# USER MANUAL

## DVA-G3672B

VERSION 1.2


D-Link®

BROADBAND

# Table of Contents

# Overview

## Introduction

The D-Link DVA-G3672B High-Speed Wireless Router is an 802.11g high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places.

Unlike most routers, the DVA-G3672B provides data transfers at up to 8X (compared to the standard 11 Mbps) when used with other D-Link AirPlus G products. The 802.11 g standard is backwards compatible with 802.11 b products. This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 802.11 g's speed when you mix 802.11 b and 802.11 g devices, but you will not lose the ability to communicate when you incorporate the 802.11g standard into your 802.11 b network. You may choose to slowly change your network by gradually replacing the 802.11 b devices with 802.11 g devices.

In addition to offering faster data transfer speeds when used with other 802.11g products, the DVA-G3672B has the newest, strongest, most advanced security features available today. When used with other 802.11 g WPA (WiFi Protected Access) and 802.1x compatible products in a network with a RADIUS server, the security features include:

For home users that will not incorporate a RADIUS server in their network, the security for the DVA-G3672B, used in conjunction with other 802.11g products, will still be much stronger than ever before. Utilizing the Pre Shared Key mode of WPA, the DVA-G3672B will obtain a new security key every time it connects to the 802.11g network. You only need to input your encryption information once in the configuration menu. No longer will you have to manually input a new WEP key frequently to ensure security, with the DVA-G3672B, you can automatically receive a new key every time you connect, vastly increasing the safety of your communications.

# Package Contents

- D-Link DVA-G3672B High-Speed 2.4GHz Wireless ADSL VOIP Router
- Power Adapter-DC 12V, 1200 mA
- Manual and Warranty on CD
- Quick Installation Guide
- Ethernet Cable (All the DVA-G3672B's Ethernet ports are Auto-MDIX)

If any of the above items are missing, please contact your reseller.

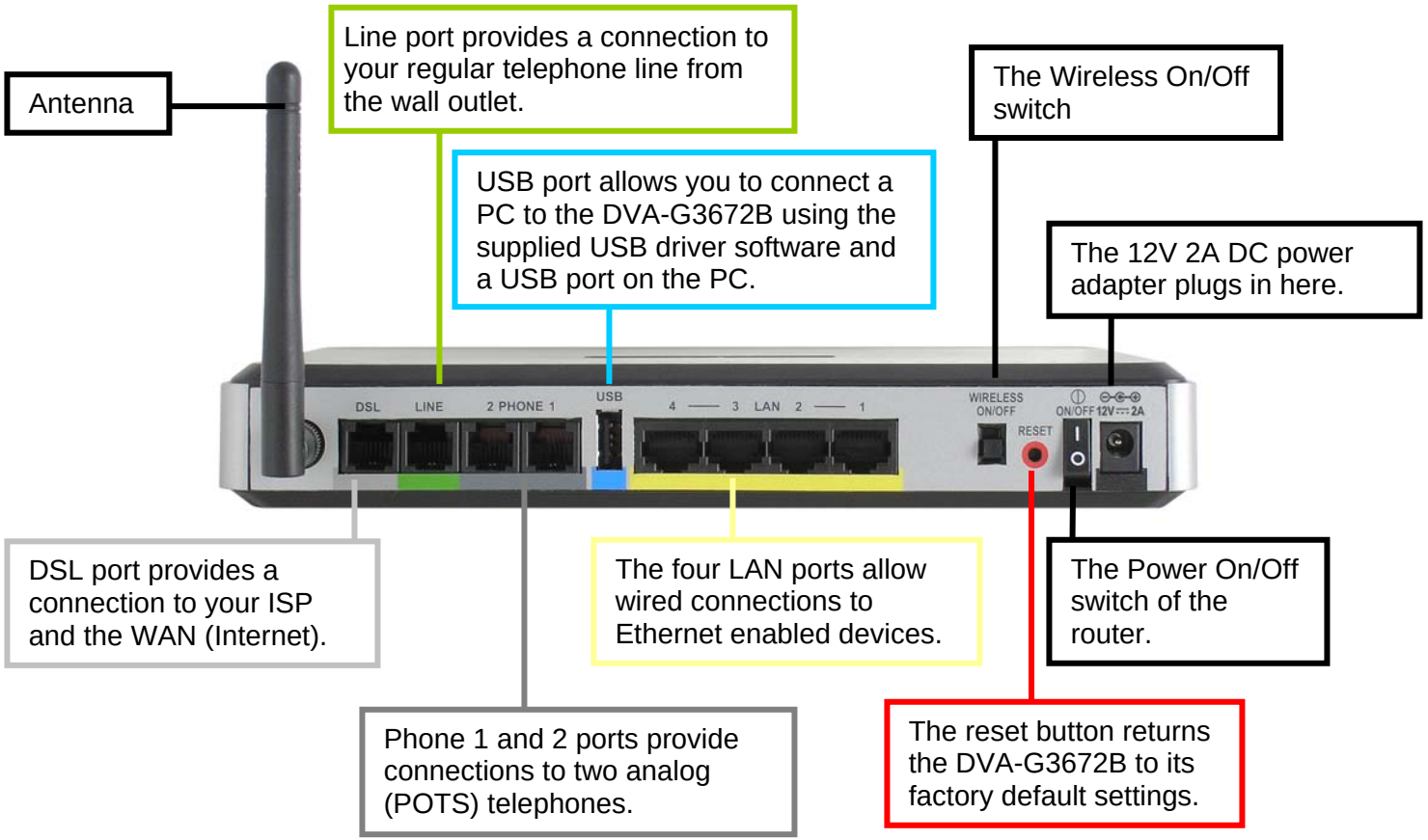
***Note:*** Using a power supply with a different voltage rating than the one included with the DVA-G3672B will cause damage and void the warranty for this product.

# System Requirements

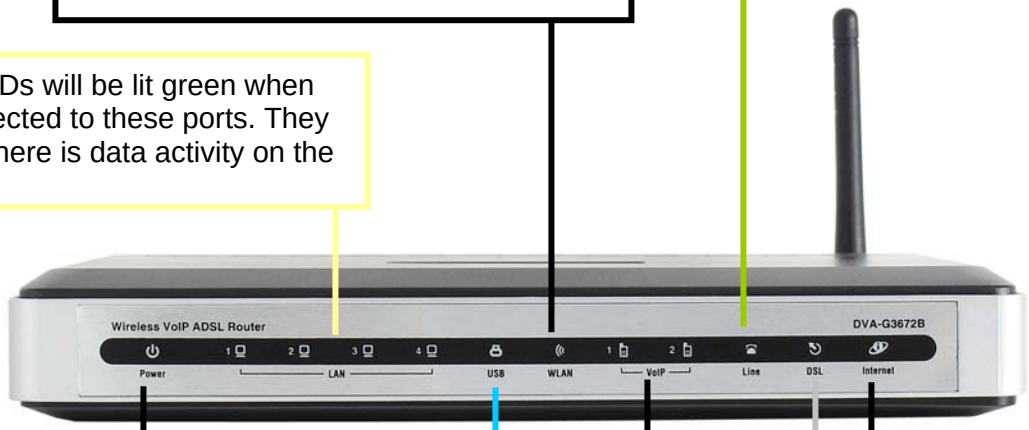
- Ethernet-Based Cable or DSL Modem
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator Version 6.0 and Above

# Hardware Overview

## Rear Panel



# Front Pannel




WLAN - This LED will be lit green when a Wireless LAN connection is detected. It will blink when there is data activity on the connection.

Line – The LED will light green when the PSTN line is connected. It will flash quickly when an incoming call via PSTN is detected.

LAN - These LEDs will be lit green when devices is connected to these ports. They will blink when there is data activity on the connection.

Power – LED will light green when power is properly connected and the Power switch

VoIP - LED will light green when the device has SIP registration. It will flash slowly when the VoIP phone is in use. The LED will flash quickly when there is an incoming call via VoIP.

Internet – LED will light green when obtaining WAN IP address from IPCP or DHCP, and DSL connection is build up. It also will light green when a static IP address is configured and PPP negotiation is successfully established.

USB- This LED will light green when a USB connection is detected. It will blink when there is data activity on the connection.

DSL - This LED will light green when a DSL is in good sync quality. It will blink when the device is synchronizing.

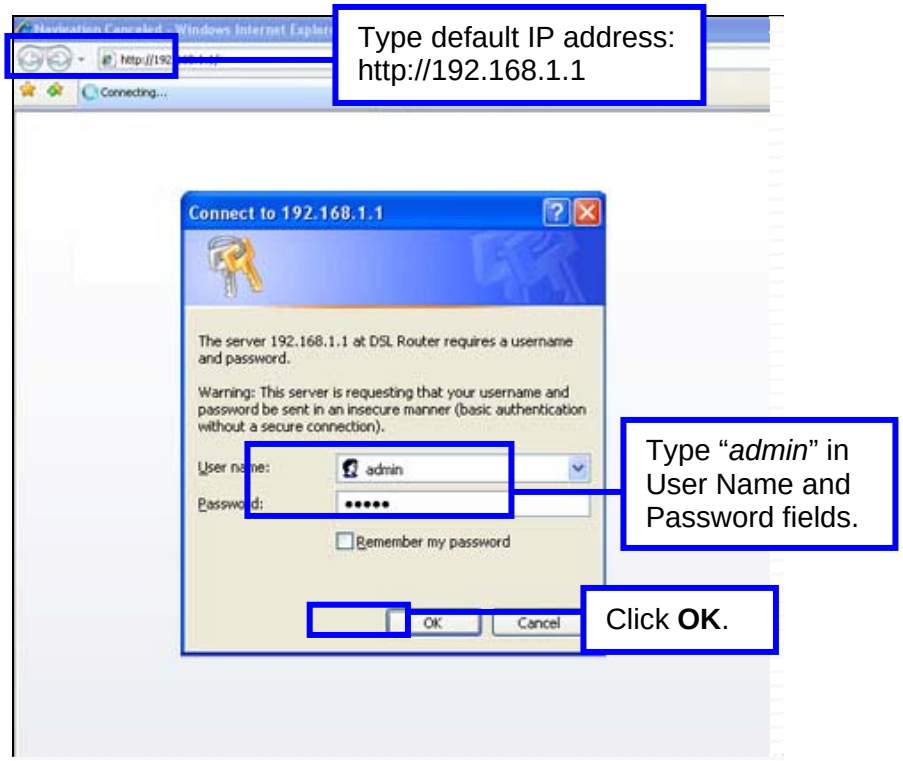
# Features

- Fully compatible with the 802.11 g standard to provide a wireless data rate of up to 54Mbps
- Backwards compatible with the 802.11 b standard to provide a wireless data rate of up to 11 Mbps
- WPA (Wi Fi Protected Access) authorizes and identifies users based on a secret key that changes automatically at a regular interval, for example:
- Pre Shared Key mode means that the home user, without a RADIUS server, will obtain a new security key every time the he or she connects to the network, vastly improving the safety of communications on the network.
- 802.1x Authentication in conjunction with the RADIUS server verifies the identity of would be clients
- Utilizes OFDM technology (Orthogonal Frequency Division Multiplexing)
- User-friendly configuration and diagnostic utilities
- Operates in the 2.4GHz frequency range
- Connects multiple computers to a Broadband (Cable or DSL) modem to share the Internet connection
- Advanced Firewall features
- Supports NAT with VPN pass-through, providing added security
- MAC Filtering
- IP Filtering
- URL Filtering
- Domain Blocking
- Scheduling
- DHCP server supported enables all networked computers to automatically receive IP addresses
- Web-based interface for Managing and Configuring
- Access Control to manage users on the network
- Supports special applications that require multiple connections
- Equipped with 4 10/100Mbps Ethernet ports, 1 WAN port, Auto MDI/MDIX

# Configuration

## Log in to Web-based Configuration

Whenever you want to configure your network or the DVA-G3672B, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the DVA-G3672B. The DVA-G3672B default IP address is: http://192.168.1.1 Both default username and password are *admin*.



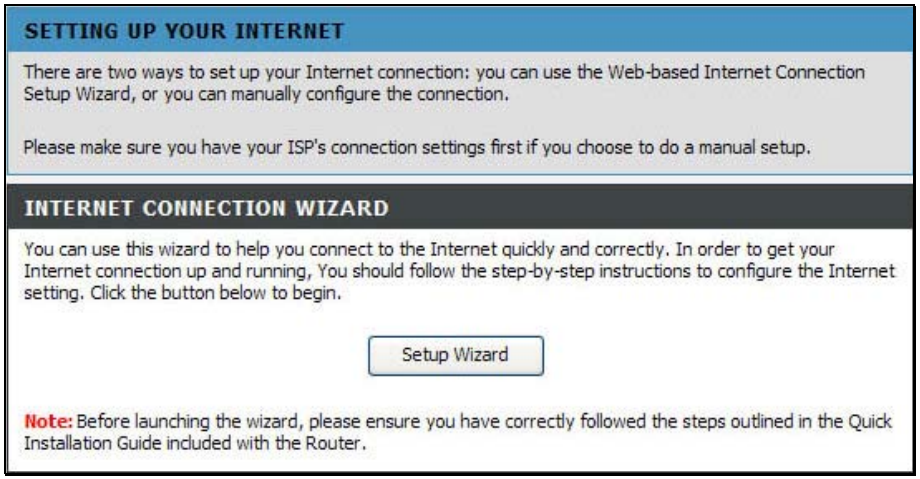

1. Open a web browser.
2. Type in the default IP address of the Router in the **Address** field.
3. Press enter to see a dialog box requesting for username and password.
4. Type *admin* in both **User Name** and **Password** fields.
5. Click **OK** to see the following webpage.


Product Page : DVA-G3672B
Site Map
Firmware Version : V1.00B01T01.RU.20071214
D-Link
DVA-G3672B
SETUP
ADVANCED
MAINTENANCE
STATUS
HELP
Wizard
Internet Setup
Wireless Settings
Local Network
Time and Date
Logout
SETTING UP YOUR INTERNET
There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.
Please make sure you have your ISP's connection settings first if you choose to do a manual setup.
INTERNET CONNECTION WIZARD
You can use this wizard to help you connect to the Internet quickly and correctly. In order to get your Internet connection up and running, You should follow the step-by-step instructions to configure the Internet setting. Click the button below to begin.
Setup Wizard
Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the Router.
Helpful Hints..
If you are setting up networking for the first time and have not configured the Router yet, click on "Setup Wizard". This will lead you through a step-by-step process to configure the Internet settings.
If you consider yourself an advanced user or have configured a router before,click Setup->Internet Setup to input all the settings manually.

# Quick Setup

The Wizard setup helps you to configure the Internet connection quickly and correctly. To access the main page, click **Wizard** in the **Setup** directory.

Click the **Setup Wizard** link in the middle of the top of the window of the Router's opening page to launch a series of setup windows.

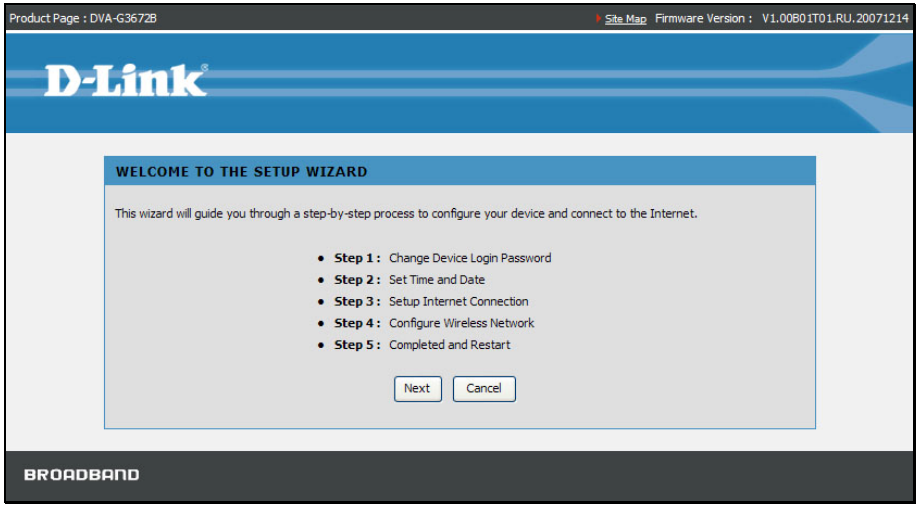



# Quick Setup – Opening Window

The first window of the Setup Wizard lists the basic steps in the process. These steps are as follows:

1. Change the Router's password.
2. Configure time and date of the Router.
3. Configure the Internet connection.
4. Configure the Wireless network connection.
5. Confirm the settings and restart the Router.

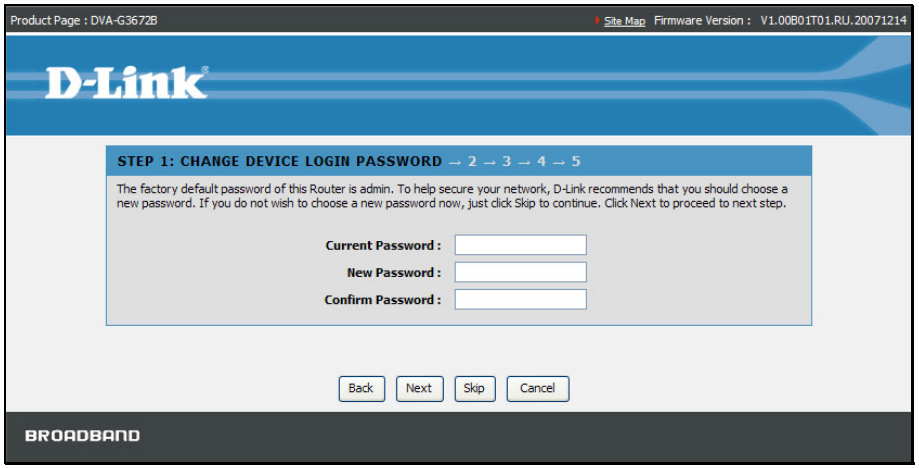
Click the **Next** button to continue.



# Quick Setup – Change the Router's Password

This window of the Setup Wizard is used to change the Router password. D-Link recommends to help secure your network, the user change the Current Password from the factory default "admin." The New Password should be between 1 and 16 alphanumeric characters.
Once you have filled out the fields in this window, including re-typing the new password in the Confirm Password field, click the **Next** button to continue.

If you do not want to change the password, click the **Skip** button to proceed to the next step.




Once you have filled out the fields in this window, including re-typing the new password in the Confirm Password field, click the **Next** button to continue.

If you do not want to change the password, click the **Skip** button to proceed to the next step.

# Quick Setup – Set Time and Date

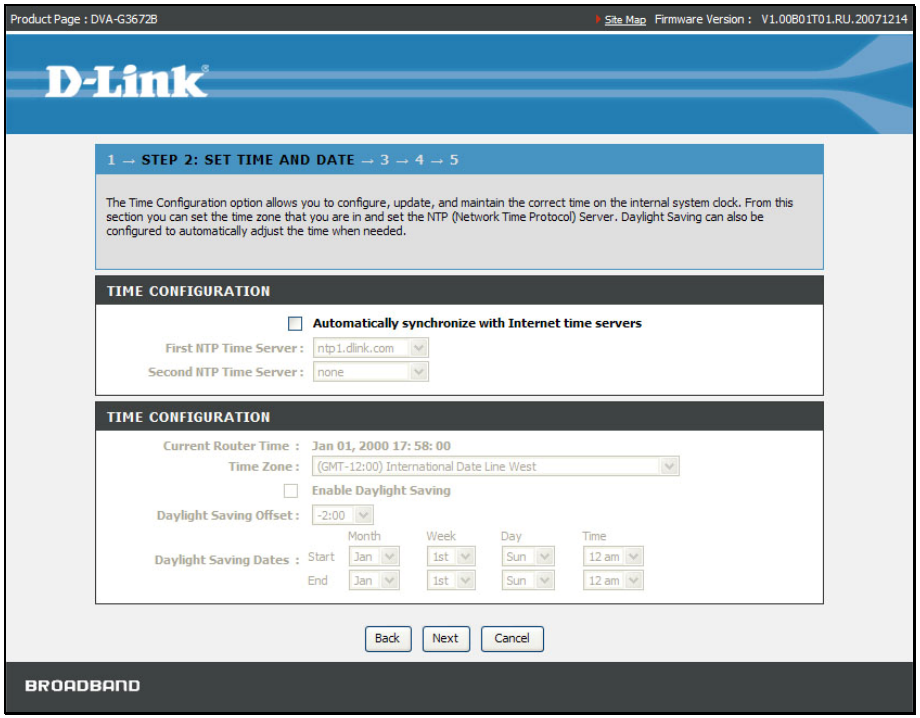
This page allows you to configure the time and date of the Router.

Select **Automatically synchronize with Internet time servers** to select first and second NTP (Network Time Protocol) server.

Select a time zone in which you are located from the **Time Zone** list.

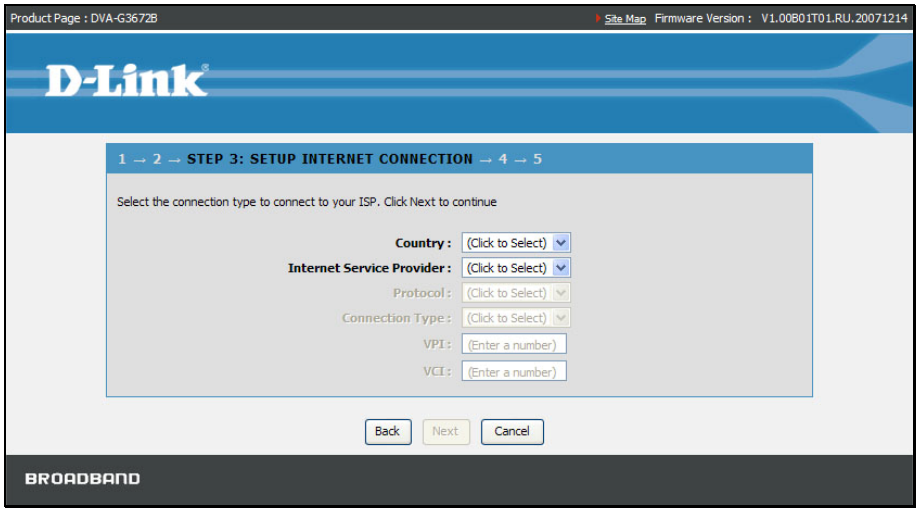
Select **Enable Daylight Saving** and configure the daylight saving information, if the area you are located has daylight saving.

Click the **Next** button to continue.



# Quick Setup – Setup Internet Connection

Now use the drop-down menus to select the Country, ISP Provider, Protocol and Connection Type used for the Internet connection, and enter VPI and VCI values if applicable. Your ISP has given this information to you—any information that is not required for your provider will automatically be grayed out in this window and subsequent Quick Setup windows.




The available Protocol modes are: *Dynamic IP*, *Static IP*, *PPPoE*, *PPPoA* and *Bridge*.

The Connection Type options are *1483 Bridged IP LLC*, *1483 Bridged IP VC-Mux*, *1483 Routed IP LLC*, *1483 Routed IP VC-Mux*, *PPPoE LLC*, *PPPoE VC-Mux*, *PPPoA LLC*, and *PPPoA VC-Mux*.

Once the Protocol option is selected, coordinate options appear below in the window. Enter values as instructed by your ISP.

Click the **Next** button when you are finished to proceed to the next Setup Wizard window.

# Quick Setup – Configure Wireless Network

This page helps you to configure the Wireless settings.

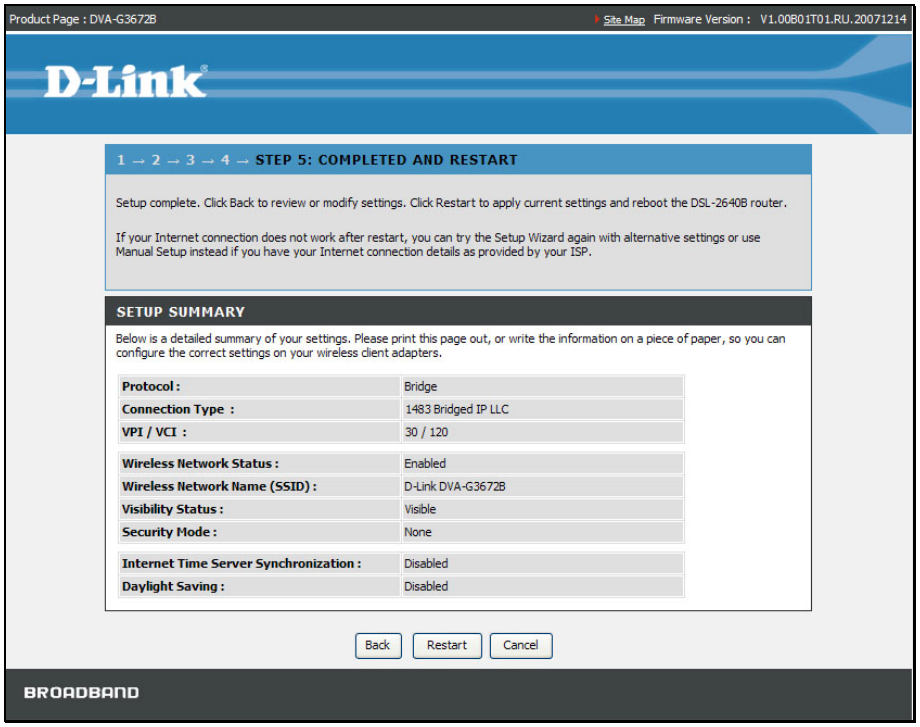
Select **Enable your Wireless Network** by default and configure the SSID, the visibility of SSIC and the Wireless network security. Deselect **Enable your Wireless Network** for skipping the wireless configurations.

Click the **Next** button to continue.

# Quick Setup – Restart the Router

This page displays the settings you made in the Wizard.

Click **Restart** to save current settings and restart the Router.



# Setup – Internet Setup

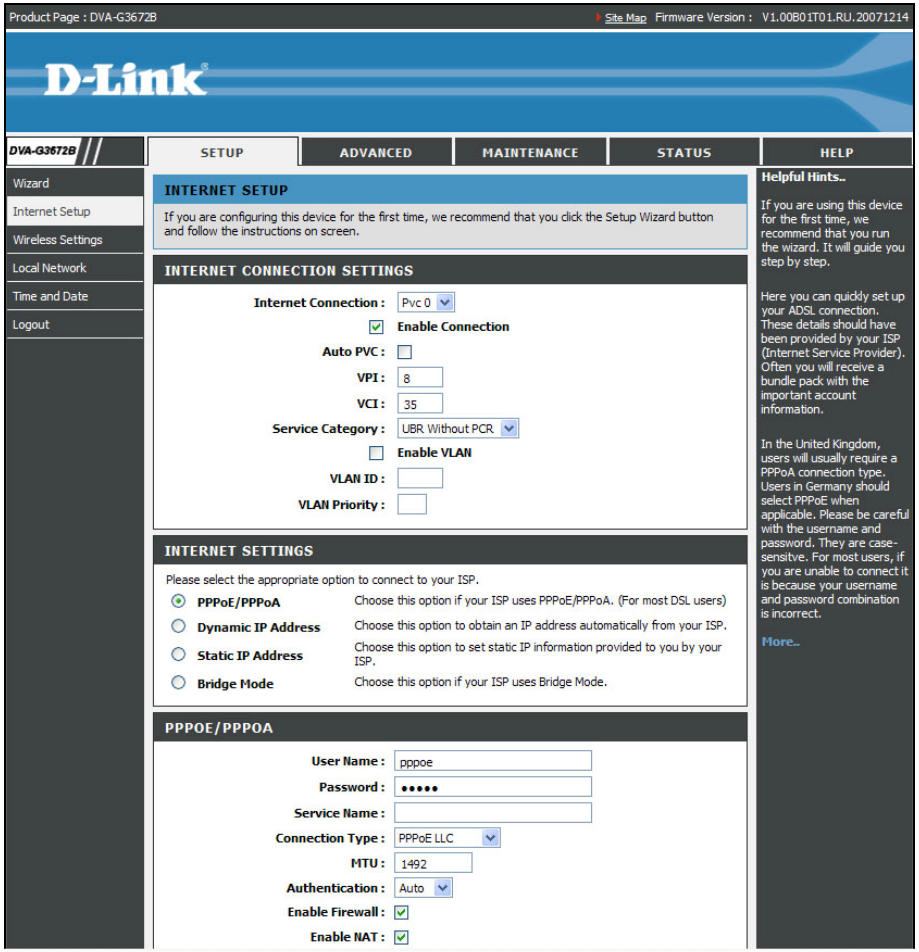
To configure the Router's basic configuration settings without running the Setup Wizard, you can access the menus used to configure Internet, Wireless, Local Network, and Time and Date settings directly from the **Setup** directory.

To access the Internet Setup window, click **Internet Setup** on the left side of the first window that appears when you successfully access the web manager.

**Internet Connection Settings**

1. Select a Connection ID in the **Internet Connection** drop-down list.
2. Select **Enable Connection** to configure the Internet Settings section.
3. If you are instructed to change the VPI or VCI values, type in the values assigned for your account, or select **Auto PVC**. Service Category drop-down menu is set at their default values for now.
4. Select **Enable VLAN**, and configure VLAN ID and VLAN Priority, if you want to use VLAN to group your networks.

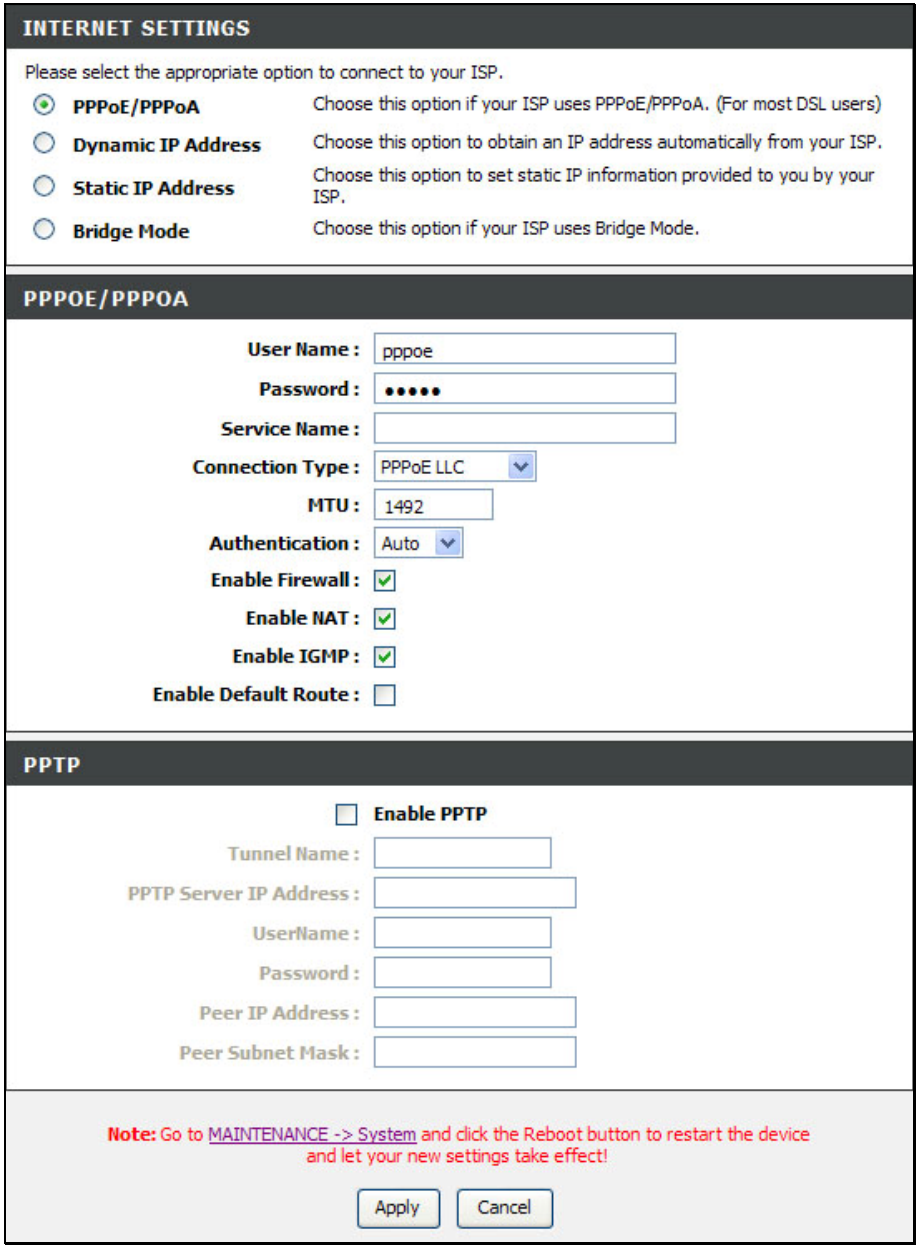
Click the **PPPoE/PPPoA** radio button to access the first Manual Internet Connection Setup window:



## Internet Setup – PPPoE/PPPoA

To configure a PPPoE or PPPoA type connection, follow these steps:

1. Type the Username and Password used for your Internet account. A typical User Name will be in the form "user1234@isp.co.uk." The Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP. The Service Name field is used for the name of your Internet Service Provider. This is optional.
2. Choose the Connection Type from the drop-down menu. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *PPPoE LLC*, *PPPoE VC-Mux, PPPoA LLC* and *PPPoA VC-Mux.* If you have not been provided specific information for the Connection Type setting, leave the default setting.
3. Leave the MTU value at the default setting unless you have specific reasons to change this.
4. Choose the correct Authentication type from the drop-down menu. Most users will want to leave the setting on *Auto*. *PAP* and *CHAP* are the other two options. The *Auto* setting will automatically detect the correct type of authentication.
5. The **Enable Firewall** should remain selected for most users. If you deselect to disable this you will not be able to use the some of the features configured in the firewall and filter windows located in the **Advanced** directory. The next chapter contains a separate section describing these Advanced features.
6. **Enable NAT** should remain selected. If you disable NAT, you will not be able to use more than one computer for Internet connections. If you are using multiple virtual connections, NAT functions system-wide, therefore if it is not selected, NAT will be disabled on all connections.



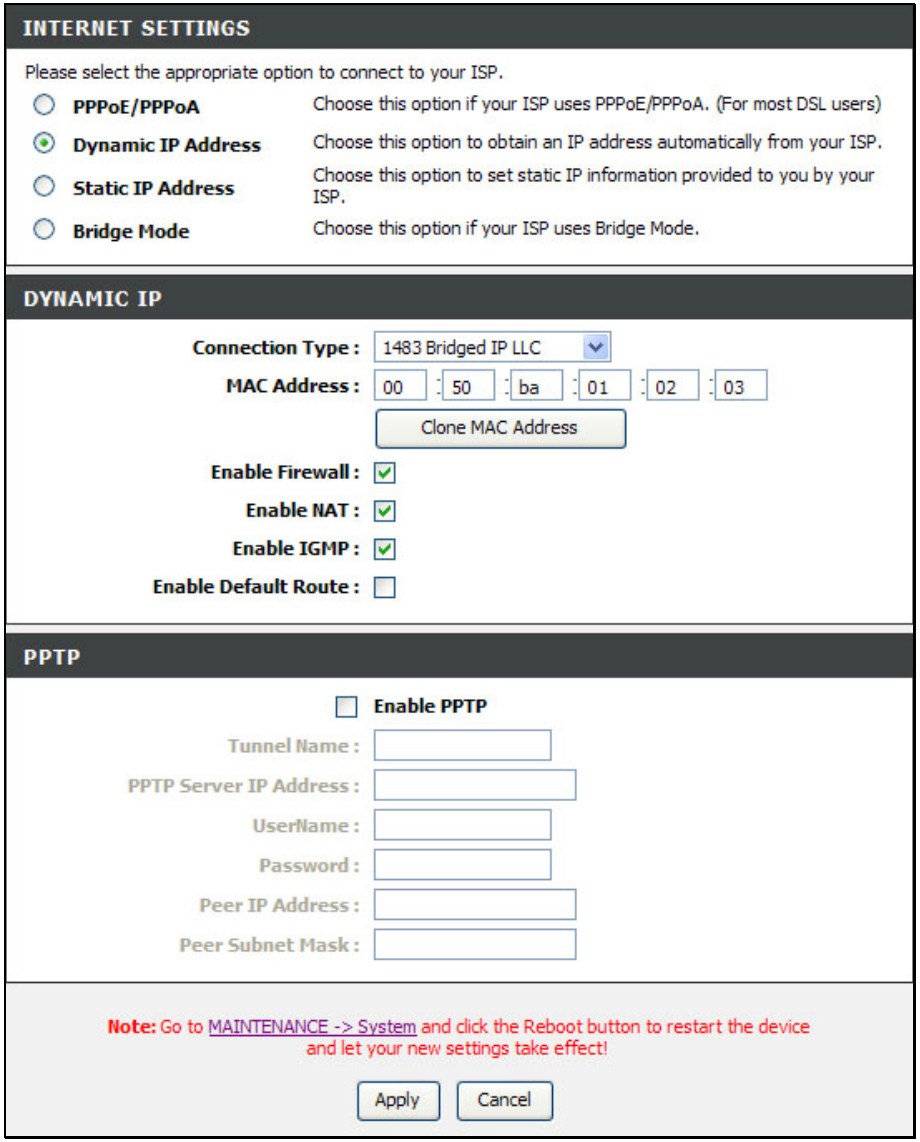
7. Most users will want to keep **Enable IGMP** selected as it allows IGMP packets to go through the WAN interface in both directions.
8. Leave **Enable Default** deselected, if you have an alternative route for Internet traffic you may disable this without effecting the Router's connection. Select **Enable Default Route** if you want to use the Router as the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer.
9. Select **Enable PPTP** and enter the Tunnel Name, PPTP Server IP Address, UserName, Password, Peer IP Address and Peer Subnet Mask to implement a tunnel sending PPP session to the peer.
10. When you are satisfied that all the settings are configured correctly, click the **Apply** button. This will save the settings.
11. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.

## Internet Setup – Dynamic IP Address

A Dynamic IP Address connection configures the Router to automatically obtain its global IP address from a DHCP server on the ISP's network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the Router requests an IP address.

To configure a Dynamic IP Address WAN connection, follow these steps:

1. Choose the Connection Type from the drop-down menu. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*. If you have not been provided specific information for the Connection Type setting, leave the default setting.
2. Some ISPs record the unique MAC Address of your computer's Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, click the **Copy MAC Address** button.
3. The **Enable Firewall** should remain selected for most users. If you deselect to disable this you will not be able to use the some of the features configured in the firewall and filter windows located in the **Advanced** directory. The next chapter contains a separate section describing these Advanced features.
4. **Enable NAT** should remain selected. If you disable NAT, you will not be able to use more than one computer for Internet connections. If you are using multiple virtual connections, NAT functions system-wide, therefore if it is not selected, NAT will be disabled on all connections.



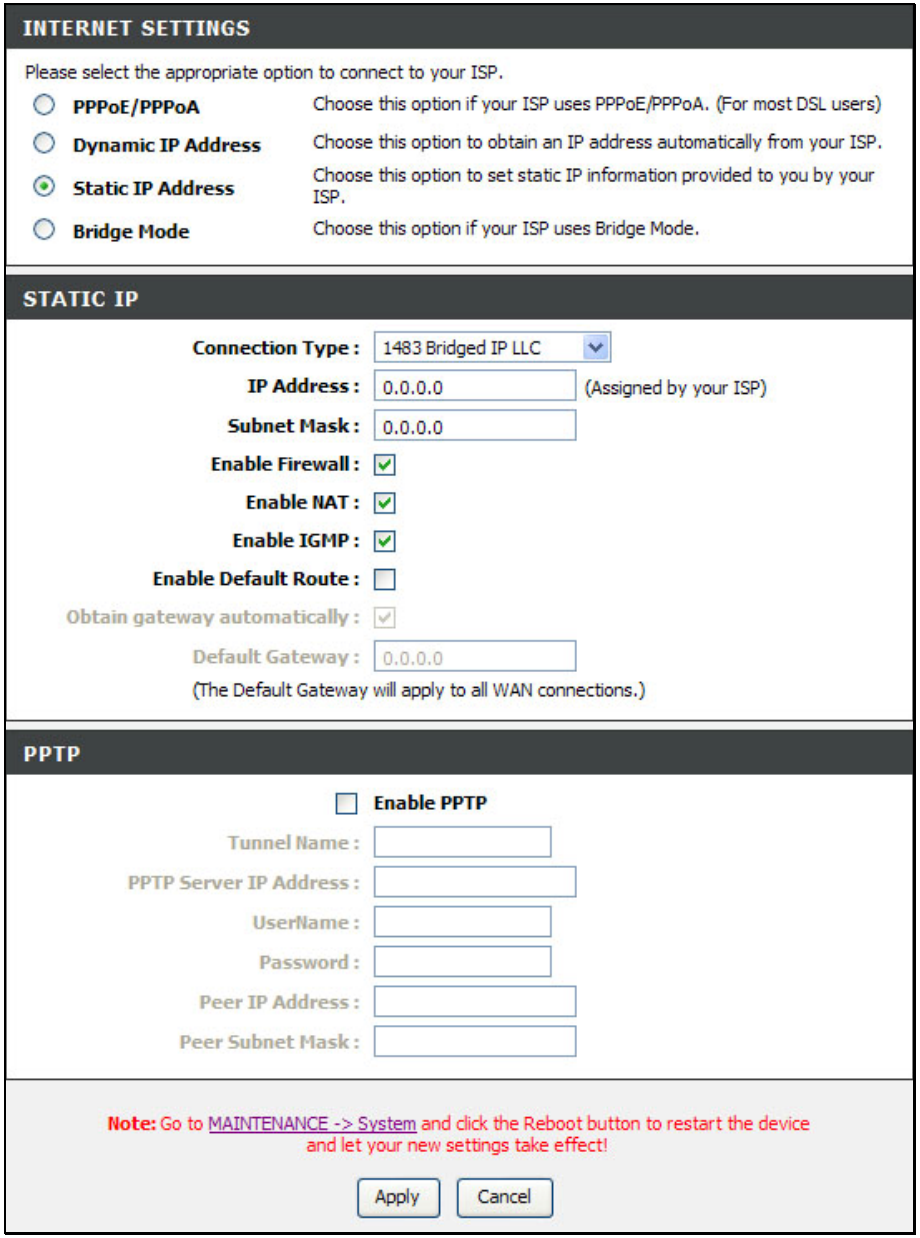
5. Most users will want to keep **Enable IGMP** selected as it allows IGMP packets to go through the WAN interface in both directions.
6. Leave **Enable Default** deselected, if you have an alternative route for Internet traffic you may disable this without effecting the Router's connection. Select **Enable Default Route** if you want to use the Router as the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer.
7. Select **Enable PPTP** and enter the Tunnel Name, PPTP Server IP Address, UserName, Password, Peer IP Address and Peer Subnet Mask to implement a tunnel sending PPP session to the peer.
8. When you are satisfied that all the settings are configured correctly, click the **Apply** button. This will save the settings.
9. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.

## Internet Setup – Static IP

When the Router is configured to use Static IP Address assignment for the WAN connection, you must manually assign a global IP Address, Subnet Mask, and Default Gateway IP address used for the WAN connection.

To configure a Static IP Address WAN connection, follow these steps:

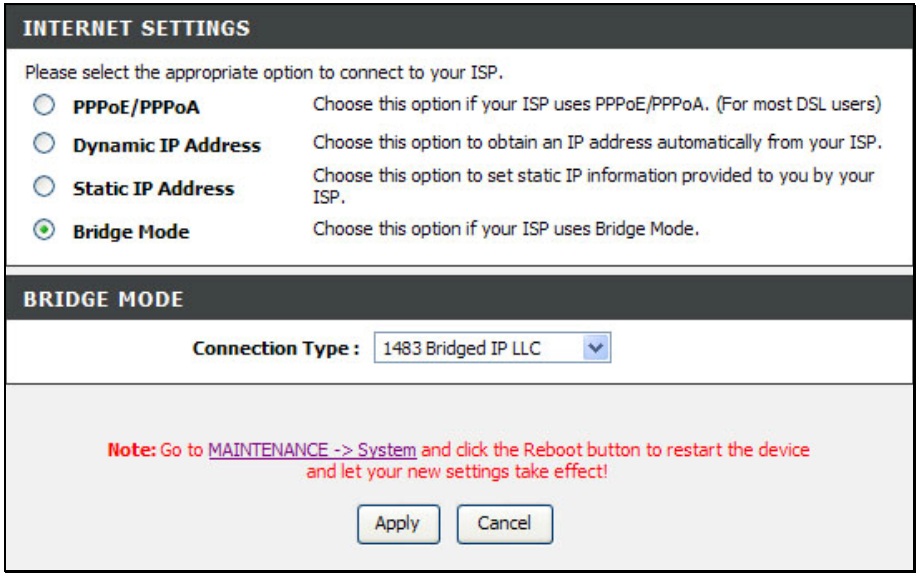
1. Choose the Connection Type from the drop-down menu. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *1483 Bridged IP LLC*, *1483 Bridged IP VC-Mux*, *1483 Routed IP LLC* and *1483 Routed IP VC-Mux*. If you have not been provided specific information for this setting, leave the default setting.
2. Change the IP Address, Subnet Mask, and Default Gateway as instructed by your ISP. These are the global IP settings for the WAN interface. This is the "visible" IP address of your account. Your ISP should have provided these IP settings to you. If your ISP also asks you to change DNS server IP addresses, enter the Preferred DNS Server and Alternate DNS Server information manually.
3. The **Enable Firewall** should remain selected for most users. If you deselect to disable this you will not be able to use the some of the features configured in the firewall and filter windows located in the **Advanced** directory. The next chapter contains a separate section describing these Advanced features.
4. **Enable NAT** should remain selected. If you disable NAT, you will not be able to use more than one computer for Internet connections. If you are using multiple virtual connections, NAT functions system-wide, therefore if it is not selected, NAT will be disabled on all connections.
5. Most users will want to keep **Enable IGMP** selected as it allows IGMP packets to go through the WAN interface in



both directions.

6. Leave **Enable Default** deselected, if you have an alternative route for Internet traffic you may disable this without effecting the Router's connection. Select **Enable Default Route** if you want to use the Router as the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer.
7. Select **Enable PPTP** and enter the Tunnel Name, PPTP Server IP Address, UserName, Password, Peer IP Address and Peer Subnet Mask to implement a tunnel sending PPP session to the peer.
8. When you are satisfied that all the settings are configured correctly, click the **Apply** button. This will save the settings.
9. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.

## Internet Setup – Bridge Mode




For Bridged connections it will be necessary for most users to install additional software on any computer that will use the Router for Internet access. The additional software is used for the purpose of identifying and verifying your account, and then granting Internet access to the computer requesting the connection. The connection software requires the user to enter the User Name and Password for the ISP account. This information is stored on the computer, not in the Router.

To configure a Static IP Address WAN connection, follow these steps:

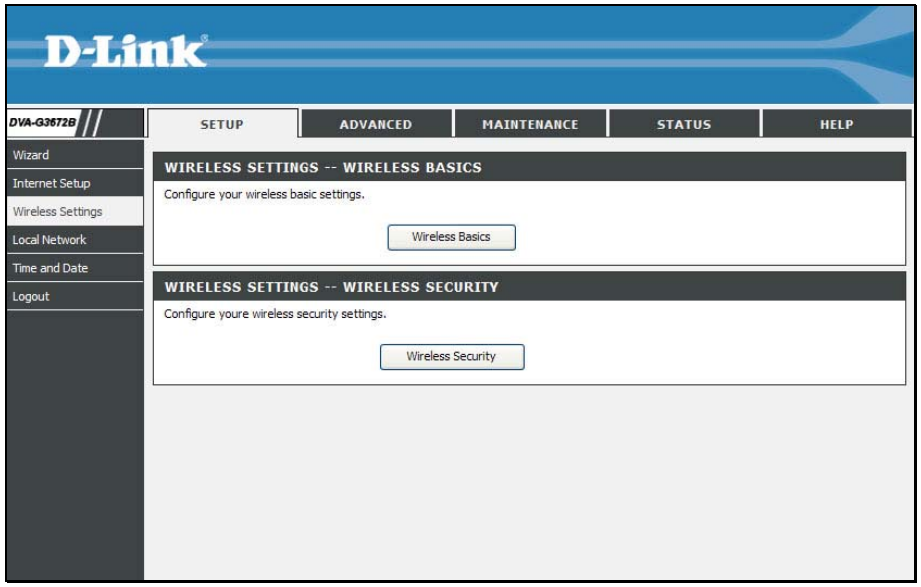
1. Choose the Connection Type from the drop-down menu. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*. If you have not been provided specific information for this setting, leave the default setting.
2. When you are satisfied that all the settings are configured correctly, click the **Apply** button. This will save the settings.

Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.

# Setup – Wireless Settings

To access Wireless Settings, click **Wireless Settings** in the **Setup** directory.

It has two subcategories: **Wireless Basics** and **Wireless Security**. You can either point to the **Wireless Settings** on the left window and click one of the submenus, or click one of the buttons in the Wireless Settings window.



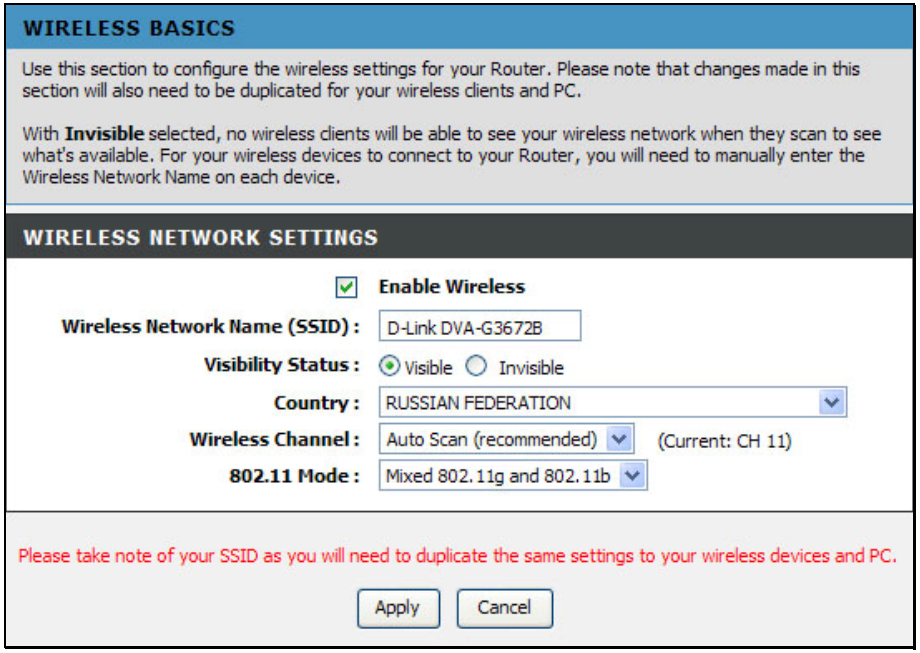
# Wireless Settings – Wireless Basics

To access Wireless Basics, point to the **Wireless Settings** on the left window and click **Wireless Basics** submenu, or click the **Wireless Basics** button in the Wireless Settings window.

The two essential settings for wireless LAN operation are the Wireless Network Name (SSID) and Wireless Channel. The SSID (Service Set Identifier) is used to identify a group of wireless LAN components. The SSID can be visible (broadcast) or hidden (not broadcast).

Follow the instructions below to change basic wireless settings.

1. The Wireless LAN is enabled by default. To disable the wireless interface, click to deselect the **Enable Wireless** check box. If the wireless interface has been disabled, click the **Enable Wireless** check box again to select it.
2. The **Wireless Network Name (SSID)** can be changed to suit your wireless network. Remember that any wireless device using the access point must have the same SSID and use the same channel.
3. The Visibility Status is **Visible** by default. To disable SSID Visibility Status, click the **Invisible** radio button.
4. Select a country where the Router is located in the **Country** drop-down list.
5. The **Wireless Channel** may be changed to channels that are available in your region. Channels available for wireless LAN communication are subject to regional and national regulation.
6. Select a wireless protocol in the **802.11 Mode** drop-down list.
7. Click **Apply** to save the settings.

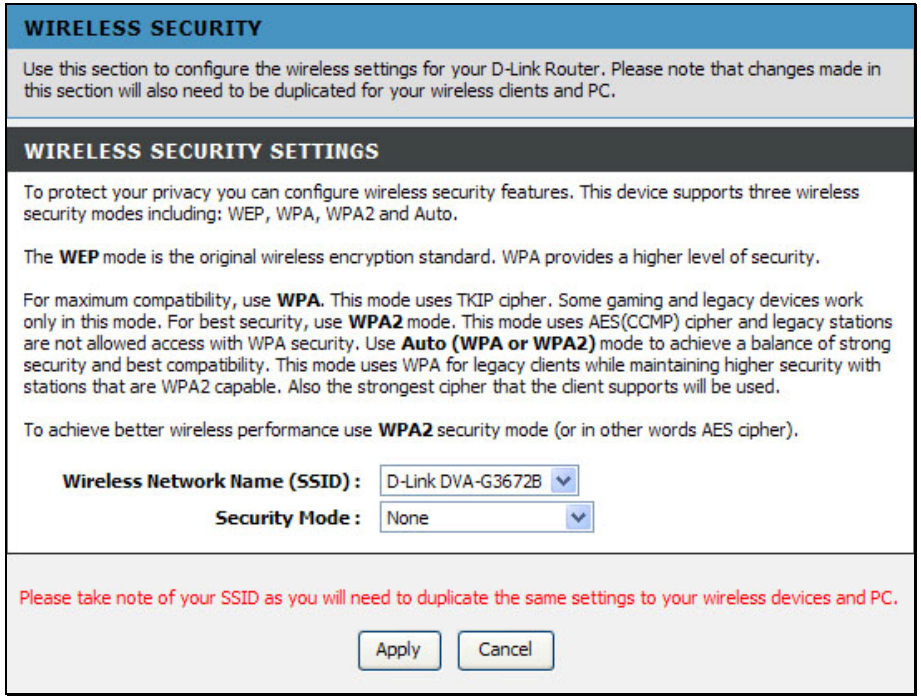


# Wireless Settings – Wireless Security

To access Wireless Security, point to the **Wireless Settings** on the left window and click **Wireless Security** submenu, or click the **Wireless Security** button in the Wireless Settings window.

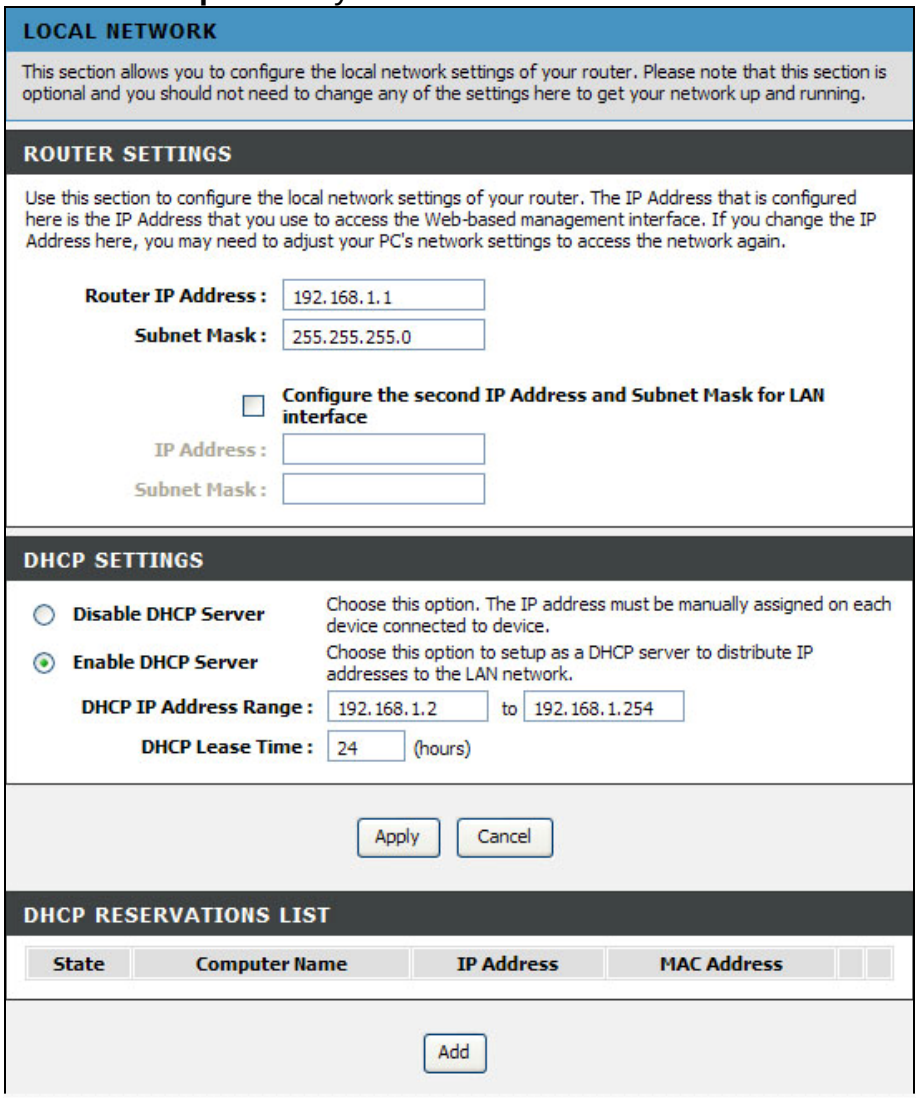
In order to protect the privacy, you can setup the wireless security. Available security modes are *WEP*, *WPA*, *WPA2* and *Auto*.

1. Select a SSID in the **Wireless Network Name (SSID)** drop-down list.
2. Select a wireless security mode in the **Security Mode** drop-down list.
3. Click the **Apply** button to save the settings.



# Setup – Local Network

To access the **Local Network** window, click the **Local Network** button in the **Setup** directory.




You can configure the local network IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your local network, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router. See the next section for information on DHCP setup.

To change the Router IP Address or Subnet Mask, type in the desired values in the Router Settings section and click the **Apply** button. Go to **Maintenance** -> **System** and click **Reboot** to restart the device. Your web browser should automatically be redirected to the new IP address. You will be asked to login again to the Router's web manager.

The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the Router though the Ethernet port. When the Router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router the range of IP addresses in the pool used for DHCP on the LAN will also be changed. The IP address pool can be up to 253 IP addresses.

There are two options for DHCP service:

- You can use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for workstations.

You may also configure DNS settings when using the Router in DHCP mode (**Advanced** > **DNS Setup**). When “Obtain DNS server address automatically“ is clicked under DNS Server Configuration on the DNS Setup window, the Router will automatically relay DNS settings to properly configured DHCP clients. To manually enter DNS IP addresses, click the “Use the following DNS server addresses“ radio button and type in a Preferred DNS Server and Alternate DNS Server in the fields provided. The manually configured DNS settings will be supplied to clients that are configured to request them from the Router.

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured DHCP as you want, click the **Apply** button to commit the new settings. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.

**Use the Router for DHCP**
To use the built-in DHCP server, click the **Enable DHCP Server** radio button in the DHCP Settings section if it is not already selected. The IP address pool settings can be adjusted. The DHCP IP Address Range starts with the lowest available IP address (default = 192.168.1.2). If you change the IP address of the Router this will change automatically to be 1 more that the IP address of the Router. The DHCP IP Address Range ends with the highest IP address number in the pool. Type in the DHCP Lease Time in the entry field provided. This is the amount of time in hours that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

**Disable the DHCP Server**
To disable DHCP, Click the **Disable DHCP Server** radio button in the DHCP Settings section and click the **Apply** button. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect. Choosing this option will gray out most of the setting options on this window and require that workstations on the local network be configured manually or use another DHCP server to obtain IP settings.

If you configure IP settings manually, make sure to use IP addresses in the subnet of the Router. You will need to use the Router’s IP address as the Default Gateway for the workstation in order to provide Internet access.

**Add DHCP Reservation List**
To add an entry to the DHCP Reservation List, click the **Add** button in the DHCP Reservation List section, type in an IP Address, either click the **Copy Your PC’s MAC Address** button or manually enter a MAC Address, enter a Computer Name if desired, and click the **Apply** button. To delete an entry from the DHCP Reservations List, click the corresponding  button. To modify a DHCP Reservations List entry, click the corresponding  button and then enter the information in the appropriate fields in the Edit DHCP Reservation (Optional) section. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.

# Setup – Time and Date

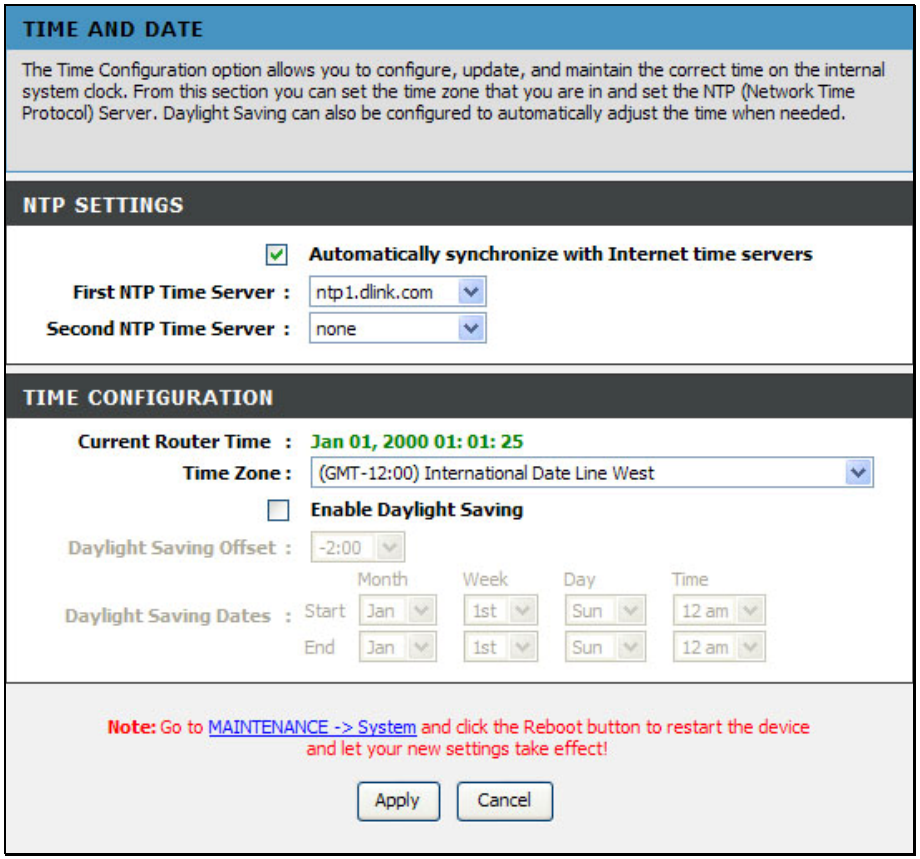
To access the **Time and Date** window, click the **Time and Date** button in the **Setup** directory.

The Router provides NTP and daylight saving to configure, update and maintain the correct time.

To configure system time on the Router, select the **Automatically synchronize with Internet time servers** check box (default) and use the drop-down menu to select the NTP server URL in the First NTP Time Server field. You may also want to choose a Second NTP Time Server using the drop-down menu.

The Router also allows you to set the time zone you are in by using the Time Zone drop-down menu. In addition, you can configure Daylight Saving by ticking the **Enable Daylight Saving** check box and then using the drop-down menus to configure the desired **Daylight Saving Offset** and Daylight Saving starting and ending dates.

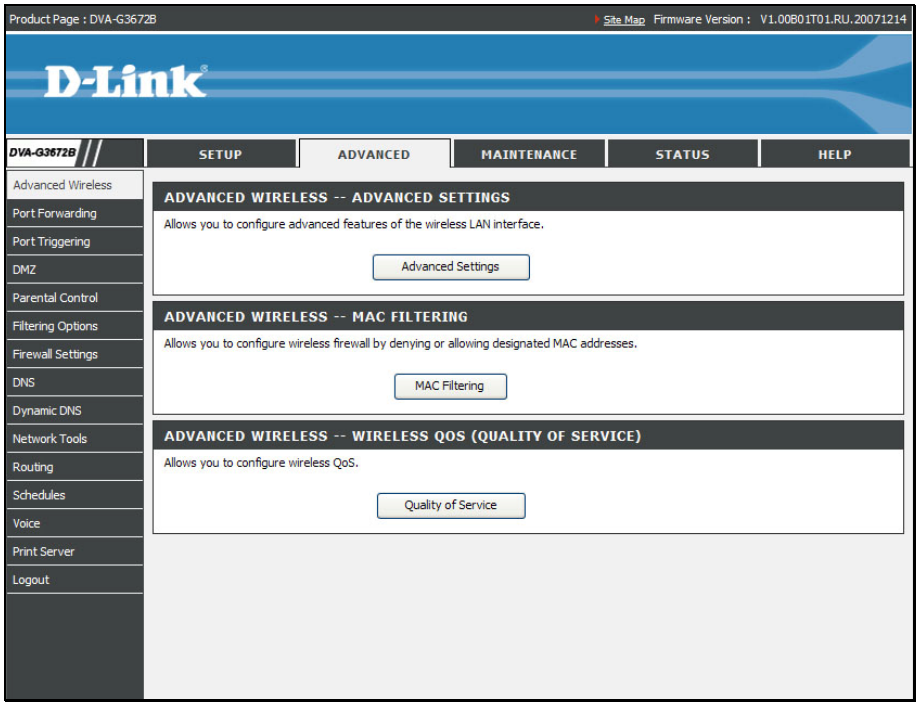
When you are finished, click the **Apply** button. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.



# Advanced – Advanced Wireless

To access Advanced Wireless, click **Advanced Wireless** in the **Advanced** directory.

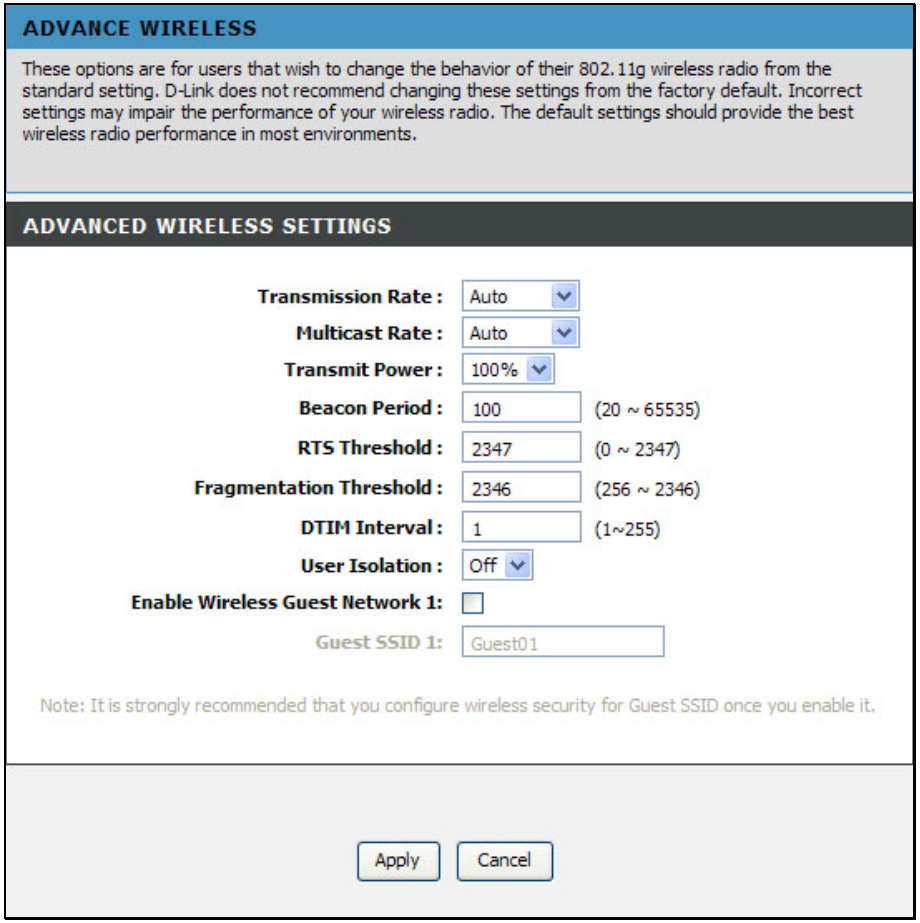
It has three subcategories: **Advanced Settings**, **MAC Filtering** and **Wireless QoS**. You can either point to the **Advanced Wireless** on the left window and click one of the submenus, or click one of the buttons in the Wireless Settings window.



# Advanced Wireless – Advanced Settings

To access Advanced Settings, point to the **Advanced Wireless** on the left window and click **Advanced Settings** submenu, or click the **Advanced Settings** button in the Wireless Settings window.

In this page, you can configure more advanced settings of 802.11g wireless radio. However, it is recommended to remain as default unless your ISP requests to change it.

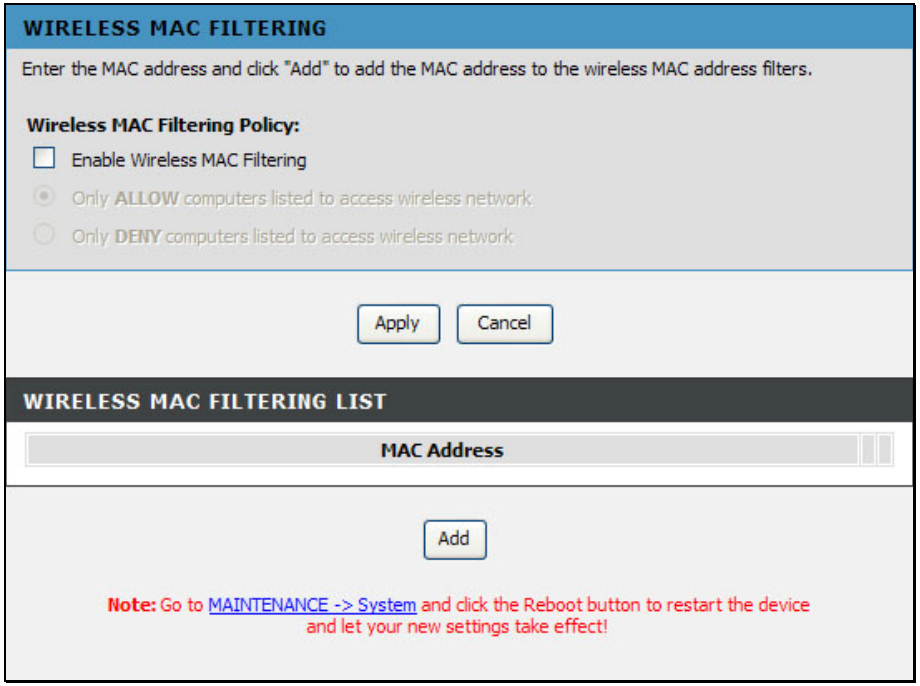


# Advanced Wireless – MAC Filtering

To access MAC Filtering, point to the **Advanced Wireless** on the left window and click **MAC Filtering** submenu, or click the **MAC Filtering** button in the Wireless Settings window.

This page can help you to allow or deny certain MAC addresses to pass through or block out.

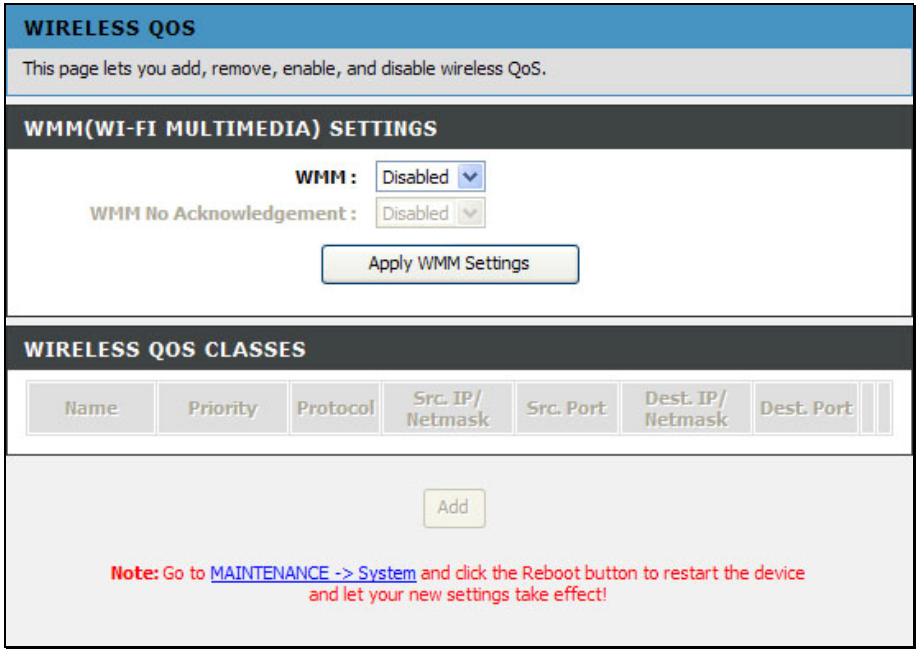
Click **Add** at the bottom of the window to enter MAC address.
Click **Apply** at the bottom of the page to add the MAC address to the wireless MAC filtering list.
Select **Enable Wireless MAC Filter** and click the **only ALLOW computers listed to access wireless network** or **only DENY computers listed to access wireless network** of the filtering policy. Click **Apply** to save the settings. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let the new settings take effect.



# Advanced Wireless – Wireless QoS

To access Wireless QoS, point to the **Advanced Wireless** on the left window and click **Wireless QoS** submenu, or click the **Quality of Service** button in the Wireless Settings window.

Select WMM to enable can control the transmitting of voice or video over wireless connection in order to provide better connection quality. Select WMM No Acknowledgement to enable could have more efficient throughout but higher error rates in a noisy Radio Frequency (RF) environment.
Click **Add** at the bottom of the window to see the Add Wireless QoS Classes section. Enter information in the section, and click **Apply**. Click **Apply WMM Settings** to save the settings. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let the new settings take effect.

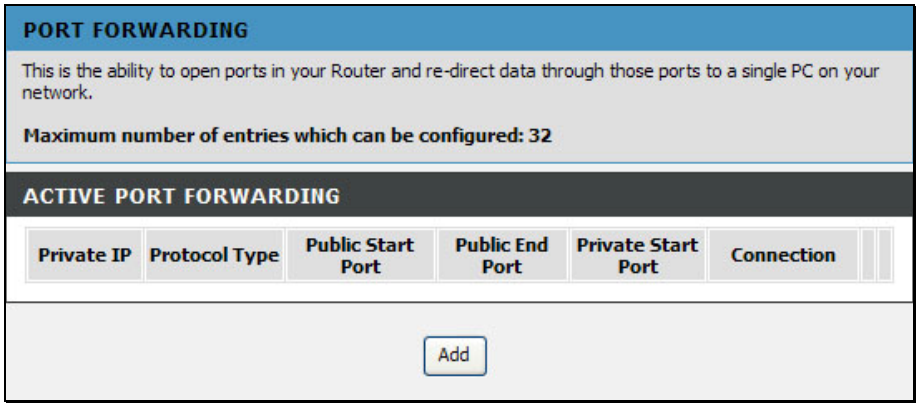


# Advanced – Port Forwarding

To access the Port Forwarding window, click the **Port Forwarding** button in the **Advanced** directory. Port Forwarding is used to redirect data to a single PC.

Click the **Add** button to set up a rule as follows.

Enter an IP address in the Private IP field, select a Protocol Type from the drop-down list, enter a range of ports in the Public Start Port and Public End Port fields, and then click the **Apply** button to see the customized rule in the ACTIVE PORT FORWARDING RULES table.



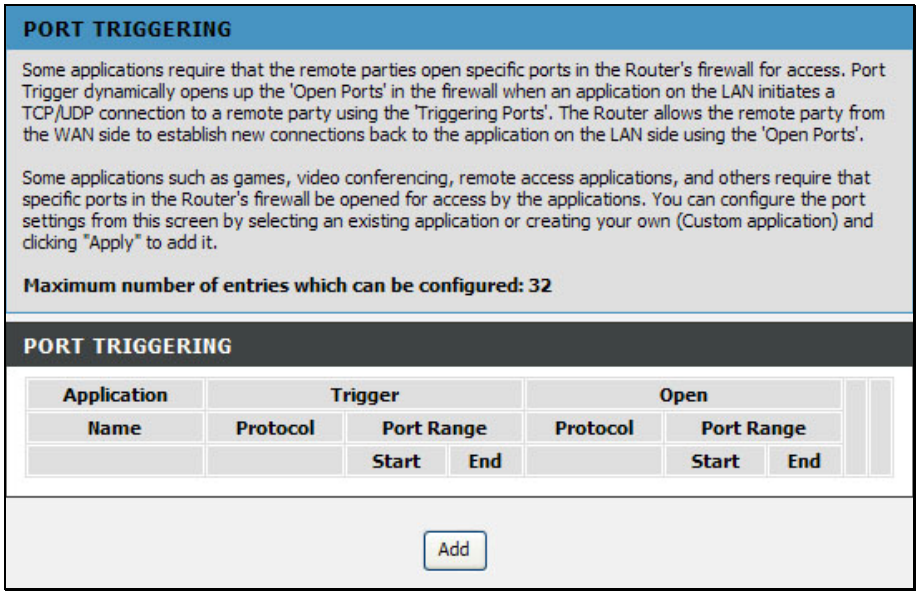
# Advanced – Port Triggering

To access the Port Triggering window, click the **Port Triggering** button in the **Advanced** directory.

Some applications require that the remote parties open specific ports in the Router's firewall for access. Port Trigger dynamically opens the Open Ports in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using Trigger Ports. The Router allows the remote party form the WAN side to establish new connections back to the application on the LAN side using the Open Ports.

Applications such as games, video conferencing, and other remote access applications require that specific ports in the Router's firewall be opened for access by applications.

Click **Add** to see the Add Port Triggering section. You can configure the port settings on this window by clicking the **Select an application** radio button and then using the drop-down list to choose an existing application, or by clicking the **Custom application** radio button and entering your own Application Rule in the field provided. Click **Apply** when you are finished with the port setting configuration. The new Application Rule will appear in the Port Triggering table.

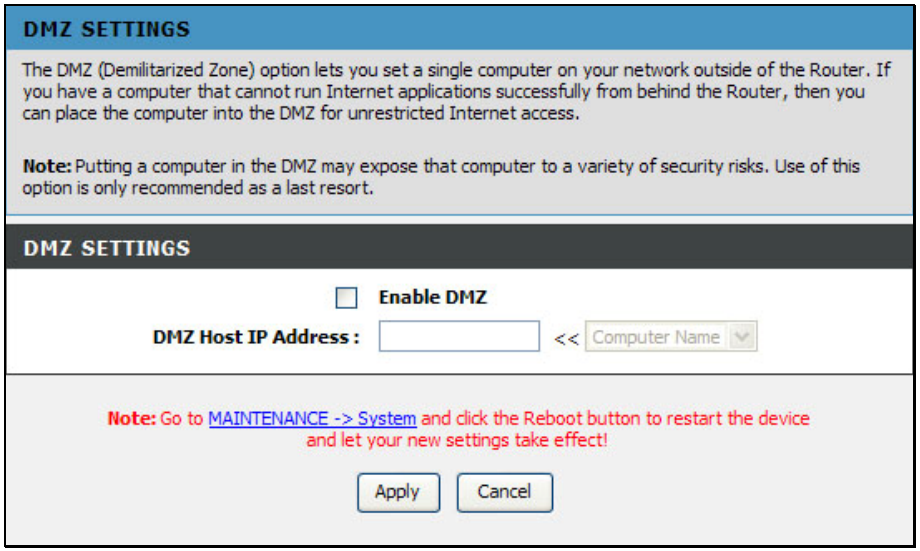


# Advanced – DMZ

To access the DMZ (Demilitarized Zone) window, click the **DMZ** button in the **Advanced** directory.

Since some applications are not compatible with NAT, the Router supports use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and will therefore be visible to agents on the Internet with the right type of software. Keep in mind that any client PC in the DMZ will be exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through the DMZ.

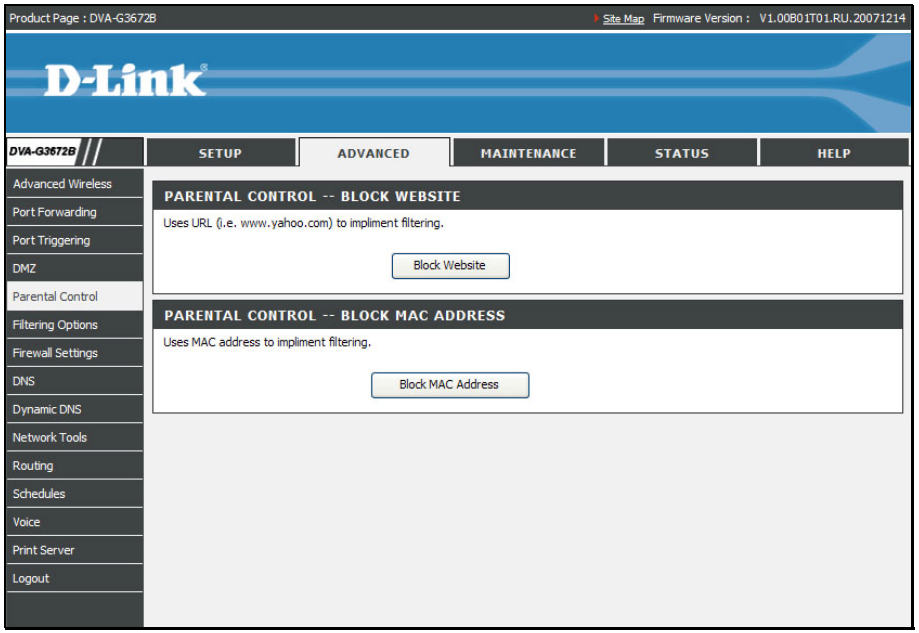
To designate a DMZ IP address, select **Enabled DMZ**, type in the IP Address of the server or device on your LAN, and click the **Apply** button. To remove DMZ status from the designated IP address, deselect the **Enable DMZ** and click **Apply**. It will be necessary to save the settings and reboot the Router before the DMZ is activated.



# Advanced – Parental Control

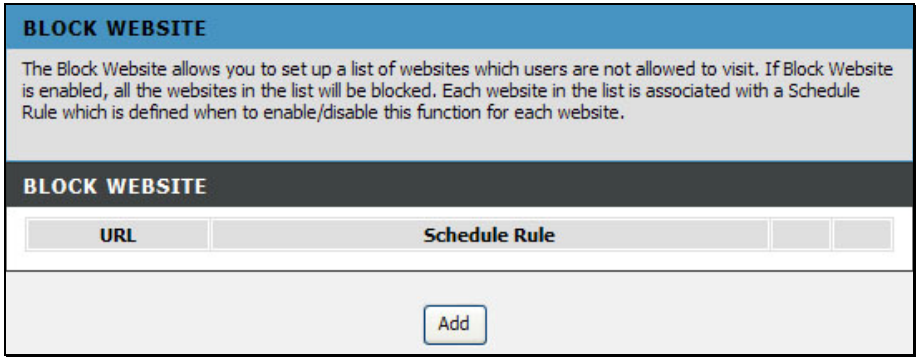
To access the Parent Control window, click the **Parent Control** button in the **Advanced** directory.

It has two subcategories: **Block Website** and **Block MAC Address**. You can either point to the **Parental Control** on the left window and click one of the submenus, or click one of the buttons in the Parental Control window.



# Parental Control – Block Website

To access Block Website, point to the **Parental Control** on the left window and click **Block Website** submenu, or click the **Block Website** button in the Parental Control window.



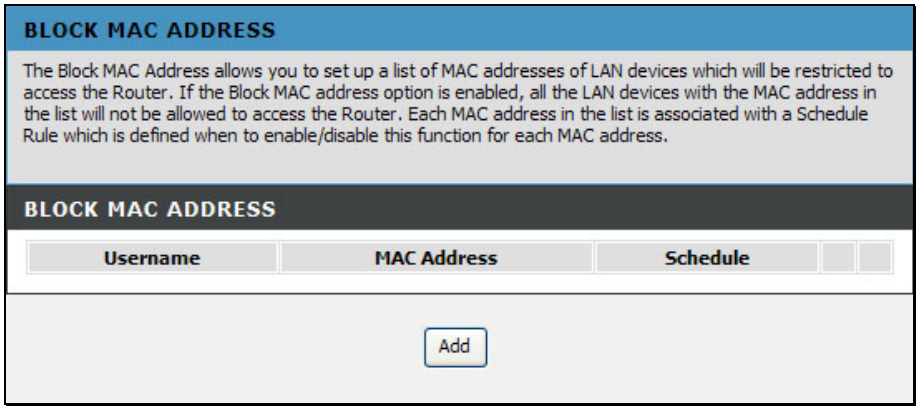

Use this window to deny access to specified websites.

Click **Add** to see the **Add Block Website** section. URL (Uniform Resource Locator) is a specially formatted text string that uniquely defines an Internet website. This section will allow users to block computers on the LAN from accessing certain URLs. This may be accomplished by simply entering the URL to be blocked in the **URL** field.

To configure for URL blocking, enter the website's address into the **URL** field, click **Schedule Rule** or **Manual Schedule** radio button. For Schedule Rule, select a rule in the drop down list. Rules in the list can be configured in **Advanced** -> **Schedules**. For manual Schedule configure as follows. Use the radio buttons to click the desired **Day(s)**, either **All Week** or **Select Day(s)** (in which case you must tick the checkboxes for the desired individual days of the week), select the desired **Start Time** and **End Time** or tick the **All Day – 24 hrs** checkbox, and then click the **Block Website** button. Click the **Apply** button to see the configured URL blocking entry is displayed in the Block Website. To remove a Blocked URL entry in the table, click the corresponding button. To modify a table entry, click the corresponding button, make the desired changes, and then click the **Apply** button.

# Parental Control – Block MAC Address

Use this window to deny access to specified MAC address.



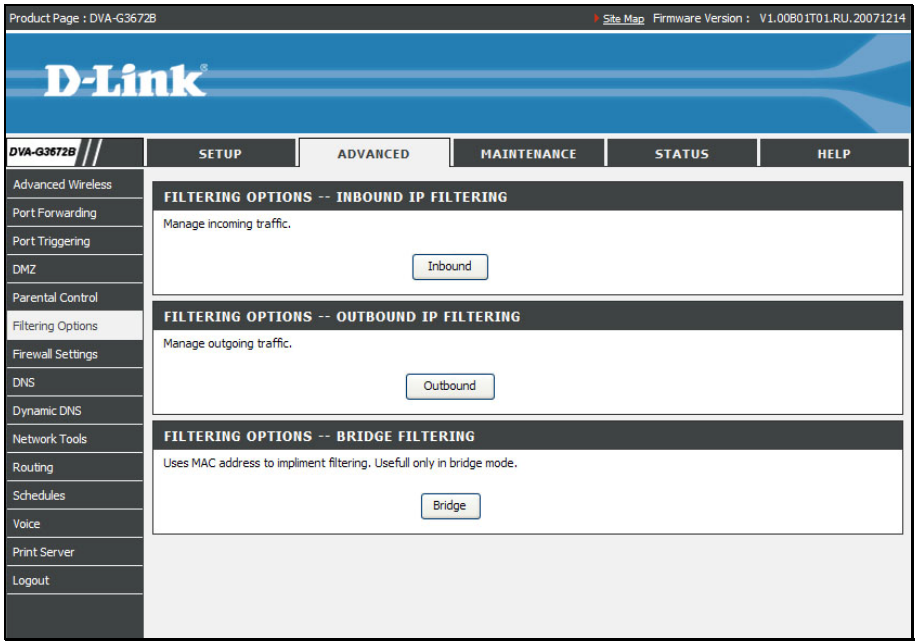

Click **Add** to see the **Add Block MAC Address** section. MAC address is a specially formatted text string (xx:xx:xx:xx:xx:xx) that uniquely identification of a device. This section will allow users to block devices with certain MAC addresses on the LAN.

To configure for MAC address blocking, enter the username into the **Username** field, click **Current PC's Mac Address** to have MAC address of current computer, or click **Other MAC Address** and enter a MAC address manually. Click **Schedule Rule** or **Manual Schedule** radio button to configure the time schedule. For Schedule Rule, select a rule in the drop down list. Rules in the list can be configured in **Advanced** -> **Schedules**. For manual Schedule configure as follows. Use the radio buttons to click the desired **Day(s)**, either **All Week** or **Select Day(s)** (in which case you must tick the checkboxes for the desired individual days of the week), select the desired **Start Time** and **End Time** or tick the **All Day – 24 hrs** checkbox, and then click the **Block Website** button. Click the **Apply** button to see the configured URL blocking entry is displayed in the Block Website. To remove a Blocked URL entry in the table, click the corresponding button. To modify a table entry, click the corresponding button, make the desired changes, and then click the **Apply** button.

# Advanced – Filtering Options

To access the Filtering Options window, click the **Filtering Options** button in the **Advanced** directory.

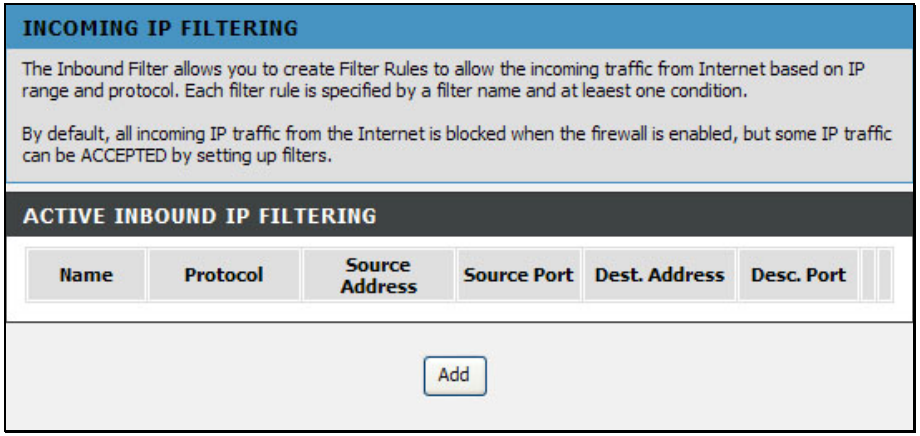
It has three subcategories: **Inbound Filtering**, **Outbound Filtering** and **Bridge Filtering**. You can either point to the **Filtering Options** on the left window and click one of the submenus, or click one of the buttons in the Filtering Options window.



# Filtering Options – Inbound Filtering

To access Inbound Filtering, point to the **Filtering Options** on the left window and click **Inbound Filtering** submenu, or click the **Inbound** button in the Filtering Options window.

The Inbound Filter allows you to create a filter rule to allow incoming IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. By default, all incoming IP traffic from the Internet is blocked when the firewall is enabled.




Click the **Add** button to see the Add Inbound IP Filtering section, enter the information in the section. Explanations of parameters are described below. Click the **Apply** button to add the entry in the Active Inbound IP Filtering table. To remove an entry in the table, click the corresponding button. To modify a table entry, click the corresponding button, make the desired changes, and then click the **Apply** button.

| Filters Parameter | Description | |
|---|---|---|
| Filter Name | Enter a name for the new filter. | |
| Protocol | Select the transport protocol (TCP and UDP, TCP, UDP, ICMP or Any) that will be used for the filter rule. | |
| Select IP Range by | Select either **IP Address** or **Netmask** to show different items. | |
| | Source IP Address | Enter the start and end IP address for the range of IP addresses which you are creating the filter rule. |
| | Source IP Address & Source Subnet Mask | This is the IP address and their associated subnets for which you are creating the filter rule. |
| Source Port | The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. | |
| Destination Port | The Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. | |

# Filtering Options – Outbound Filtering

To access Outbound Filtering, point to the **Filtering Options** on the left window and click **Outbound Filtering** submenu, or click the **Outbound** button in the Filtering Options window.

The Outbound Filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Filters are used to allow or deny LAN or WAN users from accessing the Internet or your internal network.


Click the **Add** button to see the Add Outbound IP Filtering section, enter the information in the section. Explanations of parameters are described below. Click the **Apply** button to add the entry in the Active Outbound IP Filtering table. To remove an entry in the table, click the corresponding button. To modify a table entry, click the corresponding button, make the desired changes, and then click the **Apply** button.

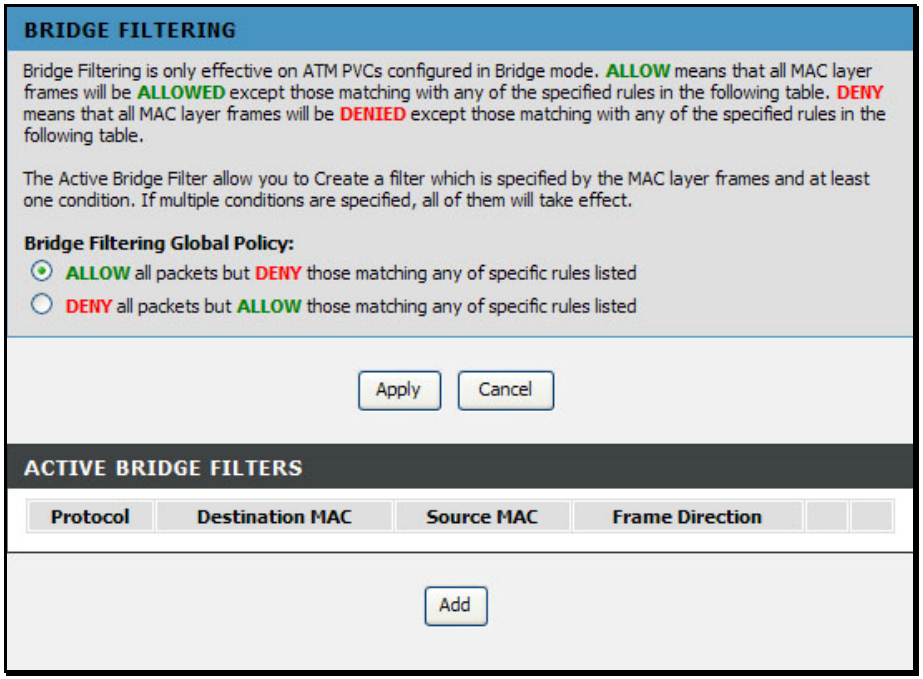
| Filters Parameter | Description | |
|---|---|---|
| Filter Name | Enter a name for the new filter. | |
| Protocol | Select the transport protocol (TCP and UDP, TCP, UDP, ICMP or Any) that will be used for the filter rule. | |
| Select IP Range by | Select either **IP Address** or **Netmask** to show different items. | |
| | Source IP Address | Enter the start and end IP address for the range of IP addresses which you are creating the filter rule. |
| | Source IP Address & Source Subnet Mask | This is the IP address and their associated subnets for which you are creating the filter rule. |
| Source Port | The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. | |
| Destination Port | The Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. | |

# Filtering Options – Bridge Filtering

To access Bridge Filtering, point to the **Filtering Options** on the left window and click **Bridge Filtering** submenu, or click the **Bridge** button in the Filtering Options window.

Bridge filters are used to block or allow various types of packets through the WAN/LAN interface. This may be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address. Filter rules can be set up for source, destination or both. You can set up filter rules and disable the entire set of rules without loosing the rules that have been configured.

Select Bridge Filtering Global Policy: **ALLOW all packets but DENY those matching any of the specific rules listed** or **DENY all packets but ALLOW those matching any of the specific rules listed** for the rules that configured below. Click the **Add** button to see the Add Bridge Filter section. Select a protocol (PPPoE, IPv4, IPv6, Apple Talk, IPX or IGMP) in the **Protocol Type** list, type in a Source MAC, a Destination MAC or both in the entry fields. Select a direction (LAN=>WAN, WAN=>LAN, or LAN<=>WAN) in the **Frame Direction** list. Click the **Apply** button to add the entry in the Active Bridge Filters table. To remove an entry in the table, click the corresponding button. To modify a table entry, click the corresponding button, make the desired changes, and then click the **Apply** button.

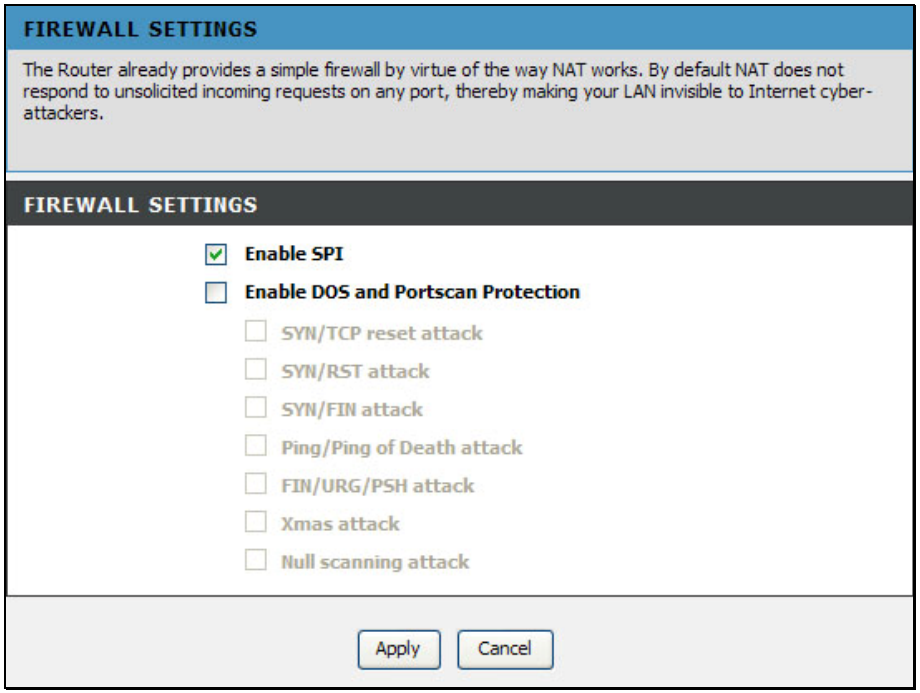


# Advanced – Firewall Settings

To access the Firewall Settings window, click the **Firewall Settings** button in the **Advanced** directory.

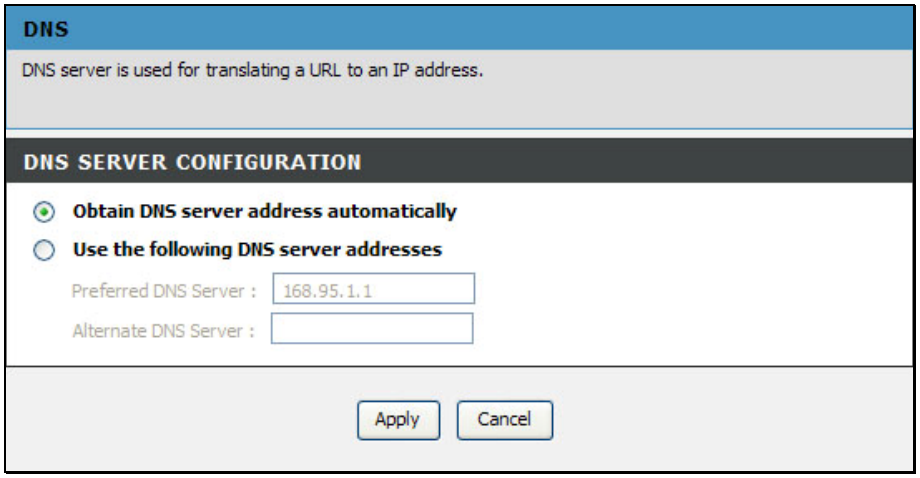
This page allows the Router to enforce specific predefined policies intended to protect against certain common types of attacks. Stateful Packet Inspection (SPI) is a packet inspection process that blocks unwanted and unrequested packets trying to reach PCs on your LAN. A DoS "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person. Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

When you have selected the desired Firewall settings by ticking the corresponding check boxes for the various types of protection offered on this window, click **Apply**.



# Advanced – DNS

To access the DNS window, click the **DNS** button in the **Advanced** directory.



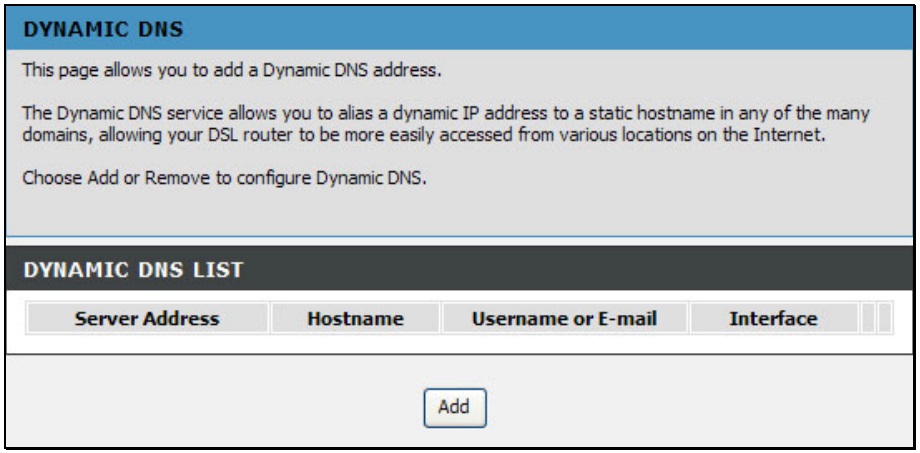

The Router can be configured to relay DNS settings from your ISP or another available service to workstations on your LAN. When using DNS relay, the Router will accept DNS requests from hosts on the LAN and forward them to the ISP's, or alternative DNS servers. DNS relay can use auto discovery or the DNS IP address can be manually entered by the user. Alternatively, you may also disable the DNS relay and configure hosts on your LAN to use DNS servers directly. Most users who are using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network, will leave DNS relay enabled (either auto discovery or user configured).

If you have not been given specific DNS server IP addresses or if the Router is not pre-configured with DNS server information, select the **Obtain DNS server address automatically** option. Auto discovery DNS instructs the Router to automatically obtain the DNS IP address from the ISP through DHCP. If your WAN connection uses a Static IP address, auto discovery for DNS cannot be used.

If you have DNS IP addresses provided by your ISP, click the **Use the following DNS server addresses** radio button and enter these IP addresses in the available entry fields for the Preferred DNS Server and the Alternative DNS Server. When you have configured the DNS settings as desired, click the **Apply** button.

# Advanced – Dynamic DNS

To access the Dynamic DNS window, click the **Dynamic DNS** button in the **Advanced** directory.



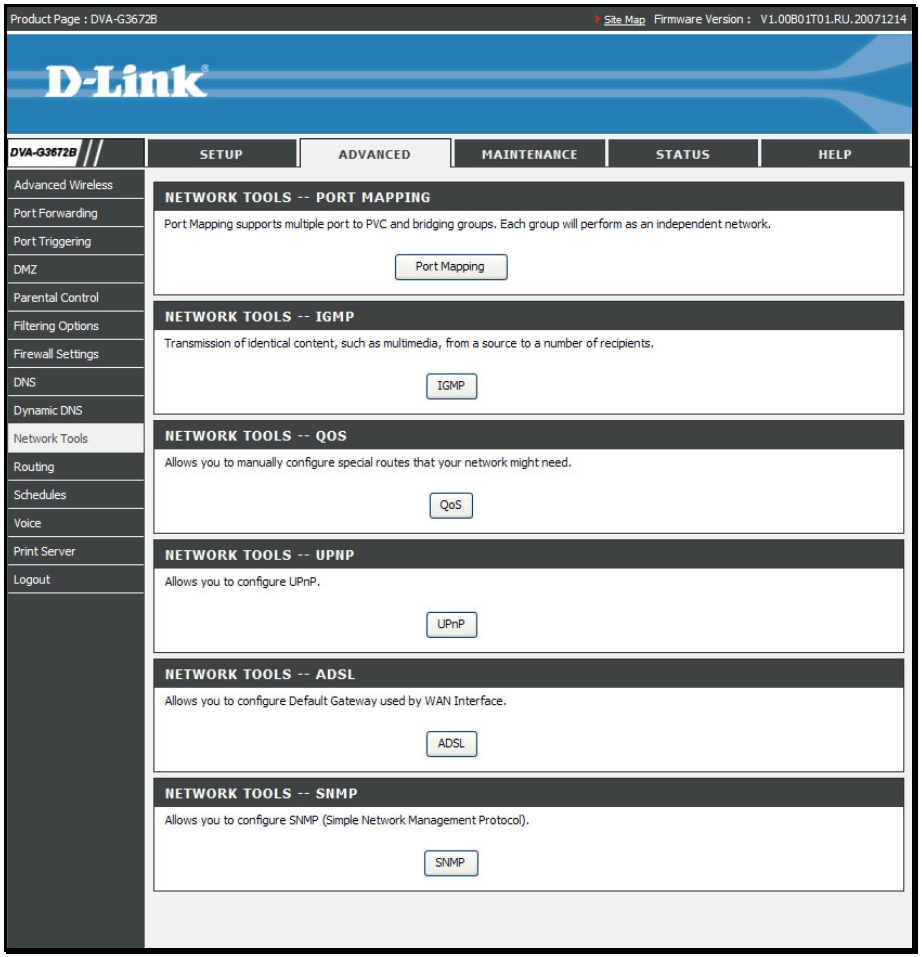

The Router supports DDNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form hostname.dyndns.org, Many ISPs assign public IP addresses using DHCP, this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS providers.

Click **Add** to see the Add DDNS Settings section. Enter the required DDNS information, click the **Apply** button to see the entry in the Dynamic DNS List table. To remove an entry in the table, click the corresponding button. To modify a table entry, click the corresponding button, make the desired changes, and then click the **Apply** button.

# Advanced – Network Tools

To access the Network Tools window, click the **Network Tools** button in the **Advanced** directory. It has six subcategories: **Port Mapping**, **IGMP**, **QoS**, **UPnP**, **ADSL** and **SNMP**.

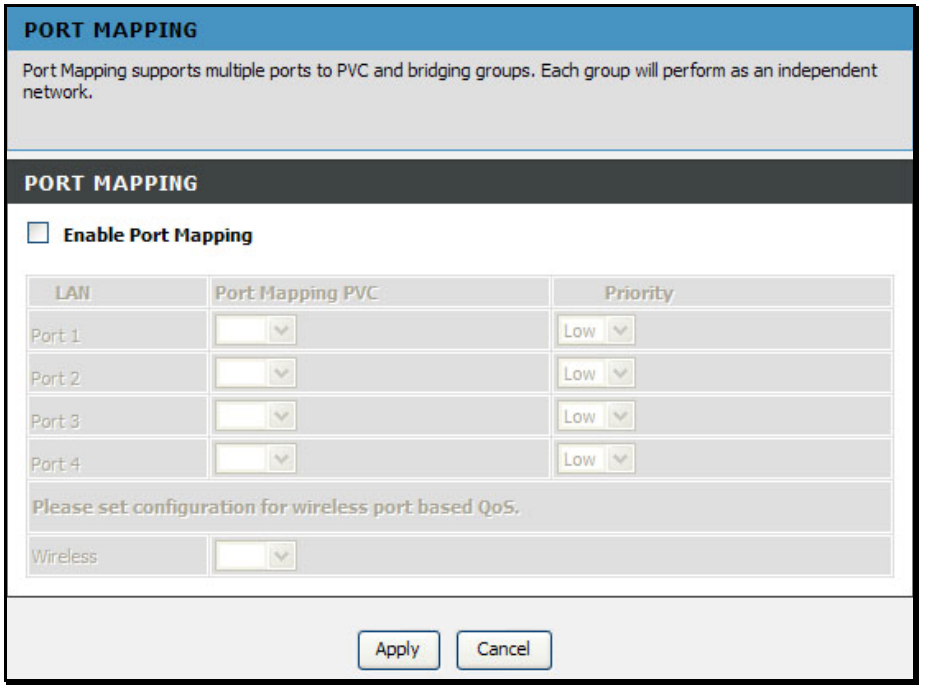
You can either point to the **Network Tools** on the left window and click one of the submenus, or click one of the buttons in the Network Tools window.



# Network Tools – Port Mapping

To access Port Mapping, point to the **Network Tools** on the left window and click **Port Mapping** submenu, or click the **Port Mapping** button in the Network Tools window.

Tick the **Enable Port Mapping** check box and select a PVC and its Priority assigning to the specific LAN port or wireless LAN. Click **Apply** to take effect.

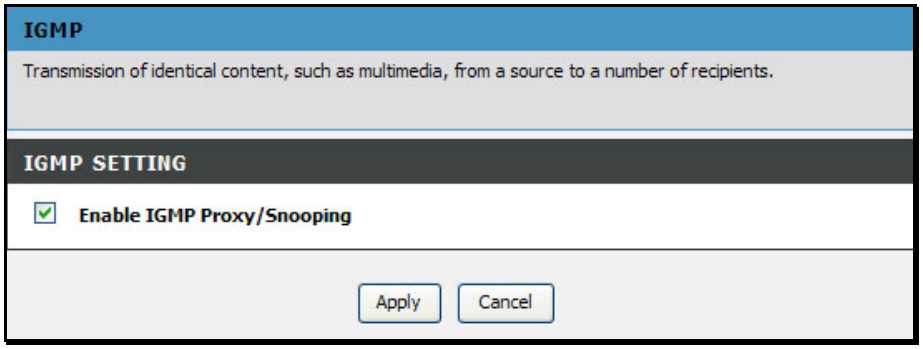


# Network Tools – IGMP

To access IGMP, point to the **Network Tools** on the left window and click **IGMP** submenu, or click the **IGMP** button in the Network Tools window.

IGMP (Internet Group Management Protocol) page is for identical content transmission.

When the **Enable IGMP Proxy/Snooping** check box is selected, Multicast packets are allowed to pass in both directions on the WAN interface. Most users will want to leave this on.

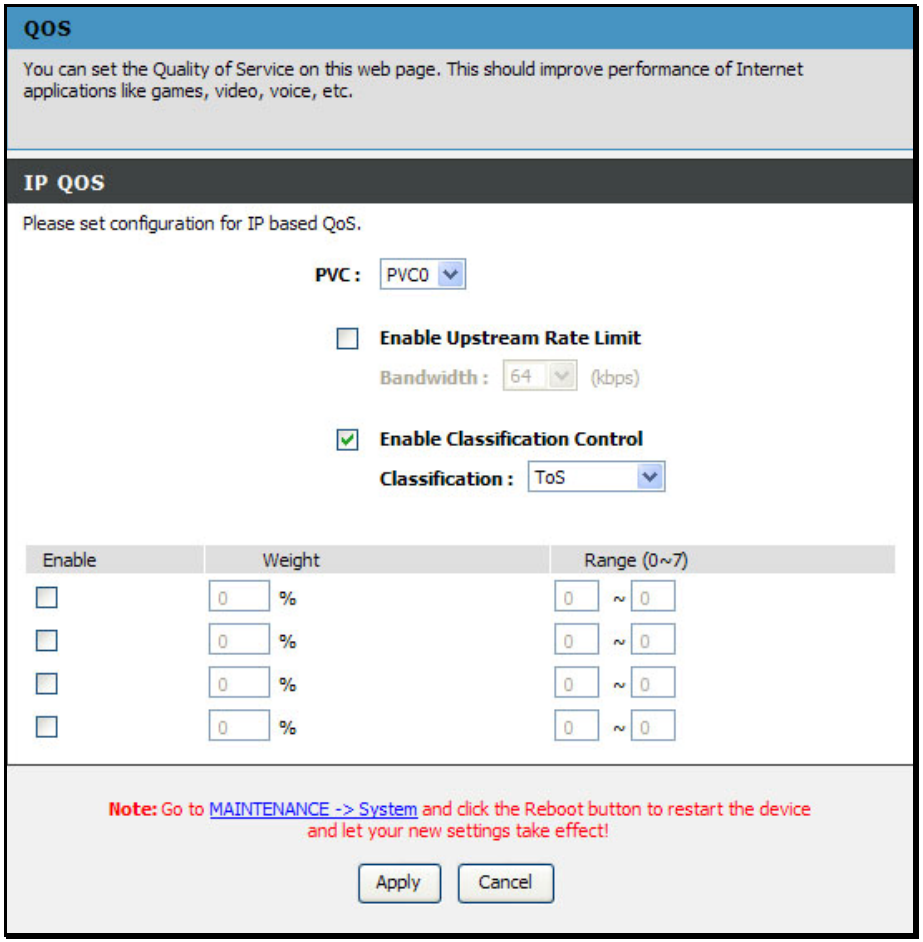


# Network Tools – QoS

To access QoS, point to the **Network Tools** on the left window and click **QoS** submenu, or click the **QoS** button in the Network Tools window.

QoS or Quality of Service allows your Router to help prioritize the data packet flow in your Router and network. This is very important for time sensitive applications such as VoIP where it may help prevent dropped calls. Large amounts of non-critical data can be scaled so as not to affect these prioritized sensitive real-time programs.

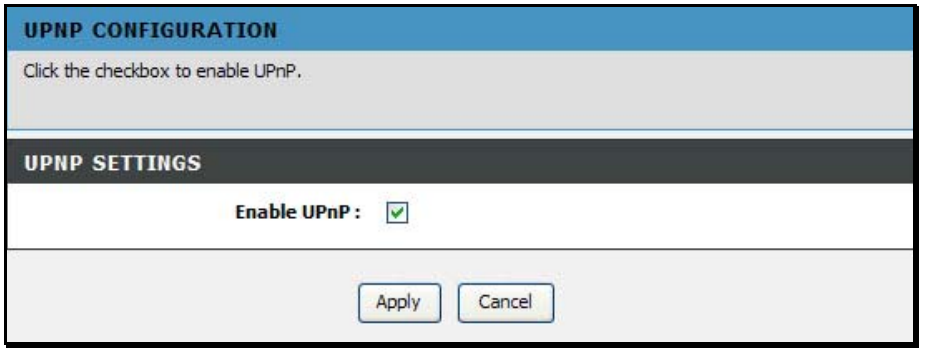
Select one of the PVC connections for QoS. The Router allows you to manually configure Upstream Rate Limit or Classification Control. Tick **Enable Upstream Rate Limit** and select a number in the **Bandwidth** list to control the transmission rate. Tick the **Enable Classification Control** check box and you can choose ToS, Application or User Define classifications. The information in the table below the selection differs based on the classifications you select.
Tick the **Enable** check box for each queue configured and enter information in the corresponding fields. Some experimentation may be necessary to achieve the optimum results with your particular ISP's connection. When you are finished, click **Apply**. Go to **Maintenance** -> **System**, and click the **Reboot** button to let your new settings take effect.



# Network Tools – UPnP

To access UPnP, point to the **Network Tools** on the left window and click **UPnP** submenu, or click the **UPnP** button in the Network Tools window.

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network. UPnP is a protocol supported by diverse networking media including Ethernet, Firewire, phone line, and power line networking.



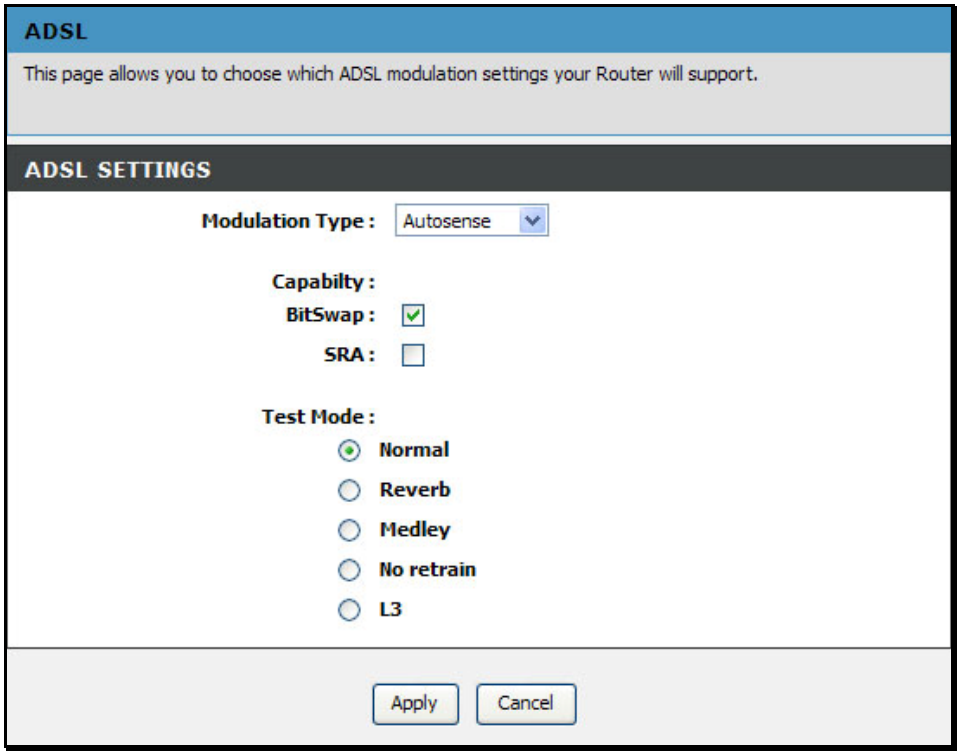

To enable UPnP for any available connection, tick the Enable UPnP check box, and click the **Apply** button.

# Network Tools – ADSL

To access ADSL, point to the **Network Tools** on the left window and click **ADSL** submenu, or click the **ADSL** button in the Network Tools window.

This window allows the user to set the configuration for ADSL protocols. For most ADSL accounts the default settings *Autosense* will work. This configuration works with all ADSL implementations. If you have been given instructions to change the Modulation method used, select the desired option from the **Modulation Type** drop-down list and click the **Apply** button.

Leave the Capability and Test Mode settings unchanged unless otherwise instructed by your ISP. Both Bitswap Enable and Seemless Rate Adaption (SRA) Enable deal with tests that determine the line condition between your Router and the ISP's Central office.

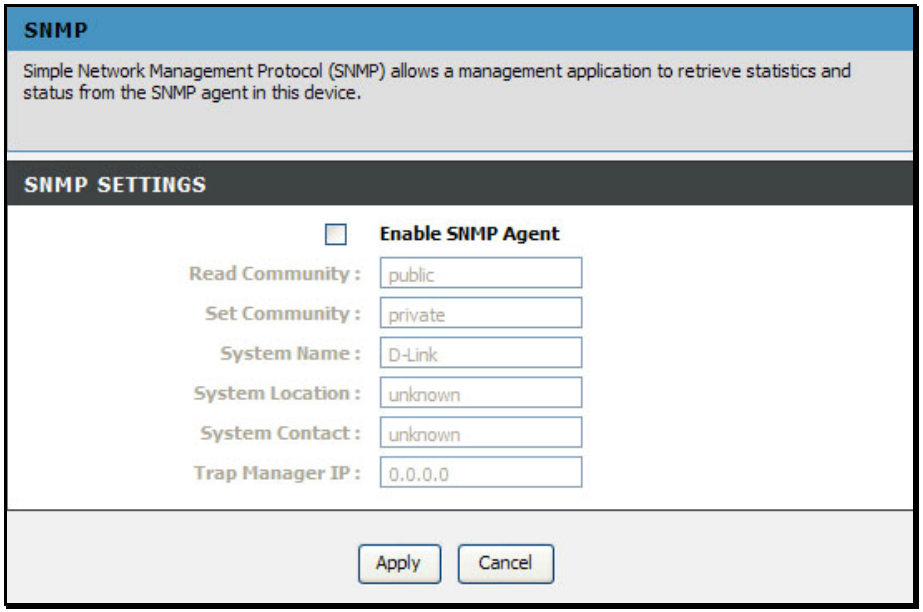


# Network Tools – SNMP

To access SNMP, point to the **Network Tools** on the left window and click **SNMP** submenu, or click the **SNMP** button in the Network Tools window.

Simple Network Management Protocol is a standard for internetwork and intranetwork management.

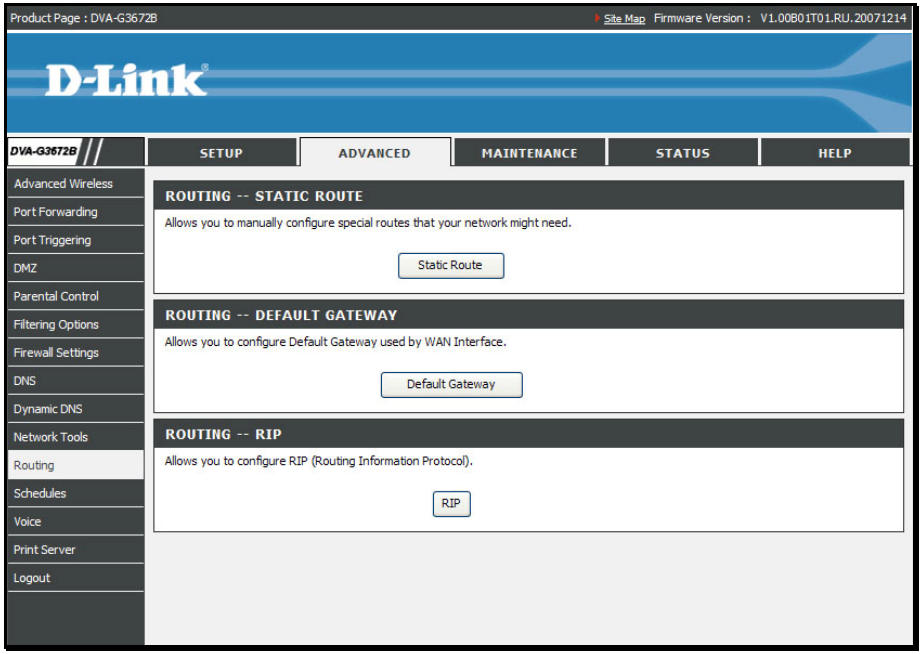
Tick the **Enable SNMP Agent** check box and configure the parameters for SNMP on this window and then click the **Apply** button.



# Advanced –Routing

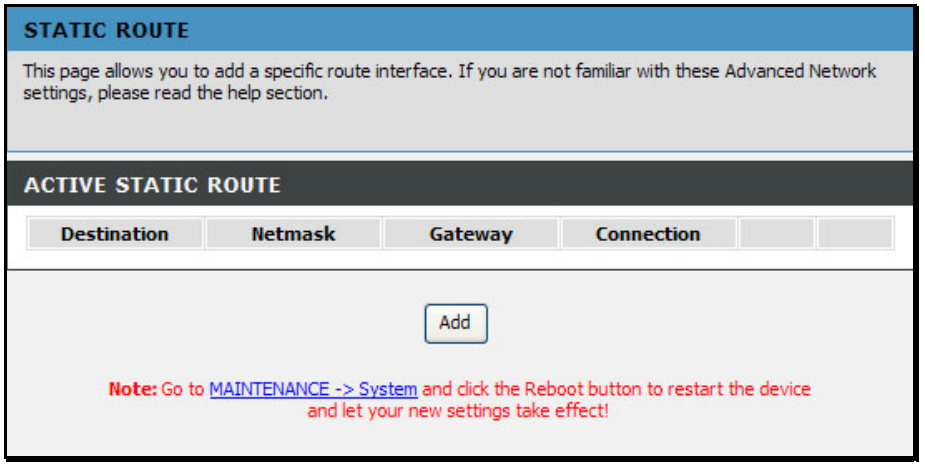
To access the Routing window, click the **Routing** button in the **Advanced** directory.

It has three subcategories: **Static Route**, **Default Gateway** and **RIP**. You can either point to the **Routing** on the left window and click one of the submenus, or click one of the buttons in the Routing window.



# Routing – Static Route

To access Static Route, point to the **Routing** on the left window and click **Static Route** submenu, or click the **Static Route** button in the Routing window.




The page allows you to manually enter the routing table.

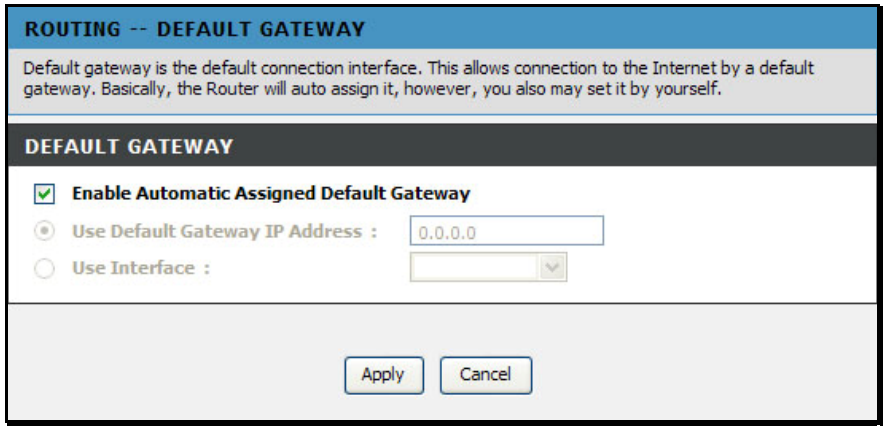
To define a gateway and hop to route data traffic, complete the fields in the Add Static Route section. Click **Apply** to see the entry in the Active Static Route table. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.

To add a static route to a specific destination IP, click **Add** to see the Add Static Route section. Enter a **Destination** IP address, **Netmask** and Gateway's IP address. Select a PVC in the **Connection** drop-down list. Click **Apply** to see the entry in the Active Static Route table. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect. To remove an entry in the table, click the corresponding button. To modify a table entry, click the corresponding button, make the desired changes, and then click the **Apply** button.

# Routing – Default Gateway

To access Default Gateway, point to the **Routing** on the left window and click **Default Gateway** submenu, or click the **Default Gateway** button in the Routing window.

This page can either automatically assign a default gateway to the device or manually type in a default gateway or the device or interface. It is recommended to leave **Enable Automatic Assigned Default Gateway** ticked to automatically detect the Gateway IP address.

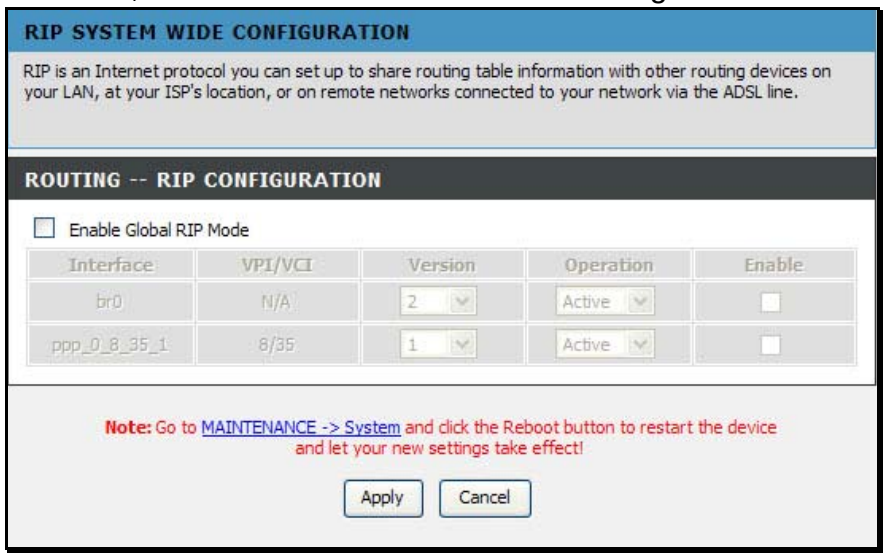



# Routing – RIP

To access RIP, point to the **Routing** on the left window and click **RIP** submenu, or click the **RIP** button in the Routing window.

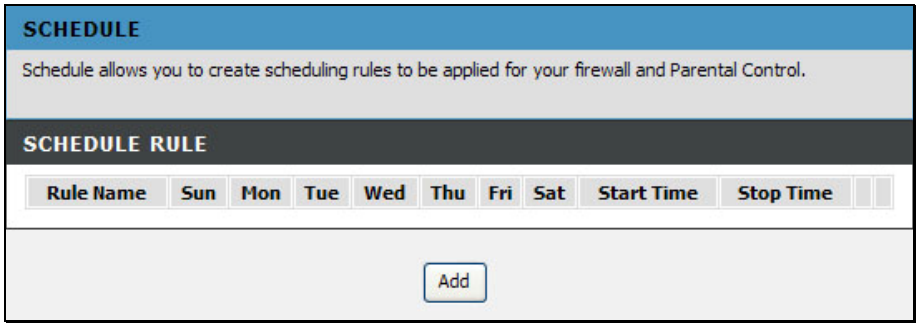
The Router supports RIP version 1 and 2 used to share routing tables with other Layer 3 routing devices on your local network or remote LAN. The Operation setting refers to the RIP request. Select *Active* to allow RIP requests from other devices. Select *Passive* to instruct the Router to make RIP requests for routing tables from other devices.

To enable RIP, tick the **Enable Global RTP Mode** check box, select the Version (1, 2, or Both) and Operation (*Active* or *Passive*), and tick the Enable check box in the corresponding entry. Click the **Apply** button. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.



# Advanced – Schedules

To access the Schedules window, click the **schedules** button in the **Advanced** directory.




You can add schedules in this page and then apply them to Parental Control.

Click **Add** to see the Add Schedule Rule section. Enter a Name for the schedule. Use the radio buttons to click the desired **Day(s)**, either **All Week** or **Select Day(s)** (in which case you must tick the checkboxes for the desired individual days of the week), select the desired **Start Time** and **End Time** or tick the **All Day – 24 hrs** checkbox. Click **Apply** to see the entry in the Schedule Rule table. To remove an entry in the table, click the corresponding button. To modify a table entry, click the corresponding button, make the desired changes, and then click the **Apply** button.

# Advanced – Voice

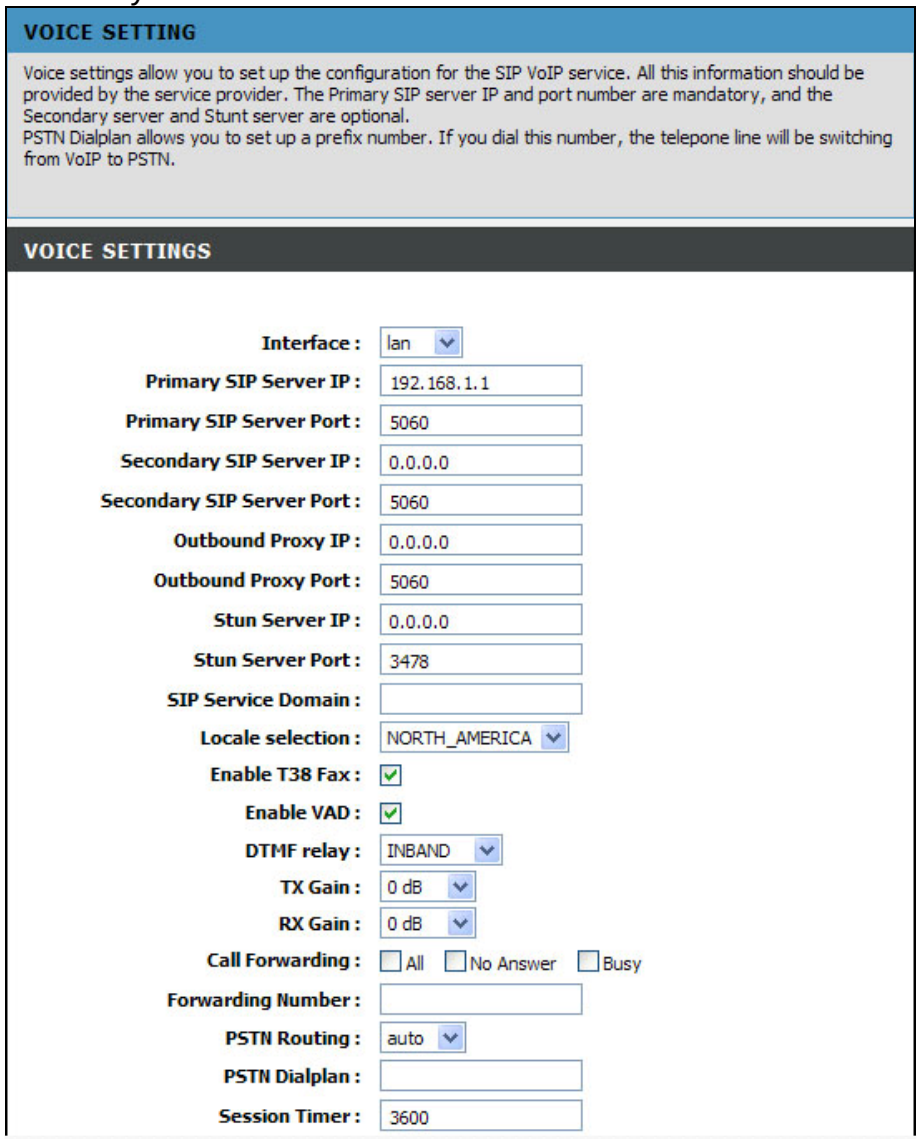
To access the Voice window, click the **Voice** button in the **Advanced** directory.

You can set up the basic VoIP settings in this page. All information in this page should be obtained by your ISP.

Voice over Internet Protocol (VoIP) is a protocol that can transmit the voice through the Internet. Session Initiation Protocol (SIP) is a widely used signaling protocol of VoIP. To start using the VoIP service, select an interface in the Interface list for the VoIP service, and enter the Primary SIP Server IP and Primary SIP Server Port. The Secondary SIP Server, Outbound Proxy IP, Stun Server and SIP Service Domain are optional. Tick **Enable T38 Fax** for sending fax data through the network. Tick **Enable VAD** to disable silent packet and send other transmission. Select a DTMF type (Inband, RFC2833 or SIP Info) in the **DTMF relay** drop-down list. Tick one of forwarding call methods for All, No Answer or Busy calls, and then type a number that calls is forwarded to. Select a routing rule of the PSTN line (auto, Line1 or Line2) in the **PSTN Routing** drop-down list. Enter digits in the **PSTN Dialplan** field for transferring VoIP service to PSTN service.

You can also set up the codec priorities in Codec Settings section. In VoIP Setting section, you can configure the user name and password for registering to SIP VoIP service.

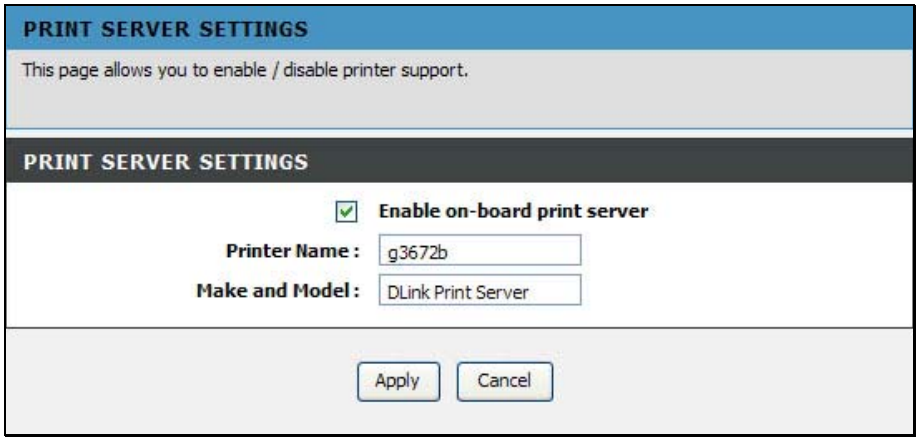
Click the **Apply** button, and go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.



# Advanced –Print Server

To access the Print Server window, click the **Print Server** button in the **Advanced** directory.

Tick the **Enable on-board print server** check box, enter a Printer Name and Model name in the fields, and click **Apply** to enable the printer server function.



# Maintenance – System

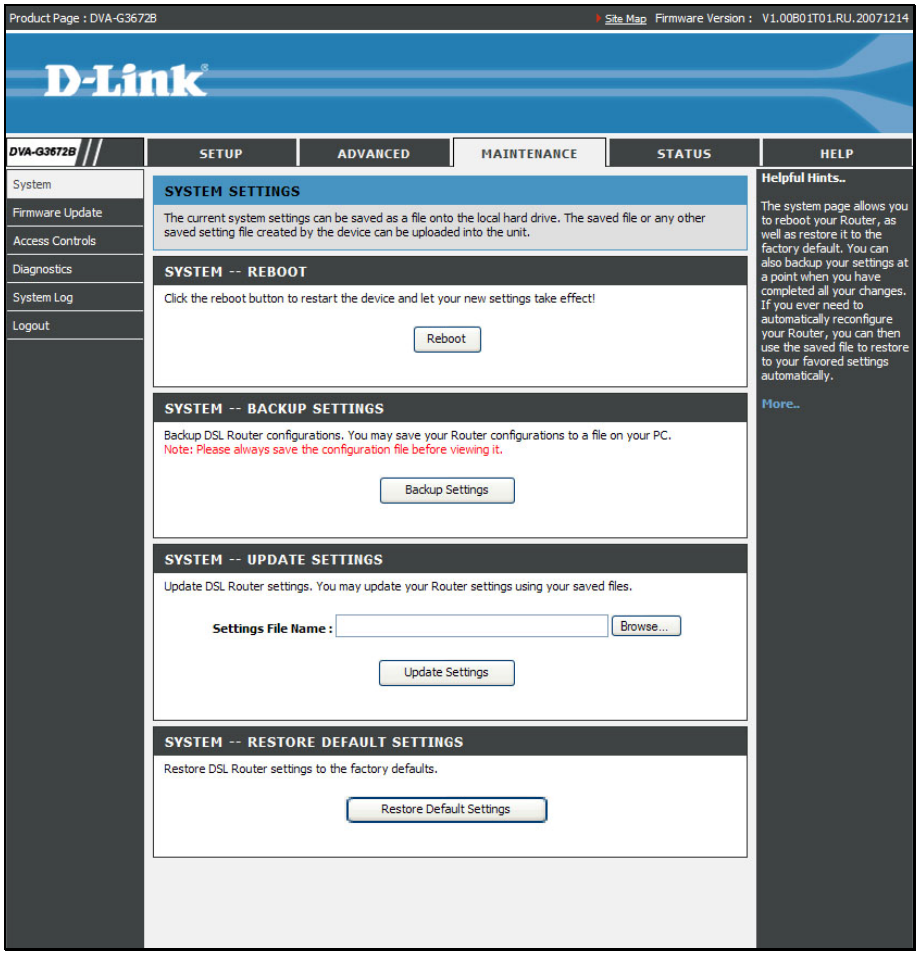
To access the System window, click the **System** button in the **Maintenance** directory.

When you configure the Router, you will need to restart the Router to take the settings effect. Click **Reboot** to restart the Router.

Once you have configured the Router to your satisfaction, it is a good idea to back up the configuration file to your computer. To save the current configuration settings to your computer, click the **Backup Settings** button. You will be prompted to select a location on your computer to put the file. The file type is bin and may be named anything you wish.

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Upload Settings** button to load the settings from your local hard drive. Confirm that you want to load the file when prompted. The Router will reboot and begin operating with the configuration settings that have just been loaded.

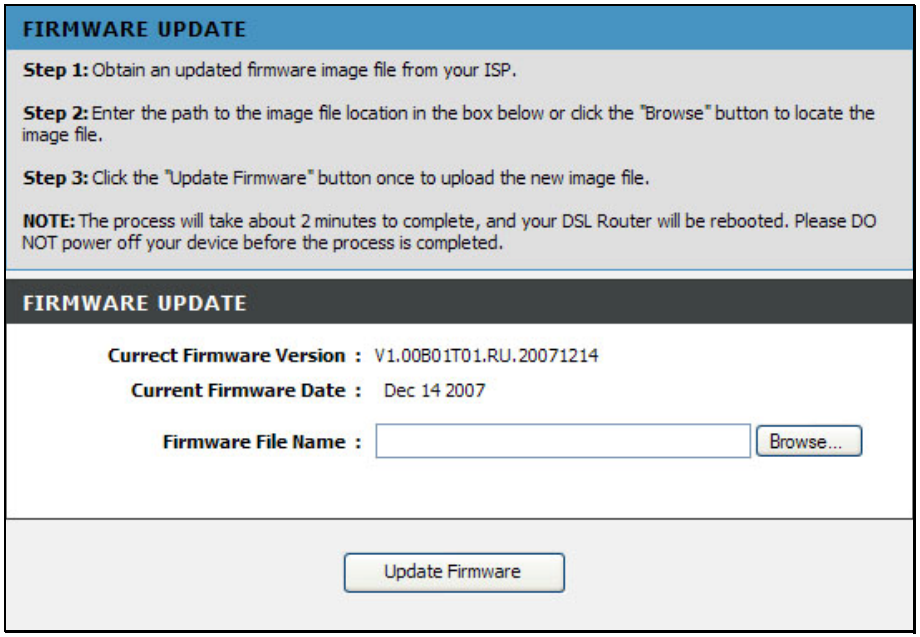
To reset the Router to its factory default settings, click the **Restore Default Settings** button. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings (192.168.1.1) and Administrator password (admin).



# Maintenance – Firmware Update

To access the Firmware Update window, click the **Firmware Update** button in the **Maintenance** directory.

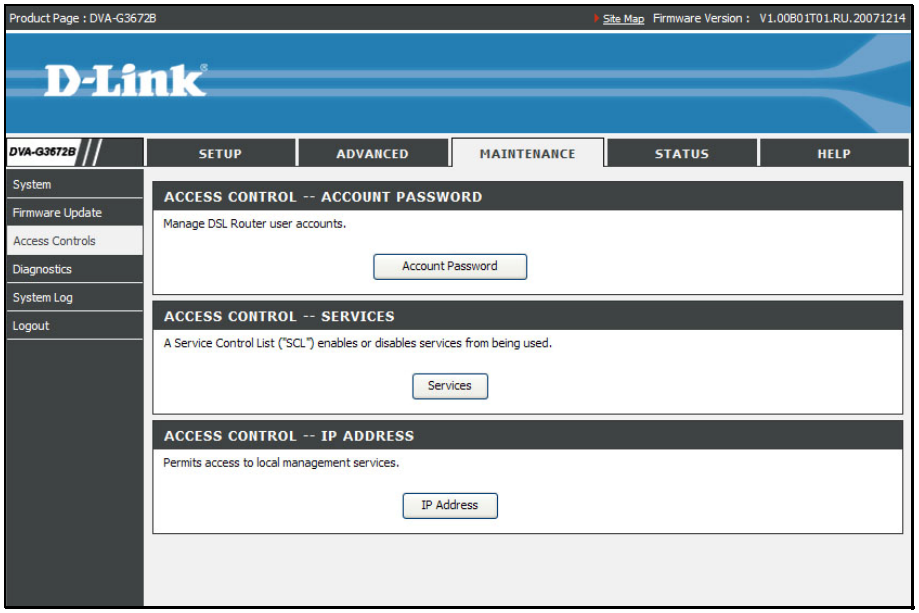
Use the Firmware Upgrade menu to load the latest firmware for the Router. Note that the Router configuration settings may return to the factory default settings, so make sure you save the configuration settings with the System menu described above. To upgrade firmware obtained from your ISP, click the **Browse** button to search for the file. Click the **Update Firmware** button to begin copying the file. The file will load and restart the Router automatically.



# Maintenance – Access Controls

To access the Access Controls window, click the **Access Controls** button in the **Maintenance** directory.

In this page, you can choose to change password, manage the service control or IP address control.

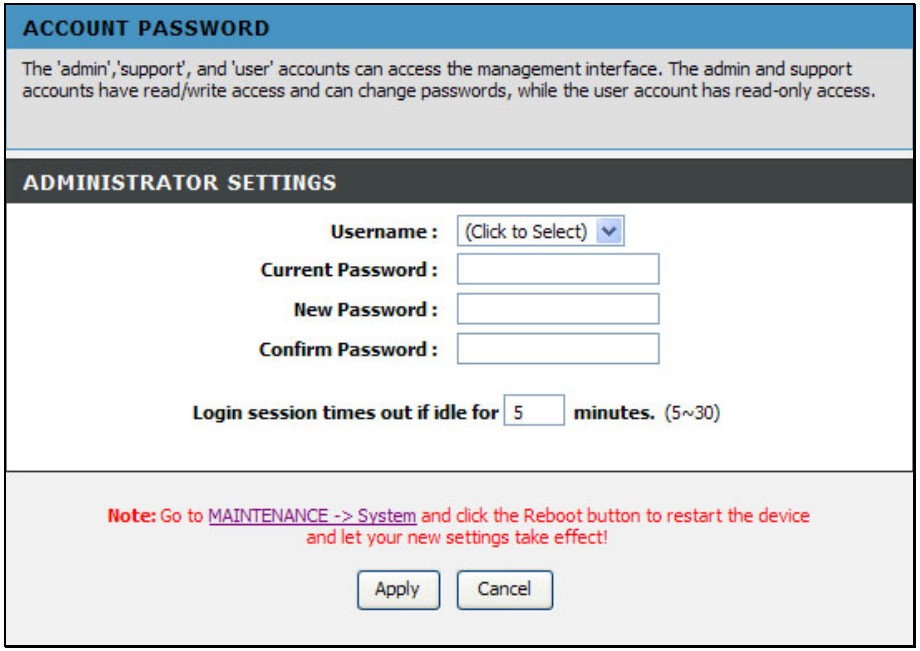


# Access Controls – Account Password

To access Account Password, point to the **Access Controls** on the left window and click **Account Password** submenu, or click the **Account Password** button in the Access Controls window.

There are three different user names for different purpose. Support is for remote supporter to login from WAN and is able to adjust TR-069 settings. User and Admin is to login from LAN. Select a user name (Admin, User or Support), type the Current Password in the first field, the New Password in the second field, and enter the password again in the Confirm Password field to be certain you have typed it correctly.

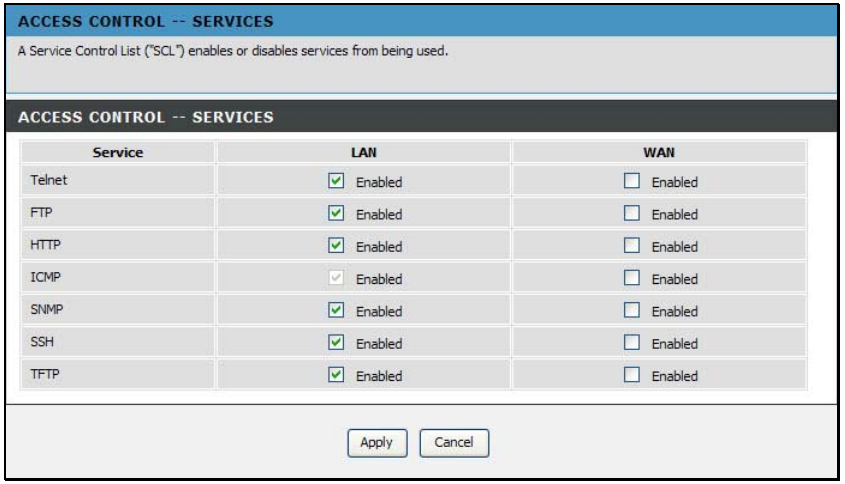
You can configure the idle time between 5 and 30 minutes for the webpage asking you to logout.
Click the **Apply** button. Go to **Maintenance** -> **System** and click **Reboot** to restart the device.



# Access Controls – Services

To access Services, point to the **Access Controls** on the left window and click **Services** submenu, or click the **Services** button in the Access Controls window.

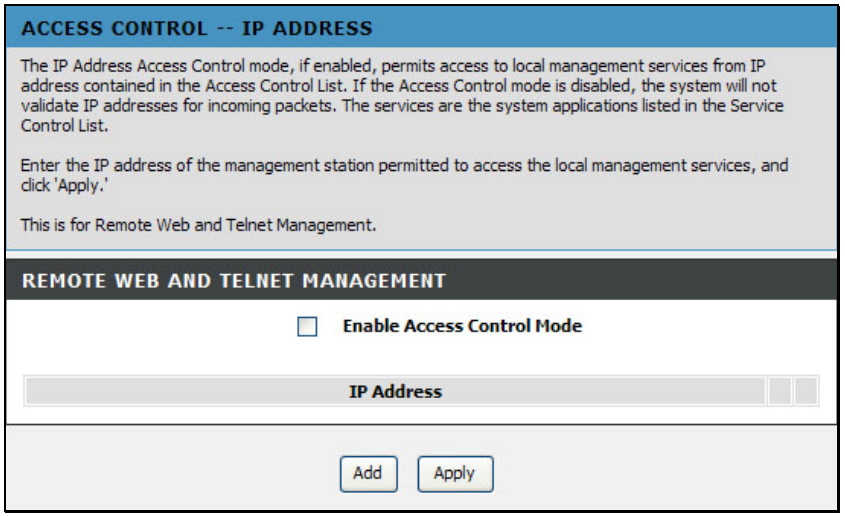
This page lists out all the available services including Telnet, FTP, HTTP, ICMP, SNMP, SSH and TFTP that can enable at LAN, WAN or both. Tick to enable the services, or deselect to disable them.




# Access Controls – IP Address

To access IP Address, point to the **Access Controls** on the left window and click **IP Address** submenu, or click the **IP Address** button in the Access Controls window.

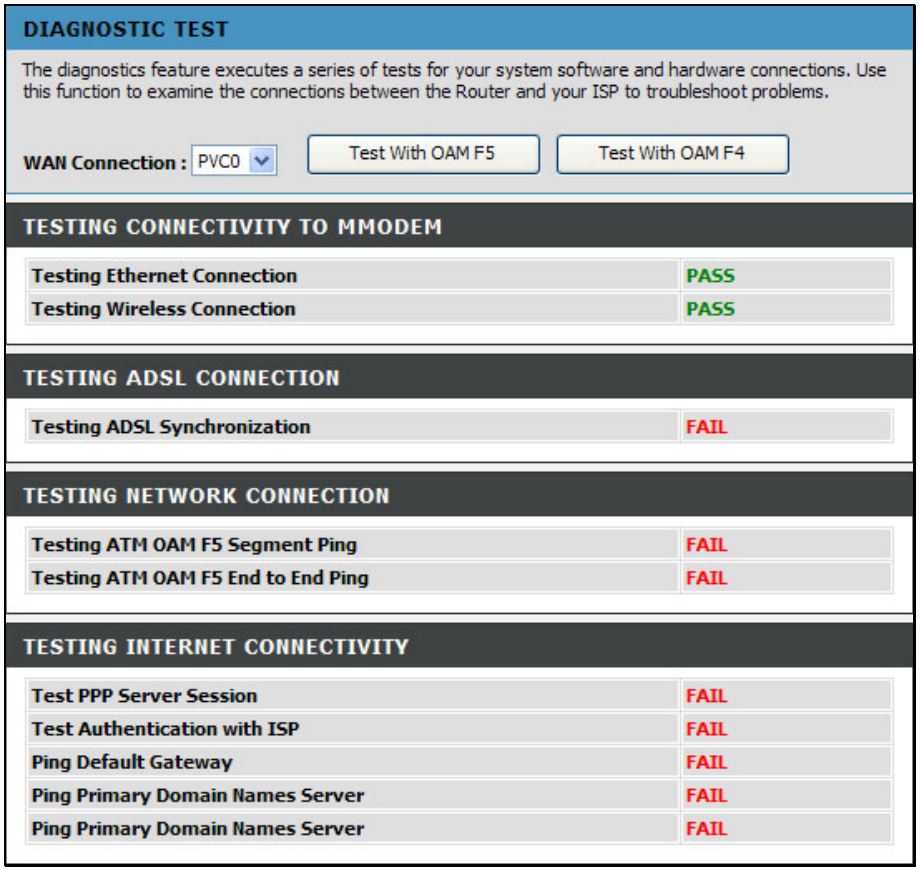
Click **Add** to see the Add IP Address section. Enter an IP address and click **Apply** in the section. The IP address will show in the table in the Remote Web and Telnet Management section. Tick the **Enable Access Control Mode** check box and click **Apply** in this section to enable the function.



# Maintenance – Diagnostics

To access the Diagnostics window, click the **Diagnostics** button in the **Maintenance** directory.

This window is used to test connectivity of the Router. A Ping test may be done through the local or external interface to test connectivity to known IP addresses. The diagnostics feature executes a series of tests of your system software and hardware connections. Use this window when working with your ISP to troubleshoot problems.

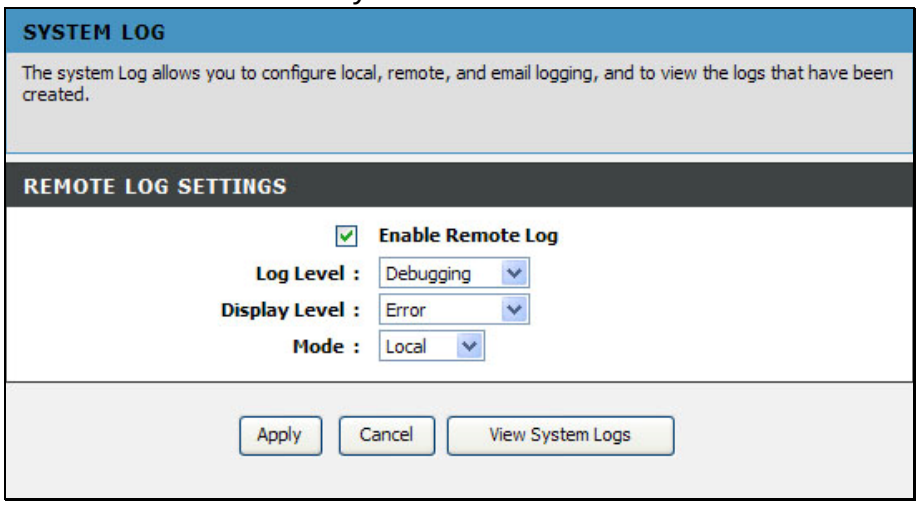


# Maintenance – System Log

To access the System Log window, click the **System Log** button in the **Maintenance** directory.

The system log allows you to configure local and remote logging, and to view the logs that have been created.

To generate a system log, tick the **Enable Remote Log** check box. Select the **Log Level** and **Display Level** from the drop-down lists. The levels available are the same for each type of level: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. Click the **Apply** button to allow your new settings to take effect.



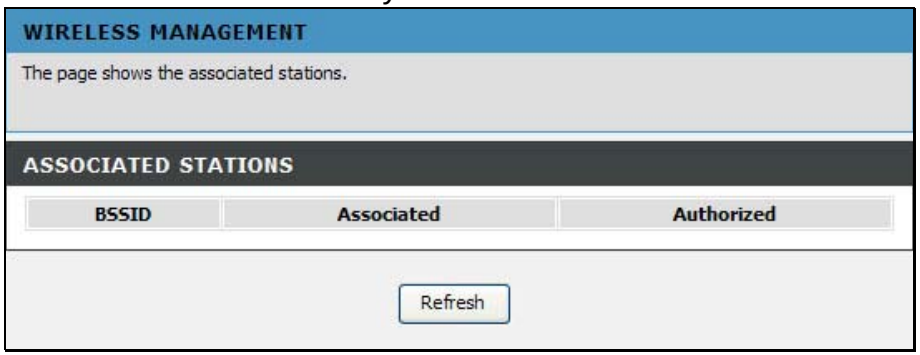
# Status – Device Info

Use the Device Information window to quickly view basic current information about the Wireless, WAN and local network interfaces, and device information including Model Name, Time and Date, and Firmware.

# Status – Wireless Clients

To access the Wireless Clients window, click the **Wireless Clients** button in the **Status** directory.

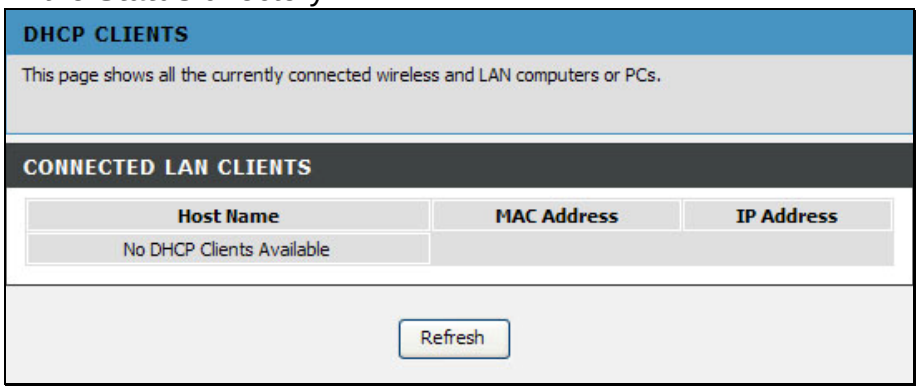
The Wireless Clients window lists out the active Wireless connection when the Wireless function is on.




# Status – DHCP Clients

To access the DHCP Clients window, click the **DHCP Clients** button in the **Status** directory.

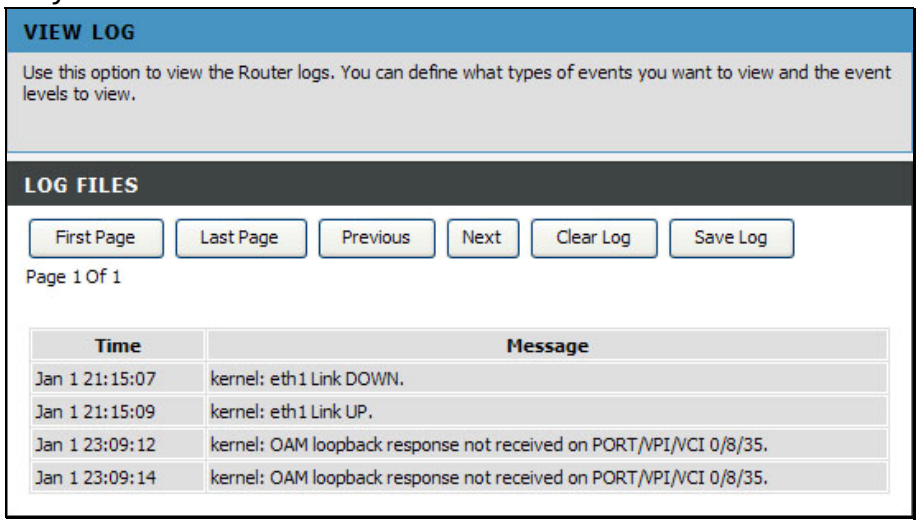
The Connected LAN Clients list displays active DHCP clients when the Router is acting as a DHCP server.



# Status – Logs

To access the Logs window, click the **Logs** button in the **Status** directory.

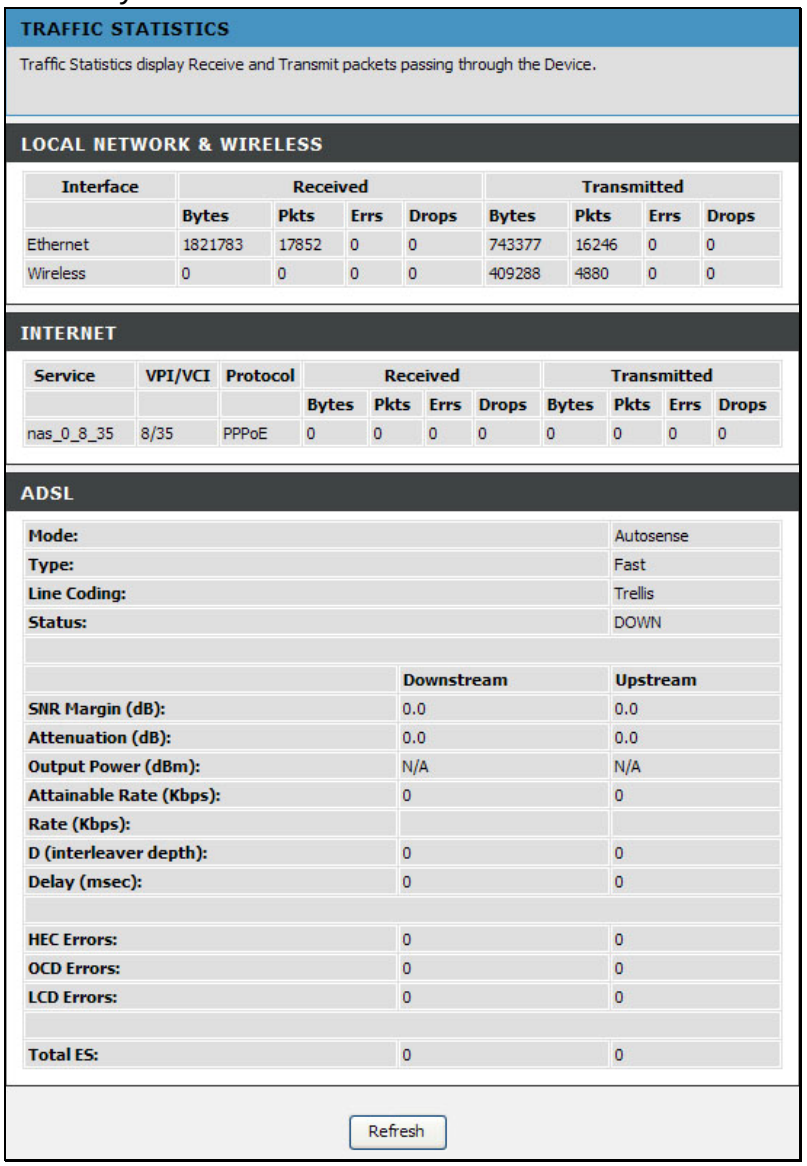
This page displays the event logs of the Router. Click **Clear Log** to delete all the records. Click **Save Log** to save the records as a *.sys file.



# Status – Statistics

To access the Statistics window, click the **Statistics** button in the **Status** directory.

Use this window to monitor traffic on the Local Network & Wireless, Internet or ADSL connections. This window also displays information concerning ADSL status.



**TRAFFIC STATISTICS**

Traffic Statistics display Receive and Transmit packets passing through the Device.

**LOCAL NETWORK & WIRELESS**

| Interface | Received | | | | Transmitted | | | |
|---|---|---|---|---|---|---|---|---|
| | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Errs | Drops |
| Ethernet | 1821783 | 17852 | 0 | 0 | 743377 | 16246 | 0 | 0 |
| Wireless | 0 | 0 | 0 | 0 | 409288 | 4880 | 0 | 0 |

**INTERNET**

| Service | VPI/VCI | Protocol | Received | | | | Transmitted | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Bytes | Pkts | Errs | Drops | Bytes | Pkts | Errs | Drops |
| nas_0_8_35 | 8/35 | PPPoE | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**ADSL**

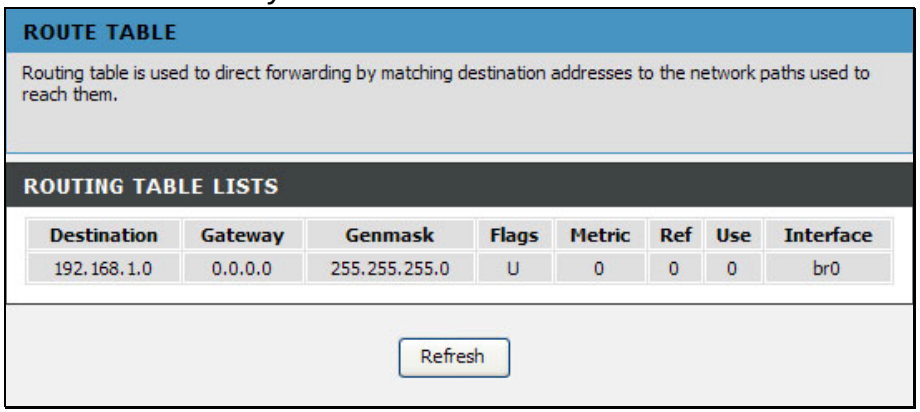
| | | |
|---|---|---|
| Mode: | | Autosense |
| Type: | | Fast |
| Line Coding: | | Trellis |
| Status: | | DOWN |
| | Downstream | Upstream |
| SNR Margin (dB): | 0.0 | 0.0 |
| Attenuation (dB): | 0.0 | 0.0 |
| Output Power (dBm): | N/A | N/A |
| Attainable Rate (Kbps): | 0 | 0 |
| Rate (Kbps): | | |
| D (interleaver depth): | 0 | 0 |
| Delay (msec): | 0 | 0 |
| HEC Errors: | 0 | 0 |
| OCD Errors: | 0 | 0 |
| LCD Errors: | 0 | 0 |
| Total ES: | 0 | 0 |

Refresh

# Status – Routing Info

To access the Routing Info window, click the **Routing Info** button in the **Status** directory.

This page displays all the routing rules information.



# Help

To access the Help window, click the **Help** directory.