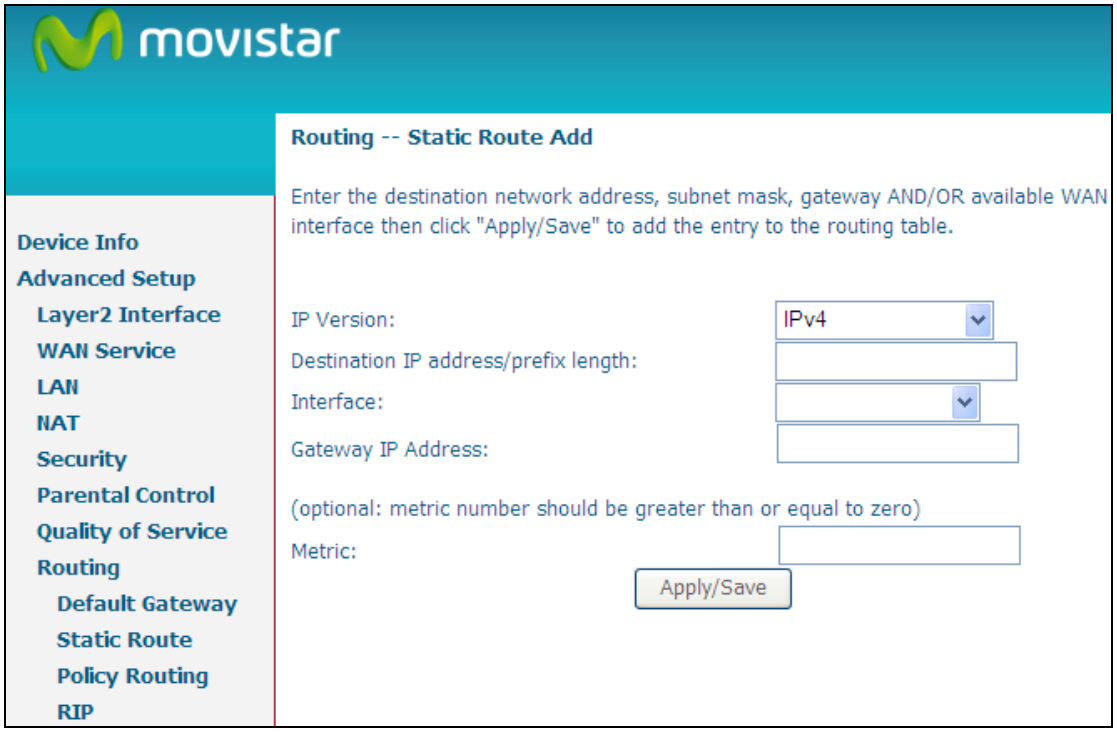
NOTE: After enabling the Automatic Assigned Default Gateway, the device must be rebooted to activate the assigned default gateway.

6.7.2 Static Route

This option allows for the configuration of static routes. Click **Add** to create a new static route. Click **Remove** to delete the selected static route.



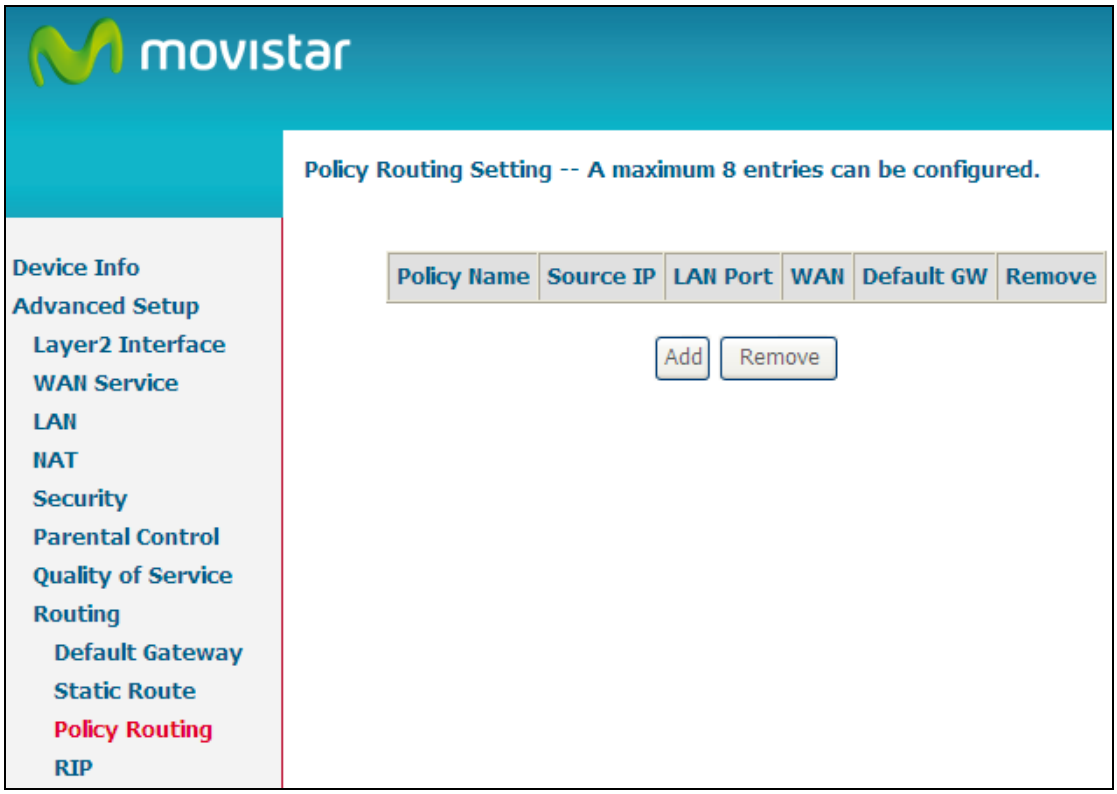
Click the **Add** button to display the following screen.



Select the IP Version and input the Destination IP address. Select the Interface and input the Gateway IP Address. Then click **Save/Apply** to add the entry to the routing table.

6.7.3 Policy Routing

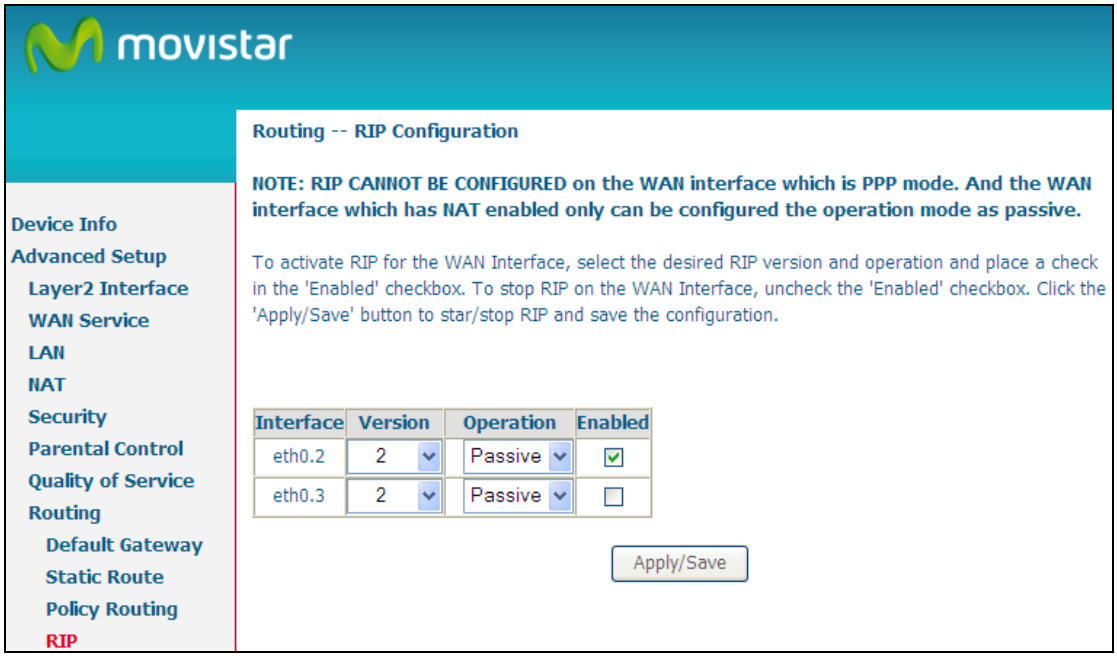
This option allows for the configuration of static routes by policy.
Click **Add** to create a routing policy or **Remove** to delete one.



On the following screen, complete the form and click **Save / Apply** to create a policy.

6.7.4 RIP

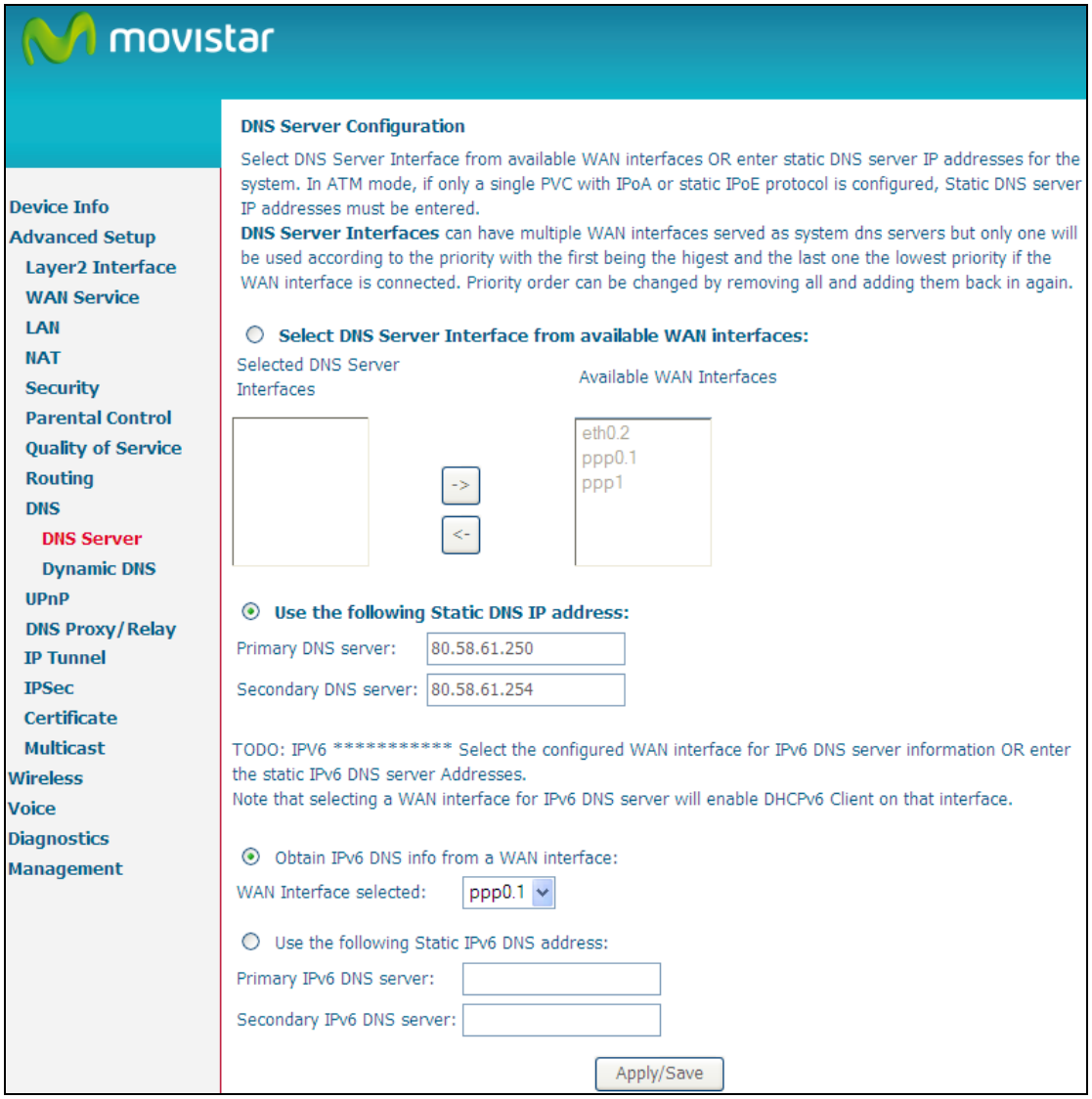
To activate RIP, configure the RIP version/operation mode and select the **Enabled** checkbox ☑ for at least one WAN interface before clicking **Save/Apply**.



6.8 DNS

6.8.1 DNS Server

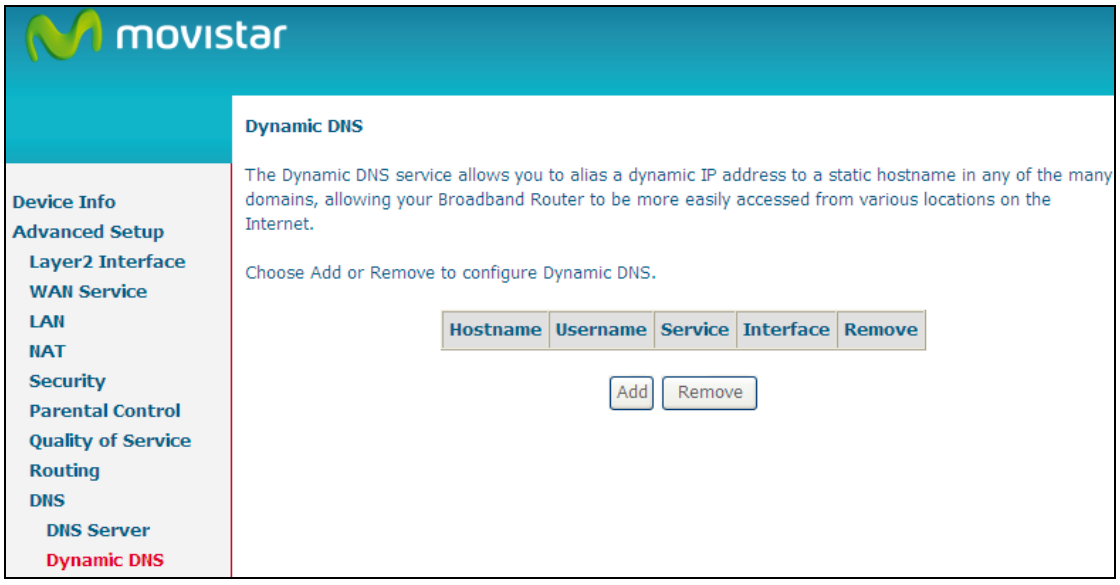
To obtain DNS information from a WAN interface, select the first radio button and then choose a WAN interface from the drop-down box. For Static DNS, select the second radio button and enter the IP Address of the primary (and secondary) DNS server(s). Click **Save / Apply** to save the new configuration.



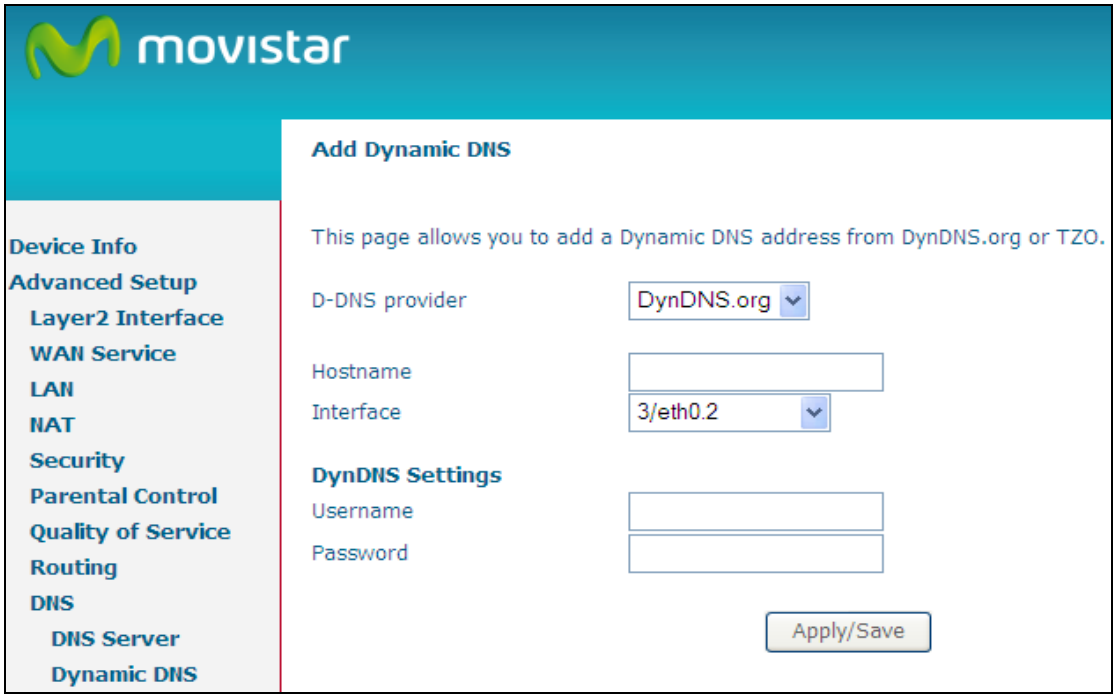
NOTE: You must reboot the router to make the new configuration effective.

6.8.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the VG-8050 to be more easily accessed from various locations on the Internet.



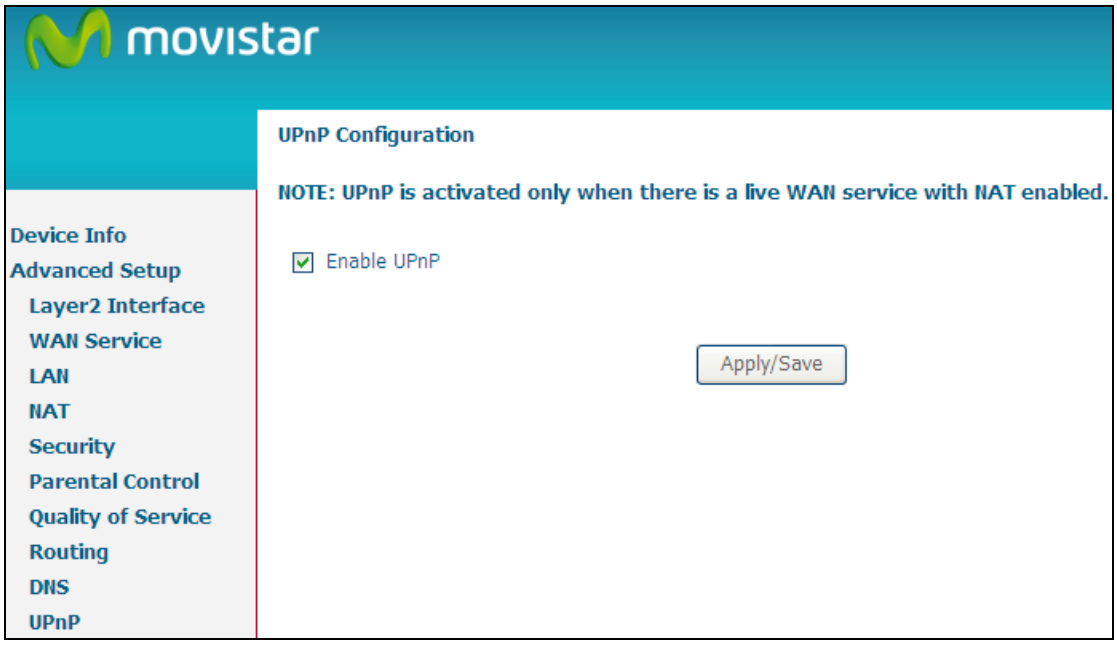
To add a dynamic DNS service, click **Add**. The following screen will display.



Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

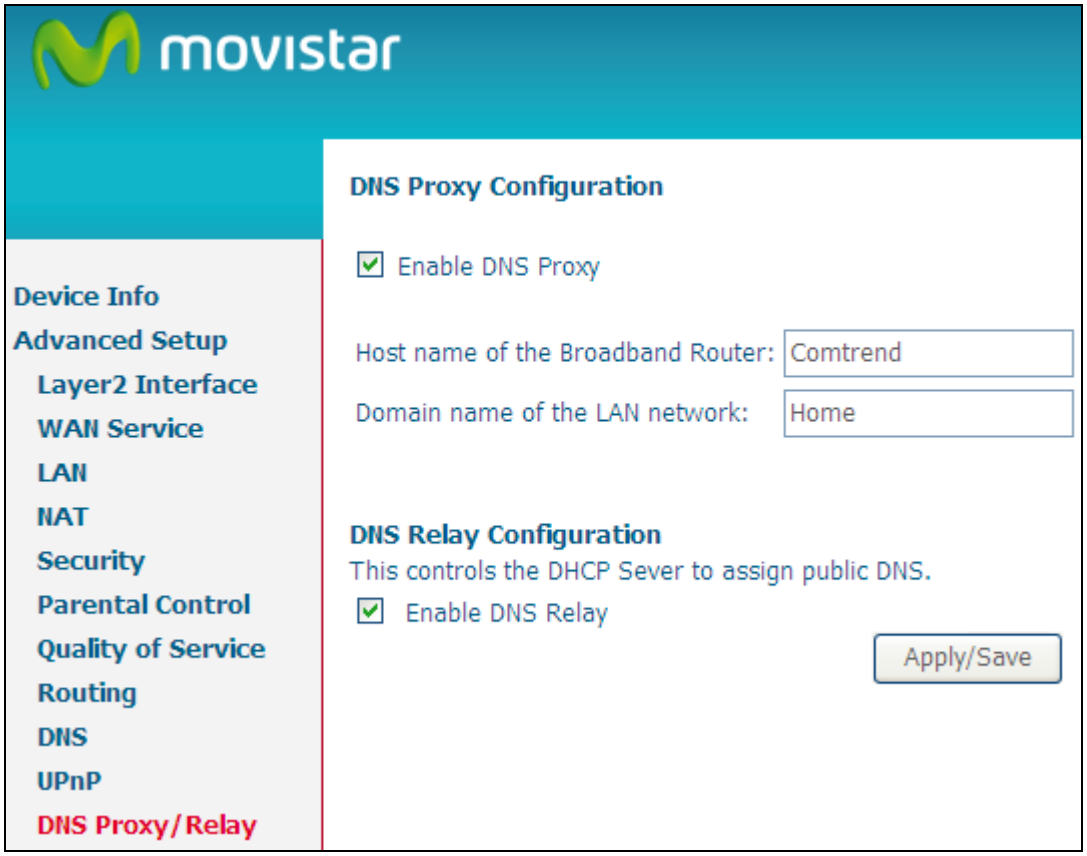
6.9 UPnP

Select the checkbox ☑ provided and click **Apply / Save** to enable UPnP protocol.



6.10 DNS Proxy/Relay

DNS proxy receives DNS queries and forwards DNS queries to the Internet. After the CPE gets answers from the DNS server, it replies to the LAN clients. Configure DNS proxy with the default setting, when the PC gets an IP via DHCP, the domain name, Home, will be added to PC's DNS Suffix Search List, and the PC can access route with "Comtrend.Home".



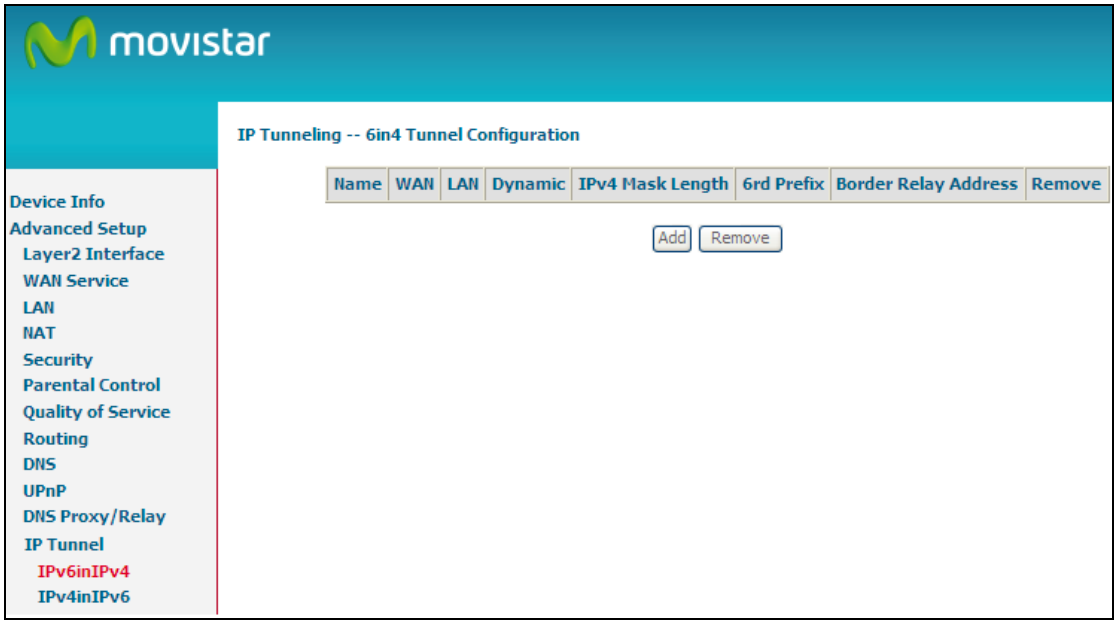
DNS Relay

When DNS Relay is enabled, the router will play a role as DNS server that send request to ISP DNS server and cache the information for later access. When DNS relay is disabled, the computer will pull information from ISP DNS server.

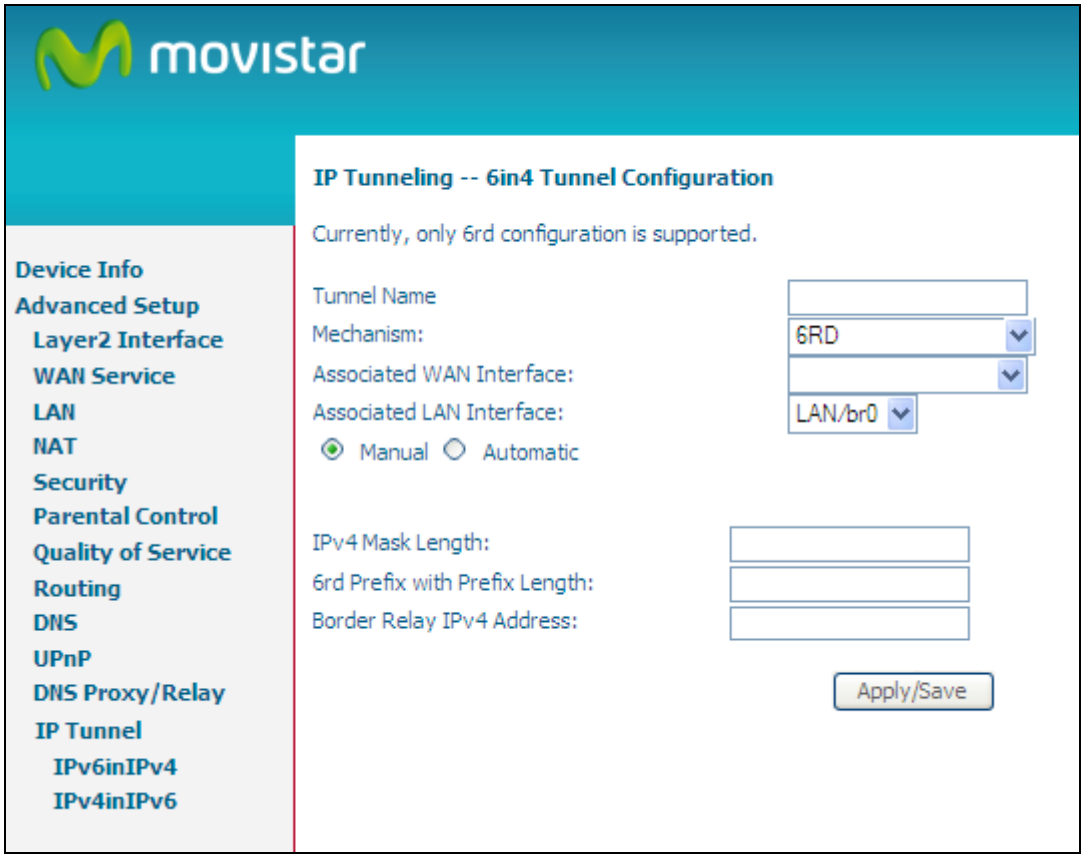
6.11 IP Tunnel

6.11.1 IPv6inIPv4

Configure 6in4 tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.



Click the **Add** button to display the following.

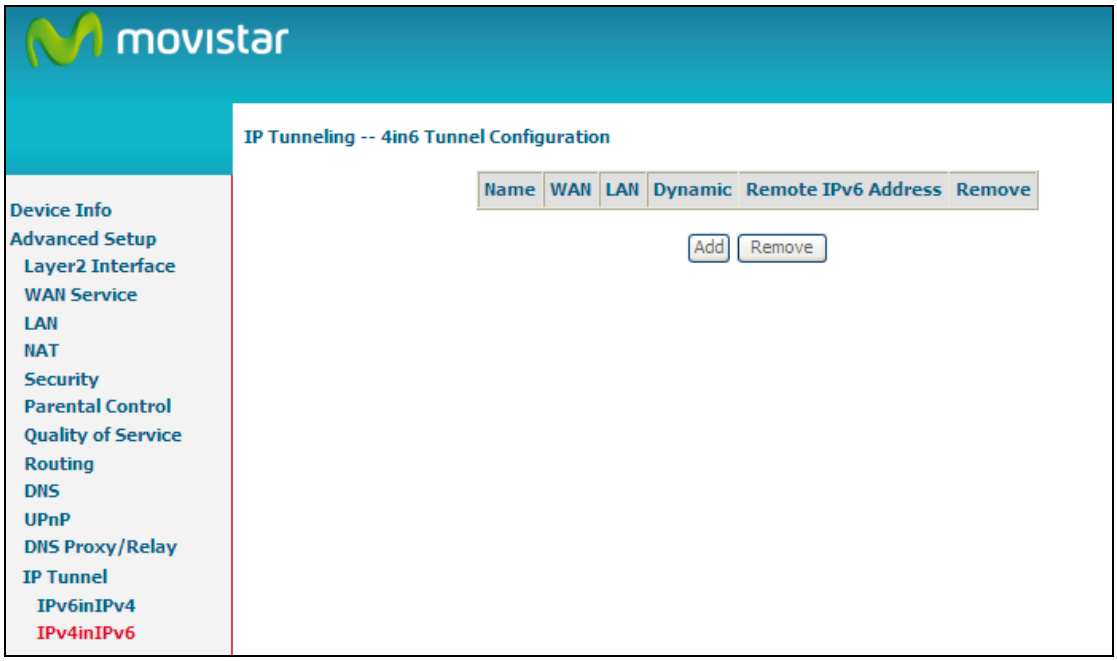


Field	Description
Tunnel Name	A name for the tunnel.
Mechanism	The mechanism that is using the tunnel. Now, only 6RD is supported.
Associated WAN Interface	The WAN interface that would sustain the tunnel.

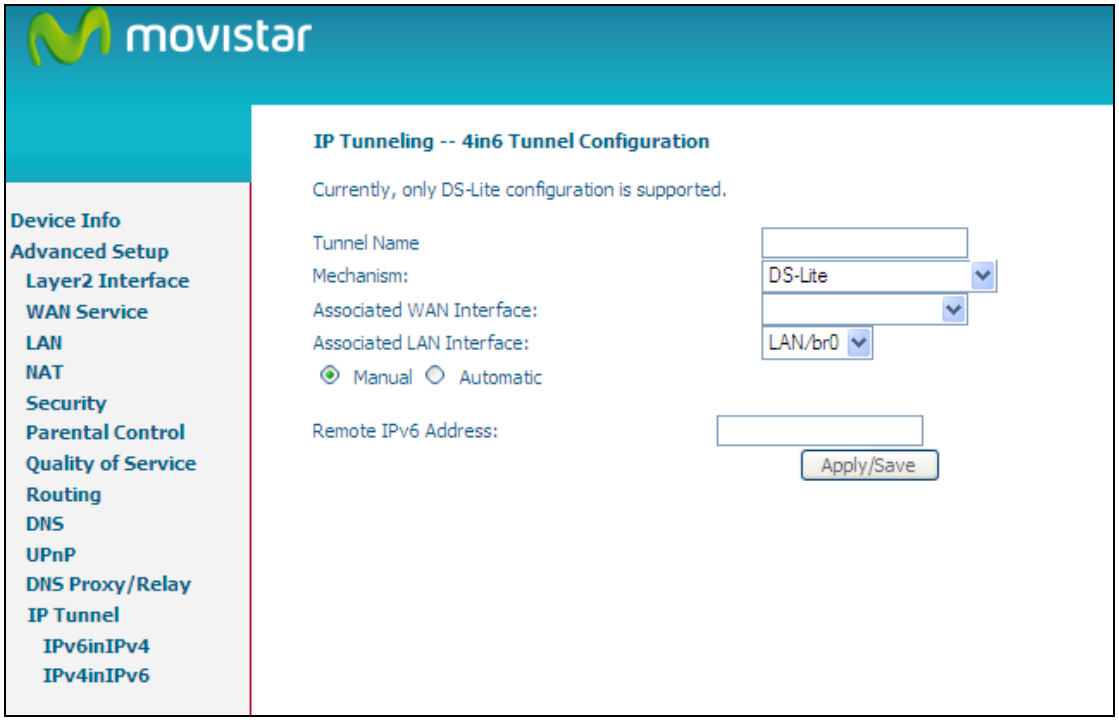
Field	Description
Associated LAN Interface	The LAN interface that would use the tunnel to forward the packets.
IPv4 Mask Length	The IPv4 subnet for WAN interface.
6rd Prefix with Prefix Length	The 6RD prefix and its length for this tunnel.
Border Relay IPv4 Address	A server that can relay the tunneled packets or simply the other tunnel point.

6.11.2 IPv4inIPv6

Configure 4in6 tunneling to encapsulate IPv4 traffic over an IPv6-only environment.



Click the **Add** button to display the following.

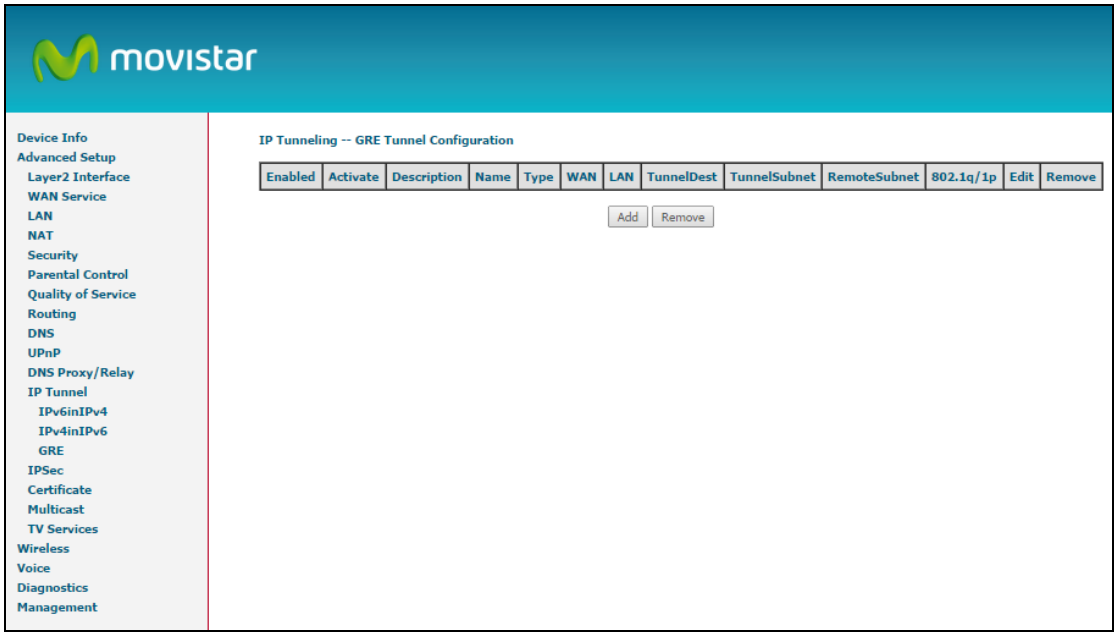


Field	Description
Tunnel Name	A name for the tunnel.
Mechanism	The mechanism that is using the tunnel. Now, only DS-Lite is supported.
Associated WAN Interface	The WAN interface that would sustain the tunnel.
Associated LAN Interface	The LAN interface that would use the tunnel to forward the packets.
Remote IPv6 Address	The peer of the tunnel.

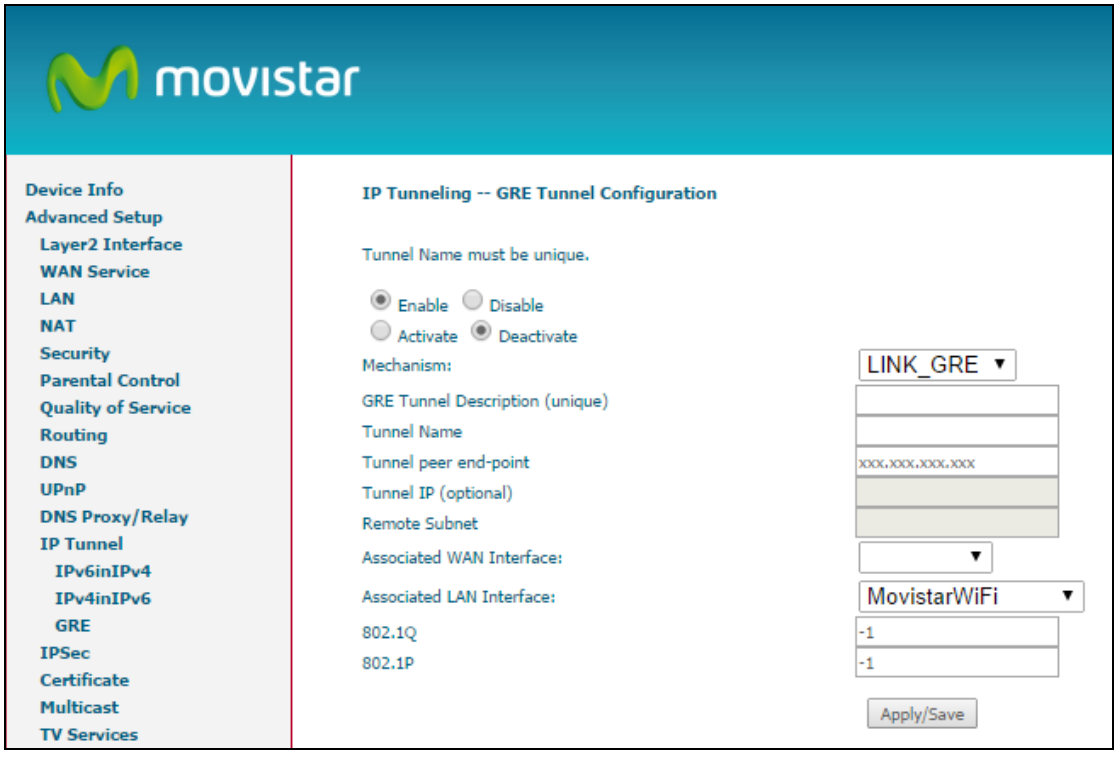
6.11.3 GRE

Note: The use of this option might be limited to some services of the operator

Configure GRE tunneling to encapsulate IP traffic over configured IPv4 links.



Click the **Add** button to display the following.

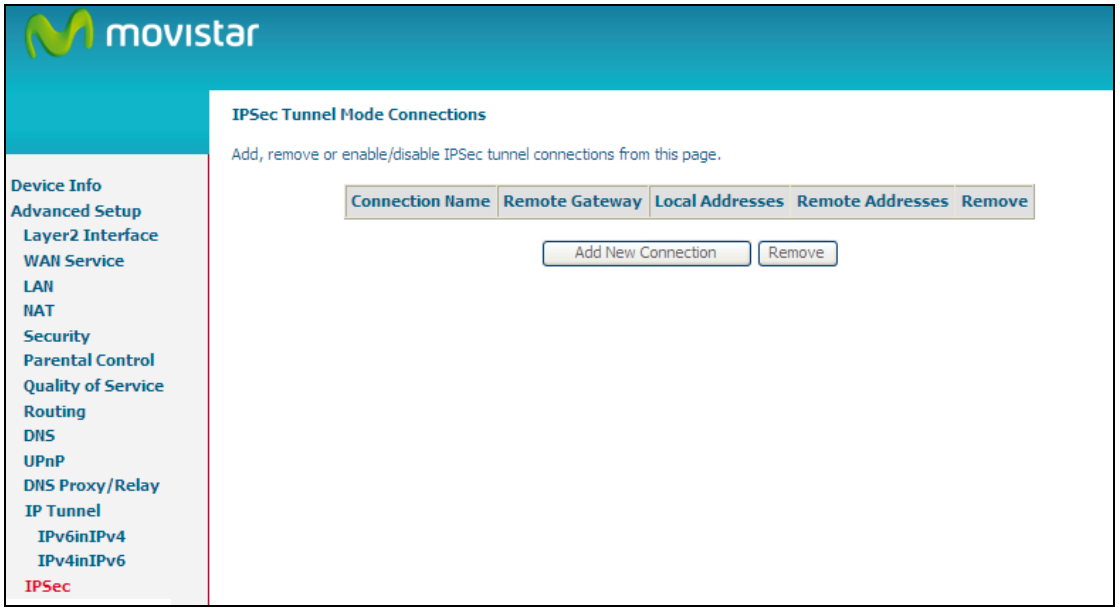


Field	Description

Field	Description
Enable/Disable	It enables the tunnel interface. If disables the tunnel interface won't appear as an available interface.
Activate/Deactivate	Enable/Disables the packet transmission through the tunnel.
Associated WAN Interface	The WAN interface that would sustain the tunnel.
Mechanism	The mechanism that is using the tunnel. It can be LINK_GRE (layer 2) or IP_GRE (routed)
GRE Tunnel Description	A string that helps to describe the tunnel.
Tunnel Name	A name for the tunnel.
Tunnel peer end point	The IP address of the tunnel end-point. This only applies when the mechanism used is IP_GRE (Routed)
Tunnel IP	Force a source IP used for the tunnel.
Remote subnet	The subnet of the remote peer end point. This only applies when the mechanism used is IP_GRE (Routed)
Associated WAN Interface	Only for IP GRE, the WAN interface where the source IP must be used.
Associated LAN Interface	Only for LINK GRE, the LAN interface (bridge) that would use the tunnel to forward the packets.
802.1Q	The VLAN TAG used for the tunnel (value of -1 means no VLAN tag is used).
802.1P	The priority (P-bit) marked on the VLAN.

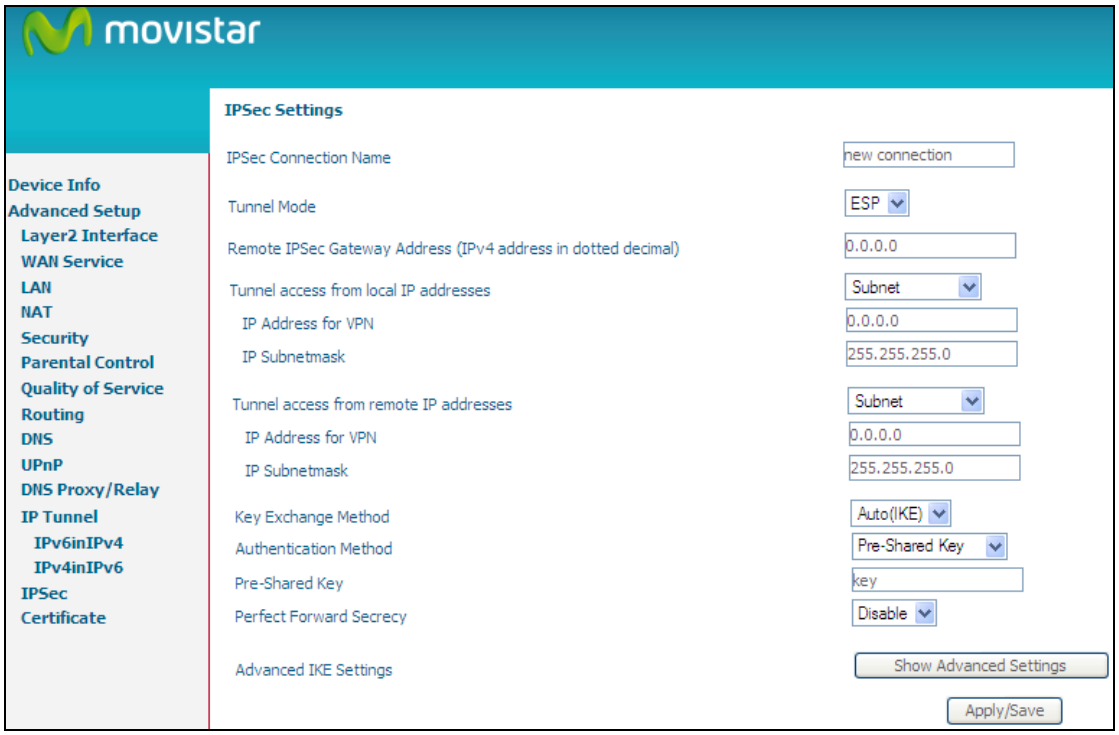
6.12 IPSec

You can add, edit or remove IPSec tunnel mode connections from this page.



Click **Add New Connection** to add a new IPSec termination rule.

The following screen will display.

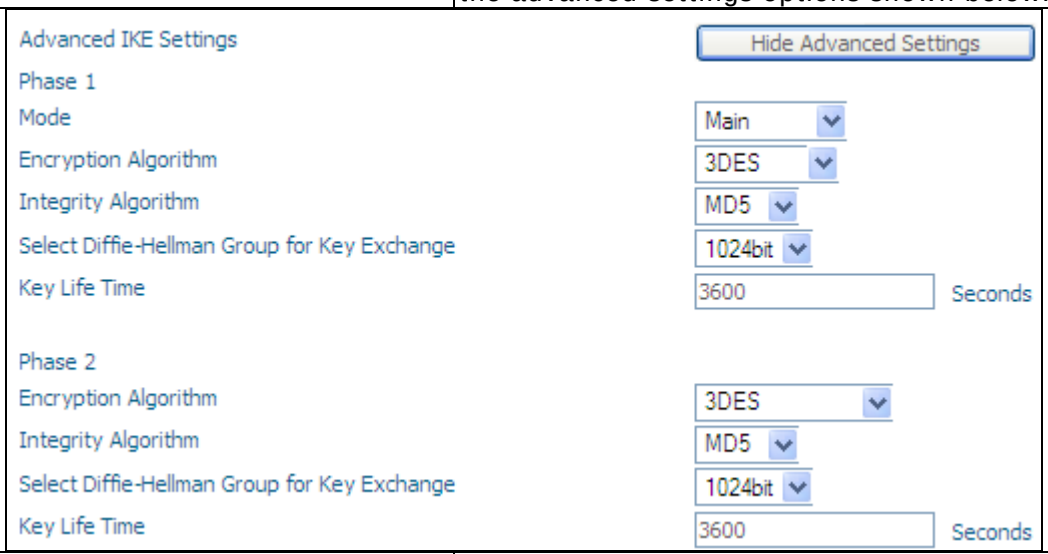


Field	Description
IPSec Connection Name	User-defined label

Tunnel Mode	Select tunnel protocol, AH (Authentication Header) or ESP (Encapsulating Security Payload) for this tunnel.
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.
Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

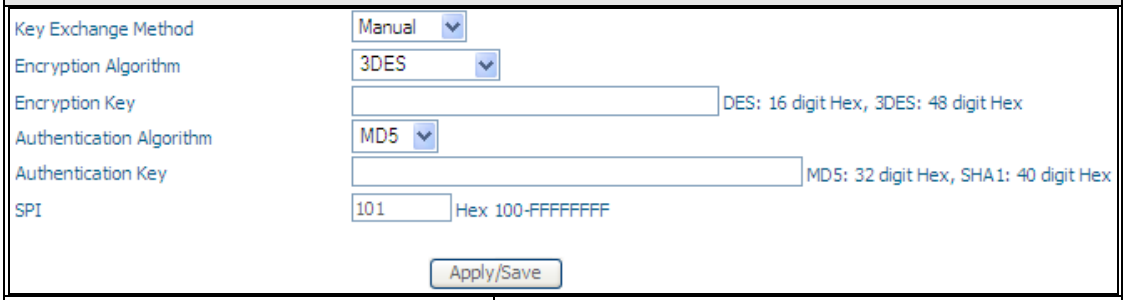
For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select **Show Advanced Settings** to reveal the advanced settings options shown below.
	
Advanced IKE Settings	Select **Hide Advanced Settings** to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a “/” character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1

Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

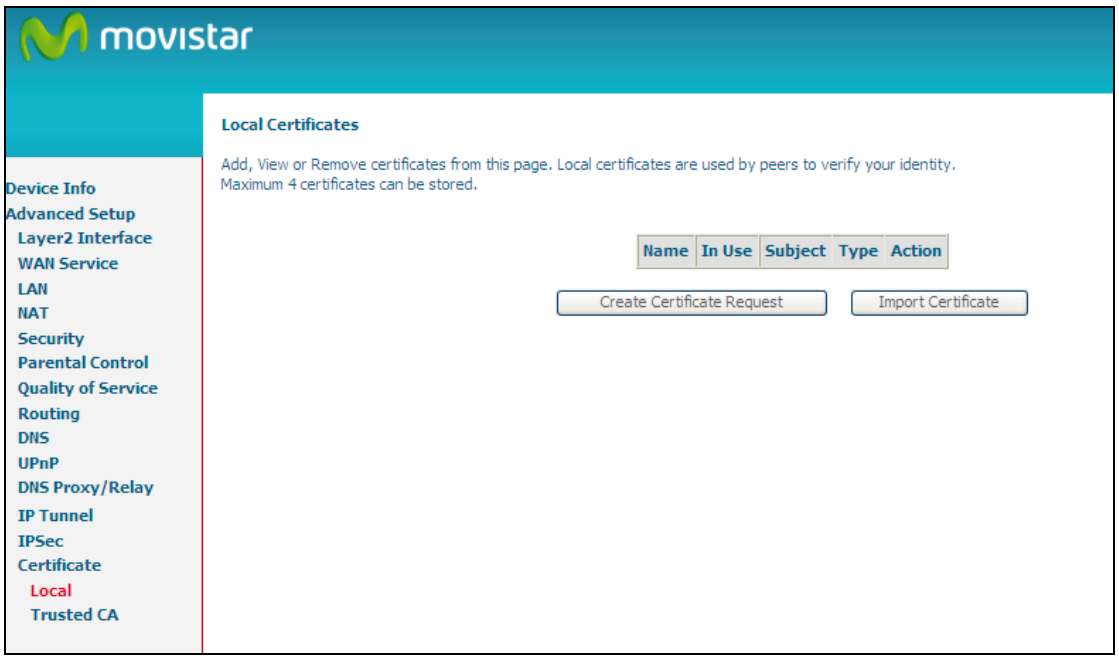
The Manual key exchange method options are summarized in the table below.

Manual Key Exchange Method	
	
Encryption Algorithm	DES / 3DES / AES (aes-cbc)
Encryption Key	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5 / SHA1
Authentication Key	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI (default is 101)	Enter a Hex value from 100-FFFFFFFF

6.13 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

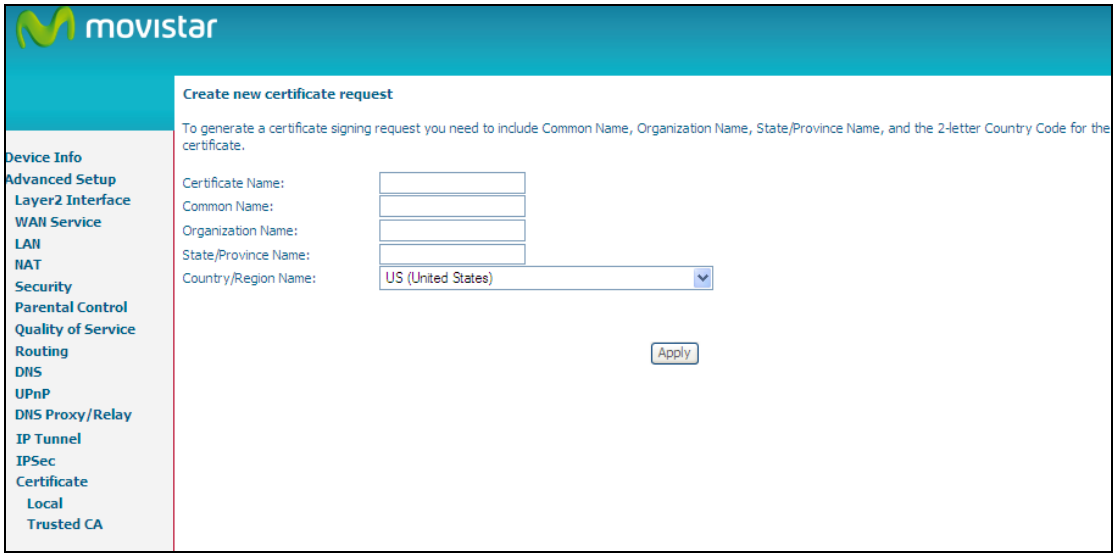
6.13.1 Local



CREATE CERTIFICATE REQUEST

Click **Create Certificate Request** to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.



The following table is provided for your reference.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

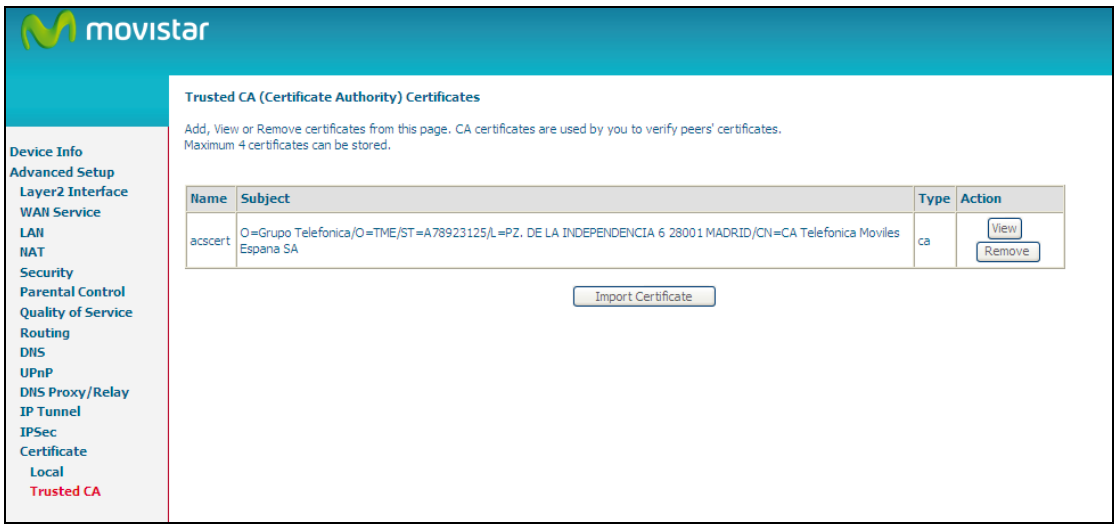
IMPORT CERTIFICATE

Click **Import Certificate** to paste the certificate content and the private key provided by your vendor/ISP/ITSP into the corresponding boxes shown below.

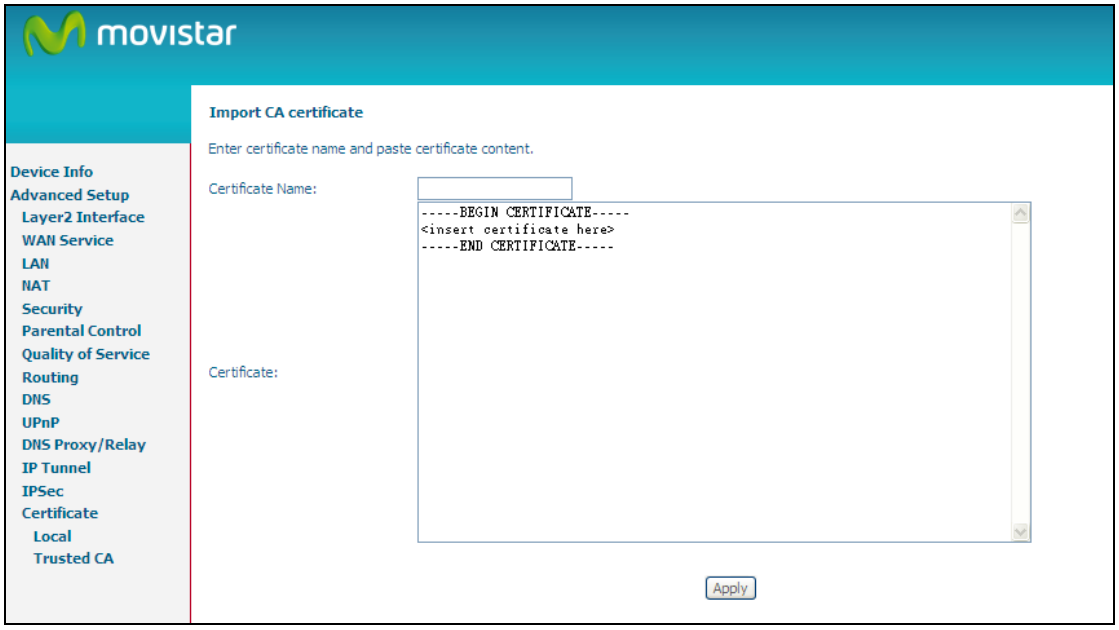
Enter a certificate name and click **Apply** to import the local certificate.

6.13.2 Trusted CA

CA is an abbreviation for Certificate Authority, which is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority; but its purpose is not encryption/decryption. Its purpose is to sign and issue certificates, in order to prove that these certificates are valid.



Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



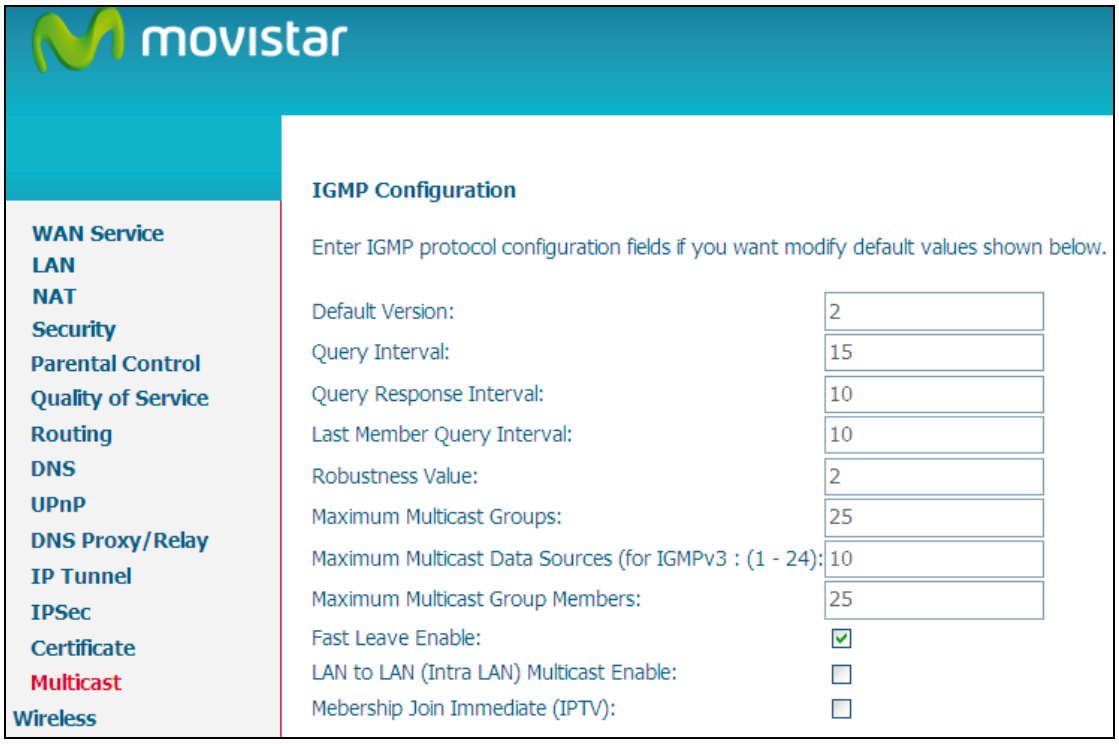
Enter a certificate name and click **Apply** to import the CA certificate.

6.14 Multicast

IP multicast is a method of forwarding the same set of IP packets to a number of hosts within a network. You can use multicast in both IPv4 and IPv6 networks to provide efficient delivery of data to multiple destinations.

Multicast involves both a method of delivery and discovery of senders and receivers of multicast data, which is transmitted on IP multicast addresses called groups. A multicast address that includes a group and source IP address is often referred to as a channel.

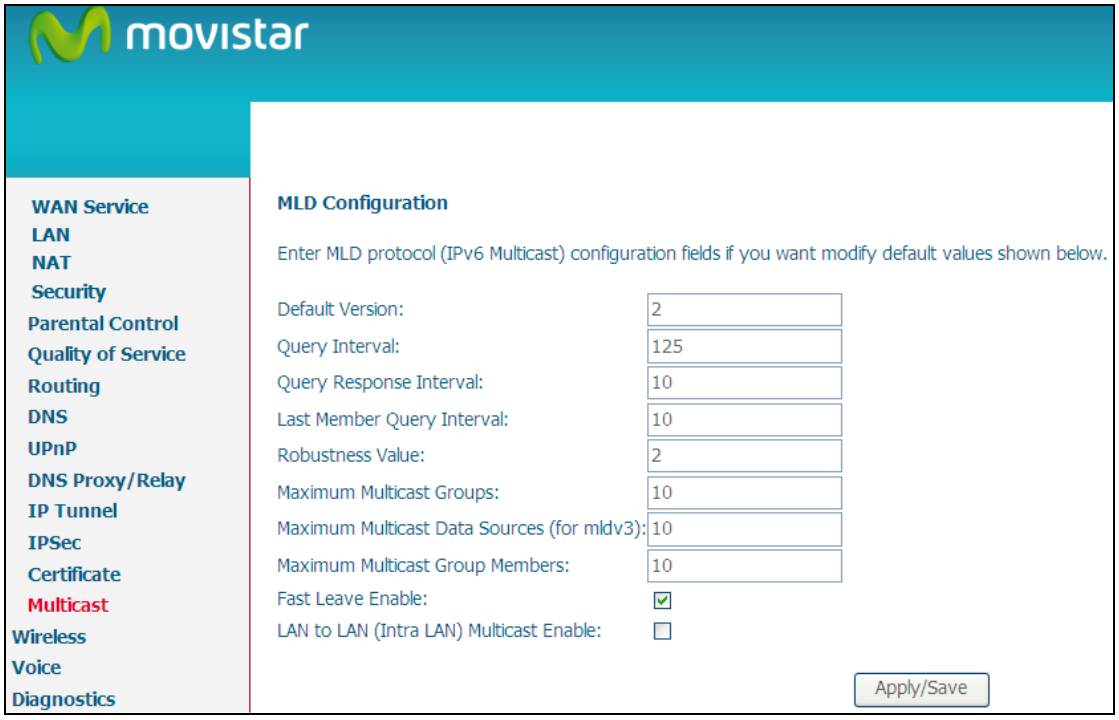
IGMP Configuration



Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.

Field	Description
Query Response Interval	The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Last Member Query Interval	The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default last member query interval is 10 seconds.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Maximum Multicast Groups	Setting the maximum number of Multicast groups.
Maximum Multicast Data Sources (for IGMPv3)	Define the maximum multicast video stream number.
Maximum Multicast Group Members	Setting the maximum number of groups that ports can accept.
Fast Leave Enable	When you enable IGMP fast-leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.
LAN to LAN (Intra LAN) Multicast Enable	Allows a multicast server to reside on the LAN side receiving IGMP packets for its use.
Membership Join Immediate (IPTV)	This is for IPTV to join the membership for video quickly; The CPE would relay the join-message with certain delay, this option would reduce the delay.

MLD Configuration



Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.
Query Response Interval	The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Last Member Query Interval	The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default last member query interval is 10 seconds.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.

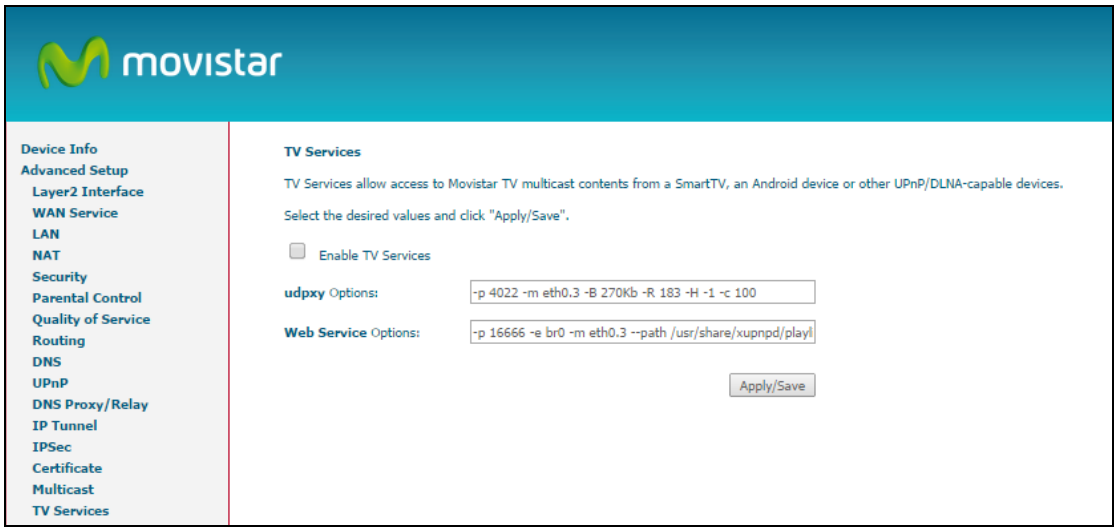
Field	Description
Maximum Multicast Groups	Setting the maximum number of Multicast groups.
Maximum Multicast Data Sources (for IGMPv3)	Define the maximum multicast video stream number.
Maximum Multicast Group Members	Setting the maximum number of groups that ports can accept.
Fast Leave Enable	When you enable IGMP fast-leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.
LAN to LAN (Intra LAN) Multicast Enable	Allows a multicast server reside on the LAN side receiving IGMP packets for its use.

6.15 TV Services

TV Services menu is reserved for the Movistar IPTV unicast conversion.

To enable the service click on the checkbox ☑ “Enable TV Services” and press **Apply / Save** button.

The values on the text boxes should not be changed or it may affect the quality of the service.

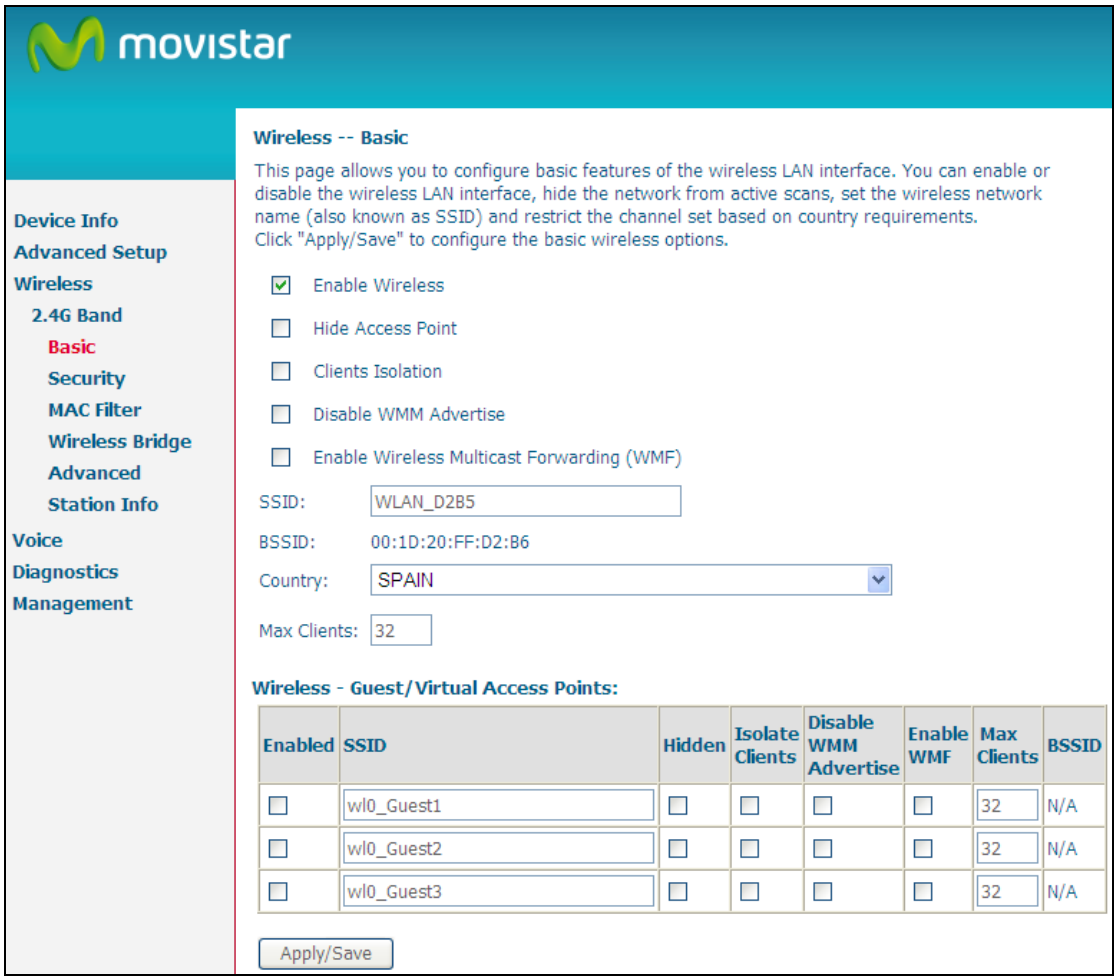


Chapter 7 Wireless 2.4G Band

The Wireless menu provides access to the wireless options discussed below.

7.1 Basic

The Basic option allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



Click **Save / Apply** to apply the selected wireless options.

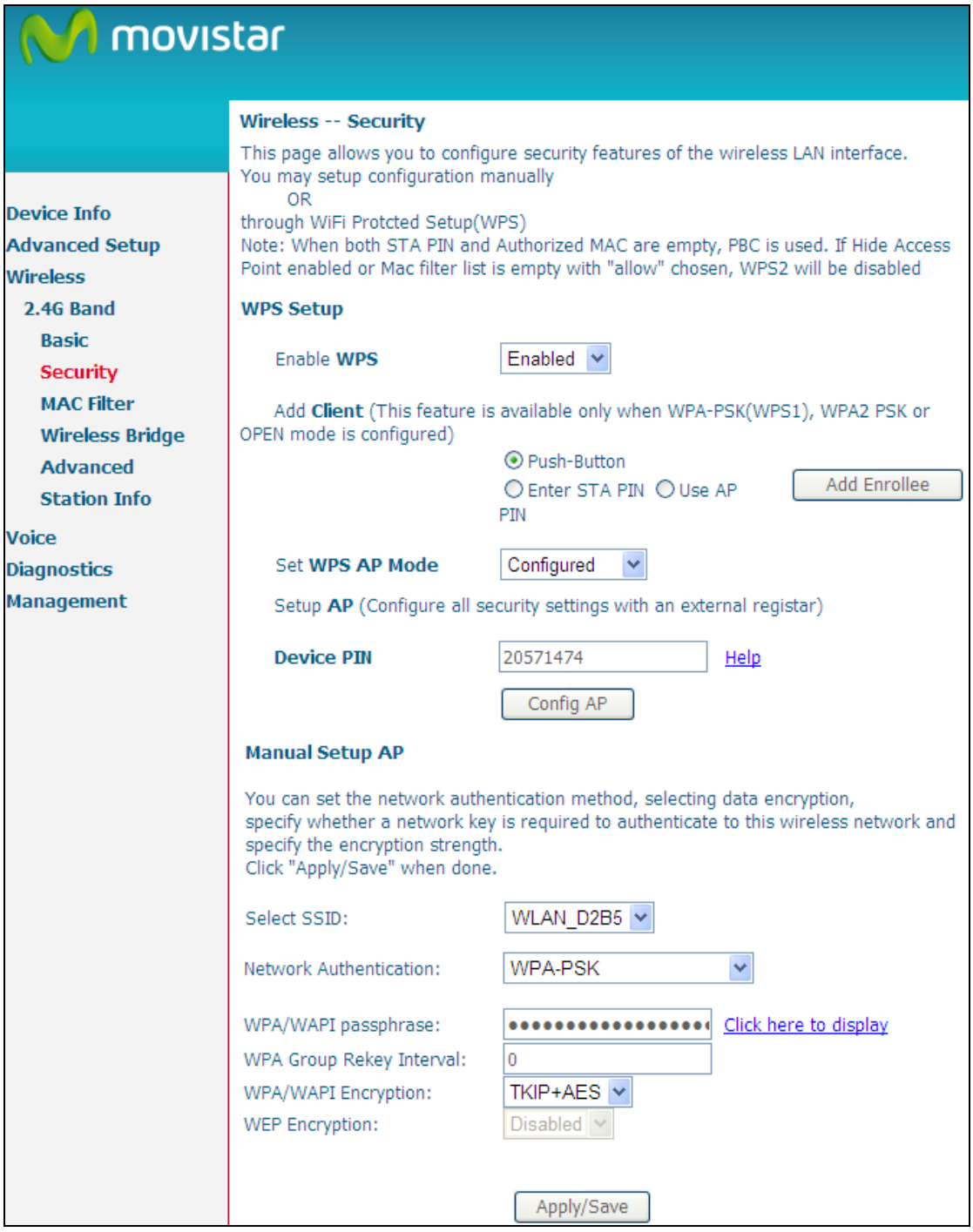
Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.

Option	Description
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open **Network Connections** from the **start** Menu and select **View Available Network Connections**. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	When enabled, it prevents client PCs from seeing one another in My Network Places or Network Neighborhood. Also, prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video). Supported in a future release.
Enable Wireless Multicast Forwarding	If want to use WLAN for multicast service, tick the box to enable.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point); and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Local regulations limit channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☑ in the **Enabled** column. To hide a Guest SSID select its checkbox ☑ in the **Hidden** column. Do the same for **Isolate Clients** and **Disable WMM Advertise**. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for **Max Clients** and **BSSID**, consult the matching entries in this table. **NOTE:** Remote wireless hosts cannot scan Guest SSIDs.

7.2 Security

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.



Click **Apply/Save** to implement new configuration settings.

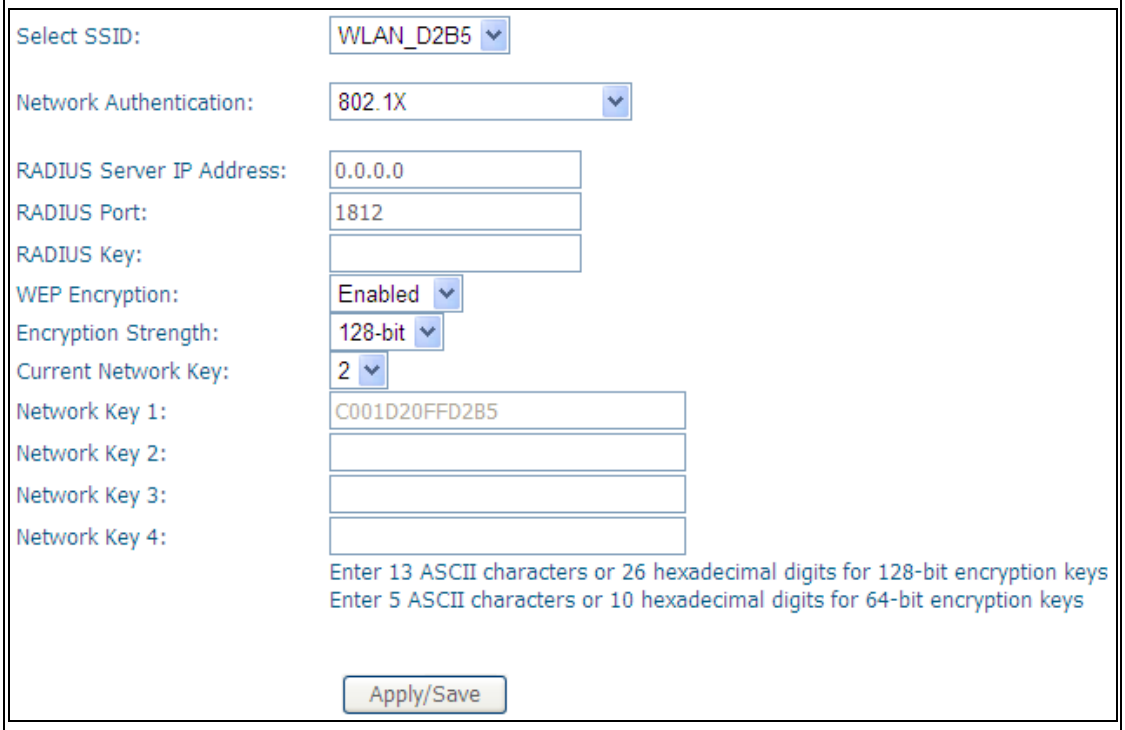
WIRELESS SECURITY

Wireless security settings can be configured according to Wi-Fi Protected Setup (WPS) or Manual Setup. The WPS method configures security settings automatically

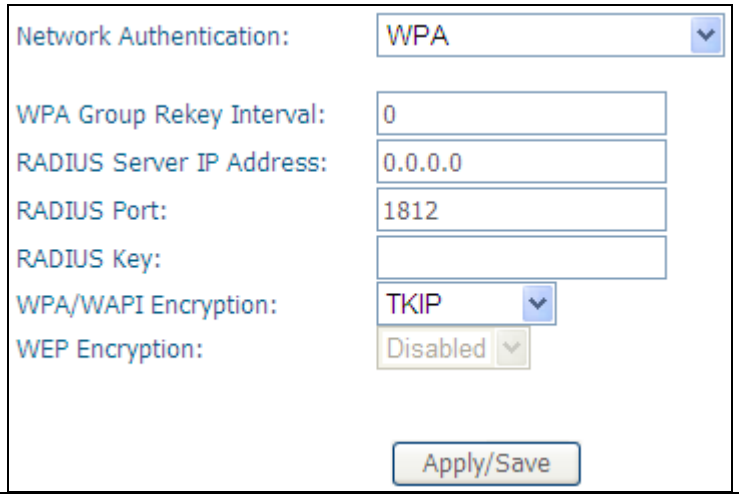
(see section 6.2.1) while the Manual Setup method requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID
Select the wireless network name from the drop-down box. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

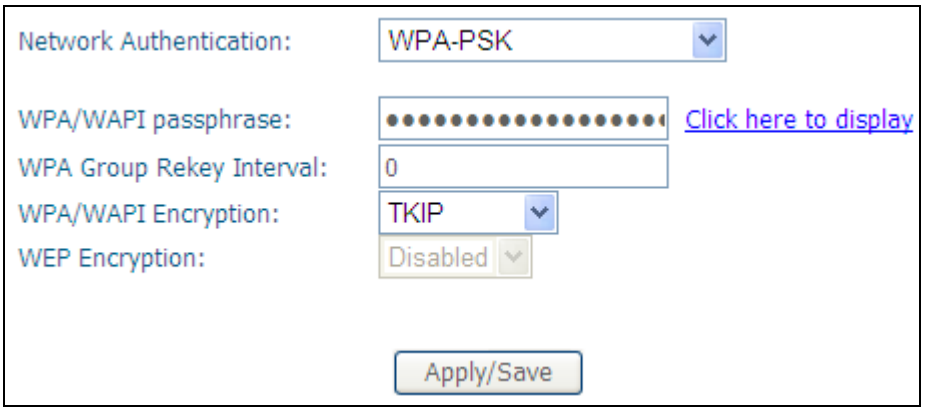
Network Authentication
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.



The settings for WPA authentication are shown below.



The settings for WPA-PSK authentication are shown next.



WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

Current Network Key

Select the required network key.

7.2.1 WPS

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The VG-8050 has both a WPS button on the rear panel and a virtual button accessed from the web user interface (WUI).

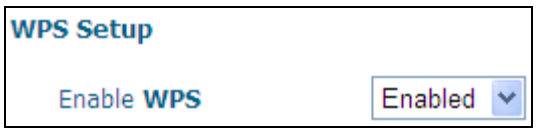
Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".

NOTE:	WPS is only available in Open, WPA-PSK, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

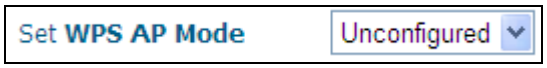
To configure security settings with WPS, follow the procedures below. You must choose either the Push-Button or PIN configuration method for Steps 6 and 7.

I. Setup

Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.

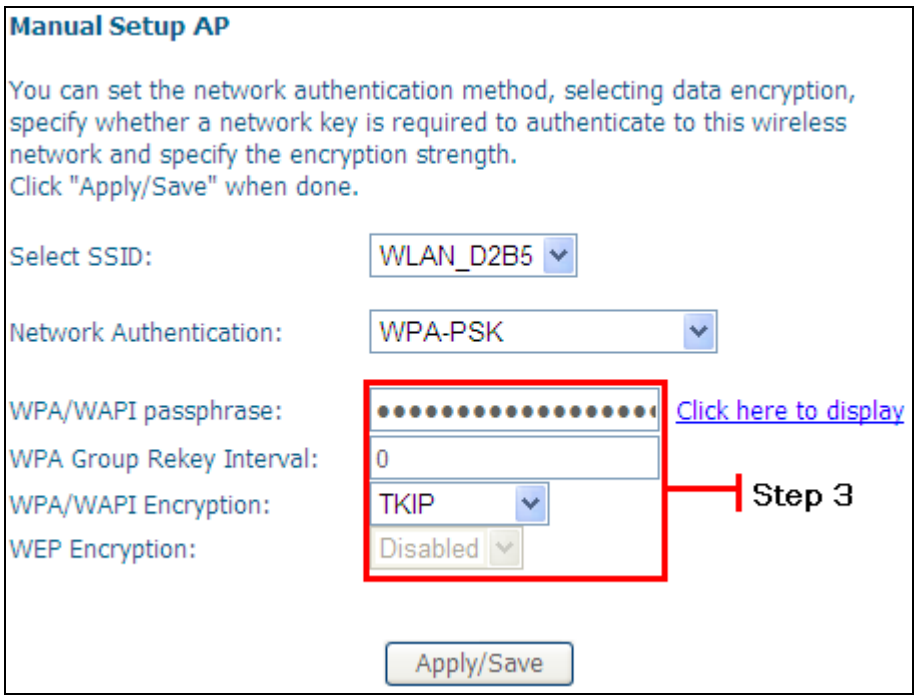


Step 2: Set the WPS AP Mode. **Configured** is used when the VG-8050 will assign security settings to clients. **Unconfigured** is used when an external client assigns security settings to the VG-8050.



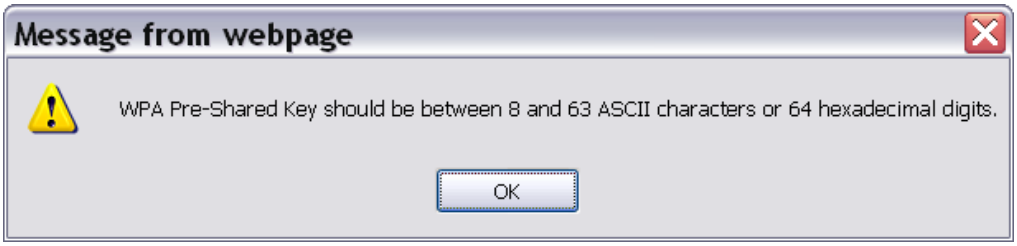
NOTES:	Your client may or may not have the ability to provide security settings to the VG-8050. If it does not, then you must set the WPS AP mode to Configured. Consult the device documentation to check its capabilities. In addition, using Windows Vista, you can add an external registrar using the **StartAddER** button (Appendix E has detailed instructions).

II. NETWORK AUTHENTICATION



Step 3: Select Open, WPA-PSK, WPA2-PSK, or Mixed WPA2/WPA-PSK network authentication mode from the Manual Setup AP section of the Wireless Security screen. The example below shows WPA2-PSK mode.

Step 4: For the Pre-Shared Key (PSK) modes, enter a WPA Pre-Shared Key. You will see the following dialog box if the Key is too short or too long.



Step 5: Click the **Save / Apply** button at the bottom of the screen.

III a. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WPS button on the rear panel of the router can be used for this purpose or the Web User Interface (WUI) can be used exclusively.

The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE:	The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 7, return to Step 6.

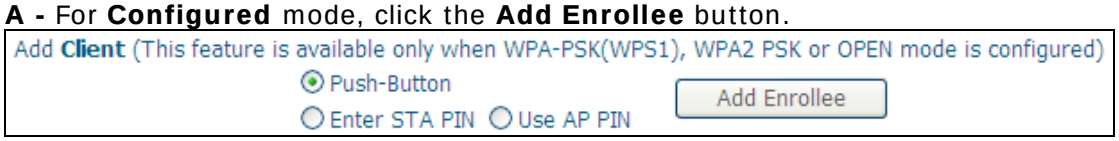
Step 6: **First method: WPS button**

Press the WPS button on the front panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

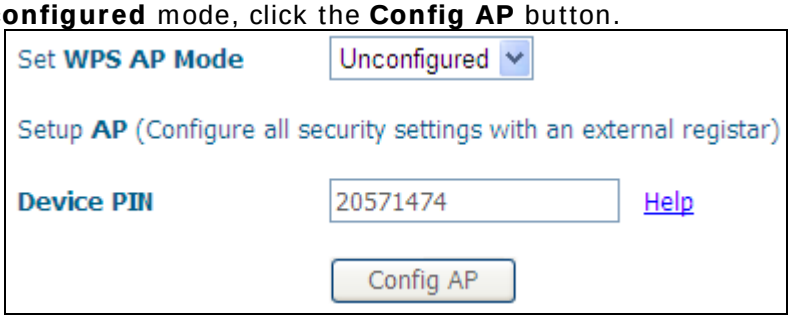
Second method: WUI virtual button

Select the Push-Button radio button in the WSC Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

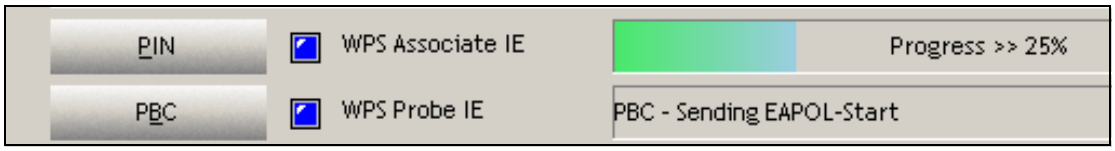
A - For **Configured** mode, click the **Add Enrollee** button.



B - For **Unconfigured** mode, click the **Config AP** button.



Step 7: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.



Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

III b. WPS – PIN CONFIGURATION

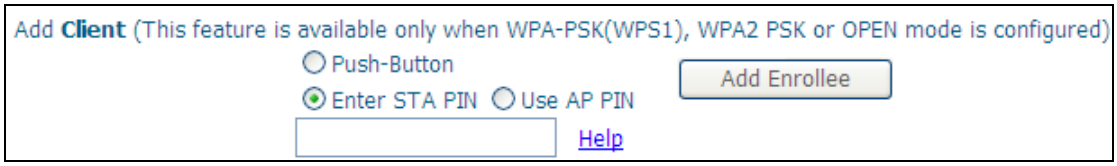
Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE:	Unlike the push-button method, the pin method has no set time limit. This means that the router will continue searching until it finds a client.

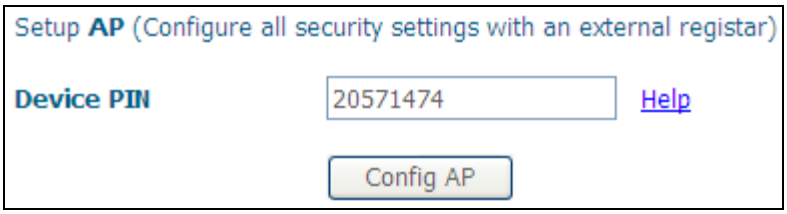
Step 6: Select the PIN radio button in the WPS Setup section of the Wireless Security screen, as shown in **A** or **B** below, and then click the appropriate button based on the WSC AP mode selected in step 2.

A - For **Configured** mode, enter the client PIN in the box provided and then click the **Add Enrollee** button (see below).



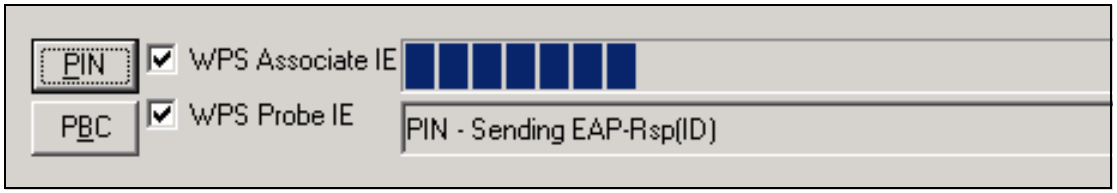
Enter STA PIN: a Personal Identification Number (PIN) has to be read from either a sticker or the display on the new wireless device. This PIN must then be inputted at representing the network, usually the Access Point of the network.

B - For **Unconfigured** mode, click the **Config AP** button.



Step 7: Activate the PIN function on the wireless client. For **Configured** mode, the client must be configured as an Enrollee. For **Unconfigured** mode, the client must be configured as the Registrar. This is different from the External Registrar function provided in Windows Vista.

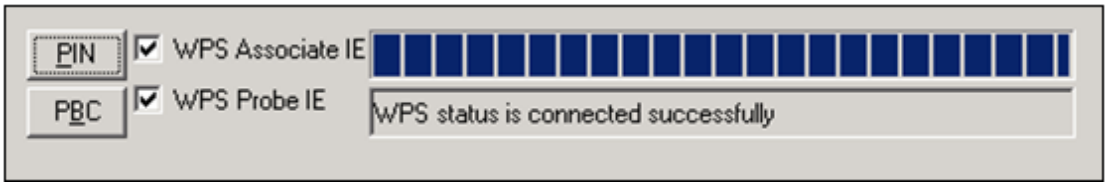
The figure below provides an example of a WPS client PIN function in-progress.



Now go to Step 8 (part IV. Check Connection) to check the WPS connection.

IV. CHECK CONNECTION

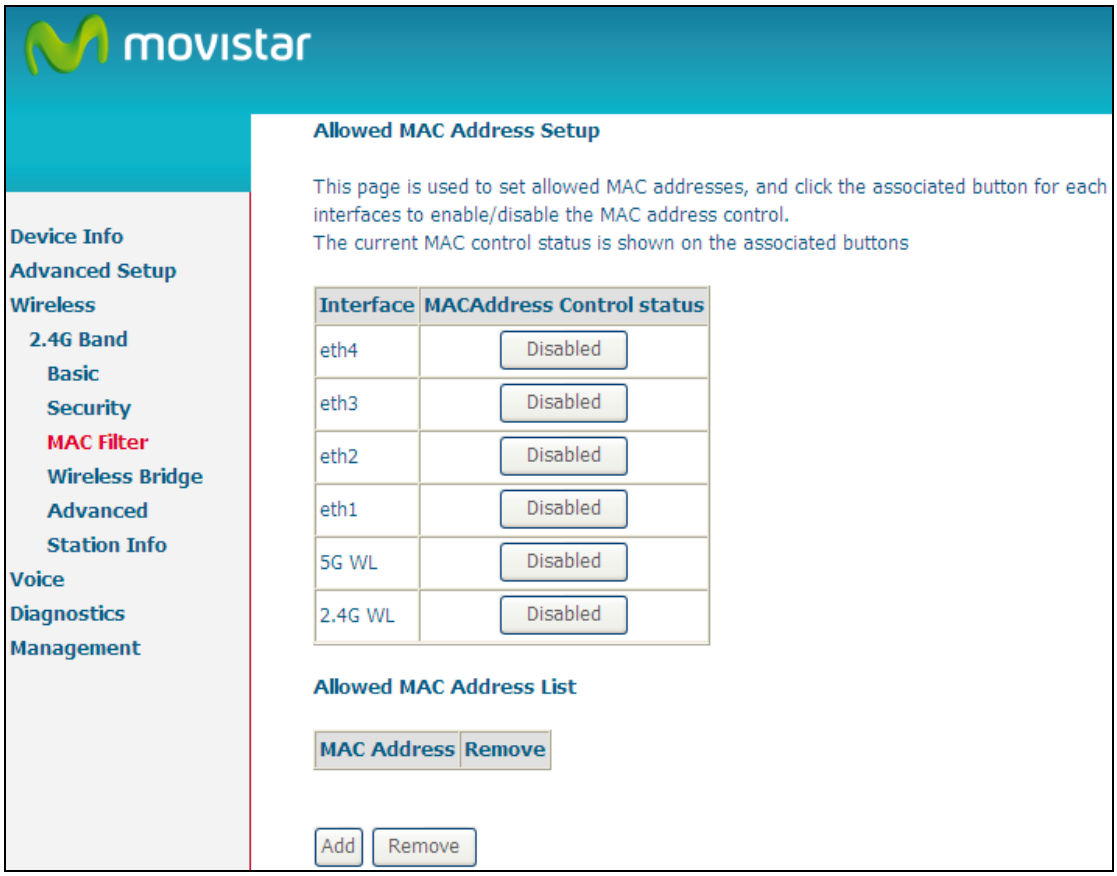
Step 8: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.



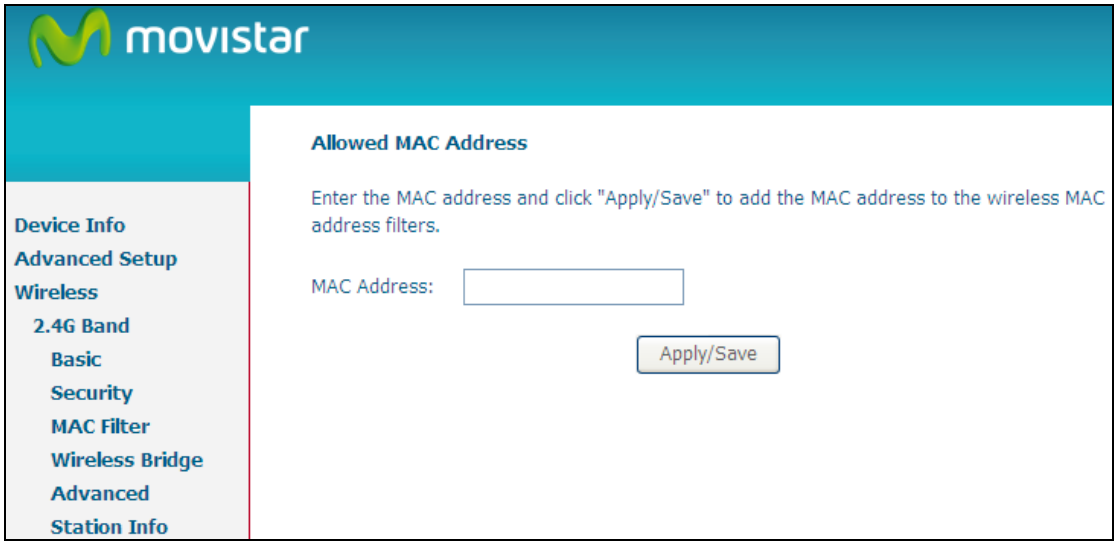
You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.

7.3 MAC Filter

This page is used to set allowed MAC addresses, and click the associated button for each interface to enable/disable the MAC address control.
The current MAC control status is shown on the associated buttons.

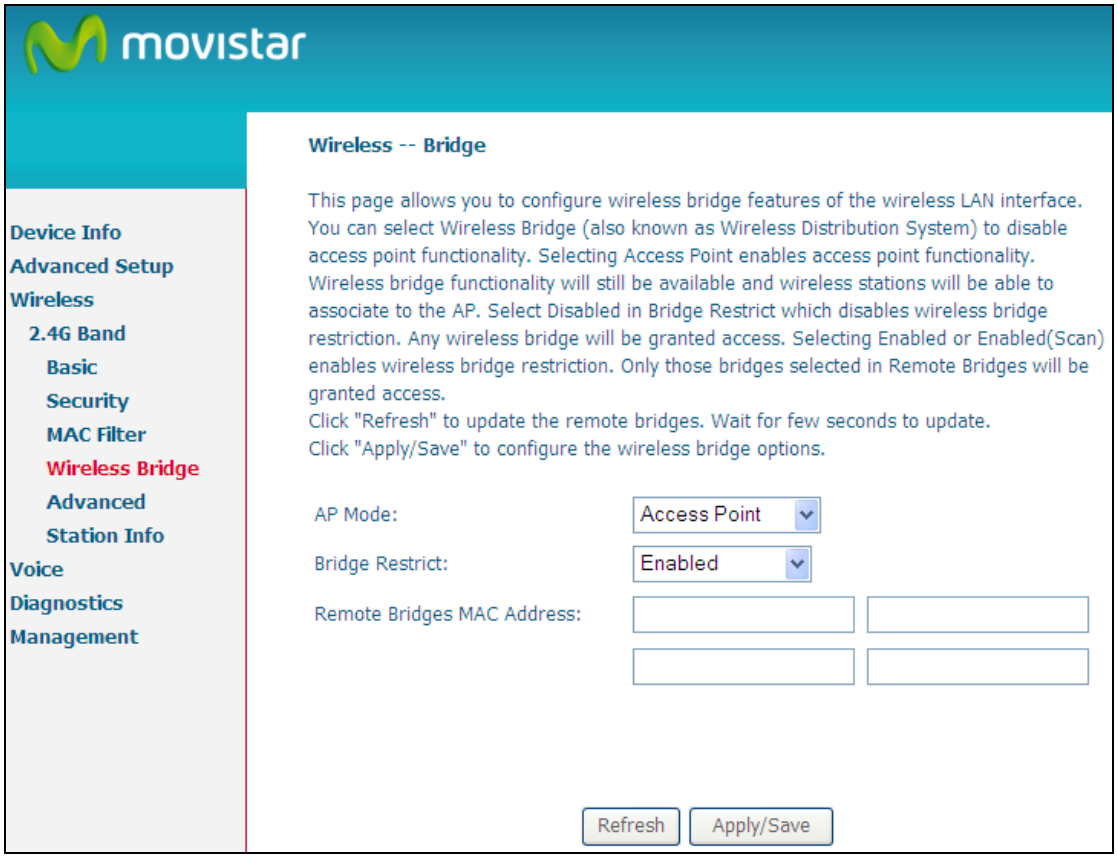


After clicking the **Add** button, the following screen appears.
Input the MAC address in the box provided, and click **Apply/Save**.



7.4 Wireless Bridge

This screen allows for the configuration of wireless bridge features of the WLAN interface. See the table beneath for detailed explanations of the various options.



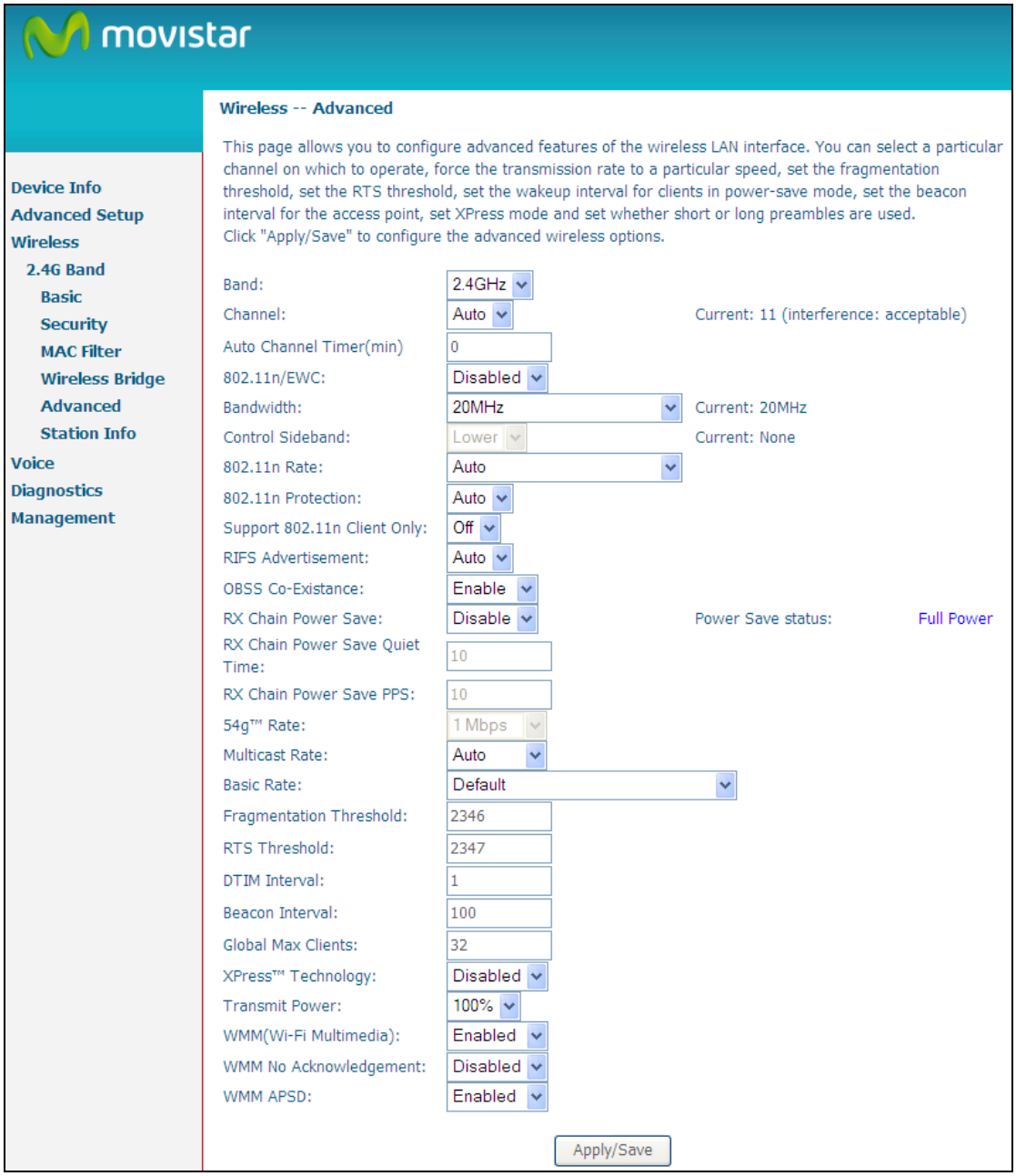
Click **Save / Apply** to implement new configuration settings.

Feature	Description

Feature	Description
AP Mode	Selecting **Wireless Bridge** (aka Wireless Distribution System) disables Access Point (AP) functionality, while selecting **Access Point** enables AP functionality. In **Access Point** mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting **Disabled** disables wireless bridge restriction, which means that any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in the Remote Bridges list will be granted access. Click **Refresh** to update the station list when Bridge Restrict is enabled.

7.5 Advanced

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Save/Apply** to set new advanced wireless options.



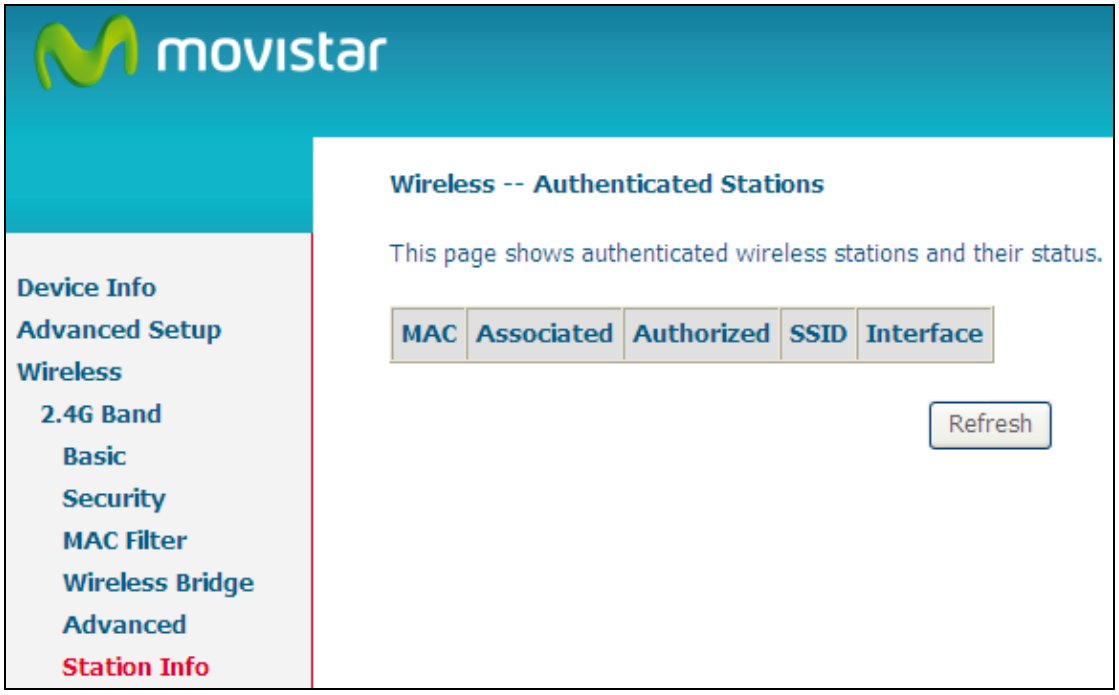
Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)

Field	Description
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Select 20GHz or 40GHz bandwidth. 40GHz bandwidth uses two adjacent 20GHz bands for increased data throughput.
Control Sideband	Select Upper or Lower sideband when in 40GHz mode.
802.11n Rate	Set the physical transmission rate (PHY).
802.11n Protection	Turn Off for maximized throughput. Turn On for greater security.
Support 802.11n Client Only	Turn Off to allow 802.11b/g clients access to the router. Turn On to prohibit 802.11b/g client's access to the router.
RIFS Advertisement	Reduced Interframe Space is the creation of a short time delay between PDUs to improve wireless efficiency.
OBSS Co-Existance	Co-existence between 20 MHZ AND 40 MHZ overlapping Basic Service Set (OBSS) in WLAN.
RX Chain Power Save	Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting for multicast packet transmit rate (1-54 Mbps)
Basic Rate	Setting basic transmission rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.

Field	Description
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Global Max Clients	The maximum number of clients that can connect to the router.
Xpress ™ Technology	Xpress Technology is compliant with draft specifications of two planned wireless industry standards.
Transmit Power	Set the power output (by percentage) as desired.
WMM (Wi-Fi Multimedia)	The technology maintains the priority of audio, video and voice applications in a Wi-Fi network. It allows multimedia service get higher priority.
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling no Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
WMM APSD	This is Automatic Power Save Delivery. It saves power.

7.6 Station Info

This page shows authenticated wireless stations and their status. Click the **Refresh** button to update the list of stations in the WLAN.



Consult the table below for descriptions of each column heading.

Heading	Description
MAC	Lists the MAC address of all the stations.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.

Chapter 8 Voice

This chapter first describes the various options for configuration of the SIP voice service. It then provides detailed instructions for making telephone calls using VoIP (Voice over IP) or PSTN (Public Switched Telephone Network) services.
Session Initiation Protocol (SIP) is a peer-to-peer protocol used for Internet conferencing, telephony, events notification, presence and instant messaging.
SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

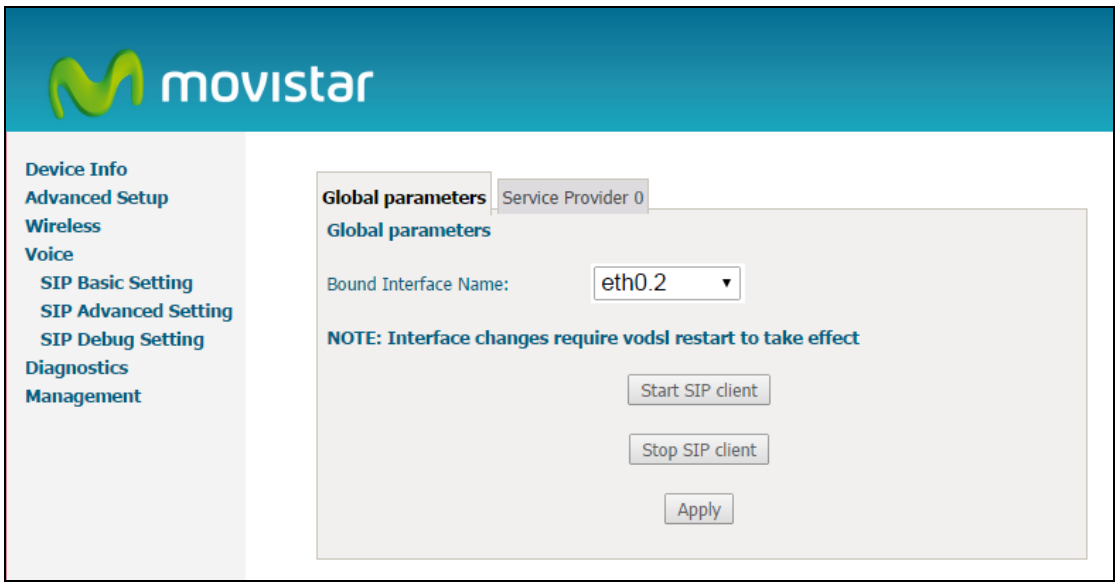
NOTE: The SIP standard is set by the Internet Engineering Task Force (IETF).

The SIP standard defines the following agents/servers:

- ☐ User Agents (**UA**) - SIP phone clients (hardware or software)
- ☐ Proxy Server – relays data between **UA** and external servers
- ☐ Registrar Server - a server that accepts register requests from **UA**
- ☐ Redirect Server – provides an address lookup service to **UA**

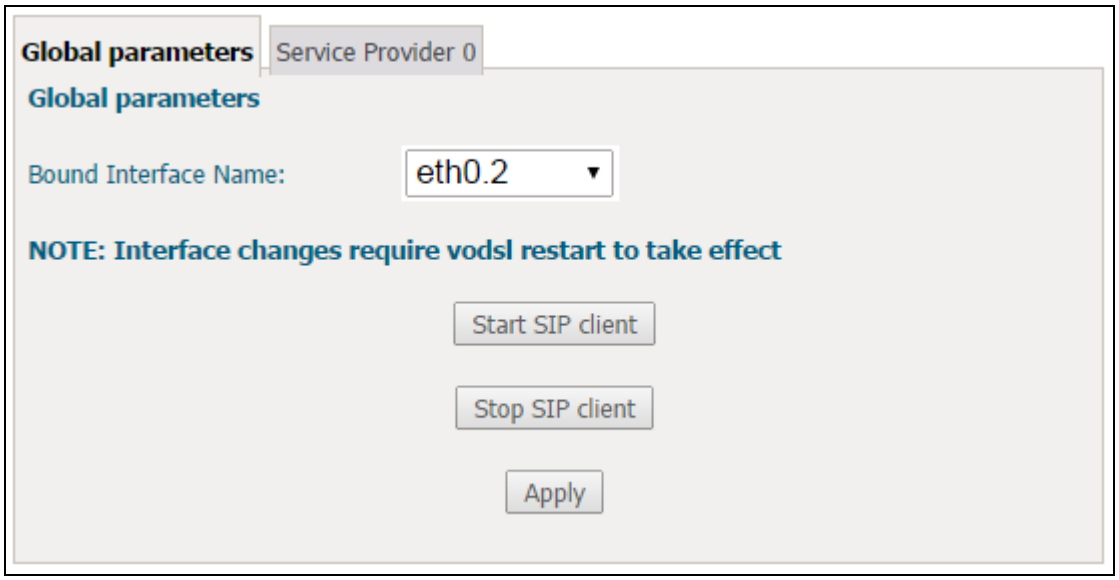
The following subsections present **Basic**, **Advanced** and **Debug** SIP screens. Each screen provides various options for customizing the SIP configuration.

8.1 SIP Basic Setting



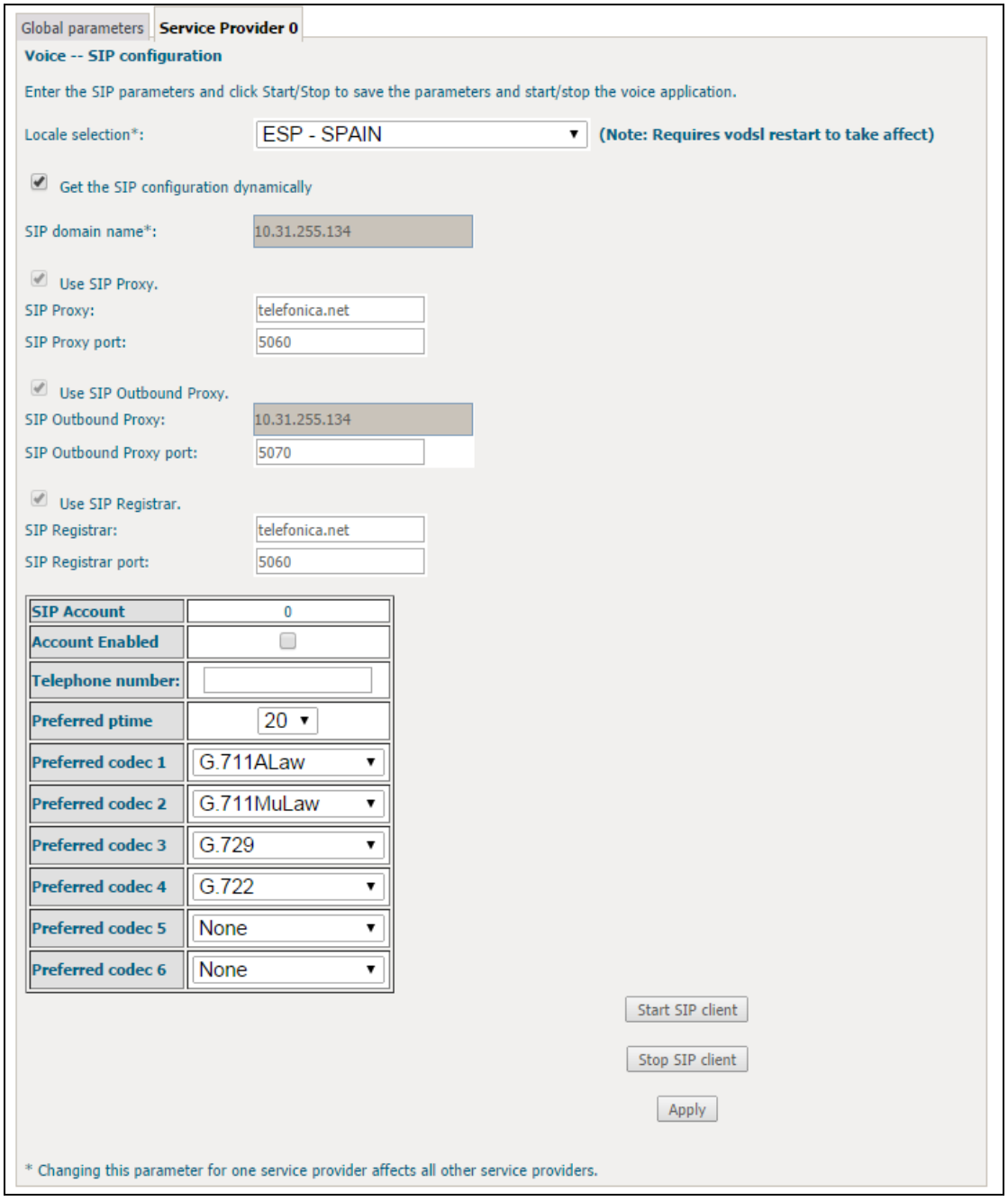
8.1.1 Global Parameters

A common parameter setting.



8.1.2 Service Provider

This screen contains basic SIP configuration settings.

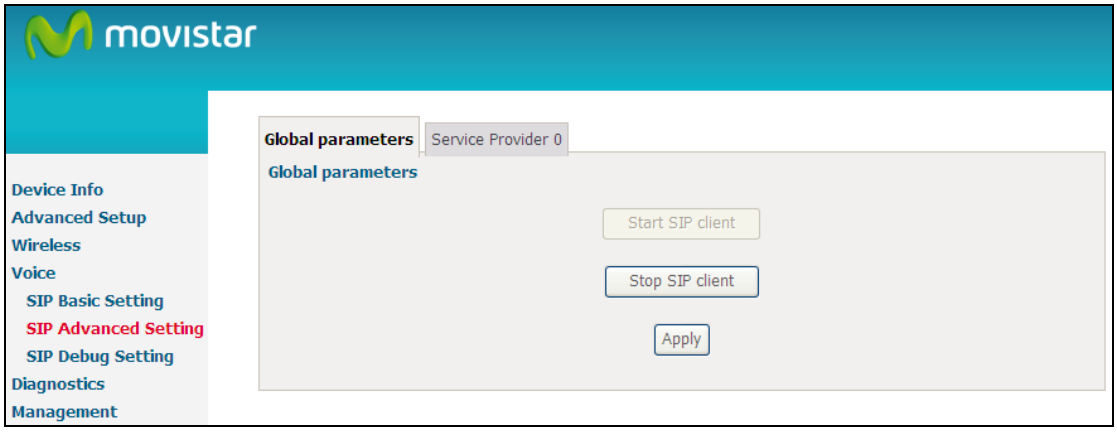


Once settings are configured click **Save** and **Apply** to begin using the service.

Field	Description
Locale Selection	Sets tone, ring type and physical characteristics for specific countries
Get de SIP configuration dinamically	The router will configure the SBC or Proxy IP address by the option 120 of the DHCP.
SIP domain name	Provided by your VoIP provider.
Use SIP proxy	Enable the SIP proxy by selecting the checkbox ☑ and setting proxy parameters.
SIP Proxy	Input IP address or domain name of the SIP proxy server, used for VOIP service.
SIP Proxy port	This value is set by your VoIP provider.
Use SIP Outbound Proxy	Enable the SIP outbound proxy by selecting the checkbox ☑ and setting outbound proxy parameters. It forwards the requests if you cannot reach SIP proxy directly.
Use SIP outbound proxy	Select if required by your VoIP provider. Input SIP Outbound Proxy IP and port.
SIP Outbound Proxy	Input SIP Outbound Proxy IP if required.
SIP Outbound Proxy port	Input SIP Outbound Proxy port number if required.
Use SIP Registrar	Enable the SIP registrar by selecting the checkbox ☑ and setting registrar parameters.
SIP Registrar	Input IP address of the SIP registrar server, used for VOIP service.
SIP Registrar port	This value is set by your VoIP provider.
FYI: *A proxy is an intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or transferred to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it.*	
SIP Account 0	**Ports Telf 1**
SIP Account	Map SIP accounts to physical ports. “0” represents to Telf1
Telephone number	The line extension or telephone number.
Preferred ptime	The time period used to digitally sample the analog voice signal. The default is 20 ms.
Preferred codec 1-6	Choose from G.711MuLaw/ALaw, G.729a, G.723.1, G.726_24/32, or GSM_AMR codecs.

8.2 SIP Advanced

This screen contains the advanced SIP configuration settings.

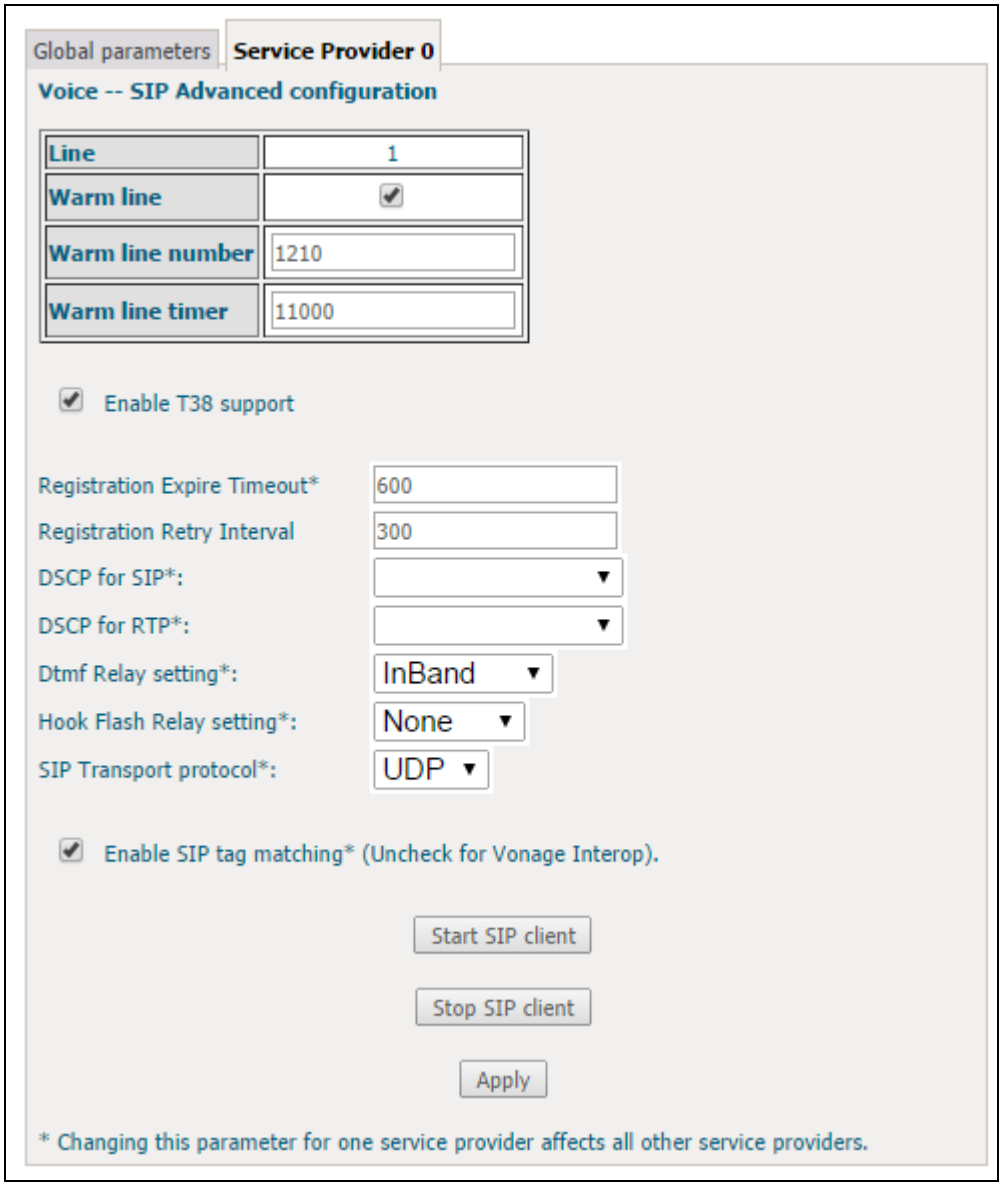


8.2.1 Global Parameters

A common parameter setting.

8.2.2 Service Provider

Configure your settings based on your service provider.



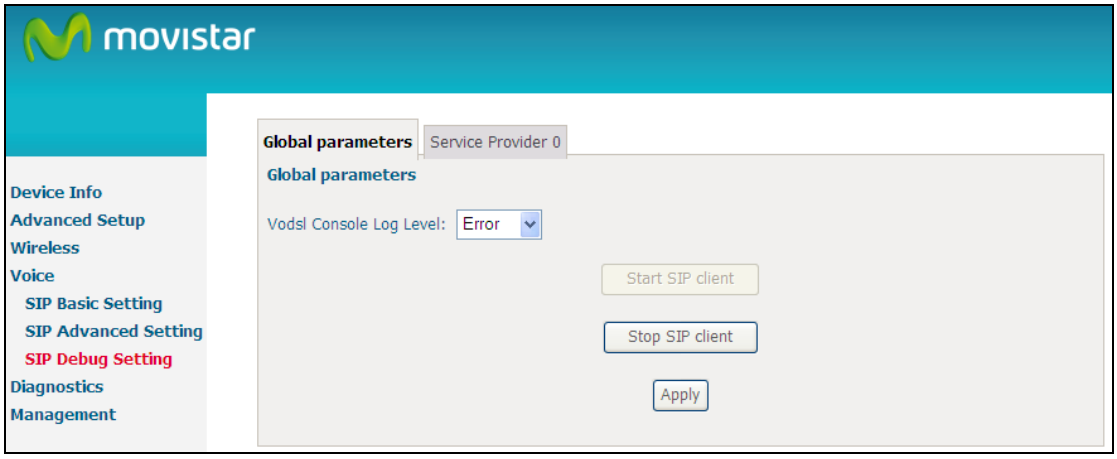
These settings are described in the tables below. Once configuration is complete, click **Save** and **Apply** to begin using the service.

Line 1	Ports Telf1
Warm line	Enables or disables the automatic dial after hook off the phone.
Warm line number	The telephone number that the SIP client will dial automatically after a configured time just after the phone has been picked off.
Warm line timer	The time between the hook off and the automatic dial (miliseconds).

Line 1	Ports Telf1
Enable T.38 support	Enable or disable T.38 Fax mode support with this checkbox ☑. You can plug a fax machine into either phone port to send or receive faxes. Functionality depends upon FAX support by your VoIP service provider.
Registration Expire Timeout	The time period the user would like the registration to be valid for the Registrar/ Proxy Server.
Registration Retry Interval	The time interval between re-registration attempts.
Max Digit Length	Sets the maximum number of digits for a phone number.
DSCP for SIP	Diff Serv Code Point (DSCP) for SIP.
DSCP for RTP	Diff Serv Code Point (DSCP) for RTP.
Dtmf Relay setting	Set the special use of RTP packets to transmit digit events.
Hook Flash Relay setting	When you integrate Voice over IP (VoIP) technologies to legacy private branch exchange (PBX) and public switched telephone networks (PSTNs), there is sometimes a need to pass a type of signaling known as 'hookflash'. A hookflash is a brief interruption in the loop current on loopstart trunks that the attached system does not interpret as a call disconnect. Once the PBX or PSTN senses the hookflash, it generally puts the current call on hold and provides a secondary dial tone or access to other features such as transfer or call waiting access. A hookflash is done by momentarily pressing down the cradle on a telephone. Some telephone handsets have a button called 'flash' or 'recall' that sends a 'timed loop break', or 'calibrated flash' which is a hookflash that has a precise timing.
SIP Transport protocol	Specify if the SIP stack will operate over USP or TCP.
Enable SIP tag matching (Uncheck for Vonage Interop).	Since CPE rely on the tags for matching purposes, implementations which support Replacements MUST support the SIP specification, which requires tags.

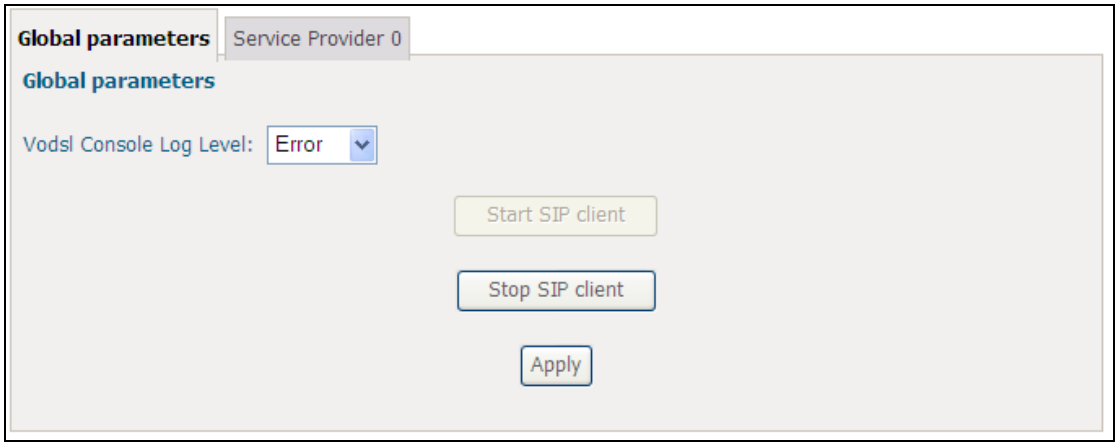
8.3 SIP Debug

This screen contains SIP configuration settings used for debugging.



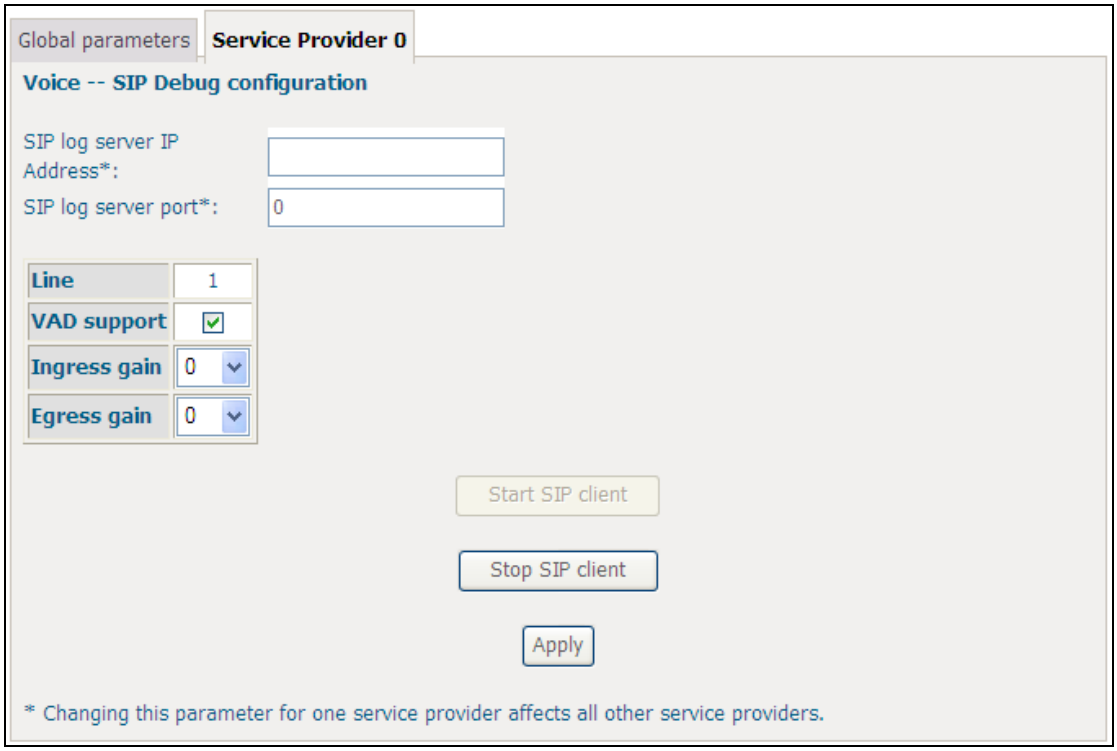
8.3.1 Global Parameters

A common parameter setting.



8.3.2 Service Provider

Configure your settings based on your service provider.



Once settings are configured click **Save** and **Apply** to begin using the service.

Checkbox ☑	**Description**
SIP log server IP address & port	Enter the IP address and port of the SIP log server.
Enable Vad Support	Select the checkbox ☑ to enable VAD support. Adjust the volume for incoming (Ingress) or outgoing (Egress) gain with the drop-down boxes.
Ingress gain	Enhances the volume of speaking (the volume heard from the other side).
Egress gain	Enhances the volume of hearing.

8.4 Telephone Calls

To make a call, simply dial the number. The dial plan (i.e. the dialed digits) is normally customized for each installation. The default dial plan is as follows (RFC 3435 format):

0[1-5]X|06[0-6]|06[8-9]|0[7-9]X|10[0-2]X|106X|10[8-9]X|112|118XX|116XXX|1[2-9]XX|50[0-8]XXXXXX|51XXXXXXX|590xxxxxxxxxx|6XXXXXXXX|7[1-4]xxxxxxx|8XXXXXXXX|9XXXXXXXX|*#X.#|*XX.#|#X.#|XX.#|X.T

When a Call Server (SIP Proxy Server) is configured into the system, the dialed digits are translated and routed by the Call Server to the correct destination as registered with the Call Server.

If no Call Server is configured, calls can still be made using 4-digit extensions, rather than using full IP addresses. The originator translates the dialed-digits to a destination device as follows:

First Digit:	Line identifier (for multi-line gateways)
Remaining digits:	Host number part of an IP address. The Network number part is considered to be the same as the caller's IP address.

Caller ID
The calling number is transmitted to the analog line for CLASS recognition. This functionality is enabled by default and cannot be disabled.

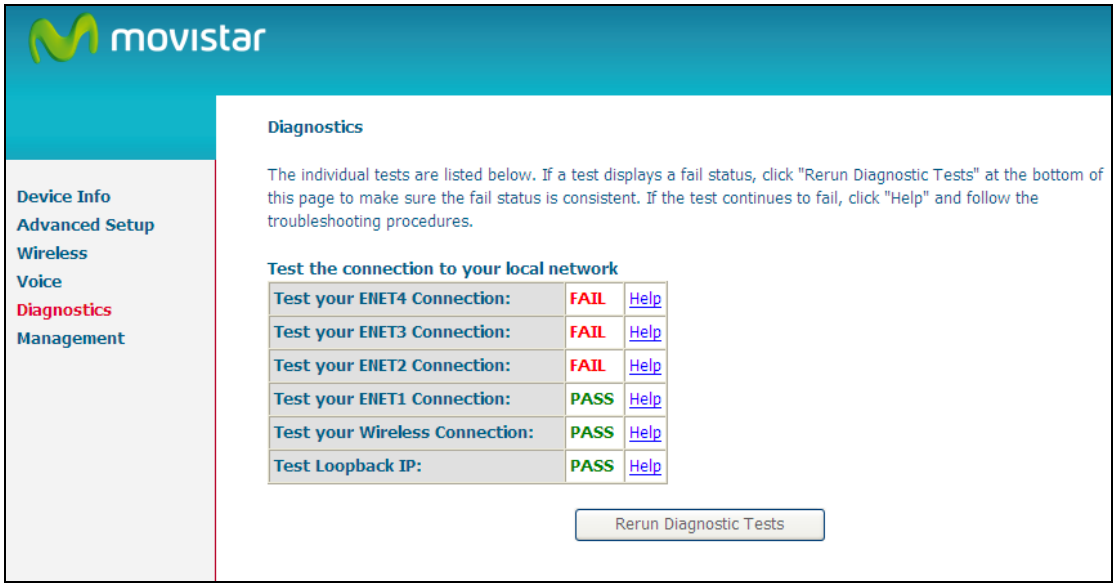
Retain a call
During conversation, to make a second call press the flash key and dial the second phone number. This action will put the first established call on hold. To switch between calls press flash key + number 2. To finish the communication with the active call press flash key + number 1. This action will reactivate the communication with the call on hold.

Conference Calling
To turn a two-party call into a three-party conference call, press flash and dial the third party. Wait for the party to answer, then press flash key + number 3. In conference mode, the conference initiator performs the audio bridge/mixing function – there are only two voice streams established.

Call Waiting
If call waiting is enabled on a line, and you hear the call waiting tone during a call, press flash key + number 2 to answer the second call. The first call is automatically placed on hold. To switch between calls, press flash key + number 2 again.

Chapter 9 Diagnostics

The first Diagnostics screen is a dashboard that shows overall connection status.
If a test displays a fail status, click the button to retest and confirm the error.
If a test continues to fail, click Help and follow the troubleshooting procedures.



Chapter 10 Management

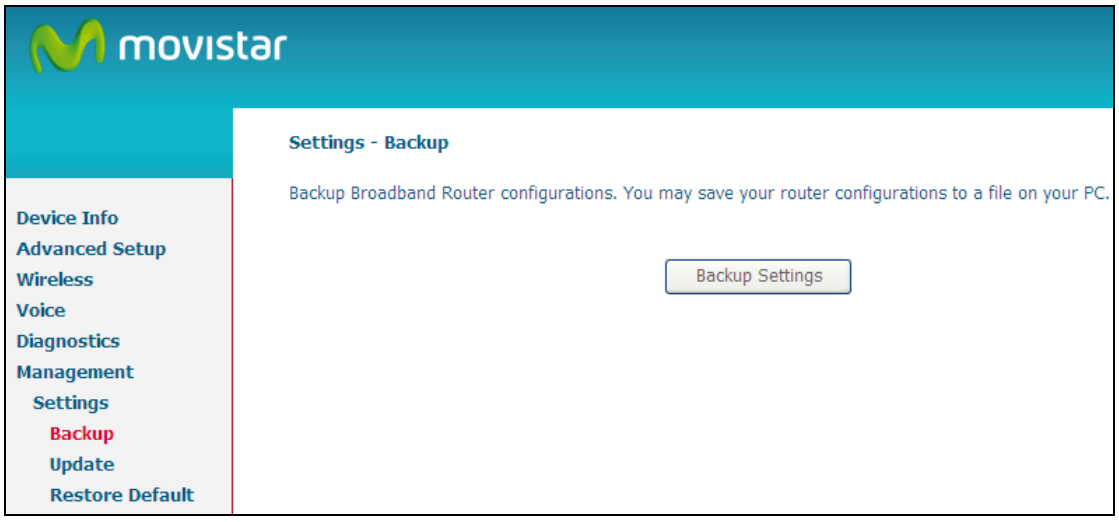
The Management menu has the following maintenance functions and processes:

10.1 Settings

This includes Backup Settings, Update Settings, and Restore Default screens.

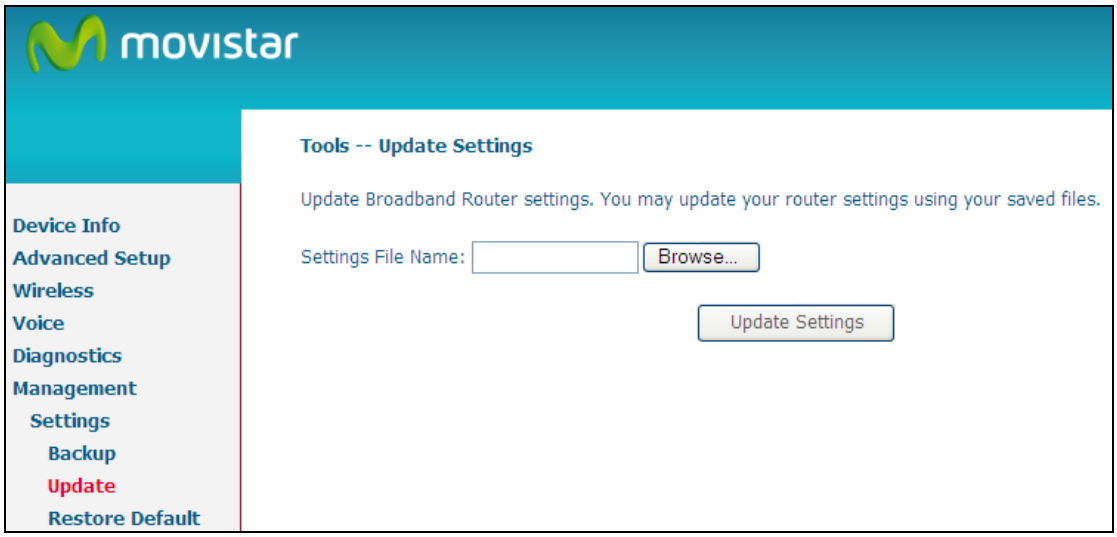
10.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for a location of the backup file. This file can later be used to recover settings on the **Update Settings** screen, as described below.



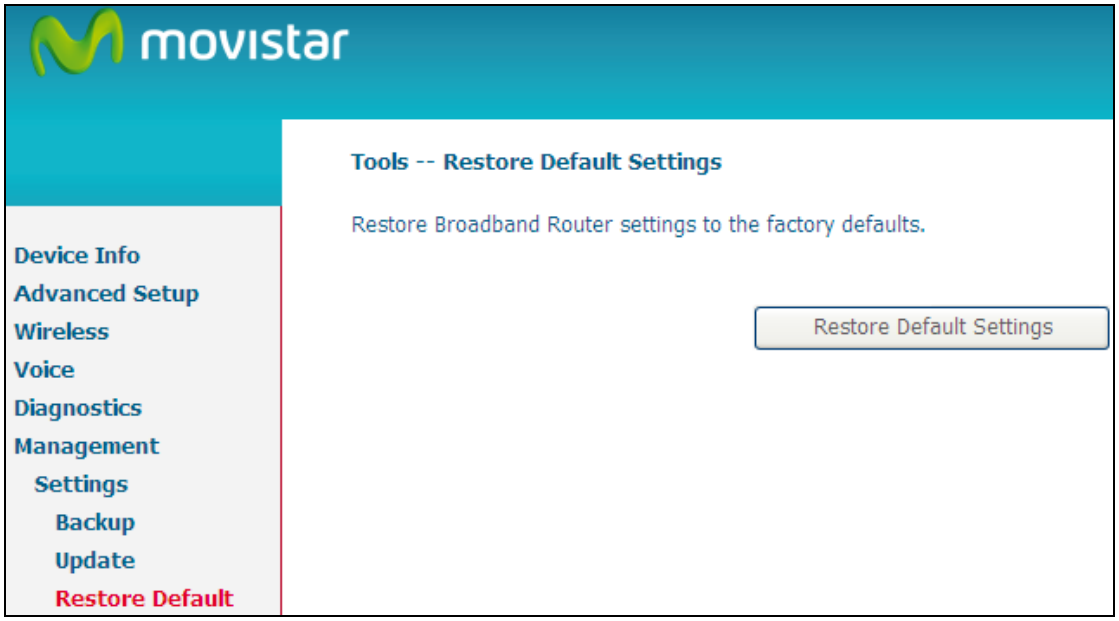
10.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Enter the file name (including folder path) in the **Settings File Name** box, or press **Browse…** to search for the file, then click **Update Settings** to recover settings.



10.1.3 Restore Default

Click **Restore Default Settings** to restore factory default settings.



After **Restore Default Settings** is clicked, the following screen appears.

DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

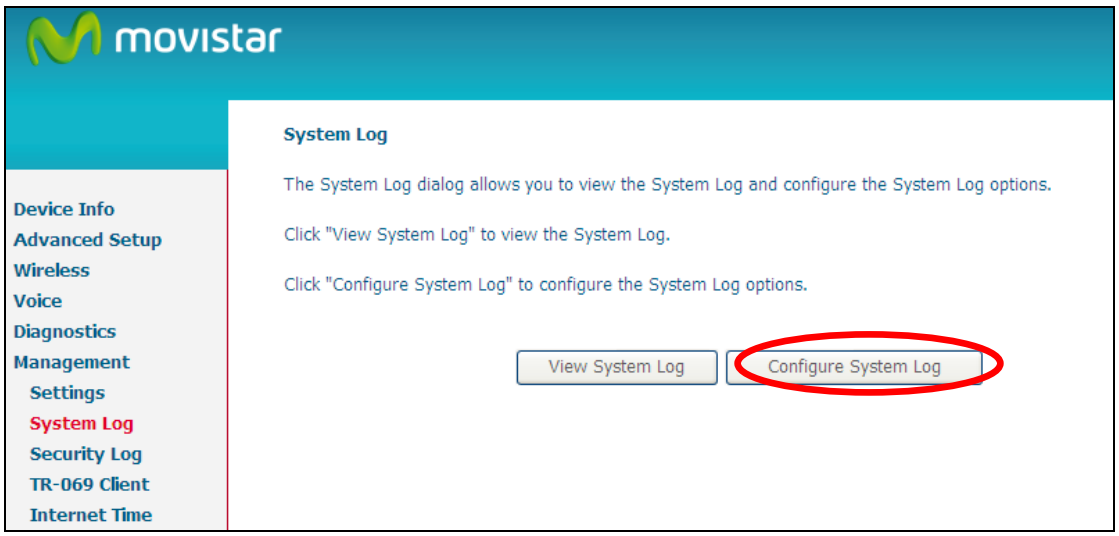
NOTE:	This entry has the same effect as the **Reset** button. The VG-8050 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for 5 seconds, the boot loader will erase the configuration data saved in flash memory.

10.2 System Log

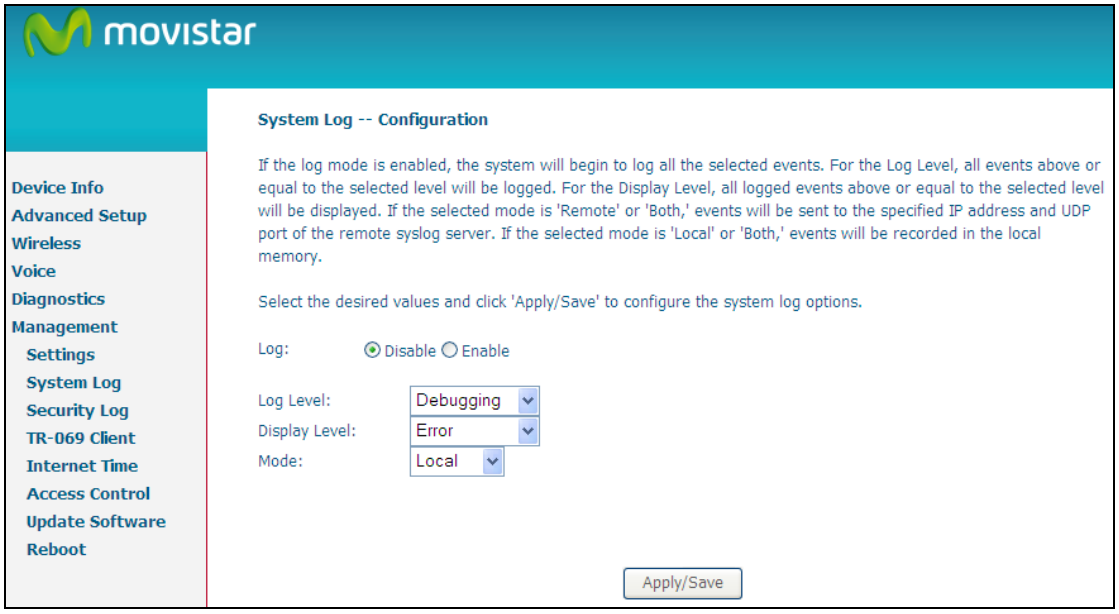
This function allows a system log to be kept and viewed upon request.

Follow the steps below to configure, enable, and view the system log.

STEP 1: Click **Configure System Log**, as shown below (circled in **Red**).



STEP 2: Select desired options and click **Apply / Save**.

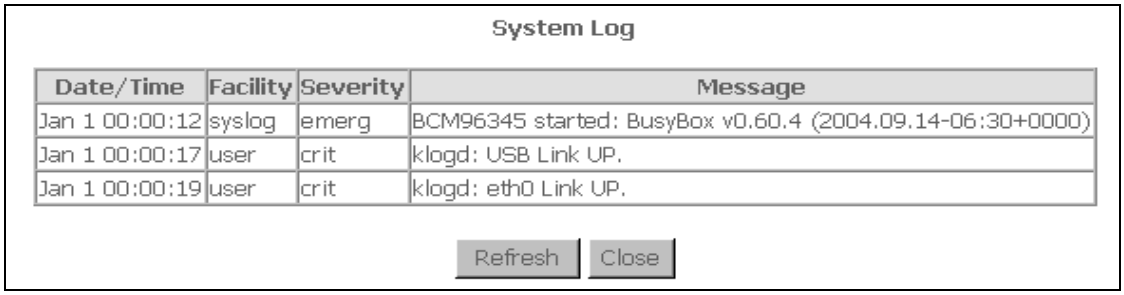


Consult the table below for detailed descriptions of each system log option.

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the **Enable** radio button and then click **Apply/Save**.
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the VG-8050 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: ☐ Emergency = system is unusable ☐ Alert = action must be taken immediately ☐ Critical = critical conditions ☐ Error = Error conditions ☐ Warning = normal but significant condition ☐ Notice= normal but insignificant condition ☐ Informational= provides information for reference ☐ Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.

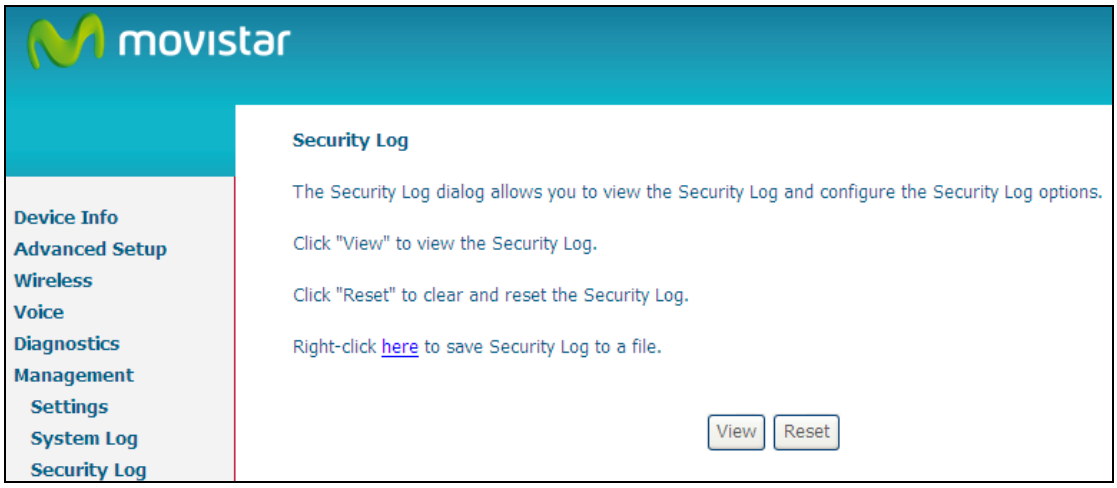
Option	Description
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

STEP 3: Click **View System Log**. The results are displayed as follows.



10.3 Security Log

The Security Log dialog allows you to view the Security Log and configure the Security Log options.

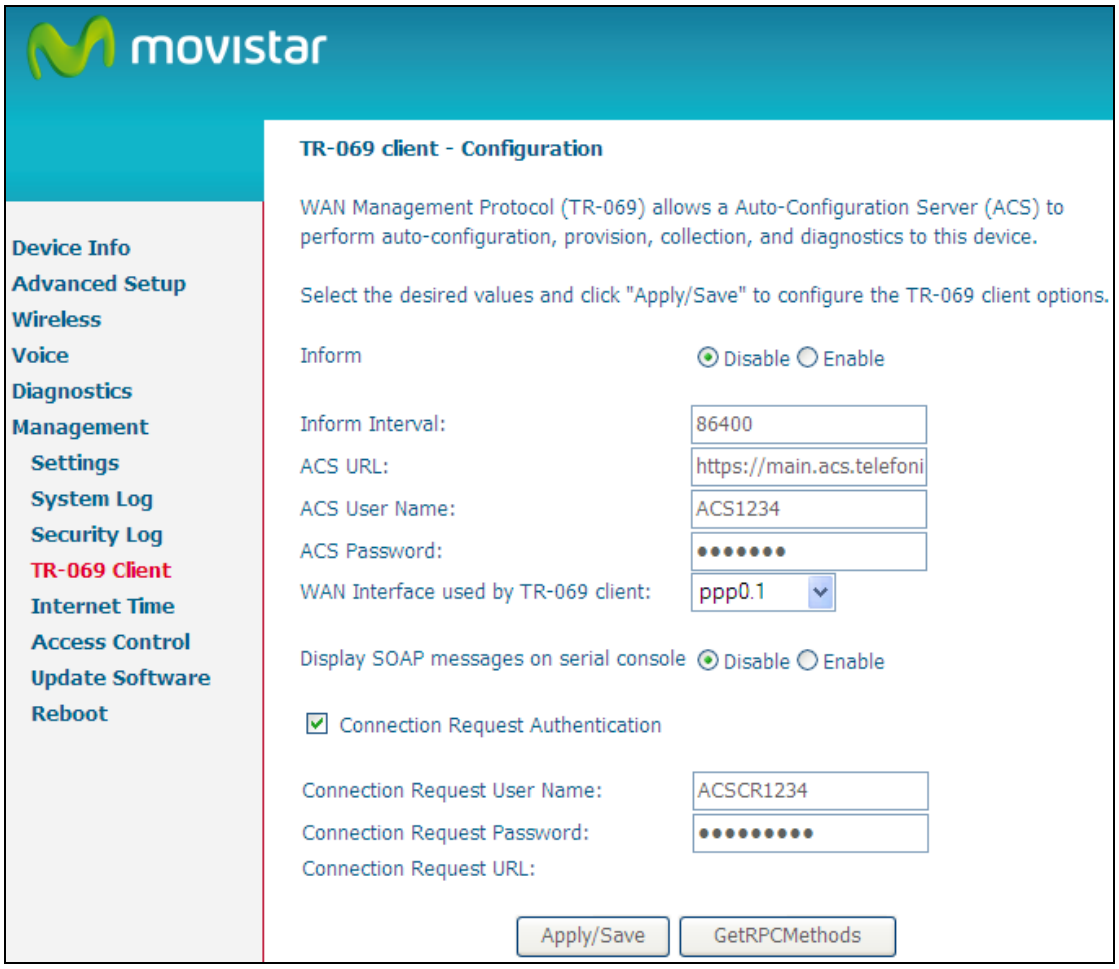


Click "View" to view the Security Log.

Click "Reset" to clear and reset the Security Log.

10.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply/Save** to configure TR-069 client options.



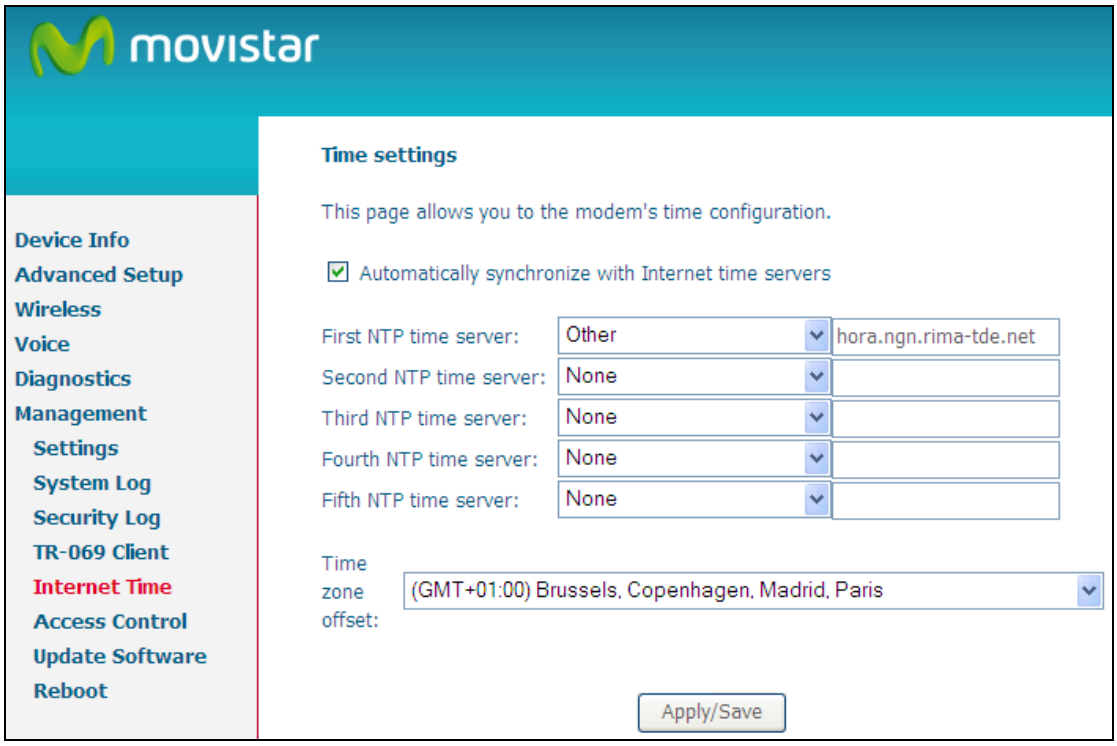
Option	Description
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The “host” portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.

Option	Description
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
Display SOAP messages on serial console	Enable/Disable SOAP messages on serial console. This option is used for advanced troubleshooting of the device.
Connection Request	
Authorization	Tick the checkbox ☑ to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	Universal Resource Locator.

The **Get RPC Methods** button forces the CPE to establish an immediate connection to the ACS. This may be used to discover the set of methods supported by the ACS or CPE. This list may include both standard TR-069 methods (those defined in this specification or a subsequent version) and vendor-specific methods. The receiver of the response MUST ignore any unrecognized methods.

10.5 Internet Time

This option automatically synchronizes the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox ☑, choose your preferred time server(s), select the correct time zone offset, and click **Save / Apply**.



NOTE:	Internet Time must be activated to use Parental Control. In addition, this menu item is not displayed when in Bridge mode since the router would not be able to connect to the NTP timeserver.

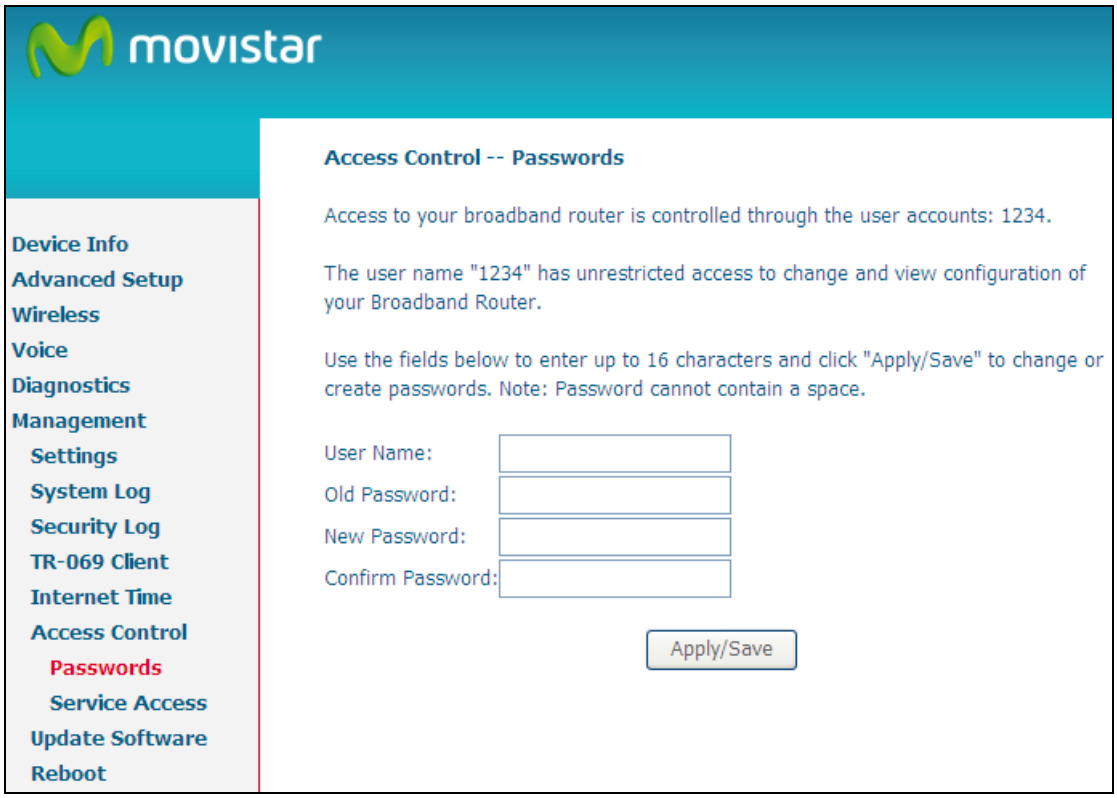
10.6 Access Control

10.6.1 Passwords

This screen is used to configure the user account access passwords for the device. Access to the VG-8050 is controlled through the following three user accounts:

☐ **1234** - this has unrestricted access to change and view the configuration.

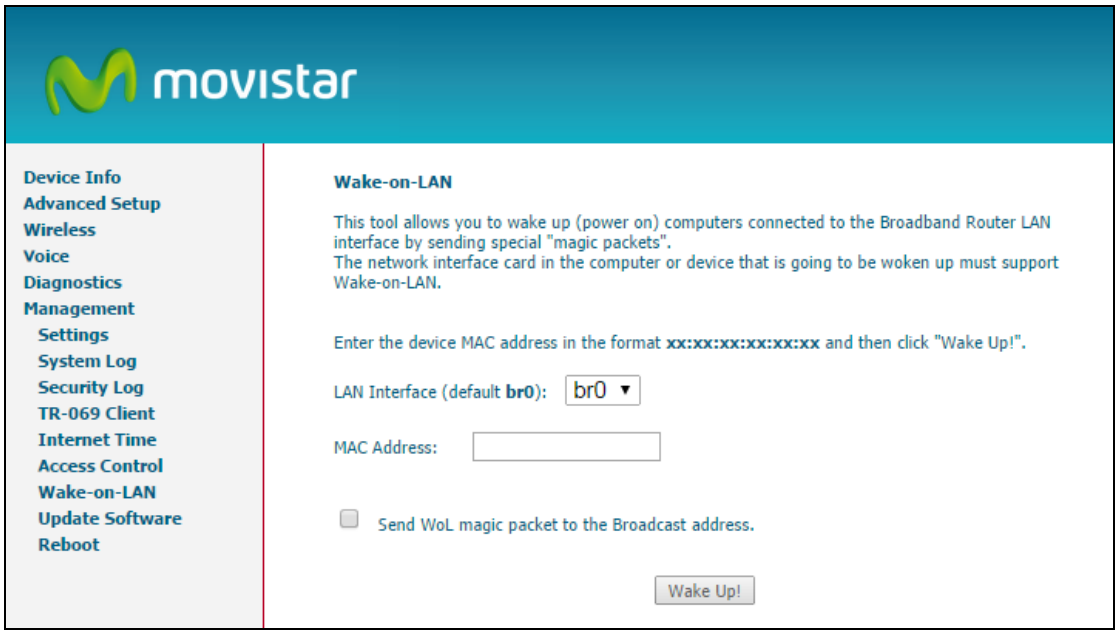
Use the fields below to change password settings. Click **Save / Apply** to continue.



NOTE: Passwords must be 16 characters or less.

10.7 Wake-on LAN

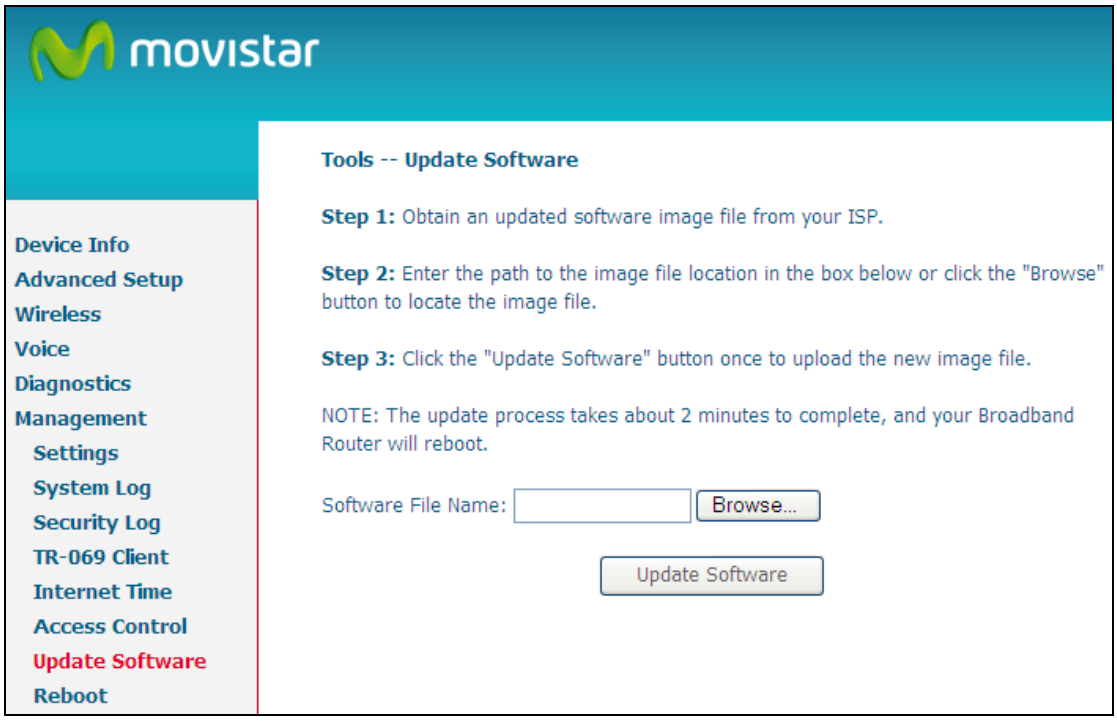
This tool allows you to wake up (power on) computers connected to the Broadband Router LAN interface by sending special "magic packets".



Enter the device MAC address (format xx:xx:xx:xx:xx:xx) of the device you wish to wake up by sending a magic packet and then click the button **Wake Up!**.

10.8 Update Software

This option allows for firmware upgrades from a locally stored file.



STEP 1: Obtain an updated software image file from your ISP.

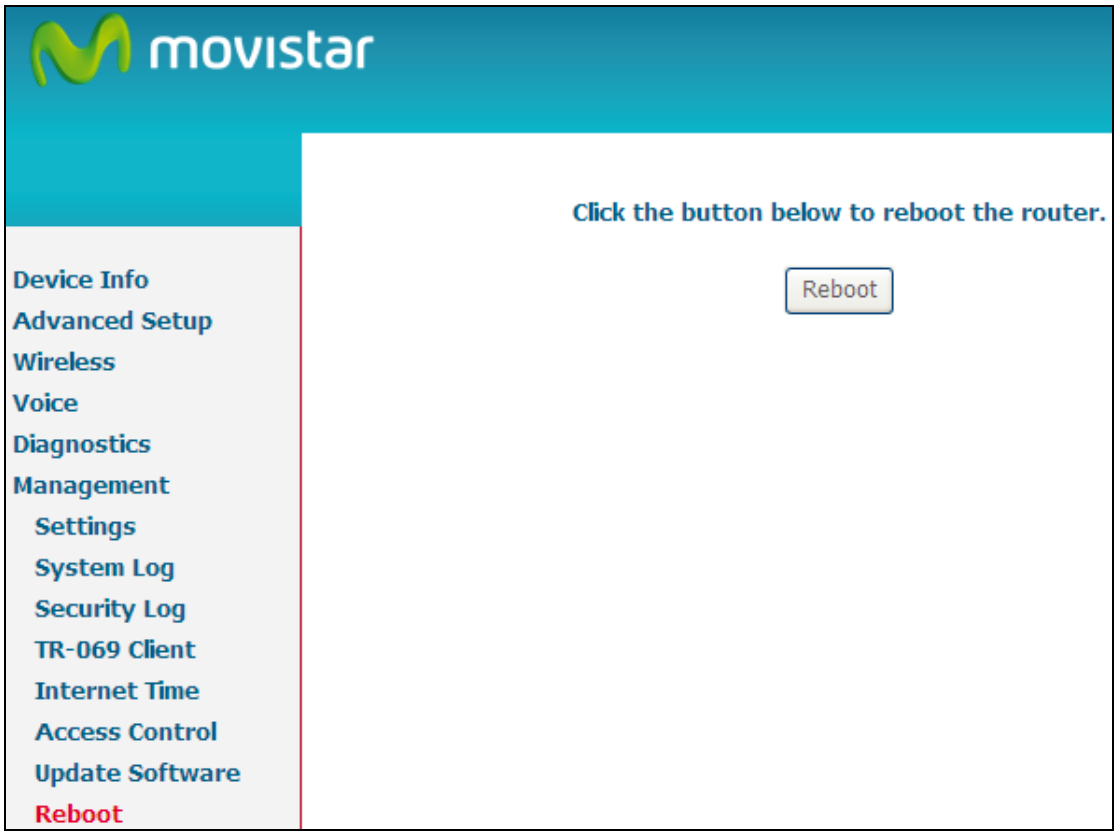
STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 3: Click the **Update Software** button once to upload and install the file.

NOTE:	The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** at the top of the Device Information screen with the firmware version installed, to confirm the installation was successful.

10.9 Reboot

To save the current configuration and reboot the router, click **Save/Reboot**.



NOTE: You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.

Appendix A – Specifications

Hardware Interface

RJ-45 X 4 for GigaLAN, RJ-45 X 4 for GigaWAN, FXS X 1, Reset Button X 1, Power switch X 1, 11n 2.4GHz WiFi On-Off/WPS button X 1, Wi-Fi external Antenna X 2, FXS X 1

LAN Interface

Standard.....IEEE 802.3, IEEE 802.3u
10/100 BaseT .....Auto-sense
MDI/MDX support.....Yes

WLAN Interface

Standard .....IEEE802.11n (IEEE802.11b/g compatible)
Encryption.....64/128-bit Wired Equivalent Privacy (WEP)
Channels.....11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate.....Up to 300Mbps at 2.4GHz
Bandwidth 20MHz/40MHz
WPA/WPA2 .....Yes
IEEE 802.1x .....Yes
Tx Beamforming.....Yes
WMM .....Yes

Management

Telnet, Web-based management, Configuration backup and restoration, Software upgrade via HTTP / TFTP / FTP server

Routing Functions

PPPoE, IPoA, Static route, NAT/PAT, DHCP Server/Client, DNS Relay, ARP

Security Functions

Authentication protocol: PAP, CHAP
Port Triggering/Forwarding, Packet filtering, SSH, Access Control,

Voice

SIP .....RFC 3261
Codec G.711, G.723.1, G.726, G.729ab
RTP .....RFC 1889
SDP .....RFC 2327
Caller ID .....ETSI based
Echo cancellation G.168
Silence suppression: Yes
Life line/Emergency call: Yes

Application Passthrough

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box

Power Supply .....Input: 100 - 240 Vac
Output: 12 Vdc / 1 A

Environment Condition

Operating temperature .....0 ~ 50 degrees Celsius
Relative humidity .....5 ~ 95% (non-condensing)

Dimensions .....280mm(W) x 48mm(H) x 210mm(D)

Kit Weight

(1* VG-8050, 1* RJ-11 cable, 1* RJ-45 cable, 1* Power Adapter, 1* CD-ROM) =1KG

Certifications..... CE

NOTE: Specifications are subject to change without notice

Appendix B – Pin Assignments

ETHERNET Ports (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix C – SSH Client

Unlike Microsoft Windows, Linux OS has a ssh client included. For Windows users, there is a public domain one called "putty" that can be downloaded from here:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the ssh client you must first enable SSH access for the LAN or WAN from the Management → Access Control → Services menu in the web user interface.

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

For WAN access, type: ssh -l support *WAN IP address*

To access the router using the Windows "putty" ssh client

For LAN access, type: putty -ssh -l root 192.168.1.1

For WAN access, type: putty -ssh -l support *WAN IP address*

NOTE: The *WAN IP address* can be found on the Device Info → WAN screen

Appendix D – Firewall

STATEFUL PACKET INSPECTION
Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

DENIAL OF SERVICE ATTACK
Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/PORT/INTERFACE FILTER
These rules help in the filtering of traffic at the Network layer (i.e. Layer 3). When a Routing interface is created, **Enable Firewall** must be checked. Navigate to Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER
Helps in setting rules to DROP packets from the LAN interface. By default, if the Firewall is Enabled, all IP traffic from the LAN is allowed. By setting up one or more filters, specific packet types coming from the LAN can be dropped.

Example 1:

Filter Name	: Out_Filter1
Protocol	: TCP
Source IP address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA

This filter will Drop all TCP packets coming from the LAN with IP Address/Subnet Mask of 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

Example 2:

Filter Name	: Out_Filter2
Protocol	: UDP
Source IP Address	: 192.168.1.45
Source Subnet Mask	: 255.255.255.0
Source Port	: 5060:6060
Dest. IP Address	: 172.16.13.4
Dest. Subnet Mask	: 255.255.255.0
Dest. Port	: 6060:7070

This filter will drop all UDP packets coming from the LAN with IP Address / Subnet Mask of 192.168.1.45/24 and a source port range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port range of 6060 to 7070.

INCOMING IP FILTER
Helps in setting rules to Allow or Deny packets from the WAN interface. By default, all incoming IP traffic from the WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, specific packet types coming from the WAN can be Accepted.

Example 1:

Filter Name	: In_Filter1
Protocol	: TCP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA
Selected WAN interface	: br0

This filter will ACCEPT all TCP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 with a source port of 80, irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:

Filter Name	: In_Filter2
Protocol	: UDP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. IP Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070
Selected WAN interface	: br0

This rule will ACCEPT all UDP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC LAYER FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective in Bridge mode. After a Bridge mode connection is created, navigate to Advanced Setup → Security → MAC Filtering in the WUI.

Example 1:

Global Policy	: Forwarded
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: NA
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule drops all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address. All other frames on this interface are forwarded.

Example 2:

Global Policy	: Blocked
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: 00:34:12:78:90:56
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule forwards all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56. All other frames on this interface are dropped.

DAYTIME PARENTAL CONTROL

This feature restricts access of a selected LAN device to an outside Network through the VG-8050, as per chosen days of the week and the chosen times.

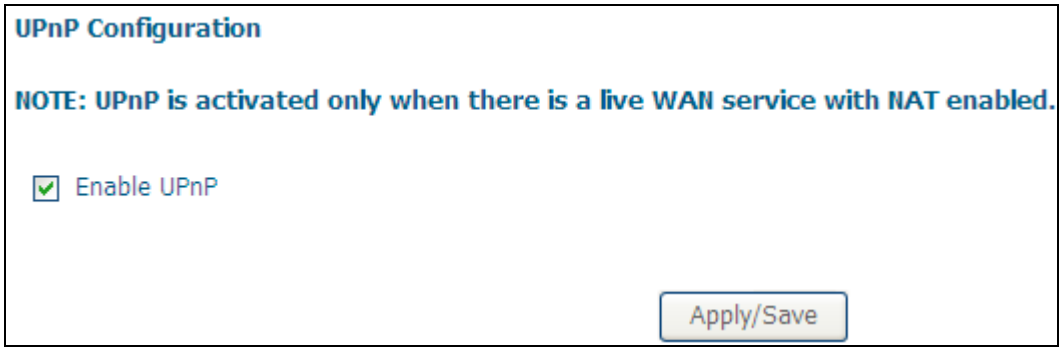
Example:		
	User Name	: FilterJohn
	Browser's MAC Address	: 00:25:46:78:63:21
	Days of the Week	: Mon, Wed, Fri
	Start Blocking Time	: 14:00
	End Blocking Time	: 18:00

With this rule, a LAN device with MAC Address of 00:25:46:78:63:21 will have no access to the WAN on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and times, this device will have access to the outside Network.

Appendix E – WPS External Registrar

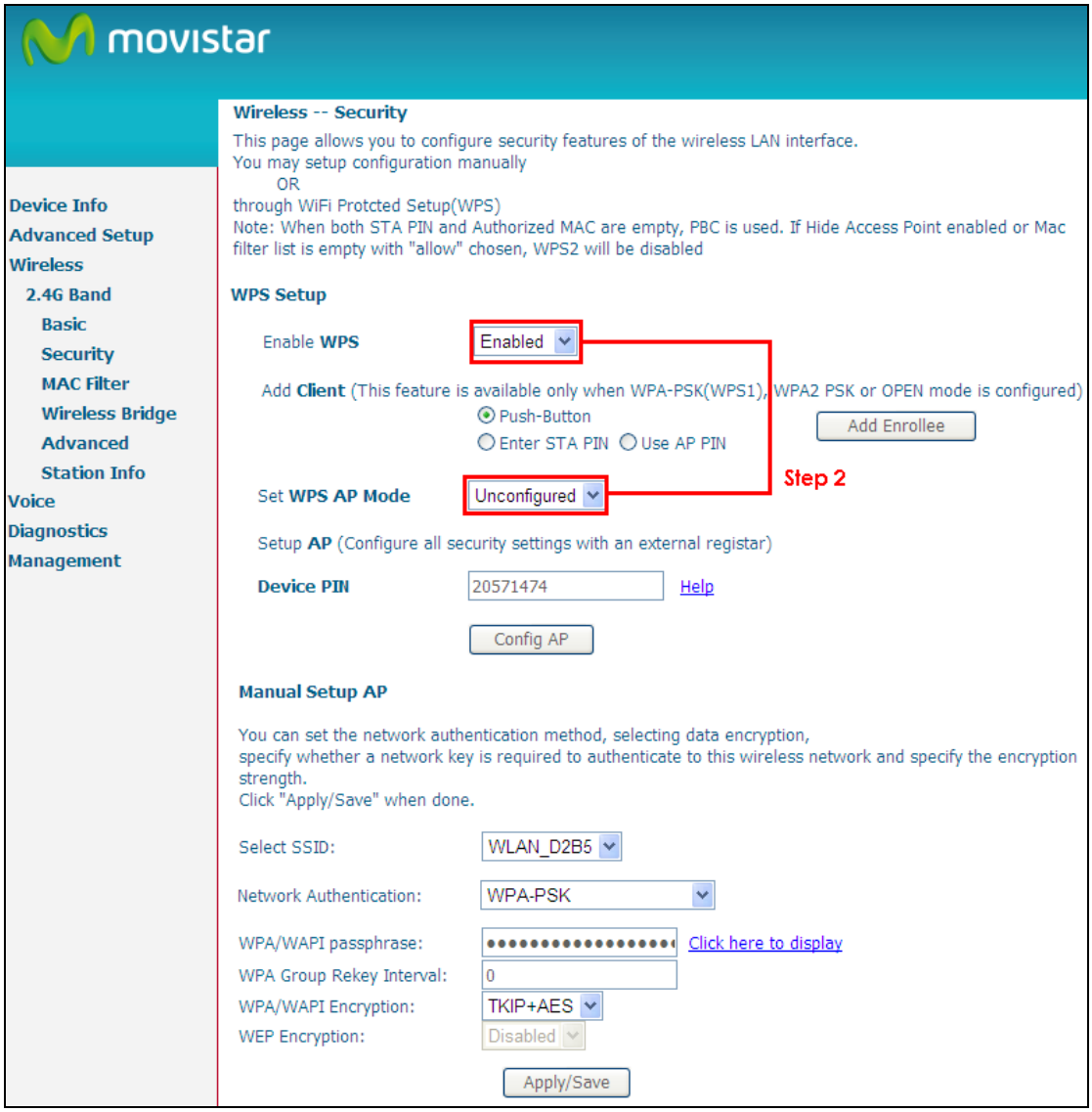
Follow these steps to add an external registrar using the web user interface (WUI) on a personal computer running the Windows Vista operating system:

Step 1: Enable UPnP on the Advanced Setup → Upnp screen in the WUI.

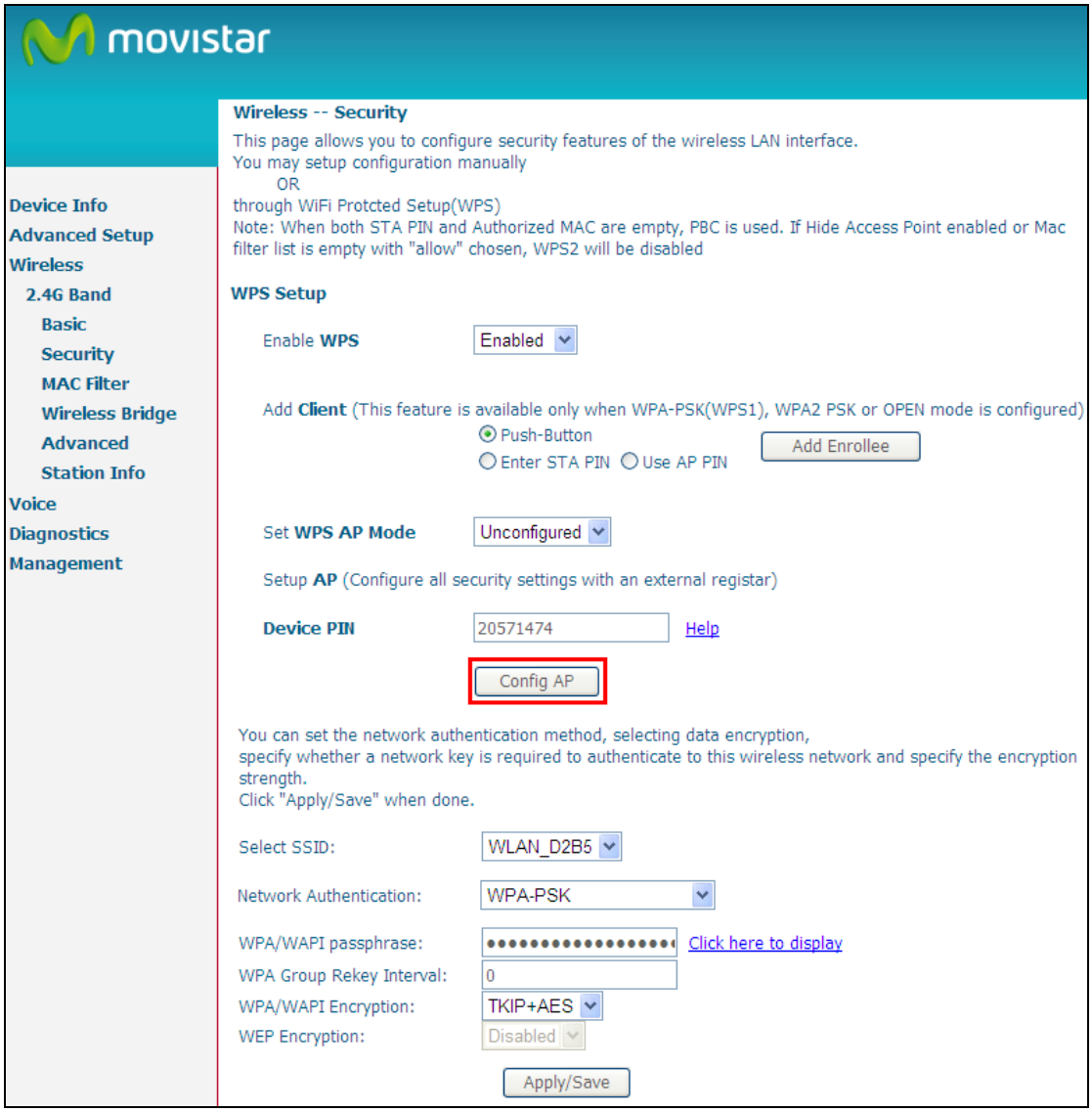


NOTE: A PVC must exist and NAT enabled to see this option.

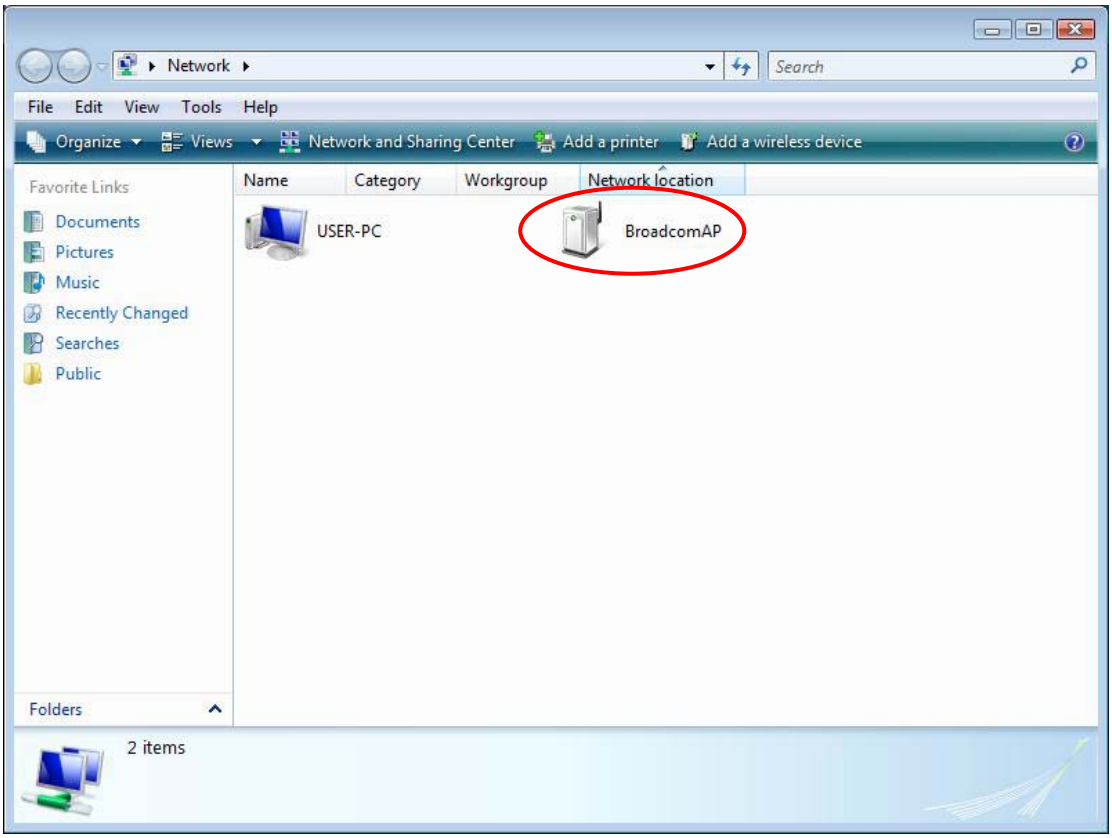
Step 2: On the Wireless → Security screen (2.4G Band), enable WPS by selecting **Enabled** from the drop down list box and set the WPS AP Mode to **Unconfigured**. Click the **Apply / Save** button at the bottom of the screen to save your new wireless security settings.


movistar
Device Info
Advanced Setup
Wireless
2.4G Band
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Voice
Diagnostics
Management
Wireless -- Security
This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled
WPS Setup
Enable WPS
Enabled
Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)
Push-Button
Enter STA PIN
Use AP PIN
Add Enrollee
Step 2
Set WPS AP Mode
Unconfigured
Setup AP (Configure all security settings with an external registar)
Device PIN
20571474
Help
Config AP
Manual Setup AP
You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.
Select SSID:
WLAN_D2B5
Network Authentication:
WPA-PSK
WPA/WAPI passphrase:
Click here to display
WPA Group Rekey Interval:
0
WPA/WAPI Encryption:
TKIP+AES
WEP Encryption:
Disabled
Apply/Save

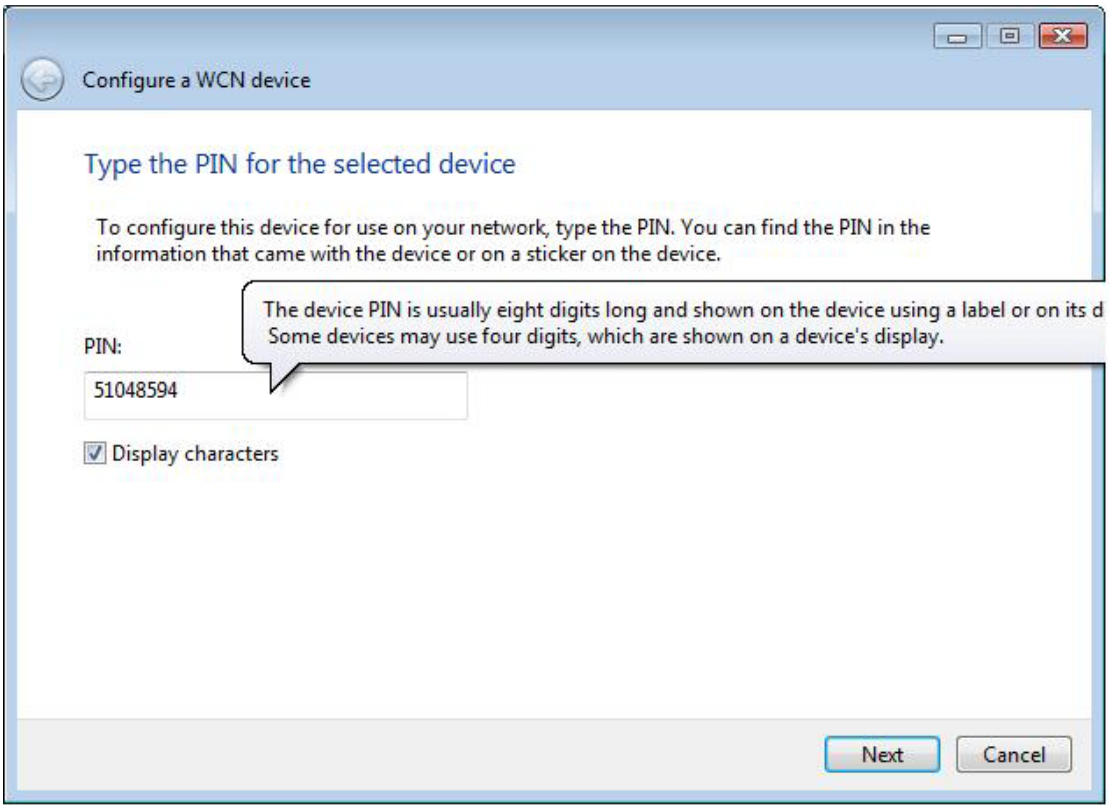
Step 3: When the screen refreshes, click the **ConfigAP** button.



Step 4: Open the Network folder in Vista and look for the BroadcomAP icon.



Step 5: Now return to the Network folder and click the BroadcomAP icon. A dialog box will appear asking for the Device PIN number. Enter the Device PIN as shown on the Wireless → Security screen. Click **Next**.



Step 6: Windows Vista will attempt to configure the wireless security settings.

Step 7: If successful, the security settings will match those in Windows Vista.

Appendix F - Connection Setup

Creating a WAN connection is a two-stage process.

1 - Setup a Layer 2 Interface (ATM, PTM or Ethernet).
2 - Add a WAN connection to the Layer 2 Interface.

The following sections describe each stage in turn.

F1 ~ Layer 2 Interfaces

Every layer2 interface operates in one of three modes: Default, VLAN Mux or MSC. A short introduction to each of these three modes is included below for reference. It is important to understand the differences between these connection modes, as they determine the number and types of connections that may be configured.

DEFAULT MODE

In this mode there is a 1:1 relationship between interfaces and WAN connections, in that an interface in default mode supports just one connection. However, unlike the multiple connection modes described below, it supports all five connection types. The figure below shows the connection type available in ETH default mode.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	IPv6 Unnumbered Model	Connect/Disconnect	Remove	Edit
eth0.3	br_eth0	Bridge	N/A	N/A	Disabled	N/A	Disabled	Disabled	Disabled	Disabled	Disabled	☐	Edit

VLAN MUX MODE

This mode uses VLAN tags to allow for multiple connections over a single interface. PPPoE, IPoE, and Bridge are supported while PPPoA and IPoA connections are not. The figure below shows multiple connections over a single VLAN Mux interface.

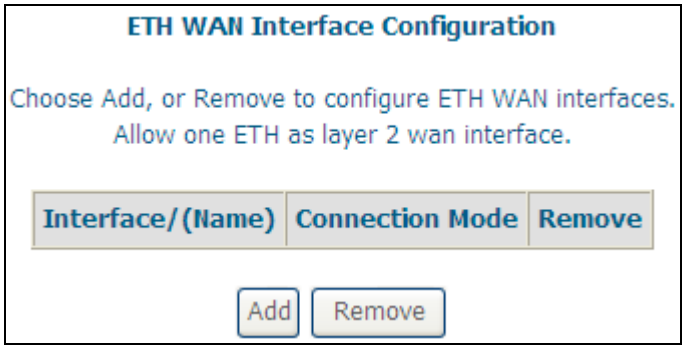
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	IPv6 Unnumbered Model	Connect/Disconnect	Remove	Edit
eth0.2	3	IPoE	4	3	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	☐	Edit
ppp0.1	6	PPPoE	1	6	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	☐	Edit

F1.1 Ethernet WAN Interface

Some models of the VG-8050 support a single Ethernet WAN interface over the ETH WAN port. Follow these procedures to configure an Ethernet WAN interface.

NOTE:	To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

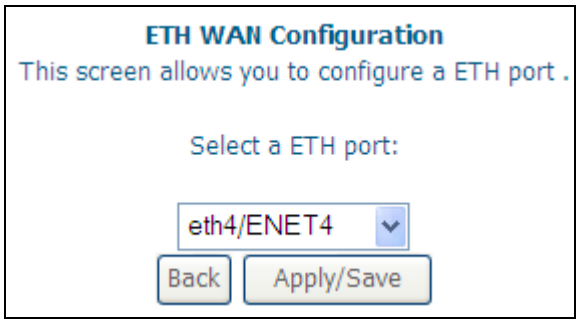
STEP 1: Go to Advanced Setup → Layer2 Interface → ETH Interface.



This table is provided here for ease of reference.

Heading	Description
Interface/ (Name)	ETH WAN Interface
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection
Remove	Select the checkbox and click **Remove** to remove the connection.

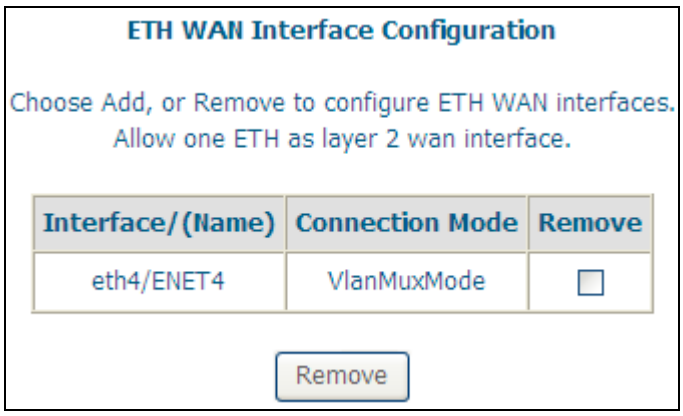
STEP 2: Click **Add** to proceed to the next screen.



STEP 3: Select a Connection Mode from the options shown above.

STEP 4: Click **Apply/Save** to confirm your choice.

The figure below shows an Ethernet WAN interface configured in Default Mode.



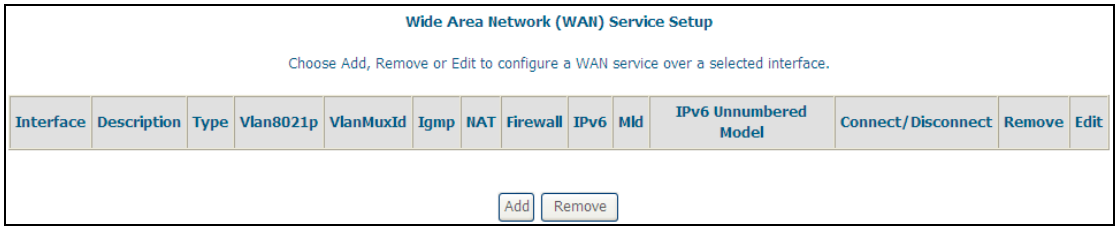
To add a WAN connection go to G2 ~ WAN Connections.

F2 ~ WAN Connections

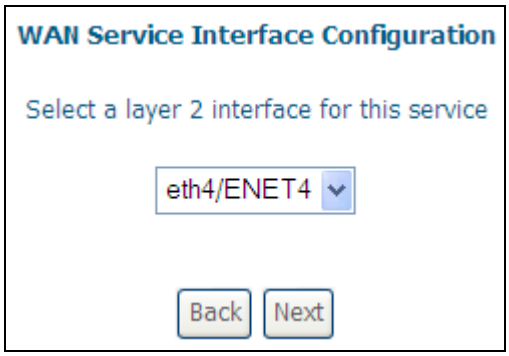
In Default Mode, the VG-8050 supports one WAN connection for each interface, up to a maximum of 8 connections. VLAN Mux and MSC support up to 16 connections.

To setup a WAN connection follow these instructions.

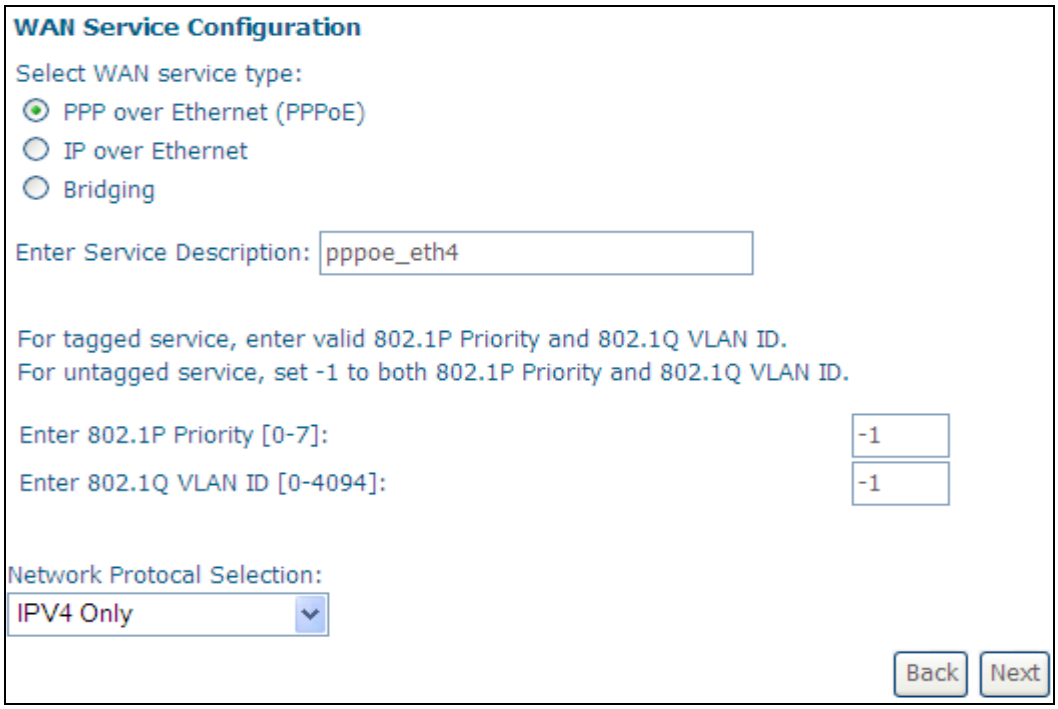
STEP 1: Go to the Advanced Setup → WAN Service screen.



STEP 2: Click **Add** to create a WAN connection. The following screen will display.



STEP 3: Choose a layer 2 interface from the drop-down box and click **Next**. The WAN Service Configuration screen will display as shown below.



NOTE:	The WAN services shown here are those supported by the layer 2 interface you selected in the previous step. If you wish to change your selection click the **Back** button and select a different layer 2 interface.

STEP 4: For VLAN Mux Connections only, you must enter Priority & VLAN ID tags.

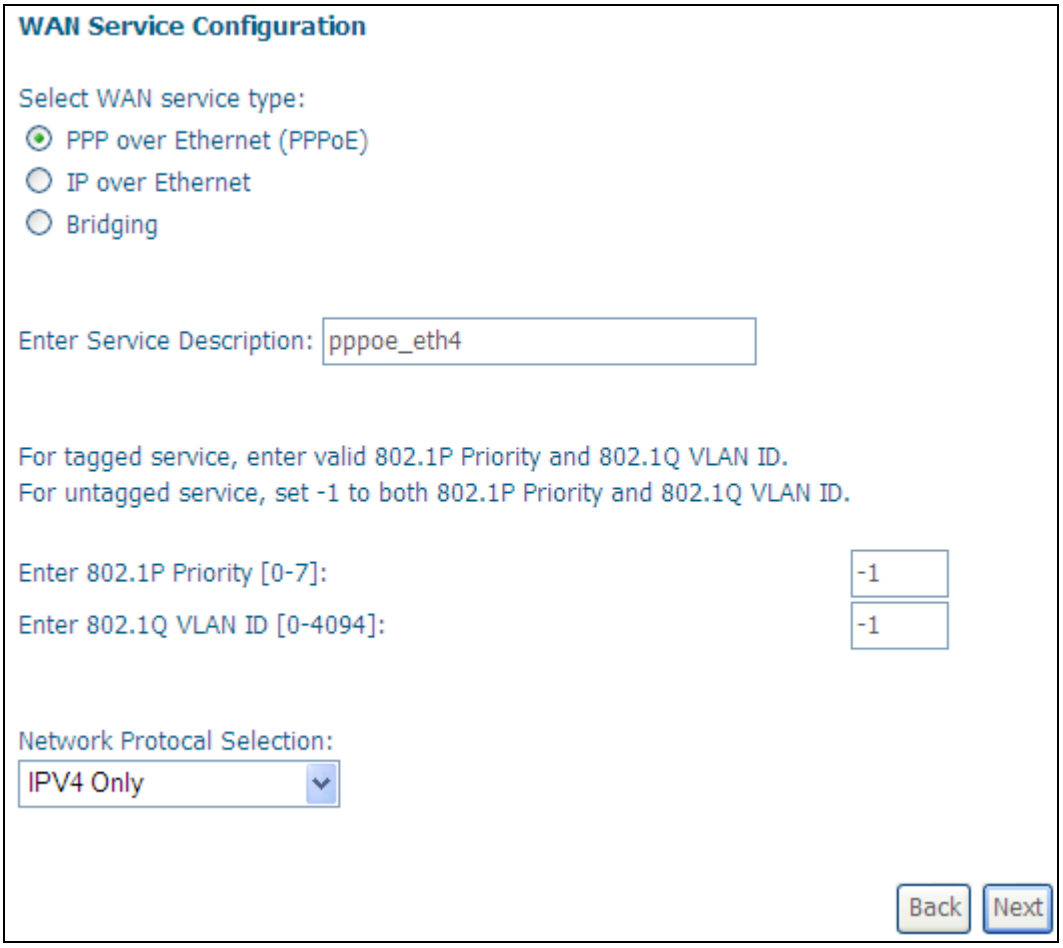
STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(1) For G2.1 PPP over ETHERNET (PPPoE), go to page 109.
(2) For G2.2 IP over ETHERNET (IPoE), go to page 115.
(3) For G2.3 Bridging, go to page 119.

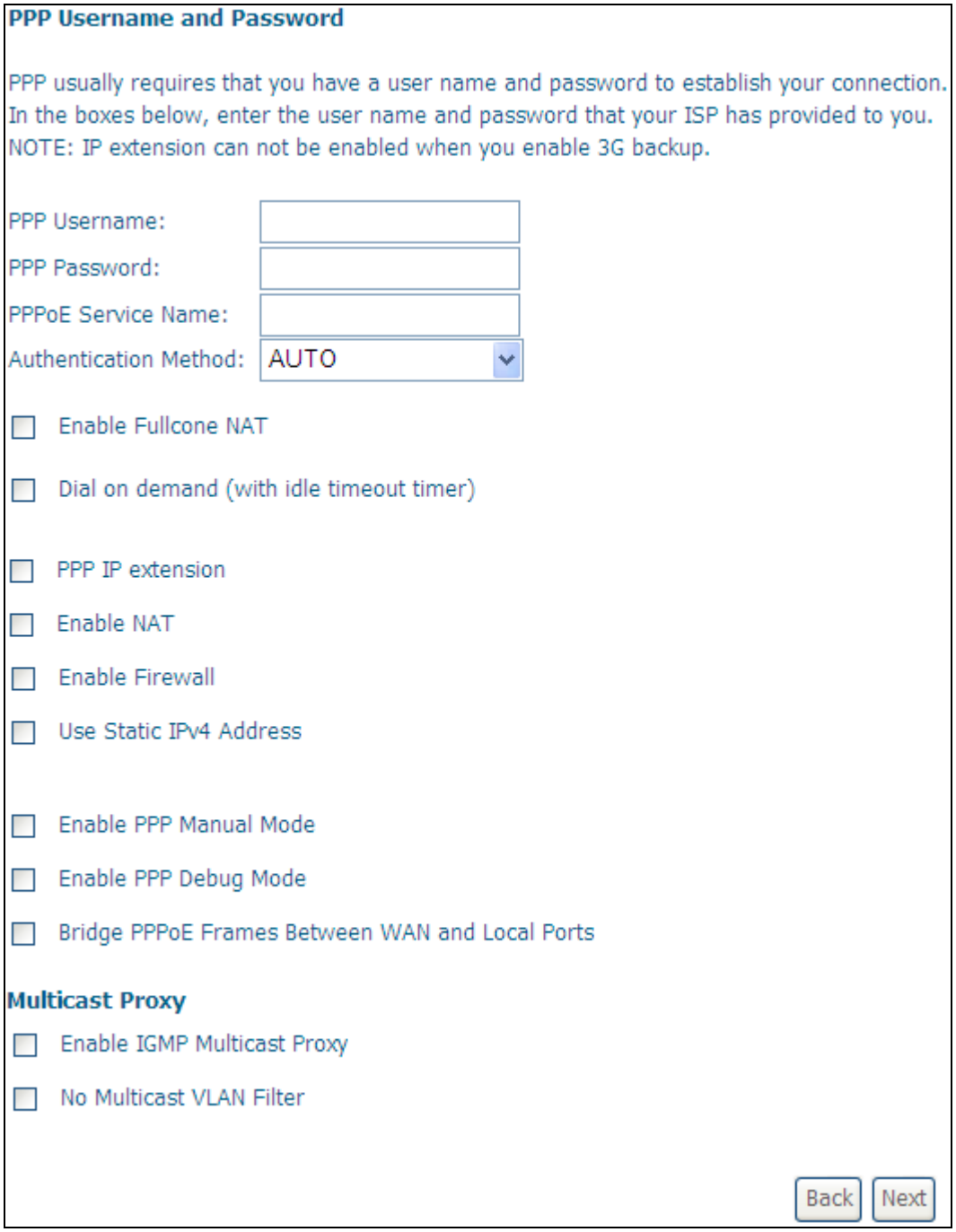
The subsections that follow continue the WAN service setup procedure.

F2.1 PPP over ETHERNET (PPPoE)

STEP 1: Select the PPP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.



STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.

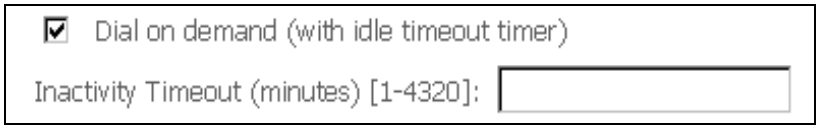


The settings shown above are described below.

PPP SETTINGS
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND
The VG-8050 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



PPP IP EXTENSION
The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specifically requires this setup, do not select it.

PPP IP Extension does the following:

- ☐ Allows only one PC on the LAN.
- ☐ Disables NAT and Firewall.
- ☐ The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- ☐ The device extends the IP subnet at the remote service provider to the LAN PC. i.e. the PC becomes a host belonging to the same IP subnet.
- ☐ The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.
- ☐ The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.

ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IPv4 Address** field. Don't forget to adjust the IP configuration to Static IP Mode as described in 3.2 IP Configuration.

ENABLE PPP MANUAL MODE
Use this button to manually connect/disconnect PPP sessions.

ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

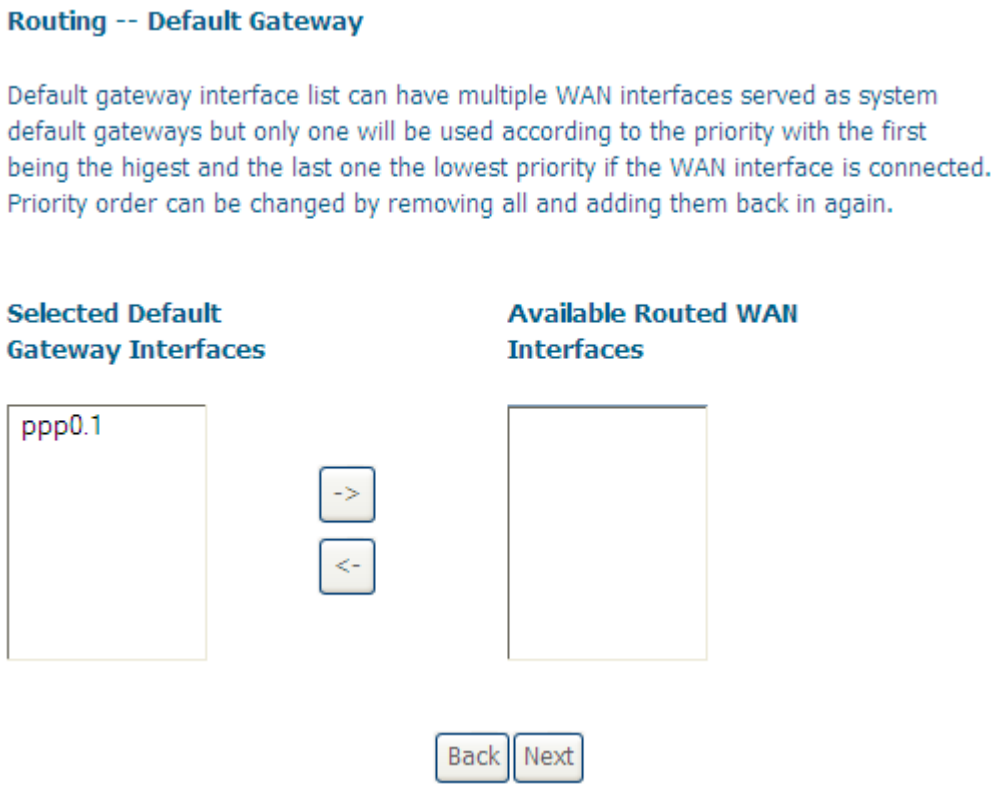
BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS
(This option is hidden when PPP IP Extension is enabled)
When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The VG-8050 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE IGMP MULTICAST PROXY
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

ENABLE MLD MULTICAST PROXY
This option displays when IPv6 is enabled. Tick the checkbox ☑ to enable Multicast Listener Discovery (MLD). This protocol is used by IPv6 hosts to report their multicast group memberships to any neighboring multicast routers.

NO MULTICAST VLAN FILTER
Tick the checkbox ☑ to Enable/Disable multicast VLAN filter.

STEP 3: Choose an interface to be the default gateway.

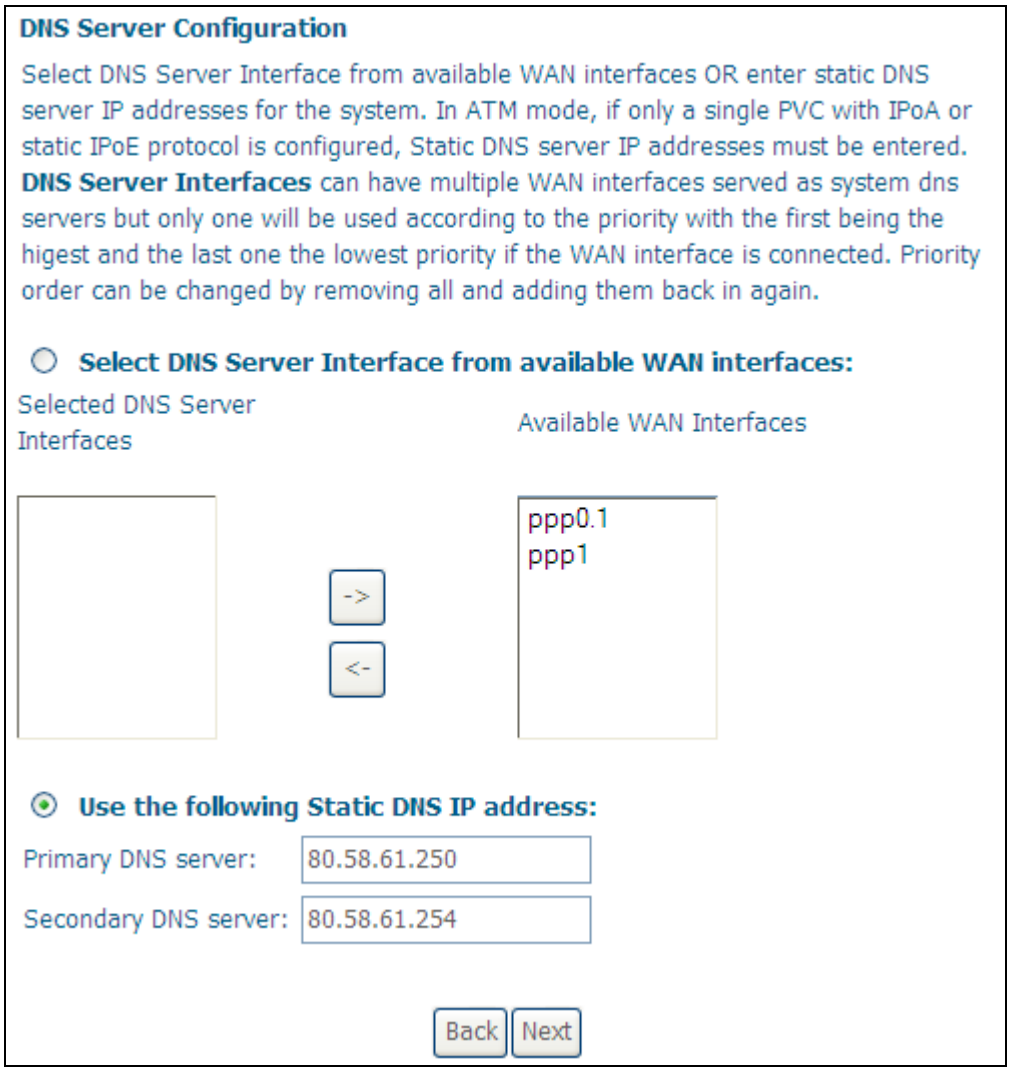


Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. Click **Next** to continue or click **Back** to return to the previous step.

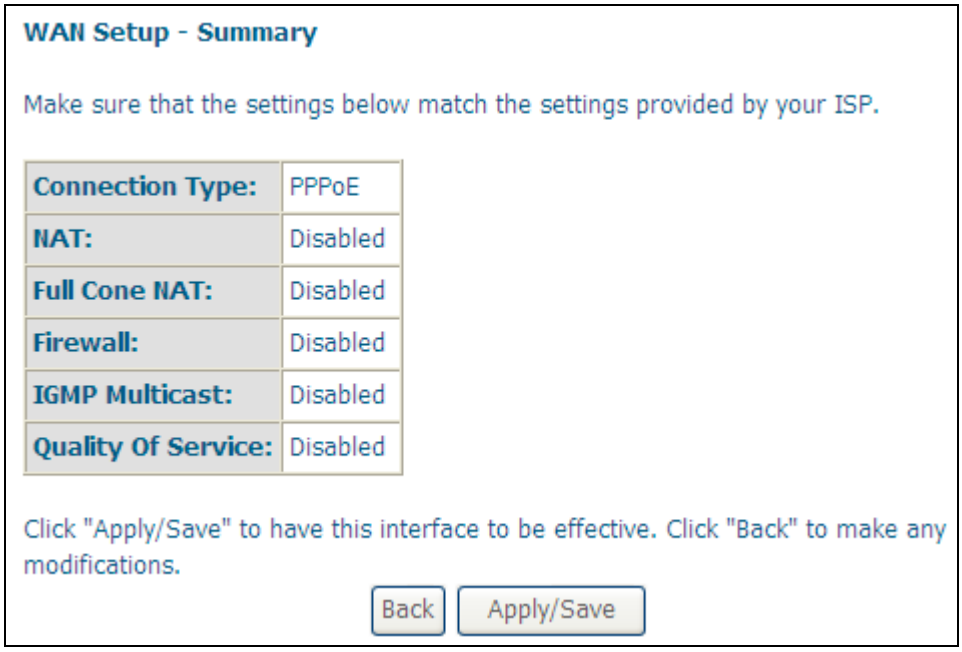
Note: In ATM mode, if only a single PVC with IPoA or static IPoE protocol is

configured, Static DNS server IP addresses must be entered.



STEP 5: Click **Next** to continue or click **Back** to return to the previous step.

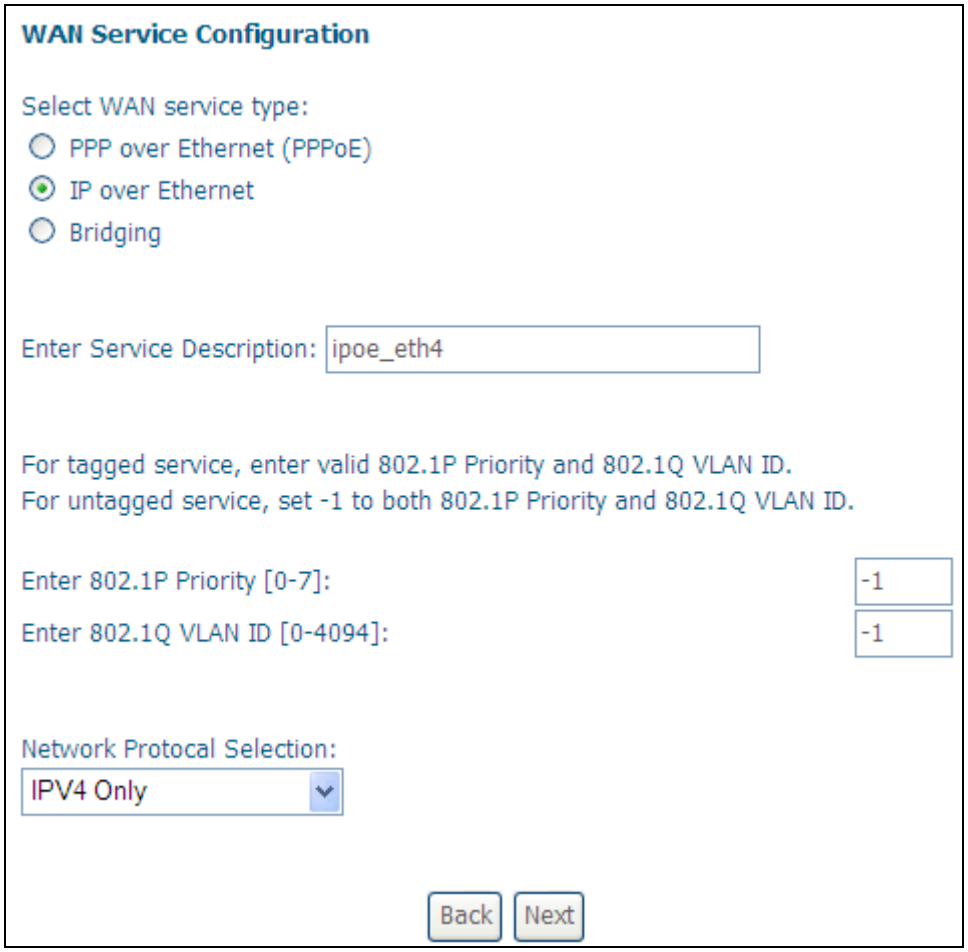
STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to modify them.



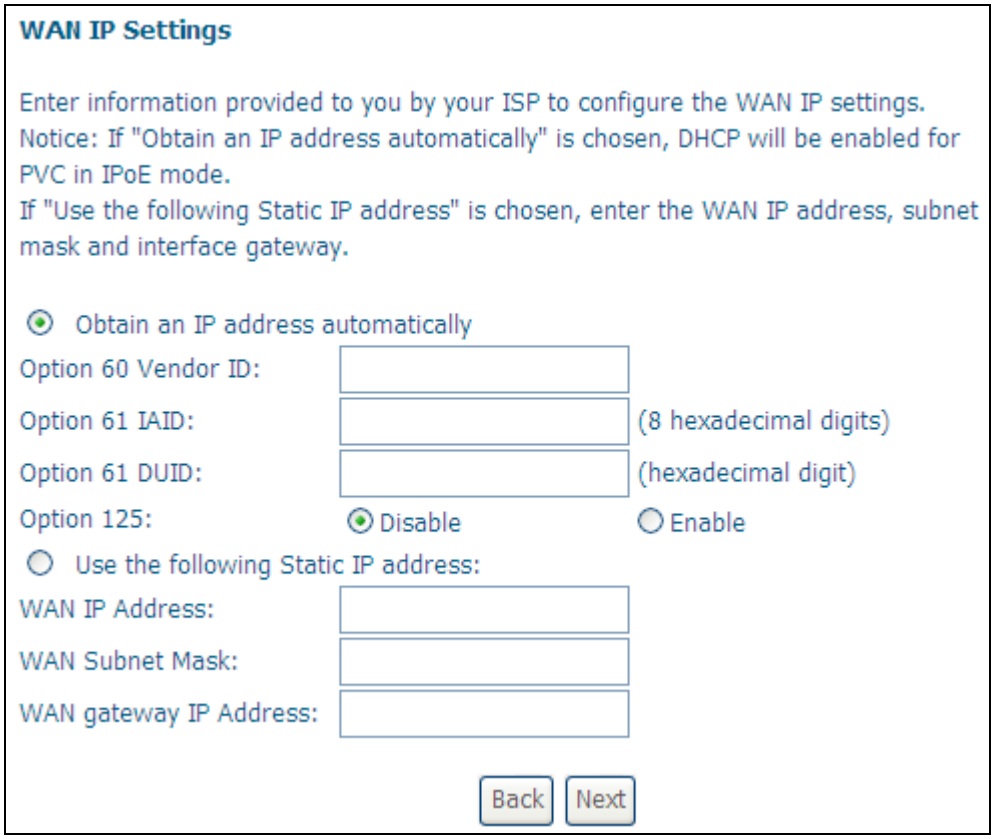
After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

F2.2 IP over ETHERNET (IPoE)

STEP 1: Select the IP over Ethernet radio button and click **Next**. You can also enable IPv6 by ticking the checkbox ☑ at the bottom of this screen.

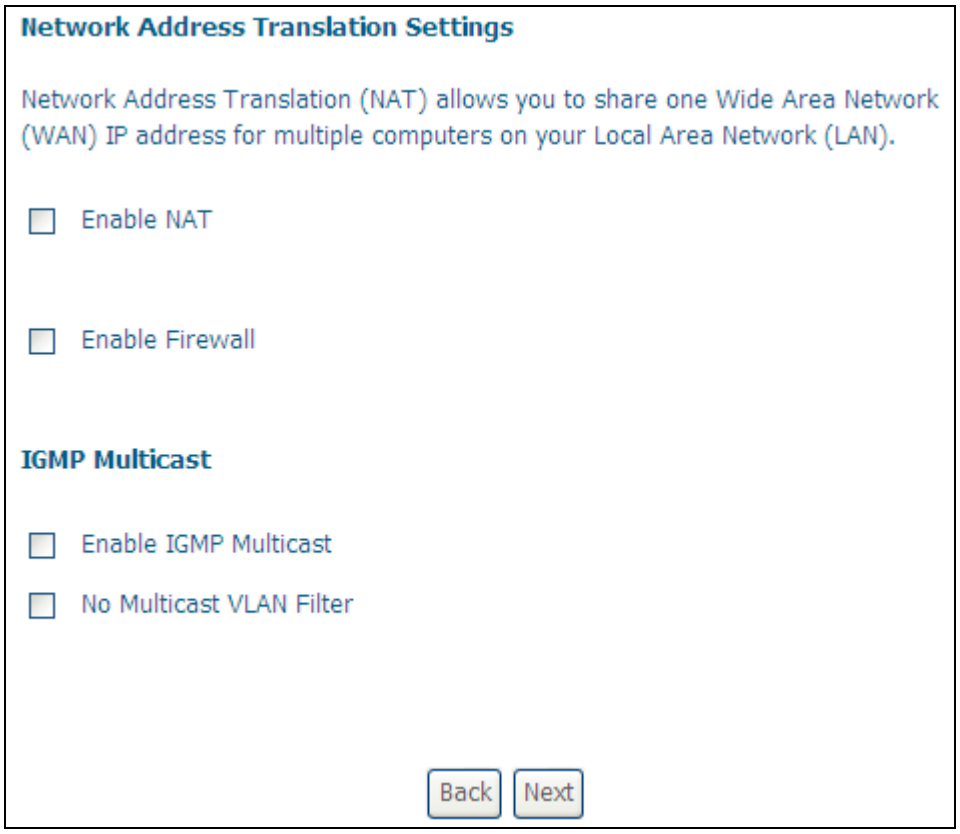


STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can instead use the **Static IP address** method to assign WAN IP address, Subnet Mask and Default Gateway manually.



Click **Next** to continue or click **Back** to return to the previous step.

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.

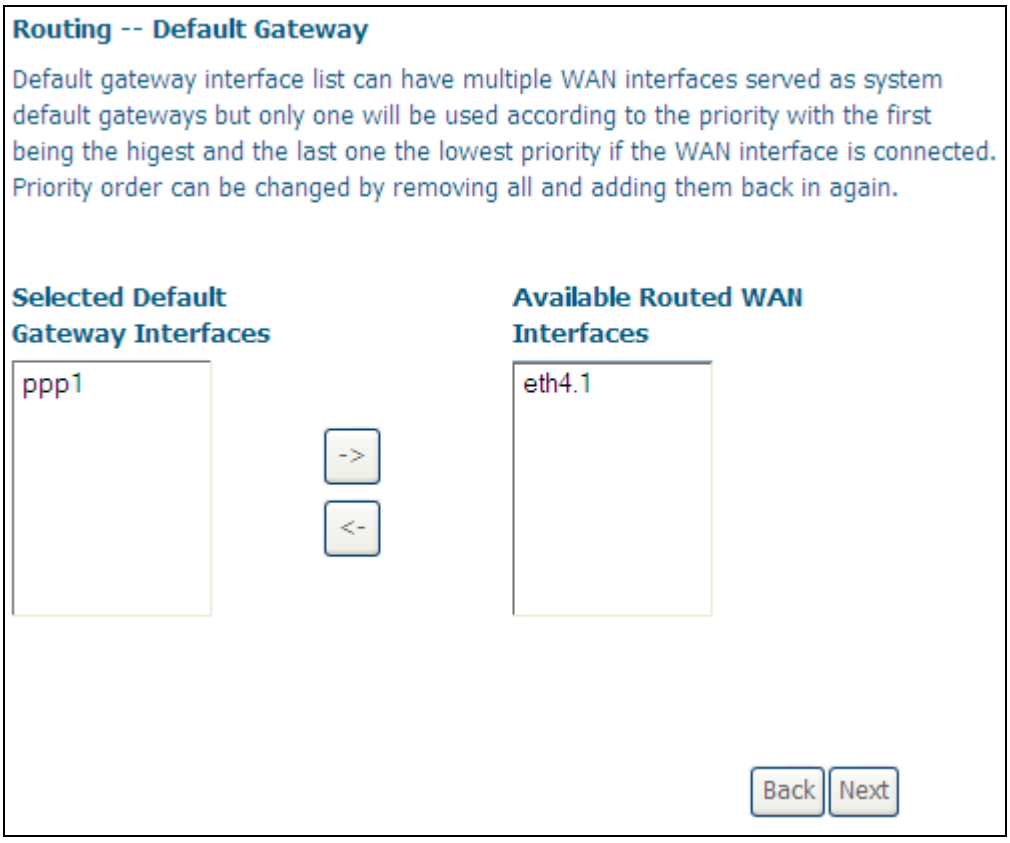


ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. IGMP is a protocol used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

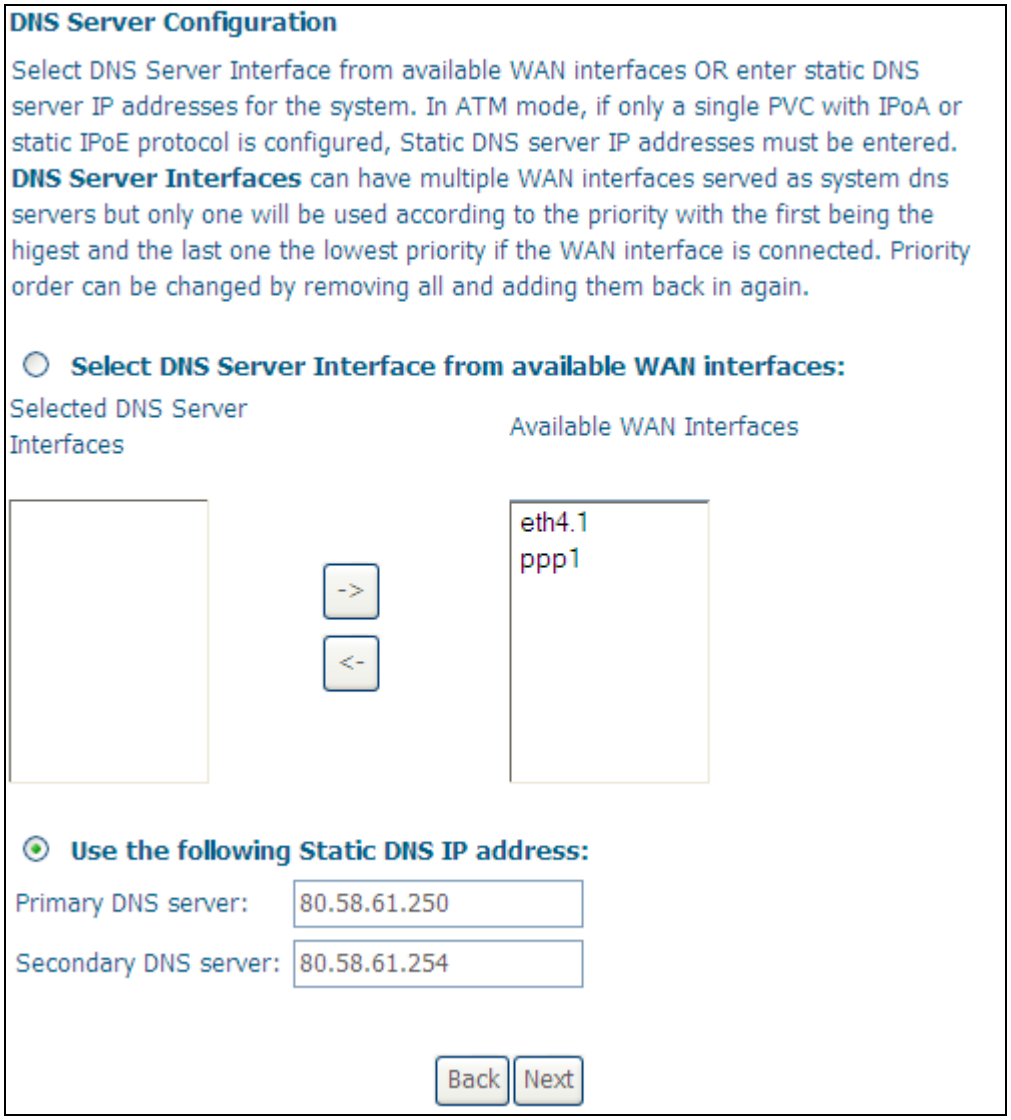
STEP 4: Choose an interface to be the default gateway.



Click **Next** to continue or click **Back** to return to the previous step.

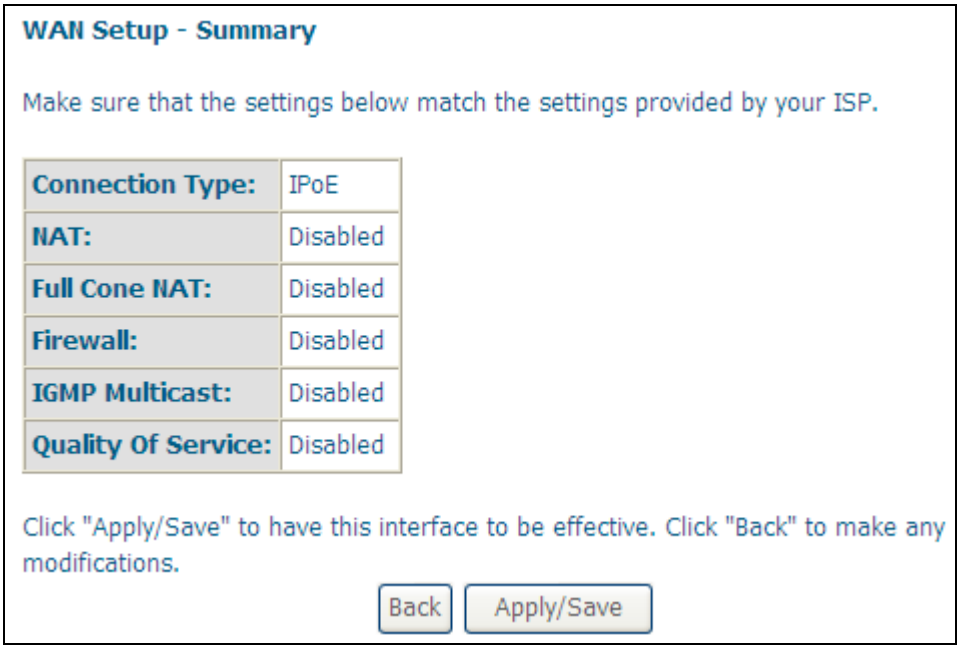
STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. Click **Next** to continue or click **Back** to return to the previous step.

Note: In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



STEP 6: Click **Next** to continue or click **Back** to return to the previous step.

STEP 7: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to modify them.

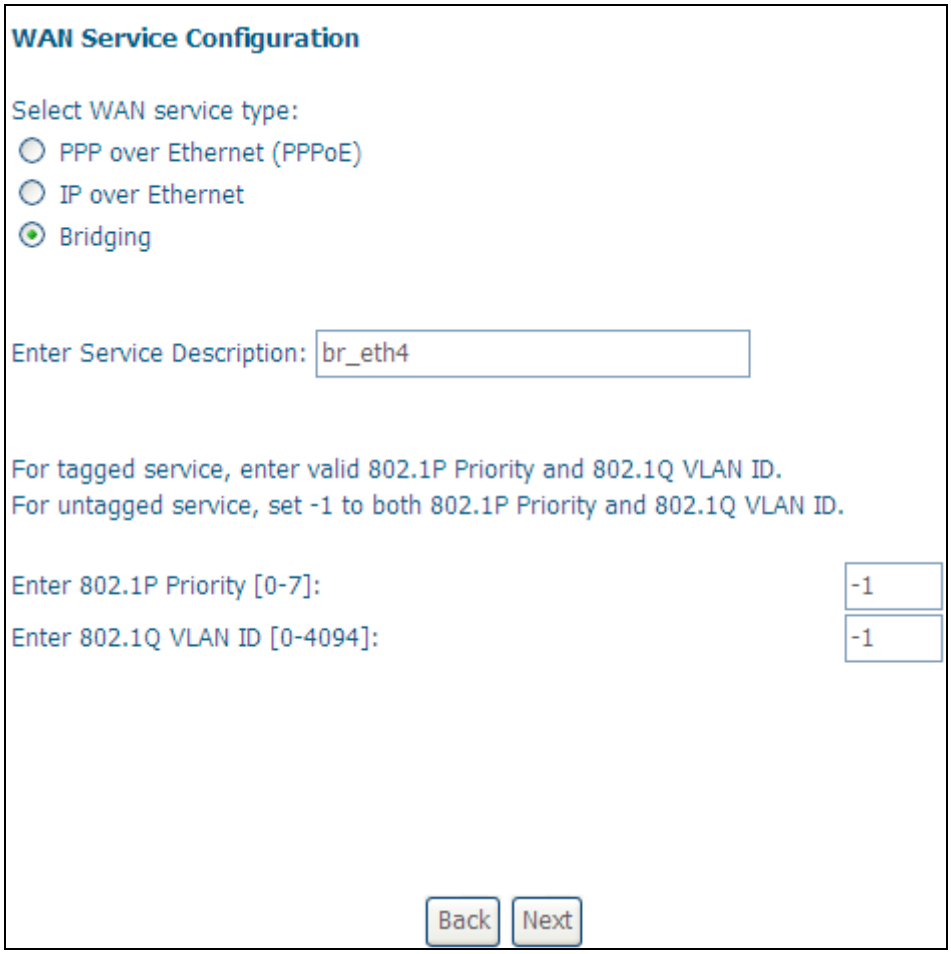


After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

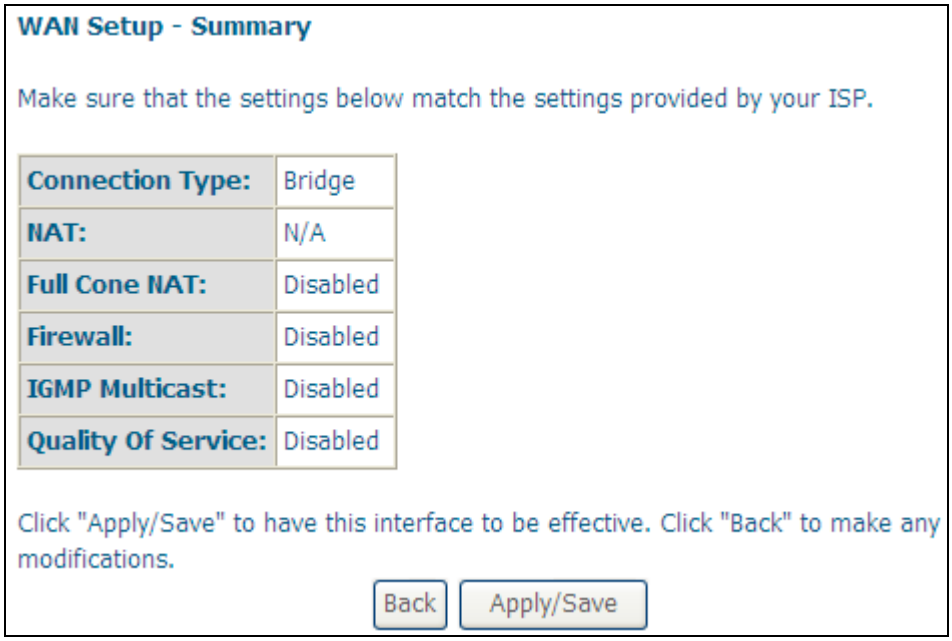
F2.3 Bridging

NOTE:	This connection type is not available on the Ethernet WAN interface.

STEP 1: Select the Bridging radio button and click **Next**.



STEP 2: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply / Save** if they are correct, or click **Back** to return to the previous screen.



After clicking **Apply/Save**, the new service should appear on the main screen. To activate it you must reboot. Go to Management → Reboot and click **Reboot**.

NOTE:	If this bridge connection is your only WAN service, the VG-8050 will be inaccessible for remote management or technical support from the WAN.