USER MANUAL

DSL-225 11N VDSL2+ 4-PORT FAST ETHERNET ROUTER

VERSION 1.00

Table of Contents

Product Overview

Package Contents

This product should contain all of the below mentioned items within its packaging:

- One DSL 225 11N VDSL2+ Wireless Router
- One Power Adapter
- One Printed User Manual (in Hebrew)
- One RJ-11 telephone cable
- One CAT-5 Ethernet cable
- One Quick Installation Guide

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 router will cause damage to this product and void the warranty for this product.

System Requirements

Network Requirements:	• 10/100Mbps Ethernet Adapter. • IEEE 802.11 b/g/n Wireless Adapter
Web User Interface Requirements:	• Windows®, Macintosh, or Linux-based Operating System. • Internet Explorer 7 or higher, Firefox 3.5 or higher, Safari 4 or higher, or Chrome 8 or higher.
Internet Requirements:	• VDSL Internet Connection Service from an ISP.

Features

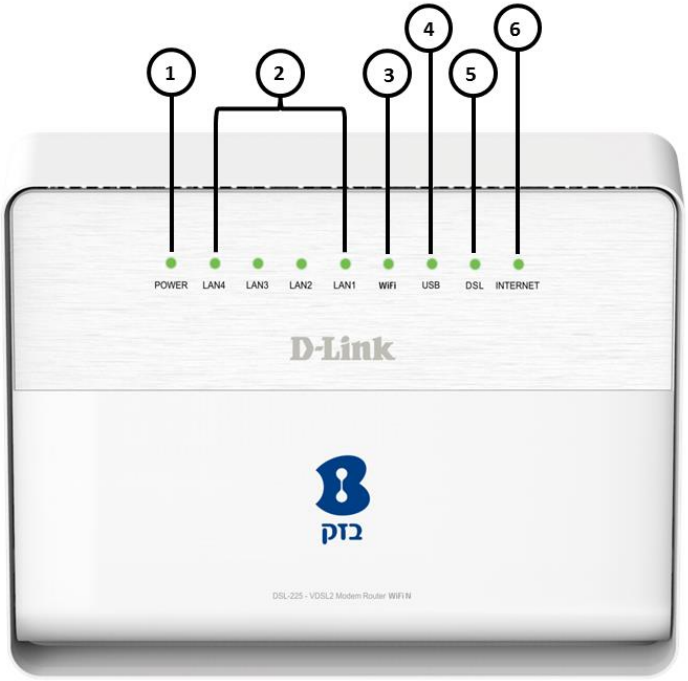
- **Faster Wireless Networking** - The router provides up to 100Mbps* for the 2.4GHz band wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.
- **Compatible with 802.11b, 802.11g and 802.11n Devices** - The router is fully compatible with the IEEE 802.11b and IEEE 802.11g standards, so it can connect with existing 802.11b, 802.11g, and 802.11n PCI, USB and Cardbus adapters.
- **DHCP Support** - Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT)** - For small office environments, the router allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user. NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.
- **Precise ATM Traffic Shaping** - Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.
- **High Performance** - Very high rates of data transfer are possible with the router. Up to 100Mbps downstream bit rate using the G.dmt standard. (For VDSL2+)
- **Full Network Management** - The router incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via a Telnet connection.
- **Easy Installation** - The router uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browsing software can be used to manage this router.
- **USB Support**- The router provides a 3.0 USB port to easily share files and printers. The router supports a USB storage option that shares files through a SAMBA file server and in addition also supports sharing USB printers to network members. Please note that the USB storage device is not included in this package and must be bought separately.

* Maximum wireless signal rate derived from IEEE standard 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Hardware Overview

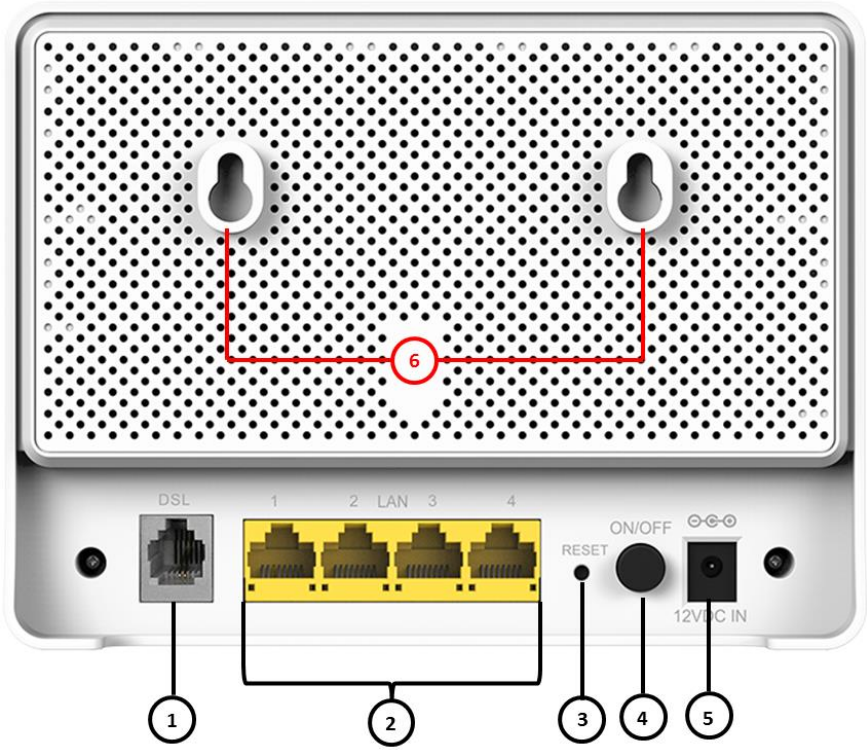
Front Panel

Number	Description
1	**Power** - A steady green light indicates the unit is powered on. When the device is powered off this remains dark. During the Power-On Self-Test this light will be red. If this light remains red after the POST, a malfunction has occurred.
2	**LAN** - A solid light indicates a valid link on startup. This light will blink when there is activity currently passing through the Ethernet port. A green light will be illuminated for a 10/100Mbps connection.
3	**2.4GHz WLAN** - Steady green light indicates a wireless connection. A blinking green light indicates activity on the WLAN
4	**USB** - Steady green light indicates a successful USB connection. A blinking green light indicates activity on the USB. Dark if no USB device is connected.
5	**DSL** - Steady green light indicates a valid VDSL connection. This will light after the VDSL negotiation process has been settled. A blinking green light indicates activity on the WAN (VDSL) interface.
6	**Internet** - Steady green light indicates a successful Internet connection. Steady red light indicates failed Internet connection. Dark if no WAN protocol is configured.



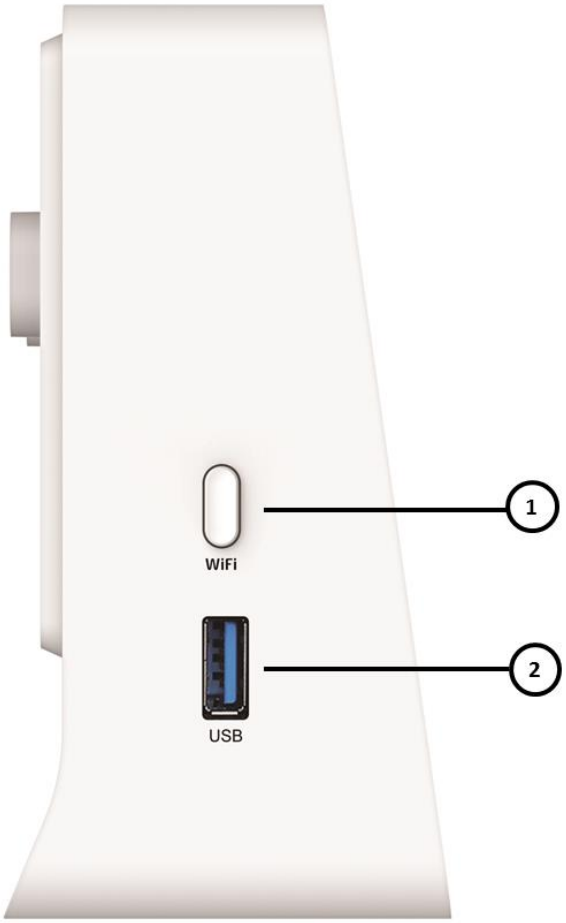
Rear Panel

Number	Description
1	**VDSL Port** - Use the DSL cable to connect to your telephone line (RJ-11 port).
2	**Ethernet Ports** - Use the Ethernet ports to connect the router to your Ethernet LAN or Ethernet devices.
3	**Reset Button** - Press and hold the button 5 seconds to restore the device to its original factory default settings.
4	**Power Button** - Push in to power-on the router. Push again to power-off the router.
5	**Power Receptor** - Receptor for the supplied power adapter.
6	**Wall-Mount Slots** – Wall-mount slots to mount the router on the wall.



Side Panel

Number	Description
1	**2.4GHz Wireless On/Off Switch Button -** Please press and hold the WiFi button for 3 seconds to turn on/turn off.
2	**USB Port** - Use the USB port to connect your USB device.



Basic Installation

This section will walk you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, or in the attic or garage.

Before You Begin

Please read and make sure you understand all the prerequisites for proper installation of your new router. Have all the necessary information and equipment on hand before beginning the installation.

Installation Notes

In order to establish a connection to the Internet it will be necessary to provide information to the router that will be stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required.

Low Pass Filters

Since VDSL and telephone services share the same copper wiring to carry their respective signals, a filtering mechanism may be necessary to avoid mutual interference. A low pass filter device can be installed for each telephone that shares the line with the VDSL line. These filters are easy to install passive devices that connect to the VDSL device and/or telephone using standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

Operating Systems

The router uses an HTML-based web interface for setup and management. The Web configuration manager may be accessed using any operating system capable of running web browser software, including Windows®, Macintosh, and Linux-based Operating Systems.

Web Browser

Any common Web browser can be used to configure the router using the Web configuration management software. The program is designed to work best with more recently released browsers such as Internet Explorer 7 or higher, Firefox 3.5 or higher, Safari 4 or higher, or Chrome 8 or higher.. The Web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)

Any computer that uses the router must be able to connect to it through one of the Ethernet ports on the router. This connection is an Ethernet connection and therefore requires that your computer be equipped with an Ethernet port as well. Most notebook computers are now sold with an Ethernet port already installed. Likewise, most fully assembled desktop computers come with an Ethernet adapter as standard equipment. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the router. If you must install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

Additional Software

It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using the device a simple bridge. For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device, not in the router itself.

If your VDSL service is delivered through a PPPoE or PPPoA connection, the information needed to establish and maintain the Internet connection can be stored in the router. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

All connections to the Internet require a unique global IP address. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN side of the bridge, such as a PC, a server, a gateway device such as a router or similar firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

Information you will need from your VDSL service provider

Username

This is the Username used to log on to your VDSL service provider's network. Your VDSL service provider uses this to identify your account.

Password

This is the Password used, in conjunction with the Username above, to log on to your VDSL service provider's network. This is used to verify the identity of your account.

WAN Setting / Connection Type

These settings describe the method your VDSL service provider uses to transport data between the Internet and your computer. Most users will use the default settings. You may need to specify one of the following WAN Setting and Connection Type configurations (Connection Type settings listed in parenthesis):

- PPPoE/PPPoA (PPPoE LLC, PPPoE VC-Mux, PPPoA LLC or PPPoA VC-Mux)
- Static IP Address (1483 Routed IP LLC or 1483 Routed IP VC-Mux)
- Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC Mux)

Modulation Type

VDSL uses various standardized modulation techniques to transmit data over the allotted signal frequencies. Some users may need to change the type of modulation used for their service. The default DSL modulation (Autosense) used for the router automatically detects all types of VDSL, VDSL2, and VDSL2+ modulation.

Security Protocol

This is the method your VDSL service provider will use to verify your Username and Password when you log on to their network. Your router supports the PAP and CHAP protocols.

VPI

Most users will not be required to change this setting. The Virtual Path Identifier (VPI) is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your VDSL service provider's network and your computer. If you are setting up the router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your VDSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

VCI

Most users will not be required to change this setting. The Virtual Channel Identifier (VCI) used in conjunction with the VPI to identify the data path between your VDSL service provider's network and your computer. If you are setting up the router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your VDSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

Information you will need about this Router

Username

This is the username needed access the router's web management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this username. The default username for the router is "**Admin**". Alternatively, you can also try "user"

Password

This is the password you will be prompted to enter when you access the router's web management interface. The default password is "**Admin**". Alternatively, you can also try "user"

LAN IP Addresses for the Router

This is the IP address you will enter into the Address field of your web browser to access the router's configuration Graphical User Interface (GUI) using a web browser. The default IP address is **10.0.0.138**. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.

LAN Subnet Mask for the Router

This is the subnet mask used by the Router, and will be used throughout your LAN. The default subnet mask is **255.255.255.0**. This can be changed later.

Information you will need about your LAN or computer

Ethernet NIC

If your computer has an Ethernet NIC, you can connect the router to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the router to connect to other computer or Ethernet devices.

DHCP Client status

Your VDSL router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the unit will assign are from **10.0.0.139** to **10.0.0.254**. Your computer (or computers) needs to be configured to obtain an IP address automatically (that is, they need to be configured as DHCP clients.)

Once you have the above information, you are ready to setup and configure your VDSL router.

Device Installation

The router connects two separate physical interfaces, a VDSL (WAN) and an Ethernet (LAN) interface. Place the router in a location where it can be connected to the various devices as well as to a power source. The router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Power on Router

The router must be used with the power adapter included with the device.

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the router and plug the adapter into a suitable nearby power source.
2. Press the Power button into the on position. You should see the Power LED indicator light up and remain lit.
3. If the Ethernet port is connected to a working device, check the Ethernet LED indicators to make sure the connection is valid. The router will attempt to establish the VDSL connection, if the VDSL line is connected and the router is properly configured this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the router can establish a connection.

Factory Reset Button

The router may be reset to the original factory default settings by using a ballpoint pen or paperclip to gently push down the reset button in the following sequence:

1. Press and hold the reset button while the device is powered on for 10-15 seconds.
2. Release the reset button.

Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address **10.0.0.138** and the subnet mask is **255.255.255.0.** The default management username is “**user**” and the default password is “**user**”.

Network Connections

Connect VDSL Line

Use the VDSL cable included with the router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the VDSL port (RJ-11 receptacle) on the rear panel of the router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The VDSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

Connect Router to Ethernet

The router may be connected to a single computer or Ethernet device through the Ethernet ports on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100Mbps. When connecting the router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port. Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 ports on the router are a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. The rules governing Ethernet cable lengths apply to the LAN to router connection. Be sure that the cable connecting the LAN to the router does not exceed 100 meters.

Hub or Switch to Router Connection

Connect the router to an uplink port (MDI-II) on an Ethernet hub or switch with a straight-through cable. If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.

Computer to Router Connection

You can connect the router directly to an Ethernet adapter card (NIC) installed on a PC using the Ethernet cable provided.

Getting Started

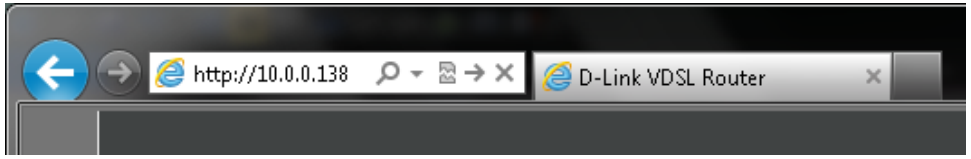
This section will show you how to set up and configure your new D-Link router using the Web-based configuration utility.

How to connect to the Web User Interface

Connect to the Router

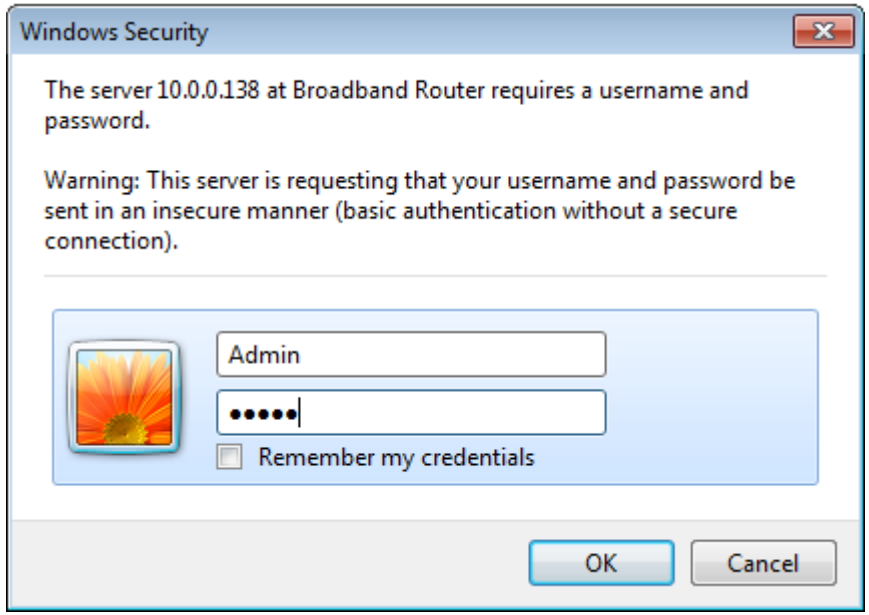
To configure the WAN connection used by the router it is first necessary to communicate with the router through its management interface, which is HTML-based and can be accessed using a web browser. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the router.

To access the web user interface, open a web-browser such as Internet Explorer and enter the IP address of the router (**10.0.0.138**) into the address bar and press the *Enter* key on your keyboard.



Type "**Admin**" in the User Name field and "**Admin**" in the Password field, and enter the validation code. Click the **Login** button to proceed. If you get a *Page Cannot be Displayed* error, please refer to the Troubleshooting section for assistance.

Tick the *Remember my login info on this computer* option to allow the browser to remember the login information for the next login.



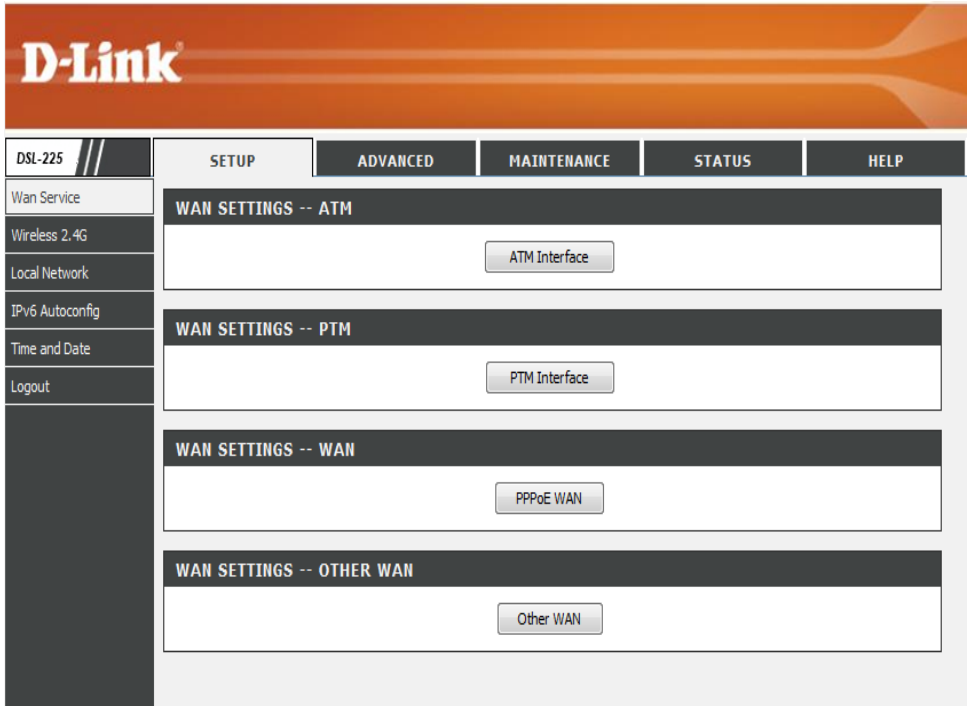
Web User Interface Configuration

After successfully logging into the Web User Interface, the following page will be displayed. This page is divided into clickable components that make the configuration of this device easier and more understandable.

The top menu lists out the **Categories** available for configuration. The categories available to configure on this device are **Setup**, **Advanced**, **Maintenance**, **Status** and **Help**.

The left menu lists out the **Pages** available, for each individual category, for configuration. In this example, we observe the pages available in the **Setup** category.

Every category will have a **Logout** option at the bottom of all the pages. This option can be used to log out from the web user interface and also close the browser.

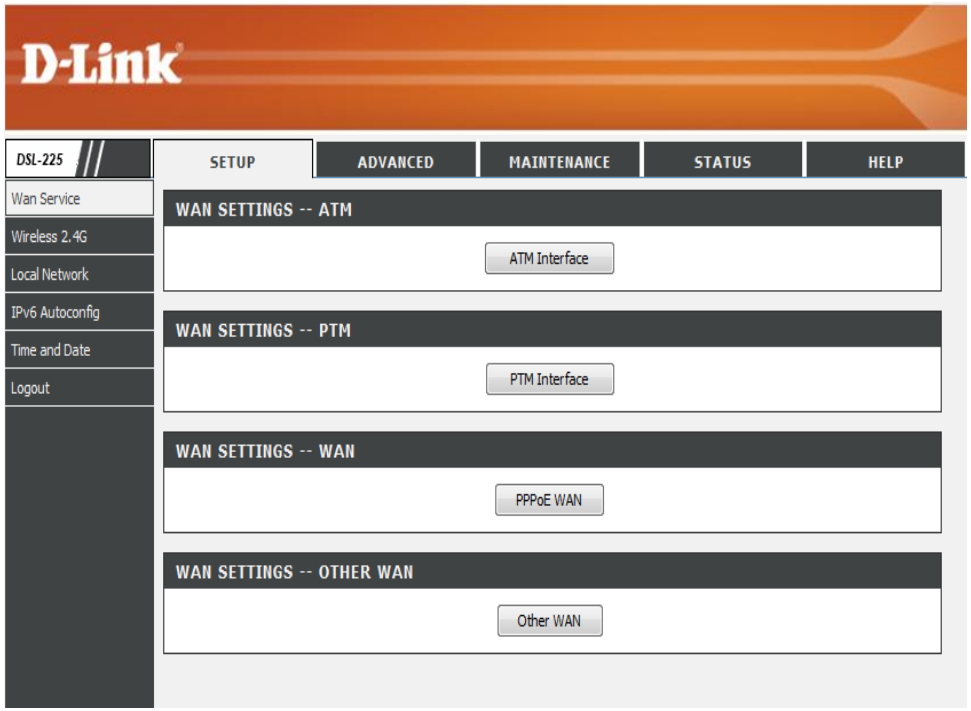


Setup Category

The **Setup** category is designed to assist the user with essential configurations, concerning the initial setup of this product.

The following pages can be found in the **Setup** category:

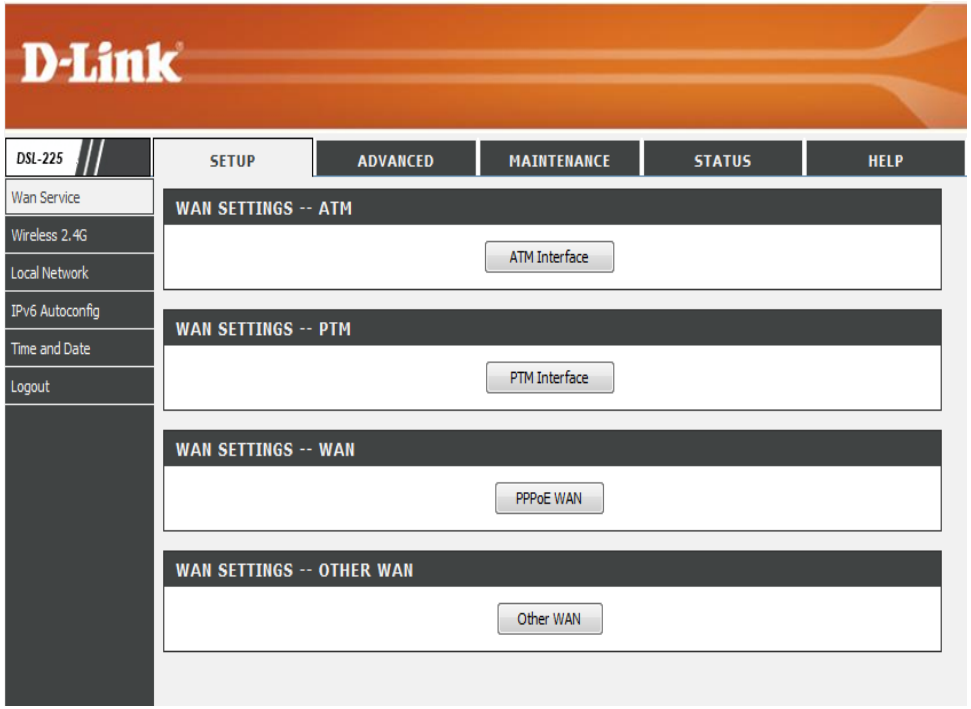
- **Wan Service** – On this page the user can configure services related to the WAN connectivity of this product.
- **Wireless 2.4G** – On this page the user can configure services related to the Wireless 2.4GHz connectivity of this product.
- **Local Network** – On this page the user can configure services related to the Local Area Network connectivity of this product. Services available for configuration are **LAN Interface** configuration and **DHCP** configuration.
- **IPv6 Autoconfig** – On this page the user can configure services related to the IPv6 connectivity of this product.
- **Time and Date** – On this page the user can configure services related to the time and date feature of this product. **Time Servers** and a **Time Zone** can be specified here.
- **Logout** – On this page the user can log out of the router.



WAN Service

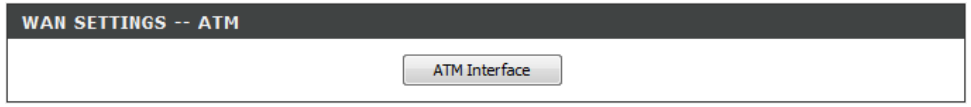
To access the **WAN Service** page, click on the **Setup** menu link, at the top, and then click on the **WAN Services** menu link, on the left.

On this page the user can configure services related to the WAN connectivity of this product.

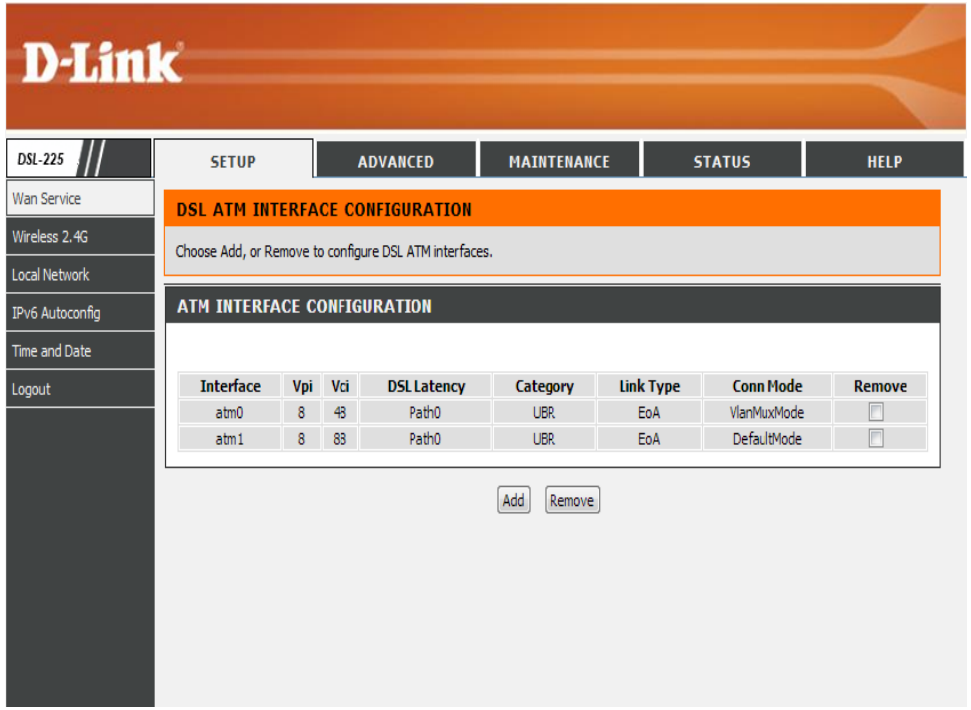


ATM Interface

Click the **ATM Interface** button to access the ATM Interface WAN Settings configuration page.



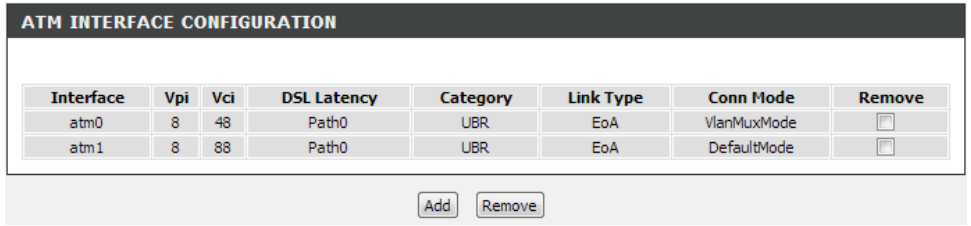
After clicking the **ATM Interface** button, the DSL ATM Interface Configuration page will be available.



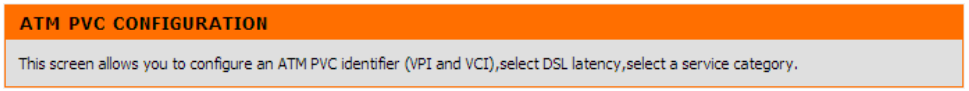
In the **ATM Interface Configuration** section, here, we can view a list of existing interfaces configured.

Click the **Add** button to add a new interface.

Select the **Remove** option and click the **Remove** button to remove the specific interface.



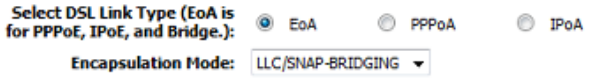
After clicking the **Add** button, the ATM PVC Configuration page will be available.



Enter the correct VPI and VCI values. These can also be changed if requested to do so by the Internet Service Provider (ISP).

Select the appropriate **DSL Latency** option. Options to choose from are **Path0 (Fast)** and **Path1 (Interleaved)**.

Here we can select the **DSL Link Type** used. The **Encapsulation Mode** will change depending on the **DSL Link Type** selected. Options to choose from are **EoA**, **PPPoA**, and **IPoA**.

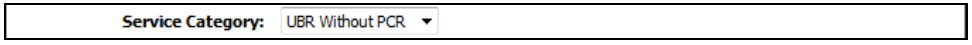


After selecting the **EoA** option, select the **Encapsulation Mode**. Options to choose from are **LLC/SNAP-BRIDGING** and **VC/MUX**.

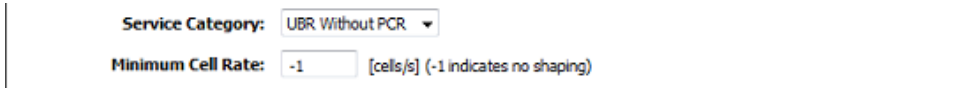
After selecting the **PPPoA,** select the **Encapsulation Mode**. Options to choose from are **VC/MUX** and **LLC/ENCAPSULATION**.

After select the **IPoA** option, select the **Encapsulation Mode**. Options to choose from are **LLC/SNAP-ROUTING** and **VC/MUX**.

Here we can select the **Service Category**. Options to choose from are **UBR Without PCR**, **UBR With PCR**, **CBR**, **Non Realtime VBR**, and **Realtime VBR**.



After selecting **UBR Without PCR**, the **Minimum Cell Rate** field will be available. Enter the **Minimum Cell Rate** value here.



After selecting **UBR With PCR**, the **Peak Cell Rate** field will be available. Enter the **Peak Cell Rate** value here.

After selecting **CBR**, the **Peak Cell Rate** field will be available. Enter the **Peak Cell Rate** value here.

After selecting **Non Realtime VBR**, the **Peak Cell Rate**, **Sustainable Cell Rate**, and **Maximum Burst Size** fields will be available. Enter the **Peak Cell Rate**, **Sustainable Cell Rate**, and **Maximum Burst Size** values here.

After selecting **Realtime VBR**, the **Peak Cell Rate**, **Sustainable Cell Rate**, and **Maximum Burst Size** fields will be available. Enter the **Peak Cell Rate**, **Sustainable Cell Rate**, and **Maximum Burst Size** values used here.

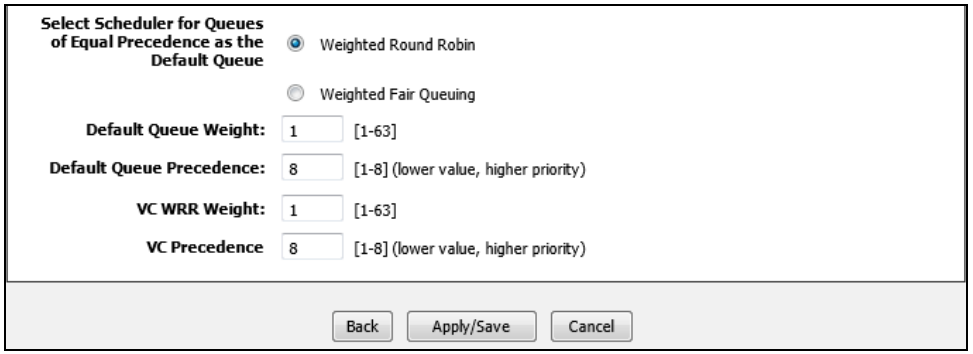
Select the **Select Scheduler for Queues of Equal Precedence as the Default Queue** option here. Options to choose from are **Weighted Round Robin** and **Weighted Fair Queuing**.

Also enter the **Default Queue Weight**, **Default Queue Precedence**, **VC WRR Weight**, and **VC Precedence** value used here.

Click the **Back** button to return to the previous page.

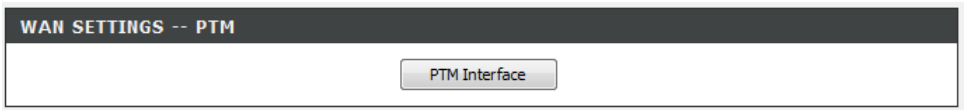
Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.



PTM Interface

Click the **PTM Interface** button to access the PTM Interface WAN Settings configuration page.

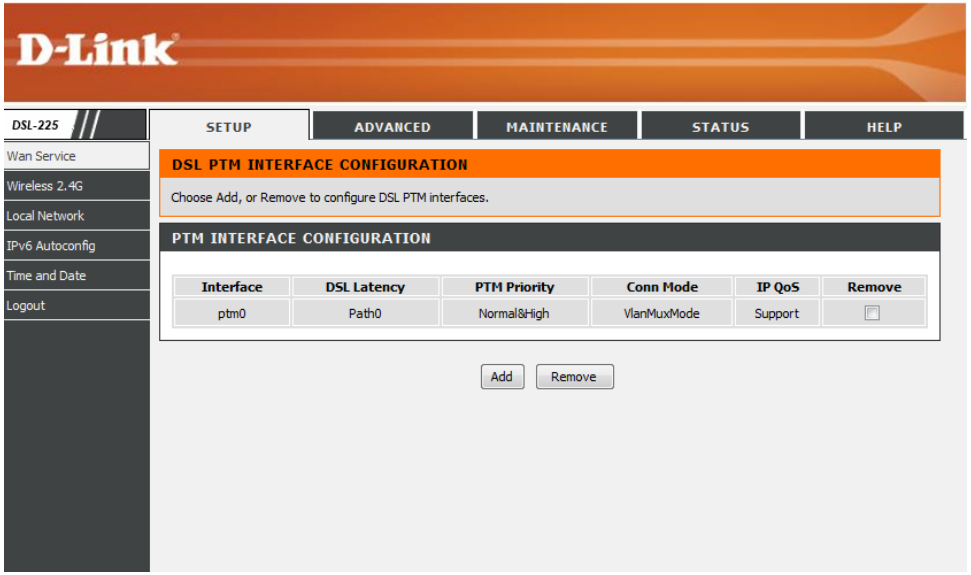


After clicking the **PTM Interface** button, the DSL PTM Interface Configuration page will be available.

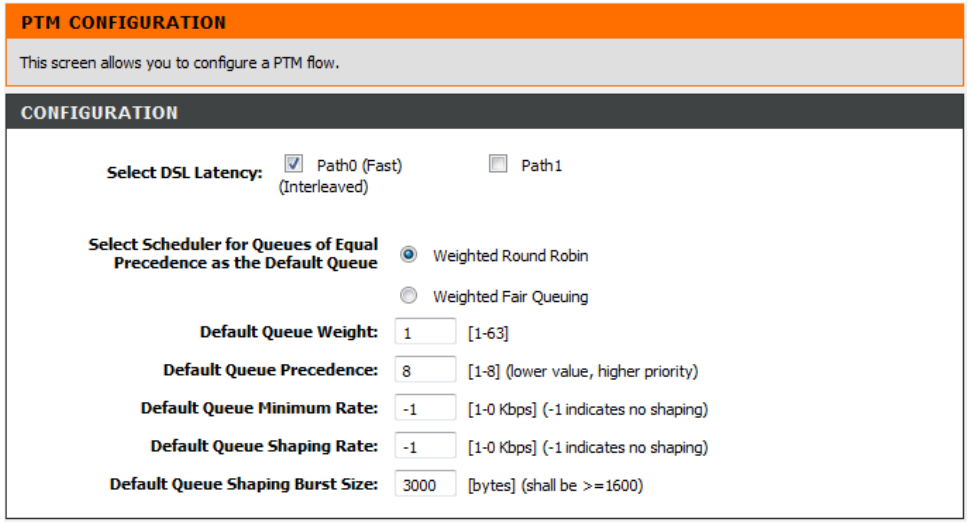
Here you can view the **Interface**, **DSL Latency**, **PTM Priority**, **Connection Mode,** and **IP QoS** settings. You can remove the configuration option by clicking the **Remove** checkbox.

Click the **Add** button to add a new interface.

Select the **Remove** option and click the **Remove** button to remove the specific interface.



After clicking the **Add** button, the **PTM Configuration** page will be available.



Select the DSL latency option here. Options to choose from are **Path0 (Fast)** and **Path1 (Interleaved)**.

Select the **Select Scheduler for Queues of Equal Precedence as the Default Queue** option here. Options to choose from are **Weighted Round Robin** and **Weighted Fair Queuing**.

Next, you have the option to edit any of the following settings:

Select a value to enter under **Default Queue Weight**.

Select a value to enter under **Default Queue Precedence**.

Select a value to enter under **Default Queue Minimum Rate**

Select a value to enter under **Default Queue Shaping Rate**

Select a value to enter under **Default Queue Shaping Burst Size**

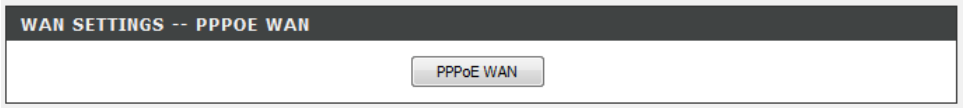
Click the **Back** button to return to the previous page.

Click the **Apply/Save** button to accept the changes.

Click the **Cancel** button to discard the changes made and return to the main page.

PPPoE WAN

Click the **PPPoE WAN** button to access the PPPoE WAN Settings configuration page.

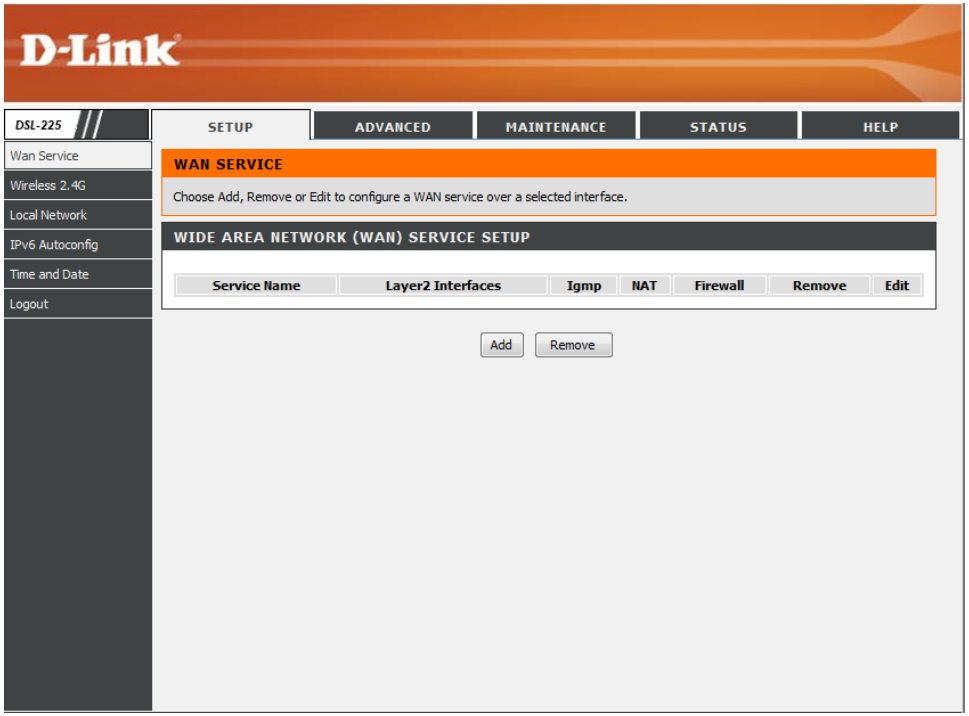


After clicking the **PPPoE WAN** button, the following page will be available. In the **Wide Area Network (WAN) Service Setup** section, a list of configured PPPoE WAN interfaces will be displayed.

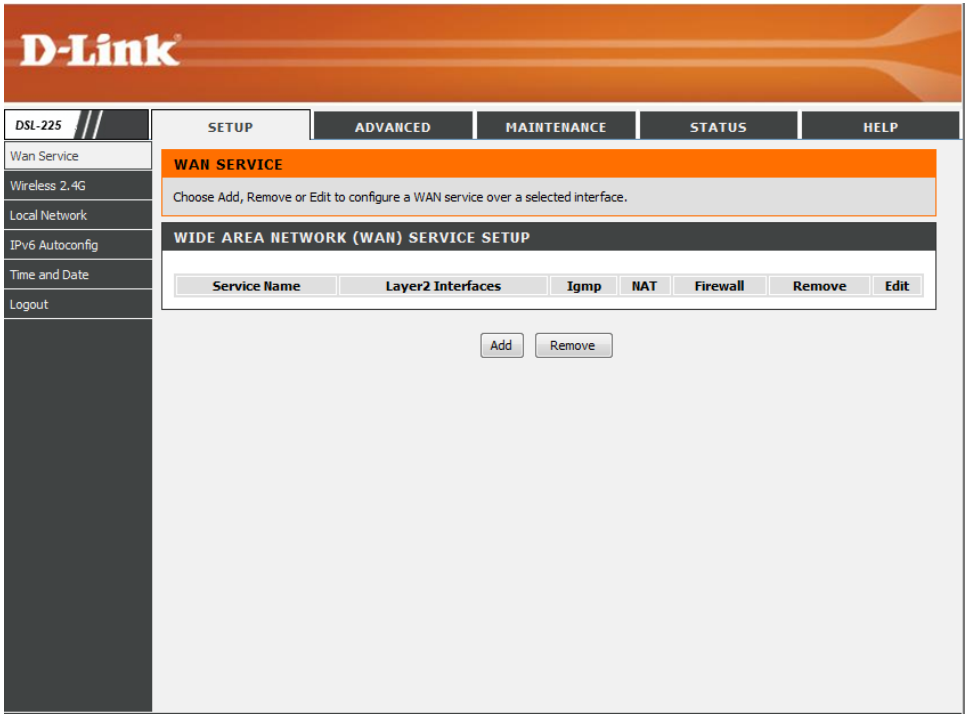
Click the **Add** button to add a new interface.

Click the **Edit** button to reconfigure an interface.

Select the **Remove** option and click the **Remove** button to remove the specific interface.

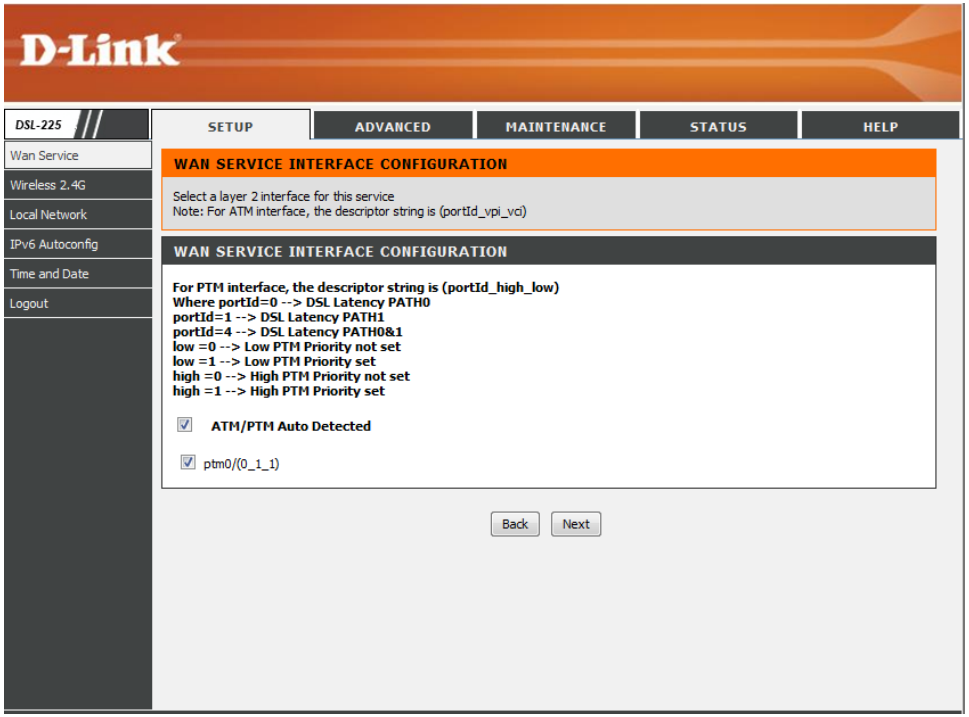


After clicking the **Add** button, the **WAN Service Interface Configuration** page is displayed.

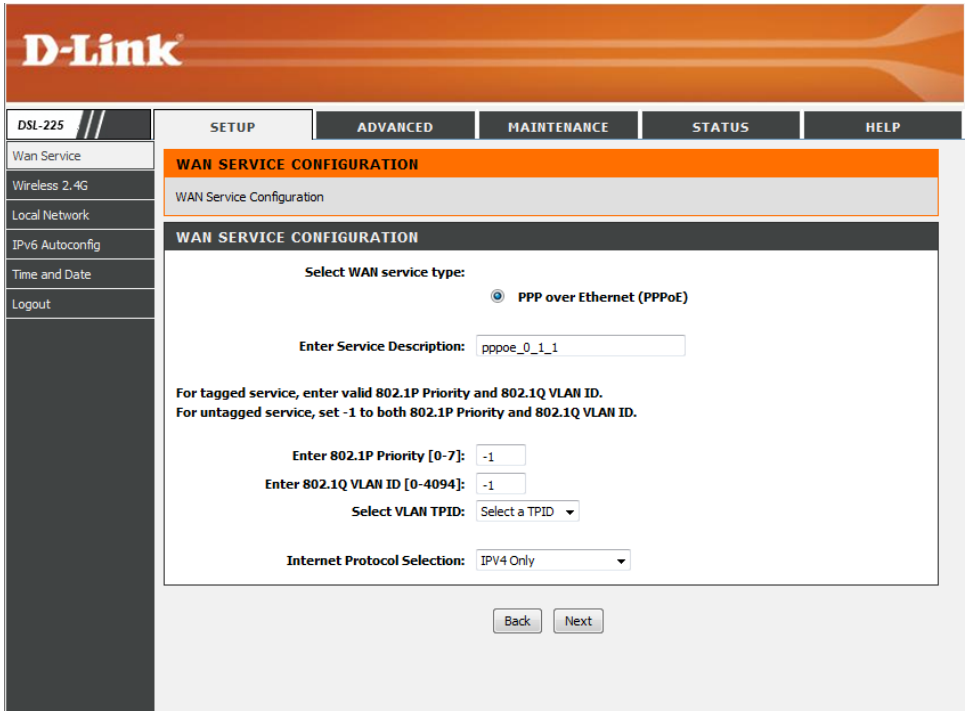


Select either **ATM/PTM Auto Detected** or **ptm0/(0_1_1)**, or both. If you select neither, you will be prompted to select either one.

Click **Next** to continue.



After clicking the **Next** button, the following page will be displayed. Here we can configure the **WAN Service Configuration**.



Select the **WAN service type**.

Click **IP over Ethernet** or click **Bridge**. When you click **IP over Ethernet**, the **Enter Service Description** field changes to **ipoe_0_1_1**. When you click **Bridge**, the **Enter Service Description** field changes to **br_0_1_1**.

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID. For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter a value in the **Enter 802.1P Priority [07]** field.

Enter a value in the **Enter 802.1Q VLAN ID [0-4094]** field.

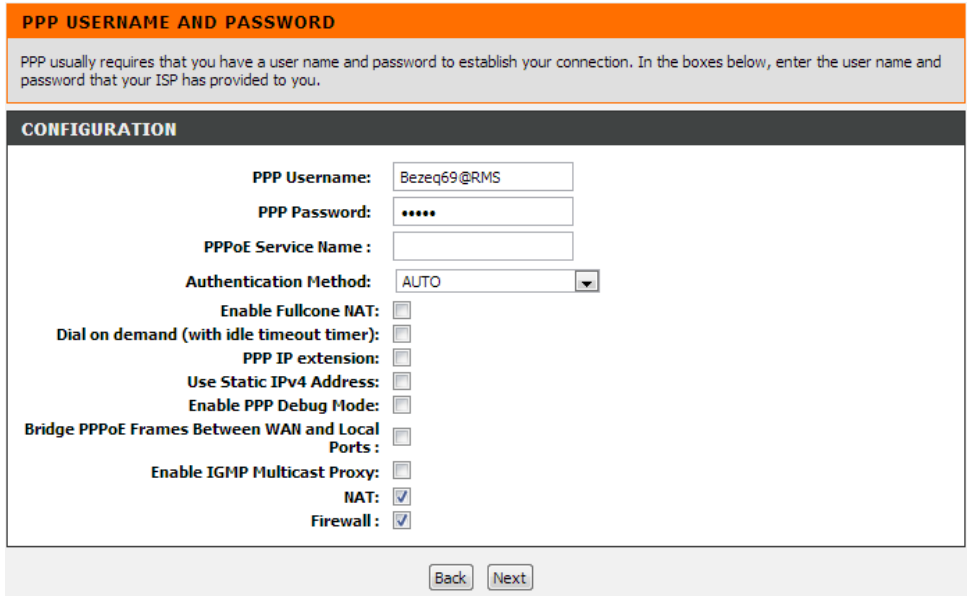
Select a **TPID VLAN** from the drop-down menu. Select either **0x8100**, **0x88A8**, or **0x9100**.

Select the **Internet Protocol Selection** from the drop-down menu. Select either **IPv4 Only**, **IPv4&IPv6(Dual Stack)**, or **IPv6 Only**.

Click the **Back** button to return to the previous page.

Click the **Next** button to continue to the next page.

The PPP Username and Password Configuration window opens.



The following parameters can be configured:

PPP Username: Enter the username provided by your ISP

PPP Password: Enter the password provided by your ISP

PPPoE Service Name: Enter the PPPoE service name provided by your ISP

Authentication Method: From the drop-down list select either **AUTO**, **PAP**, **CHAP**, **MSCHAP**

Enable Fullcone NAT: Tick this option to enable the full-cone NAT feature. If checked, a warning message appears, **ONLY IF REQUIRED—DISABLES NETWORK ACCELERATION AND SOME SECURITY**

Dial on demand (with idle timeout timer): Tick this option to enable the dial-on-demand feature. After selecting this option, enter the **Inactivity Timeout** value used here. This value must be between 1 and 4320 minutes. By default, this value is **0**.

PPP IP extension: Tick this option to enable the PPP IP extension feature.

Use Static IPv4 Address: Tick this option to manually enter and use a **Static IPv4 Address**.

Enable PPP Debug Mode: Tick this option to enable the PPP debug mode feature.

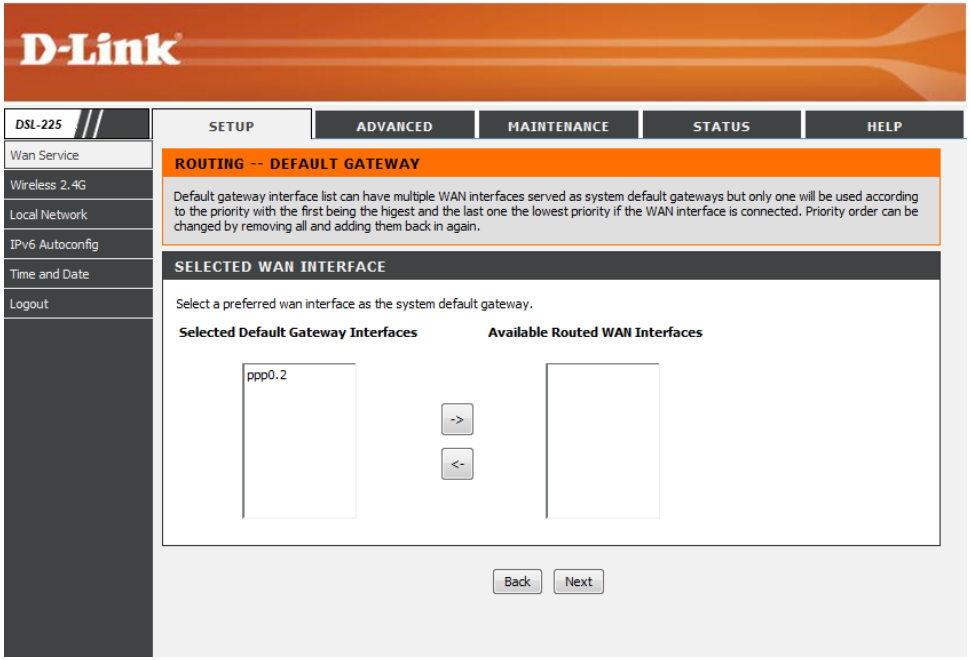
Bridge PPPoE Frames Between WAN and Local Ports: Tick this option to enable the bridging of PPPoE frames between WAN and the local ports.**Enable IGMP Multicast Proxy**: Tick this option to enable the IGMP multicast proxy feature.

Click the **Back** button to return to the previous page.

Click the **Next** button to continue to the next page.

Once you selected from the options above, click the **Next** button, the following page will be displayed. Here we can configure the interface's parameters.

In the **Routing –Default Gateway** section, select the **Default Gateway Interface**. Click **Next**.



The **DNS Server Configuration** window appears.

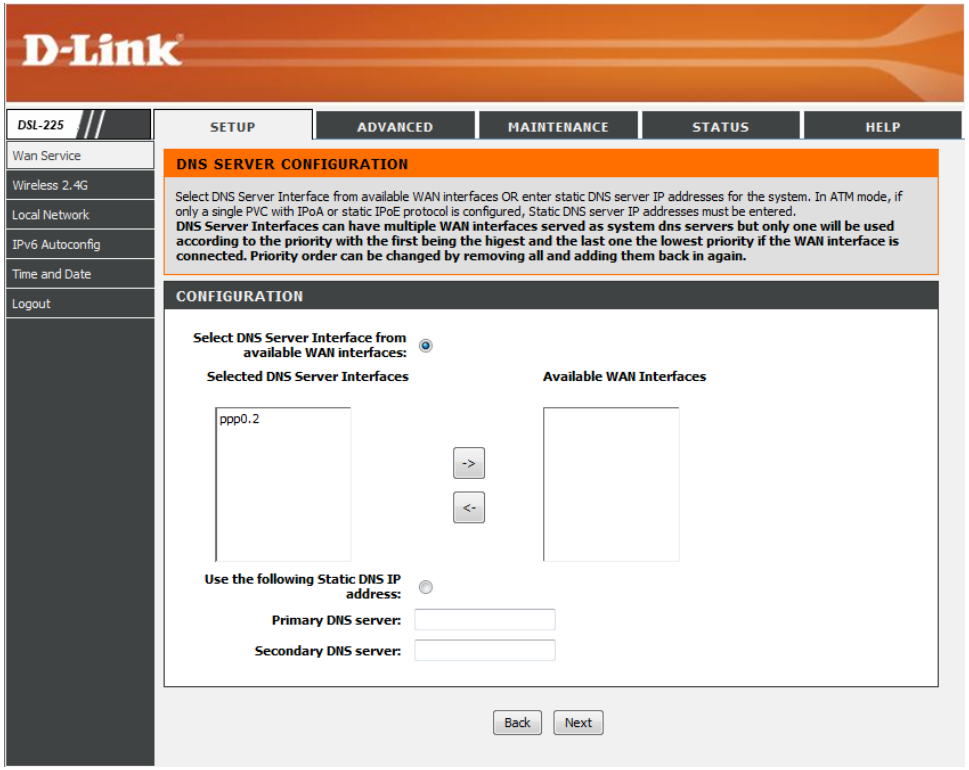
The option **Select DNS Server Interface** from available WAN interfaces is already selected.

Select the **Selected DNS Server Interfaces**.

Choose **Use the following Static DNS IP address**.

Enter a **Primary DNS server** in the field provided and/or **Secondary DNS**.

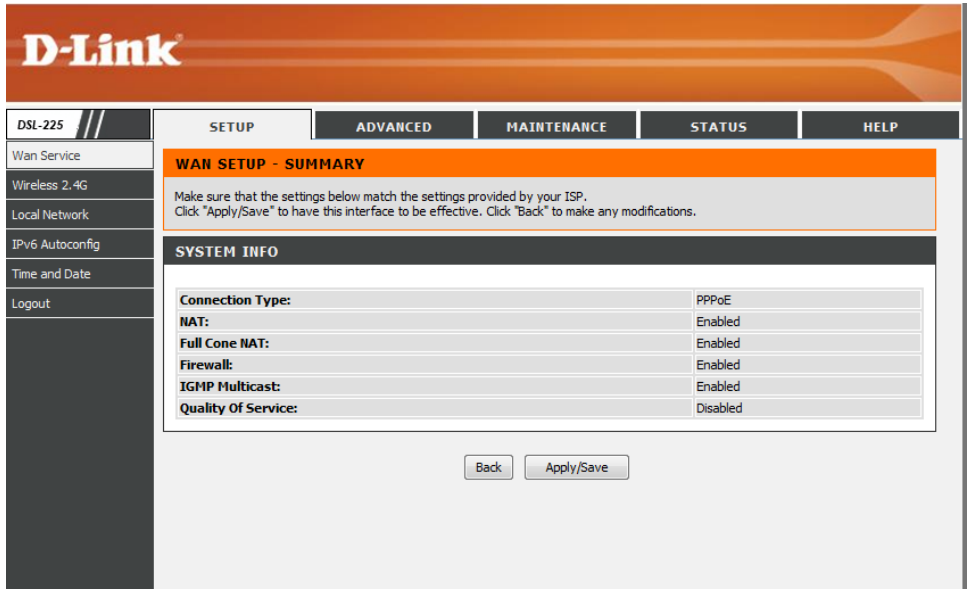
Click the **Next** button to continue.



After clicking the **Next** button, the following page will be displayed. Here we can view a summary of the interface's parameters.

Click the **Back** button to return to the previous page.

Click the **Apply/Save** button to accept the changes.



Other WAN Interface

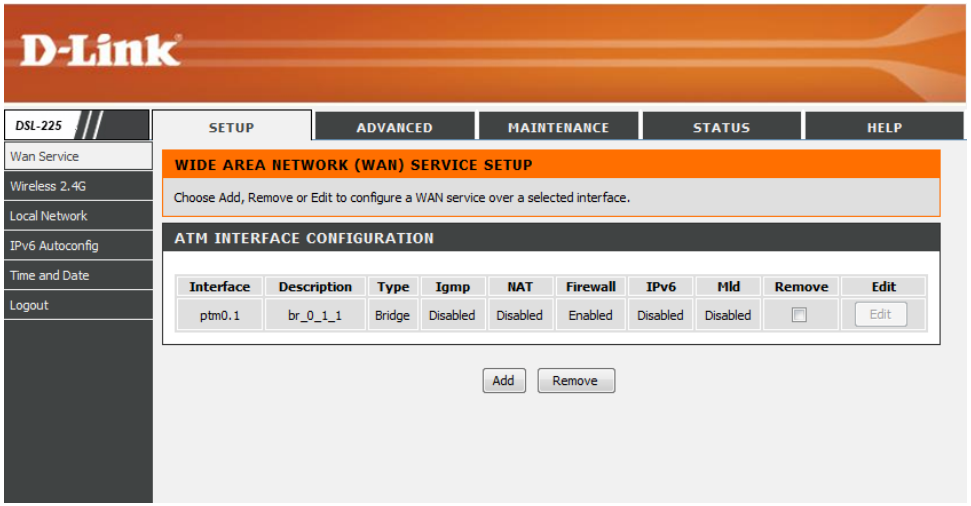
Click the **Other WAN** button to access the Other WAN Settings configuration page.

After clicking the **Other WAN** button, the following page will be available. In the **Wide Area Network (WAN) Service Setup** section, a list of configured WAN interfaces will be displayed.

Click the **Add** button to add a new interface.

Click the **Edit** button to reconfigure an interface.

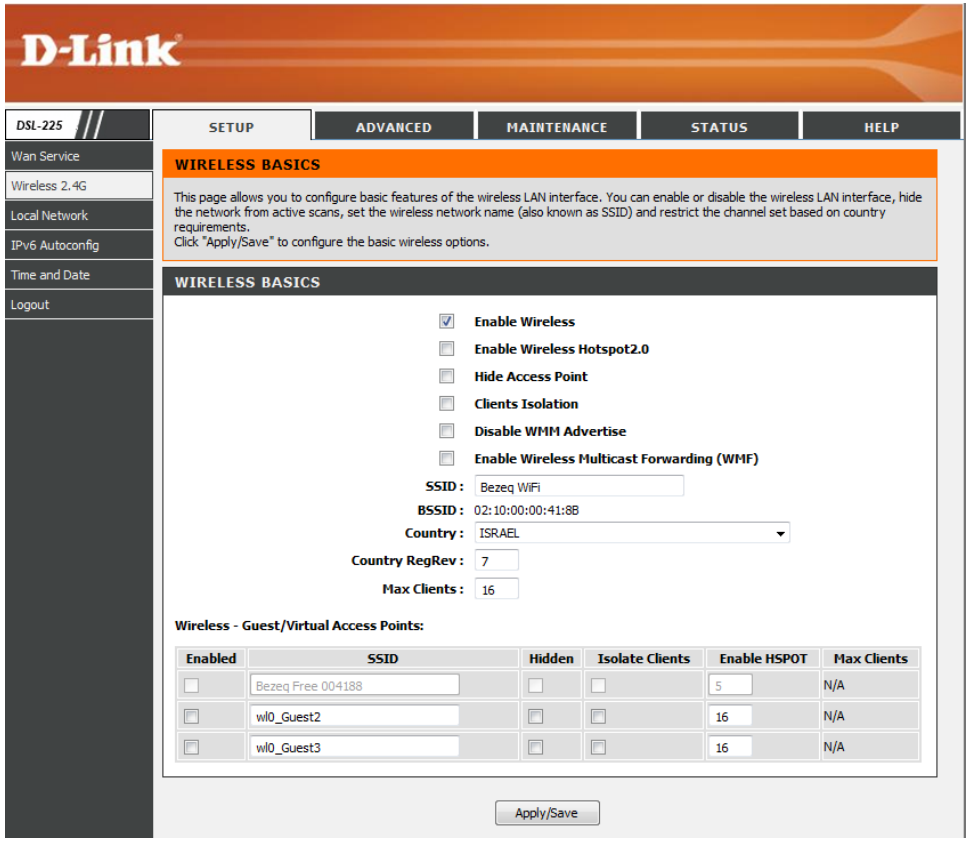
Select the **Remove** option and click the **Remove** button to remove the specific interface.



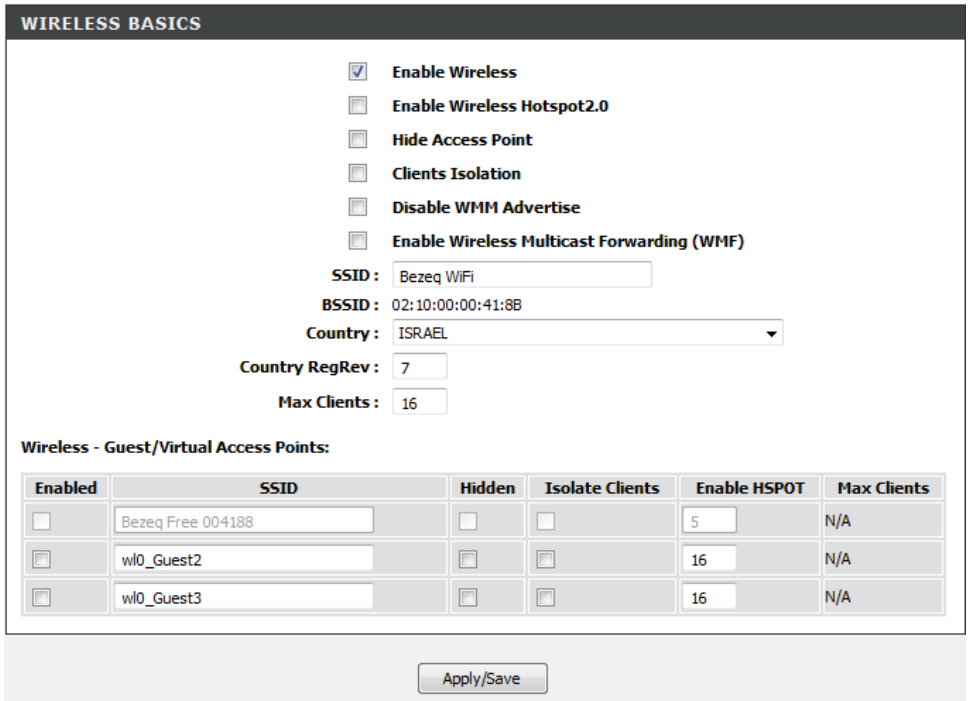
Wireless 2.4G

To access the **Wireless 2.4G** page, click on the **Setup** menu link, at the top, and then click on the **Wireless 2.4G** menu link, on the left.

On this page the user can configure services related to the Wireless 2.4GHz connectivity of this product.



In this section we can configure the following parameters.



Enable Wireless: Tick this option to enable the wireless feature on this router.

Enable Wireless Hotspot 2.0: Check this option to enable wireless hotspot 2.0.

Hide Access Point: Here we can choose to hide the Wireless SSID by selecting clicking the checkbox.

Clients Isolation: Click the checkbox to enable.

Disable WMM Advertise: Click the checkbox to enable the Wi-Fi Multimedia (WMM) advertisement feature

Enable Wireless Multicast Forwarding (WMF): Click the checkbox to enable the Wireless Multimedia Forwarding (WMF) feature.

SSID: Enter the Wireless name (SSID) here. This name will be available when wireless clients scan for available wireless networks. However, when the **Hide Access Point** option is enabled, this name will not be visible to wireless clients

BBSID: The ID is automatically set.

Country: This parameter will display the country information.

Country RegRev: Enter the country registration number here.

Max Clients: Set the number of users that can access the device.

Wireless – Guest/Virtual Access Points: Click the checkbox to enable one of the guest Access Points

Enabled – Select this option to enable the Guest/Virtual Access Point option for the entry specified.

SSID – When available enter the SSID for the Virtual Access Point (VAP) here.

Hidden – Select this option to hide the SSID of the selected VAP.

Isolate Clients – Select this option to isolate the wireless clients of the selected VAP from the rest of the network.

Enable HSPOT – Set the hotspot value per SSID

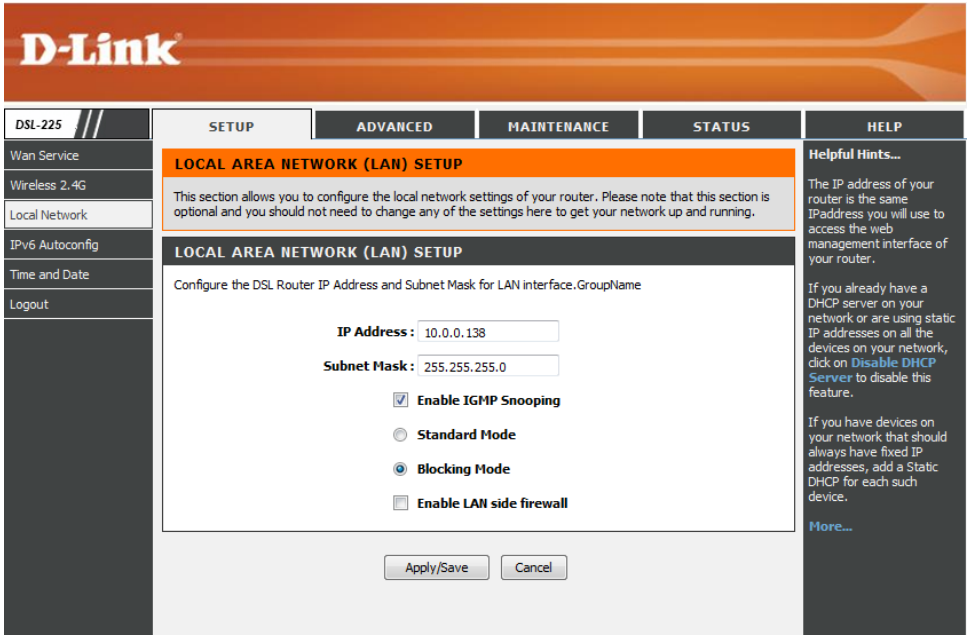
Max Clients – Enter the maximum number of wireless clients that can connect to the select VAP.

Click the **Apply/Save** button to accept the changes made.

Local Network

To access the **Local Network** page, click on the **Setup** menu link, at the top, and then click on the **Local Network** menu link, on the left.

On this page the user can configure services related to the Local Area Network connectivity of this product. Set the IP address and Subnet Mask here.



In this section we can configure the Local Area Network (LAN) parameters.

IP Address: Enter the local IP address for this router here. This IP address is also used to connect to this device's Web User Interface. **Please note** that after changing this IP address you'll be forced to log into the Web User Interface again, using the new IP address.

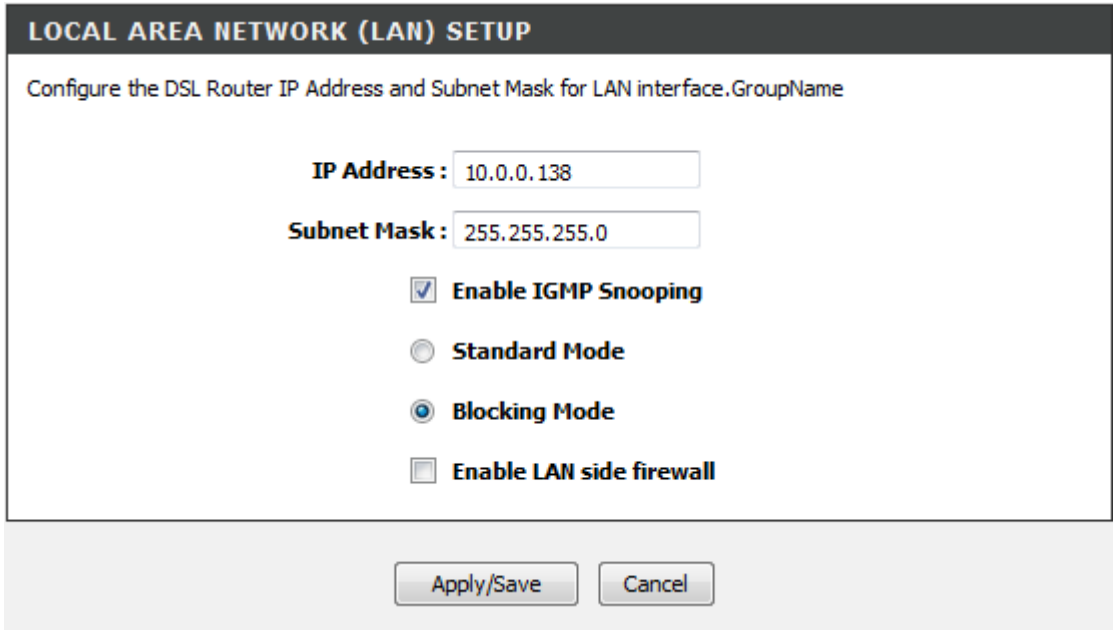
Subnet Mask: Enter the subnet mask used here.

Enable IGMP Snooping: Select this option to enable the IGMP snooping option.

Standard Mode: Select this option to enable the IGMP Snooping standard mode.

Blocking Mode: Select this option to enable the IGMP Snooping blocking mode.

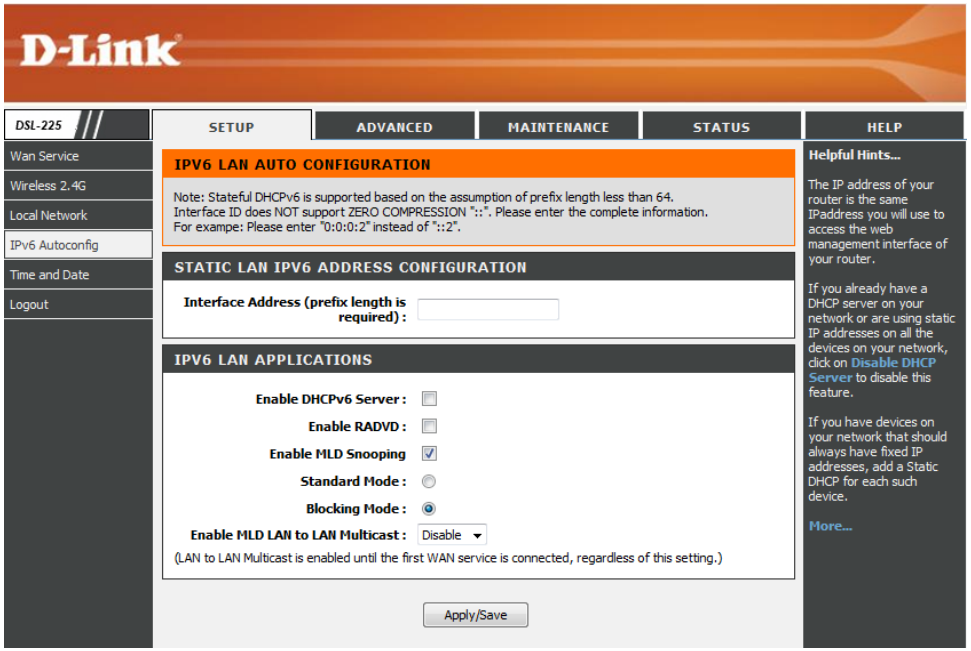
Enable LAN side firewall: Click the checkbox to enable this option.



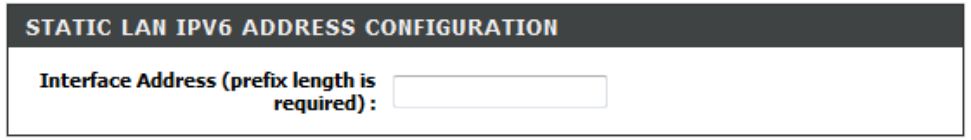
IPv6 Autoconfig

To access the **IPv6 Autoconfig** page, click on the **Setup** menu link, at the top, and then click on the **IPv6 Autoconfig** menu link, on the left.

On this page the user can configure services related to the **IPv6** connectivity of this product.



In this section we can enter the **Interface Address** used here.



Enable IPv6 LAN Applications.

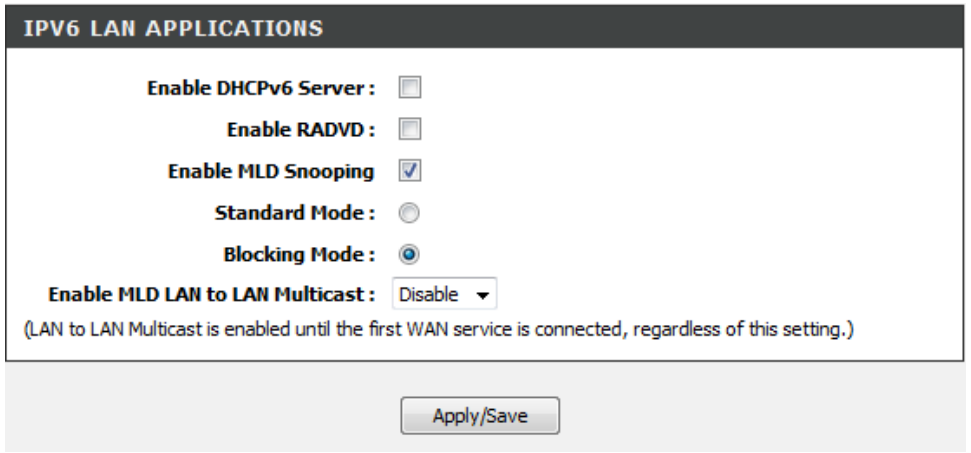
Enable DHCPv6 Server: Click the checkbox to enable the DHCPv6 Server.

Enable RADVD: Click the checkbox to enable RADVD.

Enable MLD Snooping: Click the checkbox to enable MLD Snooping. There are two options to choose from, **Standard Mode** and **Blocking Mode**.

Enable MLD LAN to LAN Multicast: Select Disable or Enable. Please read the precaution about enabling and disabling the service.

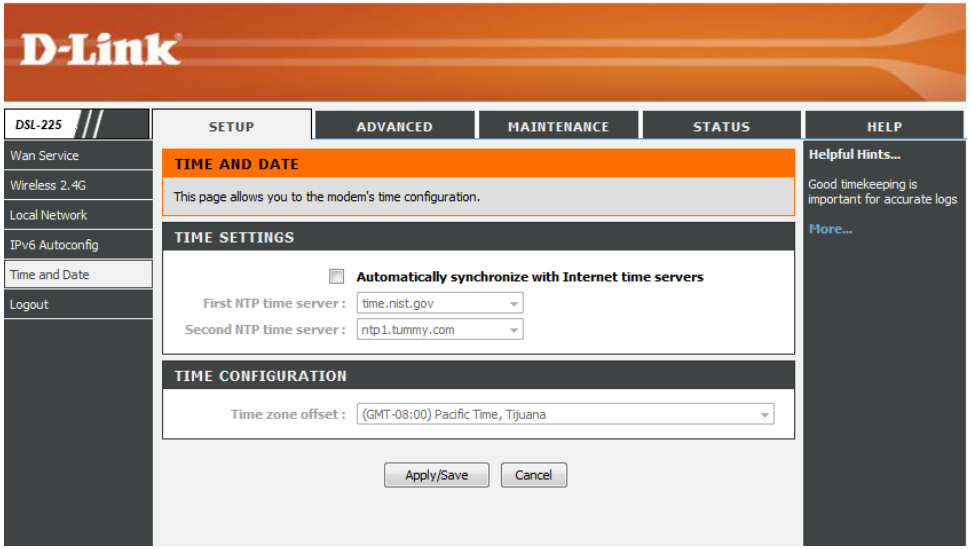
Click the **Apply/Save** button to accept the changes made.



Time and Date

To access the **Time and Date** page, click on the **Setup** menu link, at the top, and then click on the **Time and Date** menu link, on the left.

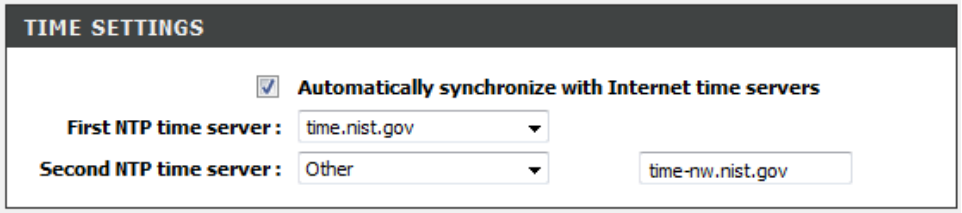
On this page the user can configure services related to the time and date feature of this product. **Time Servers** and a **Time Zone** can be specified here.



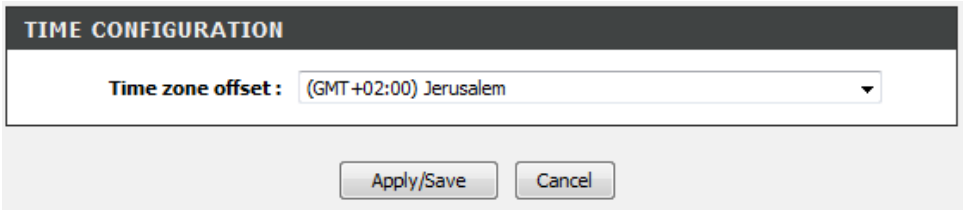
In this section we can configure the **Time Settings** for this router.

Select the **Automatically synchronize with Internet time server** option and then select the **First NTP time server** and **Second NTP time server** form the list here.

When the option **Other** is selected, manually enter the time server's URL or IP address in the space provided.



In this section we can select and configure the appropriate **Time Zone Offset**.



In this section we can configure the following parameters.

Time zone offset: Select the appropriate time zone offset here.

Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made.

Advanced Category

The **Advanced** category is designed to assist the user with more advanced configurations, concerning the other features found on this product.

The following pages can be found in the **Advanced** category:

- **Advanced Wireless 2.4G** – On this page the user can configure advanced services related to the Wireless **2.4 GHz** connectivity of this product. Services available for configuration are **Advanced Settings**, **MAC Filtering**, and **Wireless Station Information**.
- **Port Forwarding** – On this page the user can configure services related to the port forwarding feature of this product.
- **Port Triggering** – On this page the user can configure services related to the port triggering feature of this product.
- **DMZ** – On this page the user can configure services related to the DMZ feature of this product.
- **Parental Control** – On this page the user can configure services related to the parental control feature of this product. Services available for configuration are **Time Restriction** and **URL Filtering**.
- **Filtering Options** – On this page the user can configure services related to the port triggering feature of this product. Services available for configuration are **Inbound**, **Outbound**, and **Bridge Filtering**.

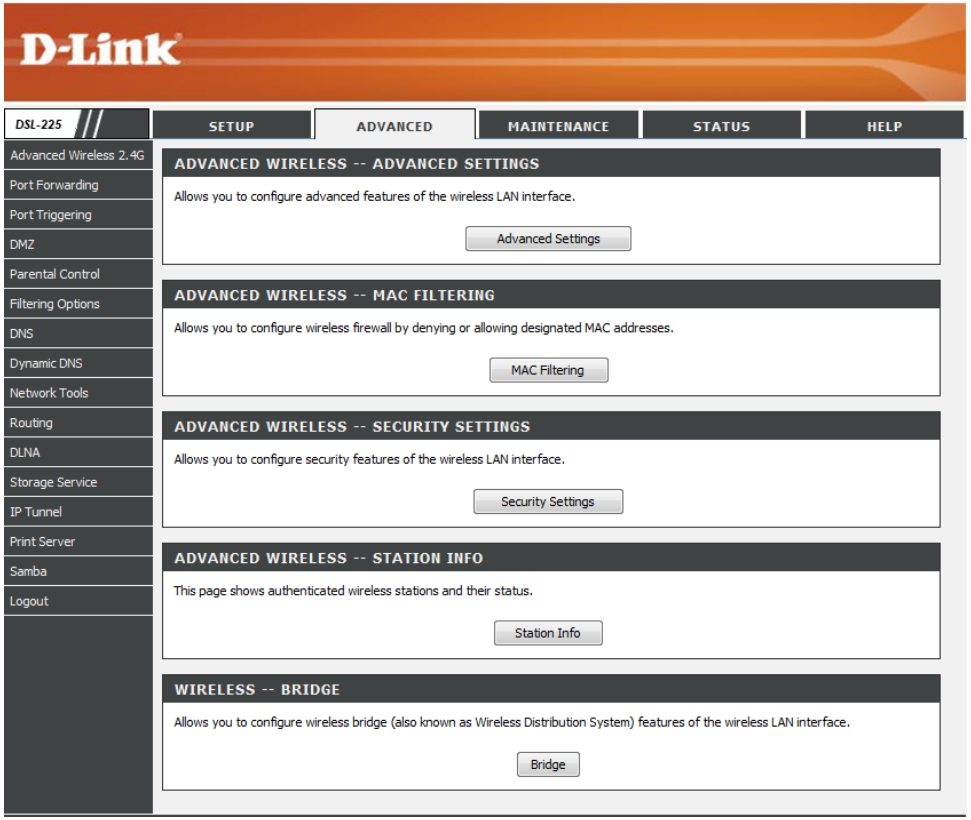
- **DNS** – On this page the user can configure services related to the DNS feature of this product.
- **Dynamic DNS** – On this page the user can configure services related to the Dynamic DNS feature of this product.
- **Network Tools** – On this page the user can configure services related to the Network Tools available on this product. Services available for configuration are **Port Mapping**, **Quality of Service**, **Queue Configuration**, **QoS Classification**, **UPnP**, **DSL Settings**, and **IGMP**.
- **Routing** – On this page the user can configure services related to the Routing feature of this product. Services available for configuration are **Static Route**, **Default Gateway**, and **RIP**.
- **DLNA** – On this page the user can configure services related to the Digital Living Network Alliance (DLNA) media server.

- **Storage Service** – On this page the user can configure services related to the Storage Services of this product.
- **IP Tunnel** – On this page the user can configure services related to IP Tunneling used on this product.
- **Print Server** – On this page the user can configure services related to the print server on this product.
- **Samba** – On this page the user can configure services related to the Samba connectivity of this product.

Advanced Wireless 2.4G

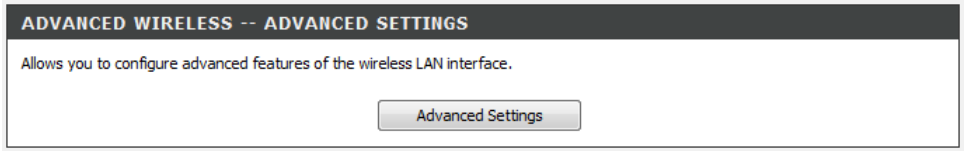
To access the **Advanced Wireless 2.4G** page, click on the **Advanced** menu link, at the top, and then click on the **Advanced Wireless 2.4G** menu link, on the left.

On this page the user can configure advanced services related to the Wireless 2.4Ghz connectivity of this product.

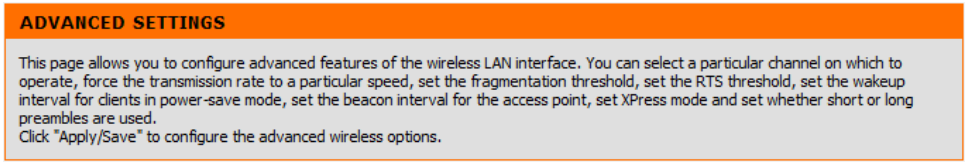


Advanced Settings

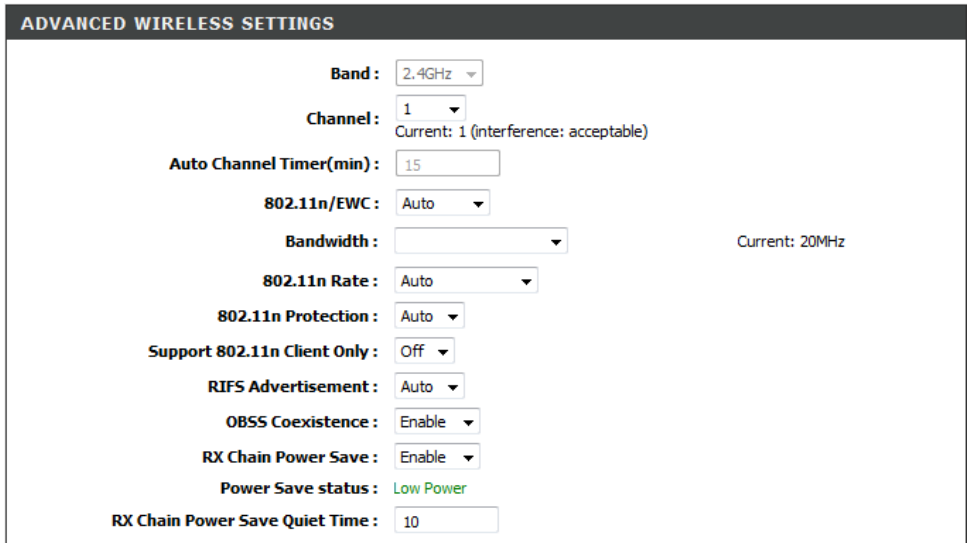
Click the **Advanced Settings** button to access the **Advanced Wireless Settings** configuration page.



After clicking the **Advanced Settings** button the following page is available.



In this section we can configure the advanced wireless settings.



Band: This parameter will display the current wireless band being configured.

Channel: Automatically select a channel or manually select the channel.

Auto Channel Timer: Enter the auto-channel timer value used here.

802.11n/EWC: Select this 802.11n/EWC option used here. Options to choose from are **Auto** and **Disabled**.

Bandwidth: Select between 20MHz or Auto 20/40MHz.

802.11n Rate: Select the 802.11n rate used here.

802.11n Protection: Select this 802.11n protection option used here. Options to choose from are **Auto** and **Off**.

Support 802.11n Client Only: Select the support for 802.11n clients only option used here. Options to choose from are **On** and **Off**.

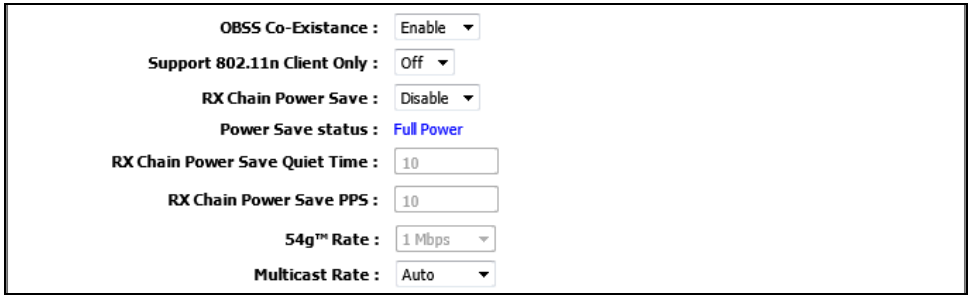
RIFS Advertisement: Select the RIFS advertisement option used here. Options to choose from are **Auto** and **Off**.

OBSS Co-Existence: Select the OBSS co-existence state here. Options to choose from are **Enable** and **Disable**.

RX Chain Power Save: Select the RX chain power save state here. Options to choose from are **Enable** or **Disable**.

Power Save status: This parameter will display the power save status.

RX Chain Power Save Quiet Time: Enter the RX chain power save quiet time value used here. This option becomes available after the **RX Chain Power Save** was enabled.



RX Chain Power Save PPS: Enter the RX chain power save PPS value used here. This option becomes available after the **RX Chain Power Save** was enabled.

54g™ Rate: Select the 54g™ rate value used here. This option becomes available after the **802.11n/EWC** option was disabled.

Multicast Rate: Select the multicast rate used here.

Basic Rate: Select the basic wireless rate used here.

Fragmentation Threshold: Enter the fragmentation threshold value used here.

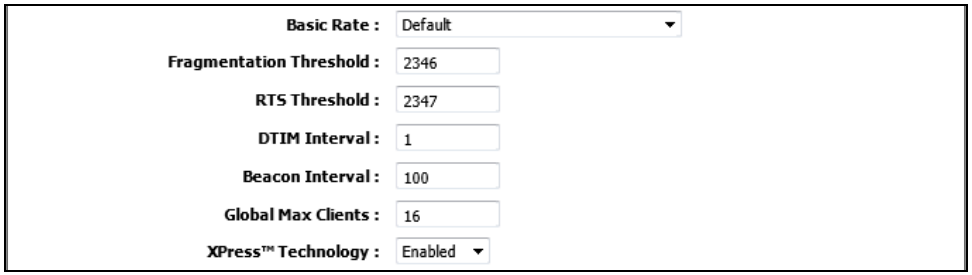
RTS Threshold: Enter the RTS threshold value used here.

DTIM Interval: Enter the DTIM Interval value used here.

Beacon Interval: Enter the beacon interval value used here.

Global Max Clients: Enter the maximum global wireless client value used here.

XPress™ Technology: Select the XPress™ technology state here. Options to choose from are **Enabled** and **Disabled**.

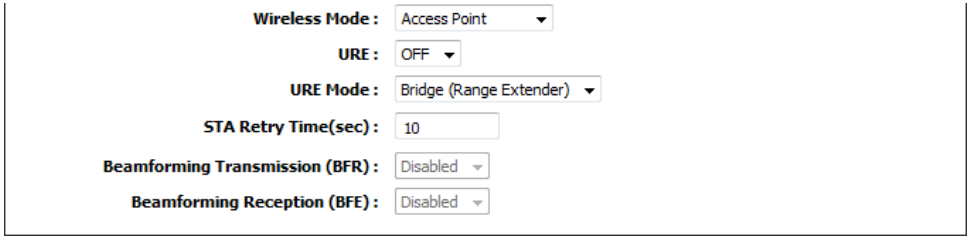


WMM (Wi-Fi Multimedia): Select the WMM (Wi-Fi Multimedia) state here. Options to choose from are **Auto**, **Enabled** and **Disabled**.

WMM No Acknowledgement: Select the WMM No Acknowledgement state here. Options to choose from are **Enabled** and **Disabled**.

WMM APSD: Select the WMM APSD state here. Options to choose from are **Enabled** and **Disabled**.

Wireless Mode: Select between Access Point and Wireless Ethernet from the drop-down menu



URE Mode: Select On or Off

STA Retry Time (sec): Select between Bridge (Range Extender) and Routed (Travel Router)

Beamforming Transmission (BFR): By default this is greyed out and disabled.

Beamforming Reception (BFE): By default this is greyed out and disabled.

Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made.

In the next section we'll discuss the Wireless **MAC Filtering** configurations.

MAC Filtering

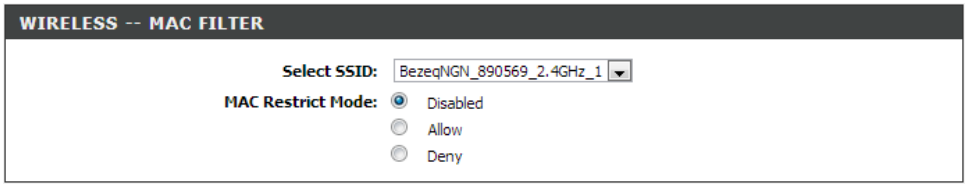
Click the **MAC Filtering** button to access the **Advanced Wireless MAC Filtering** configuration page.

After clicking the **MAC Filtering** button the following page is available.

In this section we can configure the Wireless MAC Filtering parameters.

Select SSID: Select the appropriate SSID used here.

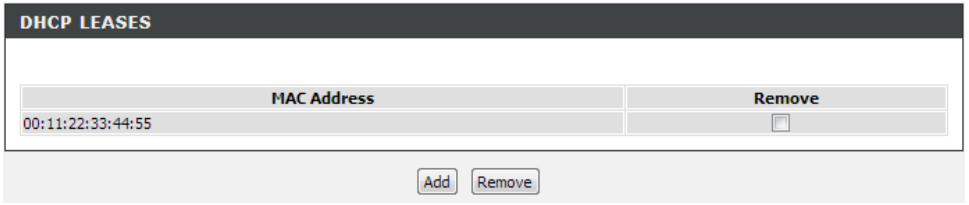
MAC Restrict Mode: Select the MAC restrict mode used here. Options to choose from are **Disabled**, **Allow**, and **Deny**.



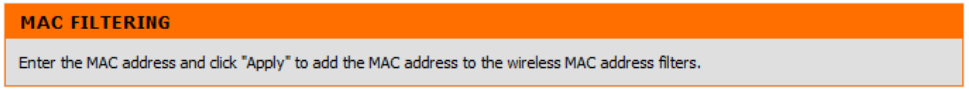
In this section a list of **DHCP Leases** will be displayed.

Click the **Add** button to add a new entry.

Select the **Remove** option and click the **Remove** button to remove the specific entry.



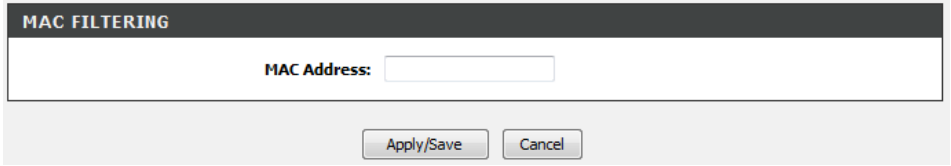
After clicking the **Add** button the following page is available.



In this section we can enter a **MAC Address** used in the MAC filtering rule here. The MAC address must use the *00:11:22:33:44:55* format.

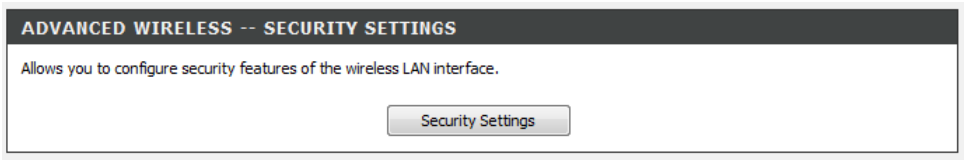
Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

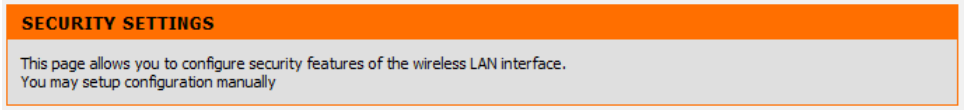


Security Settings

Click the **Advanced Settings** button to access the **Security Settings** configuration page.



After clicking the **Security Settings** button the following page is available.



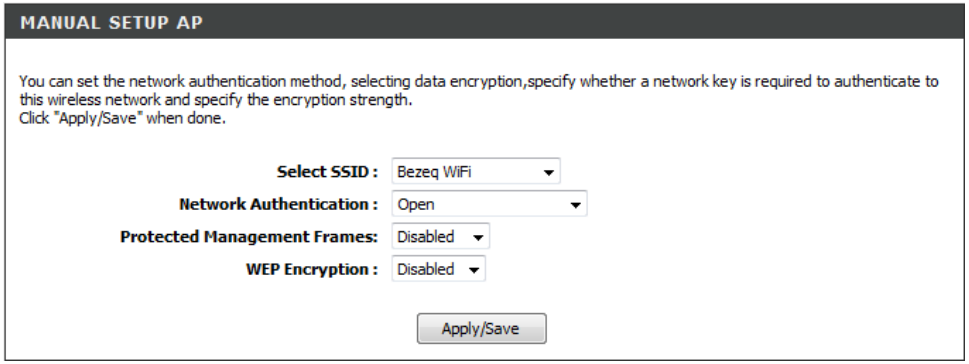
In the **Manual Setup AP** section, you can configure the following:

Select SSID: Select the SSID from the drop-down list

Network Authentication: Select the network authentication method. Options to choose from are **Open**, **Shared**, **802.1X**, **WPA2**, **WPA2-PSK**, **Mixed WPA2/WPA**, and **Mixed WPA2/WPA-PSK**.

Protected Management Frames: Select between Disabled, Capable, or Required.

WEP Encryption: Select to enable or disable WEP encryption.



Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

Wireless Security Mode – Shared

Wired Equivalent Privacy (WEP) is any entry level wireless security method that we can use to prevent unauthorized wireless access to this router. WEP is not a very secure option, but it is better than no wireless security.

After selecting to use **Shared** network authentication and enabling the WEP encryption option as your wireless security mode, the following parameters will be available to configure:

Protected Management Frames: Select to **Disable**, **Capable**, or **Required**.

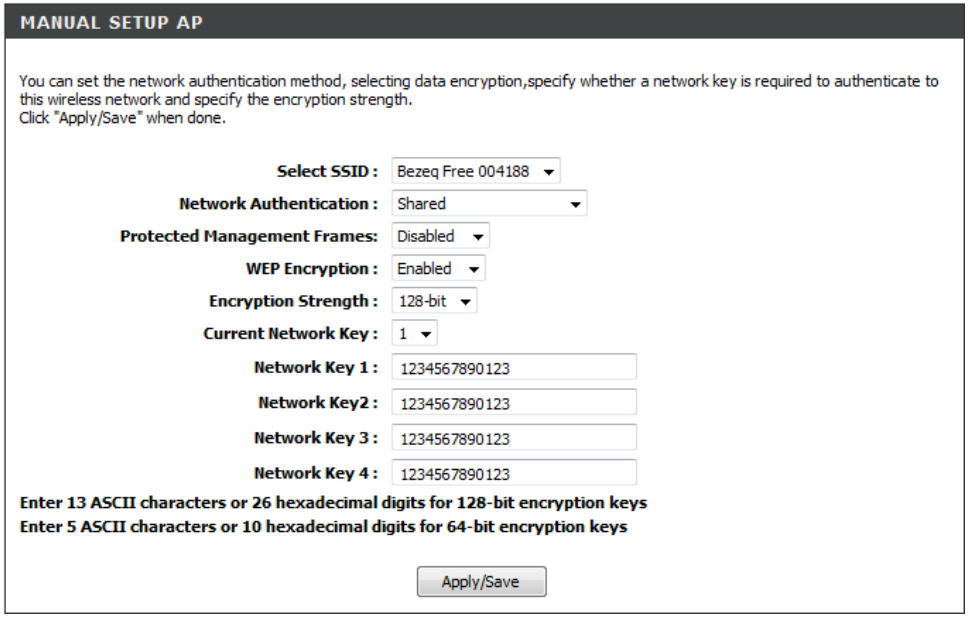
WEP Encryption: By default it's disabled.

Encryption Strength: Select the WEP key length value used here. Options to choose from are **128 bit (26 hex digits)** and **64 bit (10 hex digits)**.

Current Network Key: Select one of the 4 key options available and enter a wireless security key in the appropriate space provided. This key must be configured on all the wireless clients for them to be able to connect to your wireless network.

Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.



Wireless Security Mode – 802.1X

After selecting to use **802.1X** network authentication and enabling the WEP encryption option as your wireless security mode, the following parameters will be available to configure:

Protected Management Frames: Select to **Disable**, **Capable**, or **Required**.

RADIUS Server IP Address: Enter the IP address of the external RADIUS server used here.

RADIUS Port: Enter the external RADIUS server port number used here.

RADIUS Key: Enter the RADIUS server Shared Secret here. This key must be configured on all the wireless clients for them to be able to connect to your wireless network.

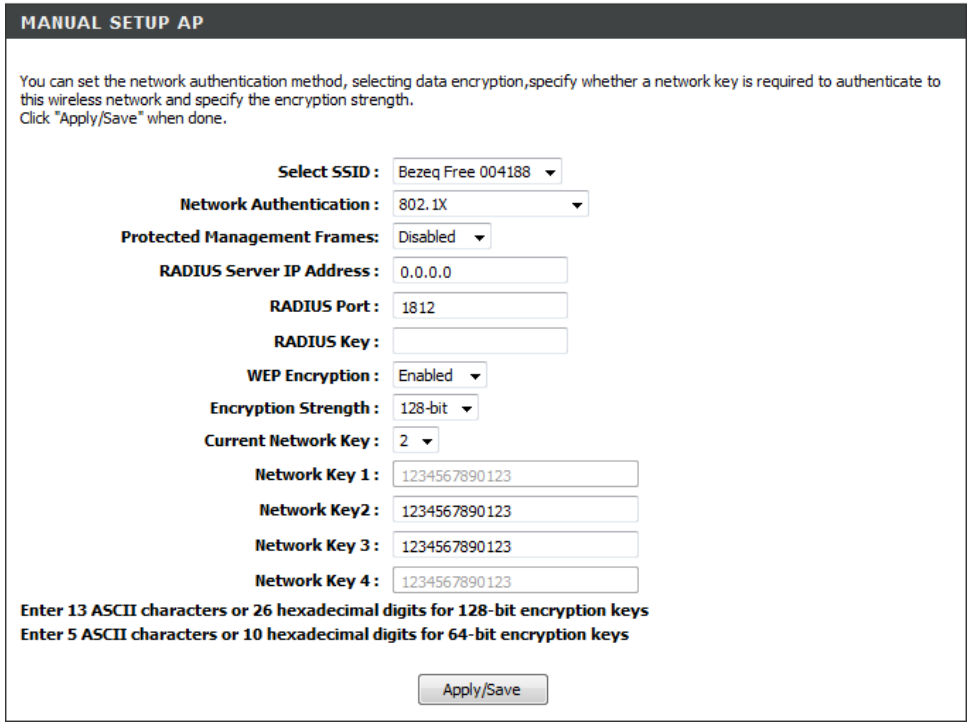
WEP Encryption: Select to enable or disable WEP encryption.

Encryption Strength: Select the WEP key length value used here. Options to choose from are **128 bit (26 hex digits)** and **64 bit (10 hex digits)**.

Current Network Key: Select one of the 4 key options available and enter a wireless security key in the appropriate space provided. This key must be configured on all the wireless clients for them to be able to connect to your wireless network.

Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.



Wireless Security Mode – WPA2

Wi-Fi Protected Access (WPA2) is the most advanced wireless security method that we can use to prevent unautherized wireless access to this router. **WPA2-Enterprise** requires the use of an external RADIUS server.

After selecting to use **WPA2** network authentication as your wireless security mode, the following parameters will be available to configure:

Protected Management Frames: Select to **Disable**, **Capable**, or **Required**.

WPA2 Preauthentication: Select to enable or disable the WPA2 pre-authentication option here.

Network Re-auth Interval: Enter the network re-authentication interval value here.

WPA Group Rekey Interval: Enter the group key update interval value here.

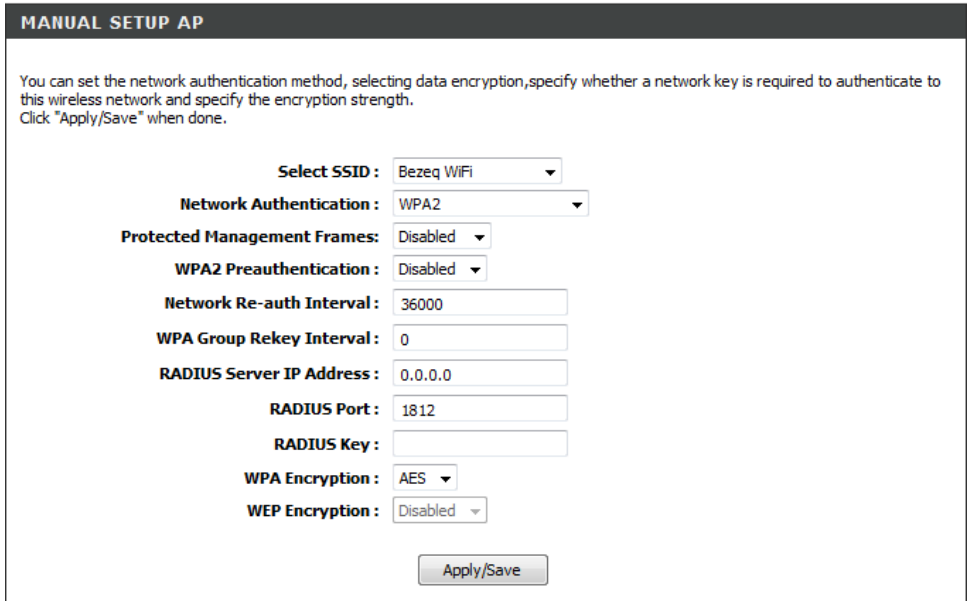
RADIUS Server IP Address: Enter the IP address of the external RADIUS server used here.

RADIUS Port: Enter the external RADIUS server port number used here.

RADIUS Key: Enter the RADIUS server Shared Secret here. This key must be configured on all the wireless clients for them to be able to connect to your wireless network.

WPA Encryption: Select the WPA2 encryption method here. Options to choose from are **TKIP**, **AES**, and **TKIP+AES**.

WEP Encryption: By default this is disabled.



Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

Wireless Security Mode – WPA2-PSK

Wi-Fi Protected Access (WPA2) is the most advanced wireless security method that we can use to prevent unautherized wireless access to this router. **WPA2 PSK** does not require an authentication server.

After selecting to use **WPA2-PSK** network authentication as your wireless security mode, the following parameters will be available to configure:

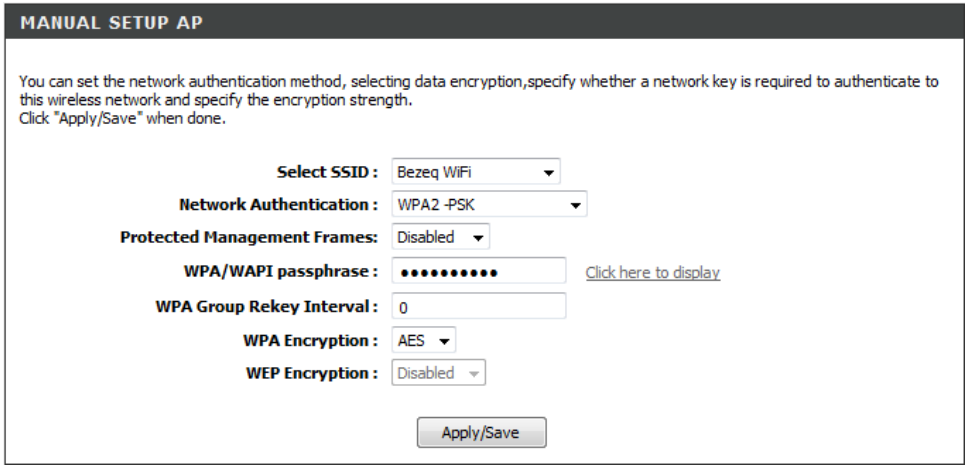
Protected Management Frames: Select to **Disable**, **Capable**, or **Required**.

WPA/WAPI passphrase: Enter the WPA2-PSK wireless Pre-Shared Key here. This key must be configured on all the wireless clients for them to be able to connect to your wireless network. Click the '*Click here to display*' option to display the pass-phrase entered.

WPA Group Rekey Interval: Enter the group key update interval value here.

WPA Encryption: Select the WPA2 encryption method here. Options to choose from are **TKIP**, **AES**, and **TKIP+AES**.

WEP Encryption: By default this is disabled.



Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

Wireless Security Mode – Mixed WPA2/WPA

Wi-Fi Protected Access (WPA) is a more advanced wireless security method that we can use to prevent unautherized wireless access to this router. **Wi-Fi Protected Access (WPA2)** is the most advanced wireless security method that we can use to prevent unautherized wireless access to this router. This option allows us to have both **WPA** and **WPA2** available for client connectivity.

After selecting to use **Mixed WPA2/WPA** network authentication as your wireless security mode, the following parameters will be available to configure:

Protected Management Frames: Select to **Disable**, **Capable**, or **Required.**

WPA2 Preauthentication: Select to enable or disable the WPA2/WPA pre-authentication option here.

Network Re-auth Interval: Enter the network re-authentication interval value here.

WPA Group Rekey Interval: Enter the group key update interval value here.

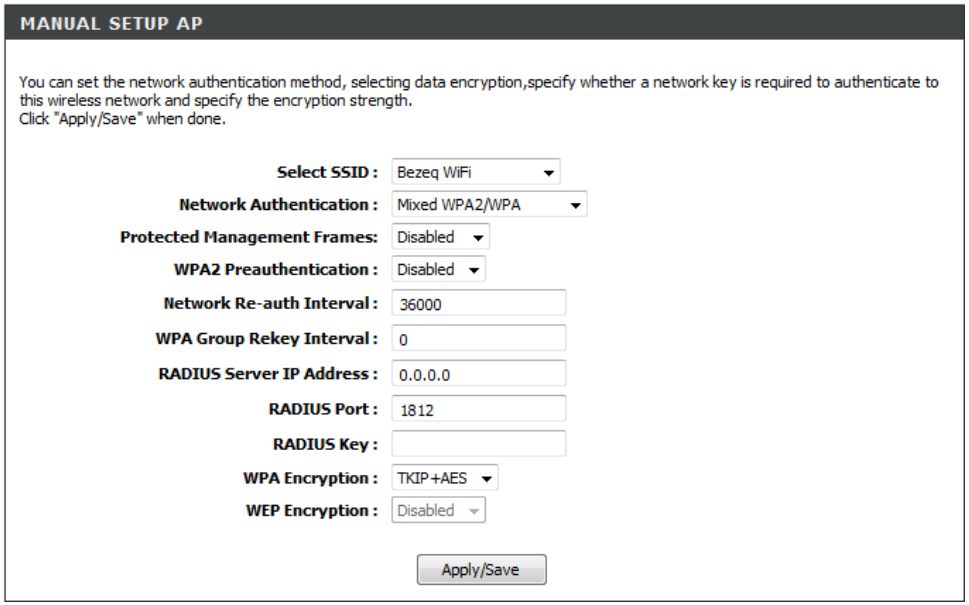
RADIUS Server IP Address: Enter the IP address of the external RADIUS server used here.

RADIUS Port: Enter the external RADIUS server port number used here.

RADIUS Key: Enter the RADIUS server Shared Secret here. This key must be configured on all the wireless clients for them to be able to connect to your wireless network.

WPA Encryption: Select the WPA2/WPA encryption method here. Options to choose from are **TKIP**, **AES**, and **TKIP+AES**.

WEP Encryption: By default this is disabled.



Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

Wireless Security Mode – Mixed WPA2/WPA-PSK

Wi-Fi Protected Access (WPA) is a more advanced wireless security method that we can use to prevent unautherized wireless access to this router. **Wi-Fi Protected Access (WPA2)** is the most advanced wireless security method that we can use to prevent unautherized wireless access to this router. This option allows us to have both **WPA** and **WPA2** available for client connectivity.

After selecting to use **Mixed WPA2/WPA-PSK** network authentication as your wireless security mode, the following parameters will be available to configure:

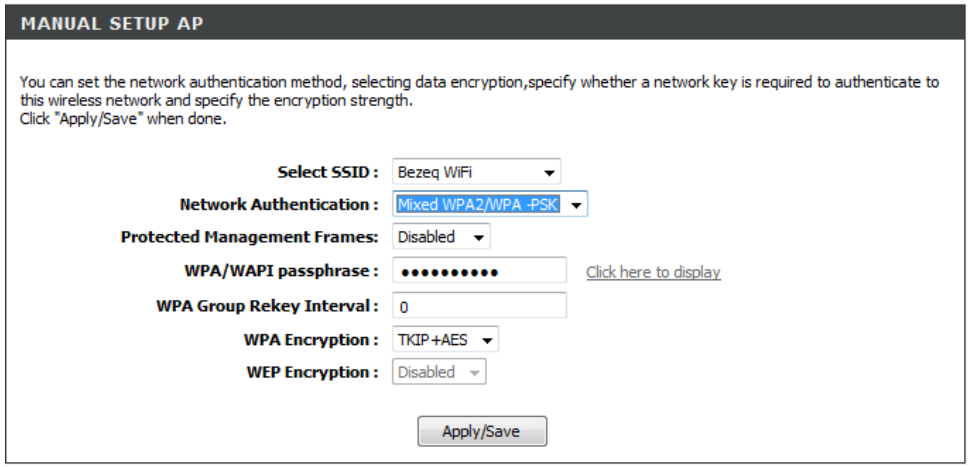
Protected Management Frames: Select to **Disable**, **Capable**, or **Required**.

WPA/WAPI passphrase: Enter the WPA2/WPA-PSK wireless Pre-Shared Key here. This key must be configured on all the wireless clients for them to be able to connect to your wireless network. Click the '*Click here to display*' option to display the pass-phrase entered.

WPA Group Rekey Interval: Enter the group key update interval value here.

WPA Encryption: Select the WPA2 encryption method here. Options to choose from are **TKIP**, **AES**, and **TKIP+AES**.

WEP Encryption: By default this is disabled.



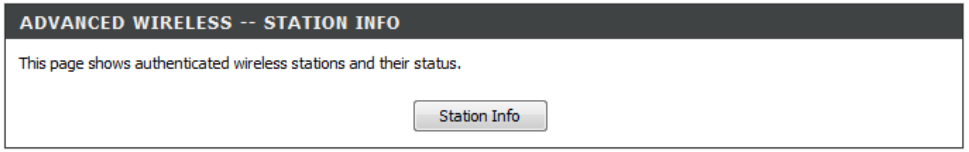
Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

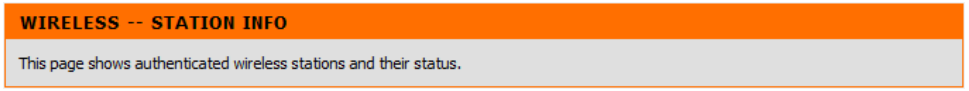
In the next section we'll discuss the Wireless **Station Information** configurations.

Station Info

Click the **Advanced Settings** button to access the **Advanced Wireless Station Info** configuration page.

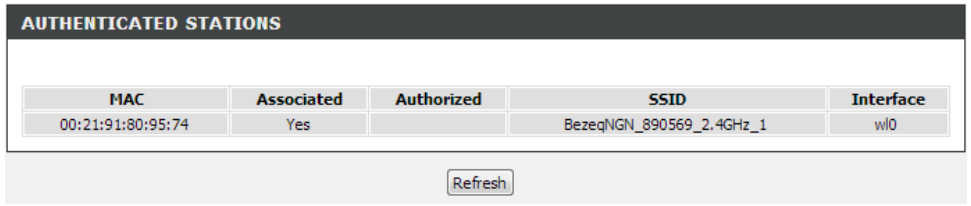


After clicking the **Station Info** button the following page is available.



In this section a list of wireless **Authenticated Stations** are displayed.

Click the **Refresh** button to refresh the information in this table.

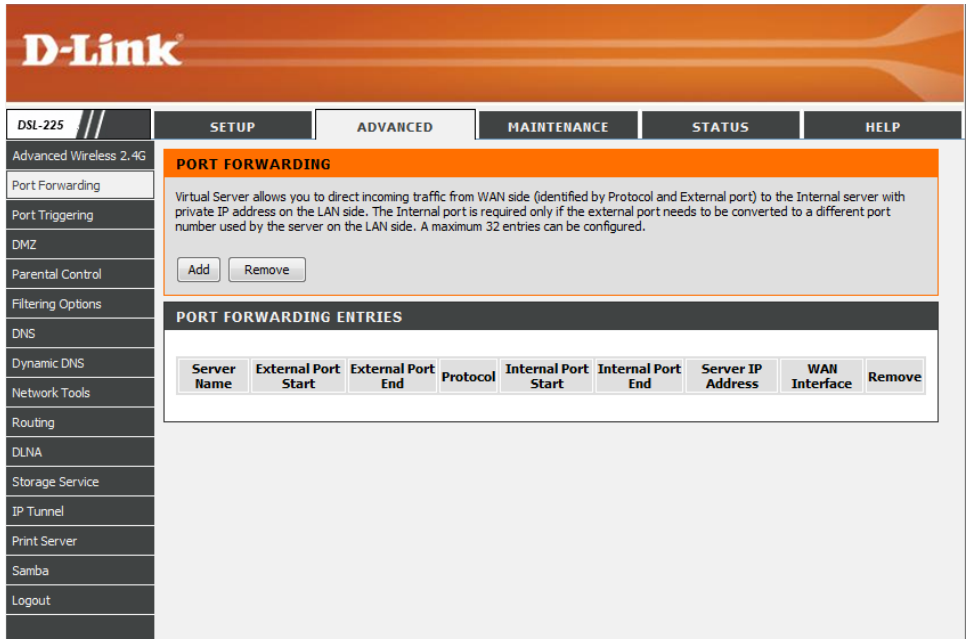


Port Forwarding

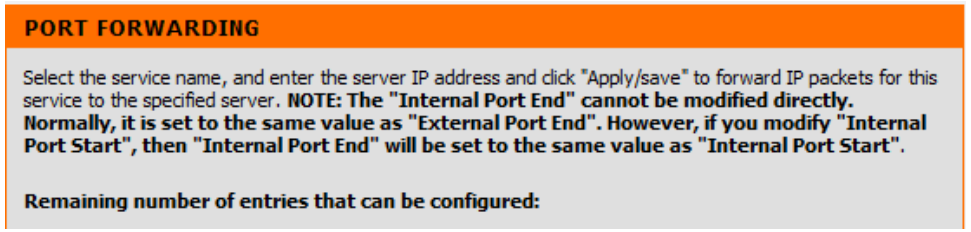
To access the **Port Forwarding** page, click on the **Advanced** menu link, at the top, and then click on the **Port Forwarding** menu link, on the left.

On this page the user can configure services related to the port forwarding feature of this product.

Click the **Add** button to add a new entry.
Click the **Remove** button to remove an entry.



After clicking the **Add** button, the following page is available.



In this section we can configure **Port Forwarding** rules.

Use Interface: Select an existing interface from the list that will be associated with this rule.

Select a Service: Select a service from the list. These pre-defined services will contain all the parameters needed to create a successful rule.

Custom Service: If the service is not located in the list, we can create our own service. Enter the service name for the rule here.

Server IP Address: Enter the server IP address here.

External Port Start: Enter the external starting port number here.

External Port End: Enter the external ending port number here.

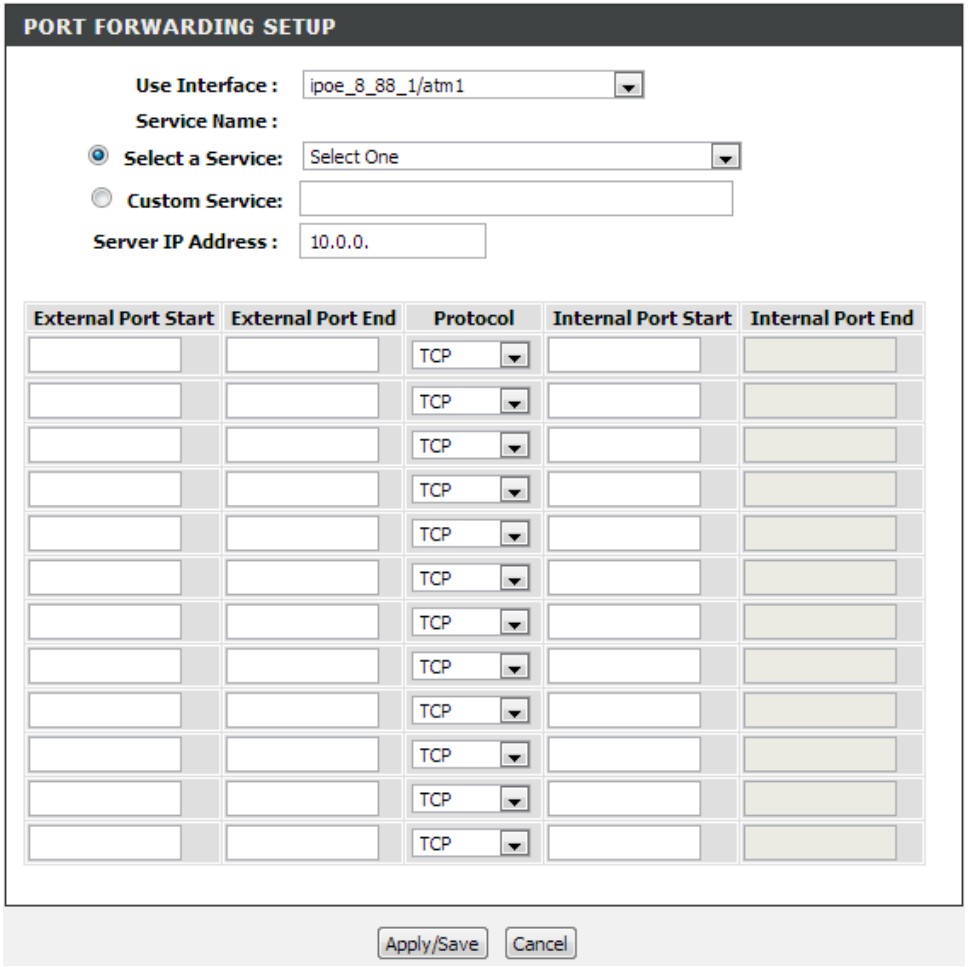
Protocol: Select the appropriate protocol used here. Options to choose from are **TCP/UDP**, **TCP**, and **UDP**.

Internal Port Start: Enter the internal starting port number here.

Internal Port End: Enter the internal ending port number here.

Click the **Apply/Save** button to accept the changes made.

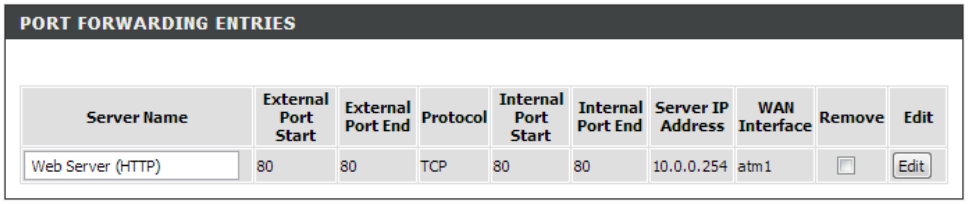
Click the **Cancel** button to discard the changes made and return to the main page.



In this section a list of port forwarding rules will be displayed.

Click the **Edit** button to modify an existing entry.

Select the **Remove** option and click the **Remove** button to remove the specific interface.

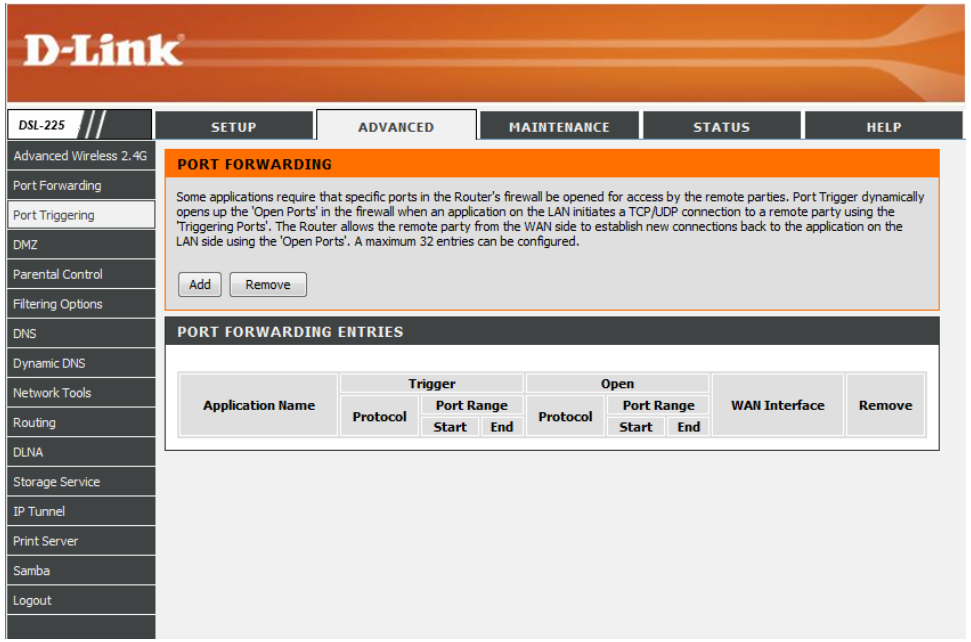


Port Triggering

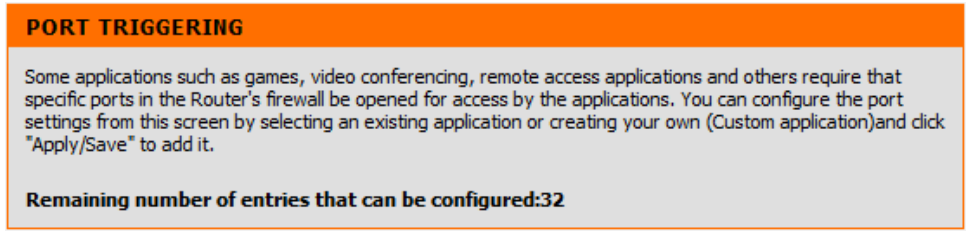
To access the **Port Triggering** page, click on the **Advanced** menu link, at the top, and then click on the **Port Triggering** menu link, on the left.

On this page the user can configure services related to the port triggering feature of this product.

Click the **Add** button to add a new interface.
Click the **Remove** button to remove an entry.



After clicking the **Add** button, the following page is available.



In this section we can create a new port triggering rule.

Use Interface: Select the interface that will be associated with this rule here.

Select an application: Select an application from the list here. These pre-defined applications will contain all the parameters needed to create a successful rule.

Custom application: If the application is not located in the list, we can create our own application. Enter the custom application name for the rule here.

Trigger Port Start: Enter the starting trigger port number here.

Trigger Port End: Enter the ending trigger port number here.

Trigger Protocol: Select the trigger protocol used here. Options to choose from are **TCP/UDP**, **TCP**, and **UDP**.

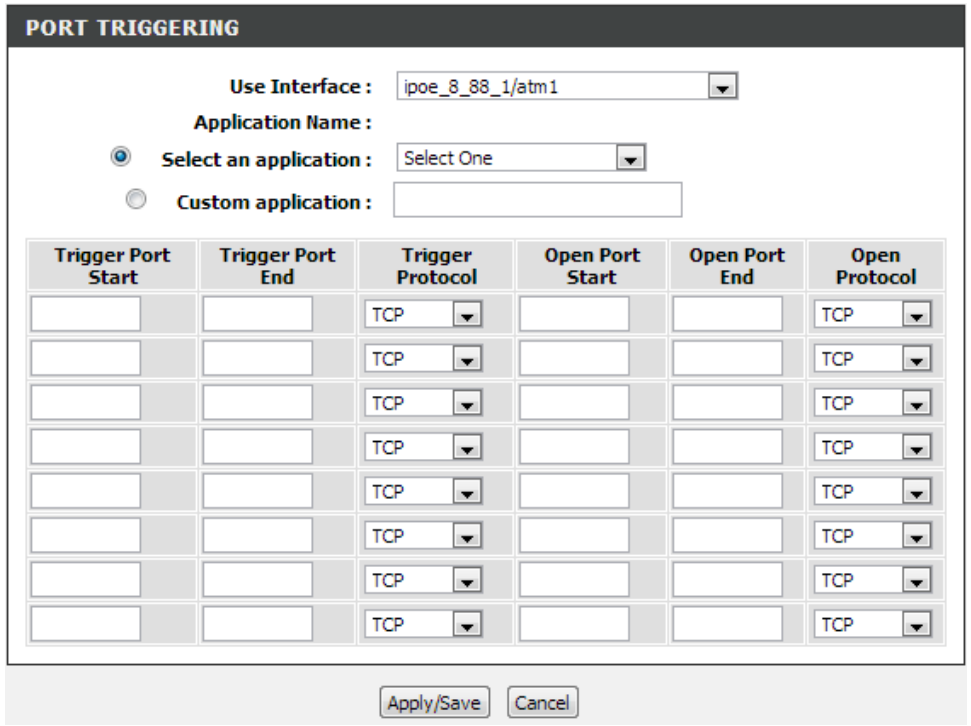
Open Port Start: Enter the starting open port number here.

Open Port End: Enter the ending open port number here.

Open Protocol: Select the open protocol used here. Options to choose from are **TCP/UDP**, **TCP**, and **UDP**.

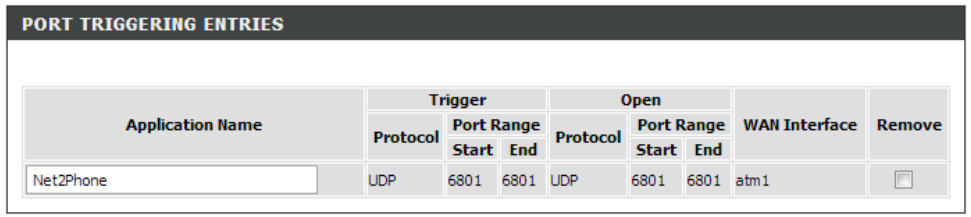
Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.



In this section a list of port triggering rules will be displayed.

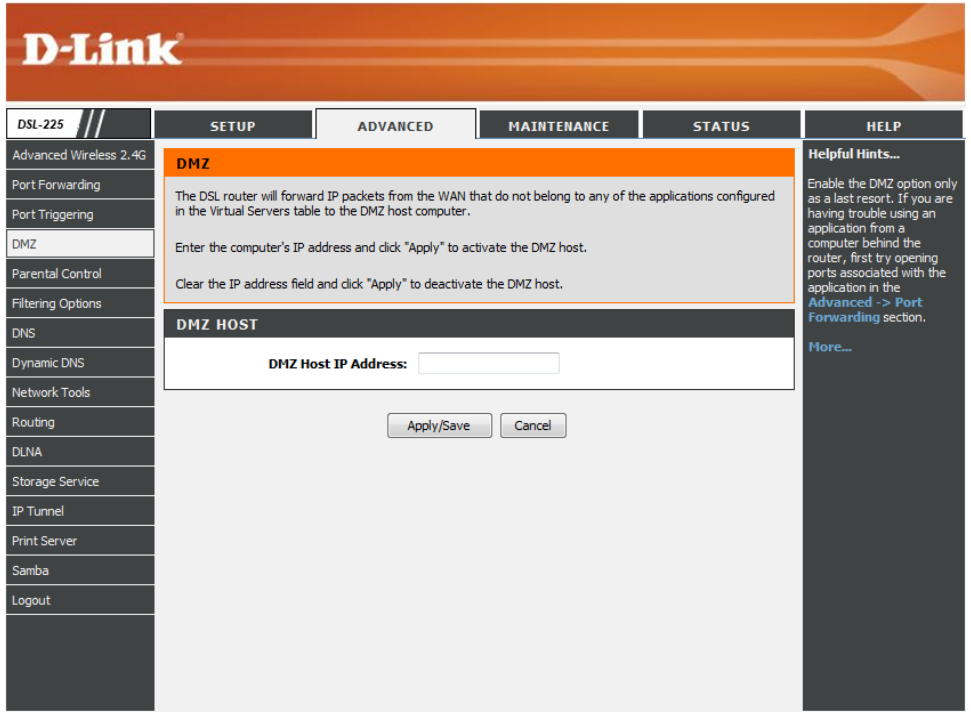
Select the **Remove** option and click the **Remove** button to remove the specific interface.



DMZ

To access the **DMZ** page, click on the **Advanced** menu link, at the top, and then click on the **DMZ** menu link, on the left.

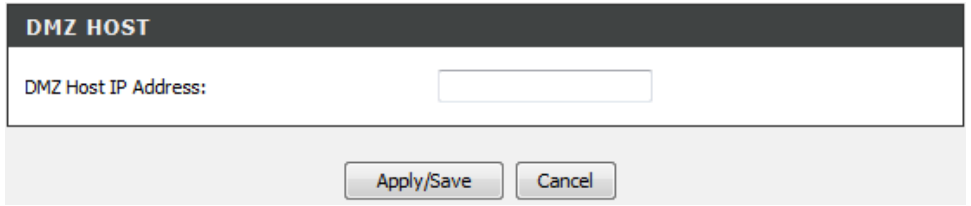
On this page the user can configure services related to the DMZ feature of this product.



In this section we can configure the **DMZ Host** by entering the **DMZ Host IP Address** here.

Click the **Apply/Save** button to accept the changes made.

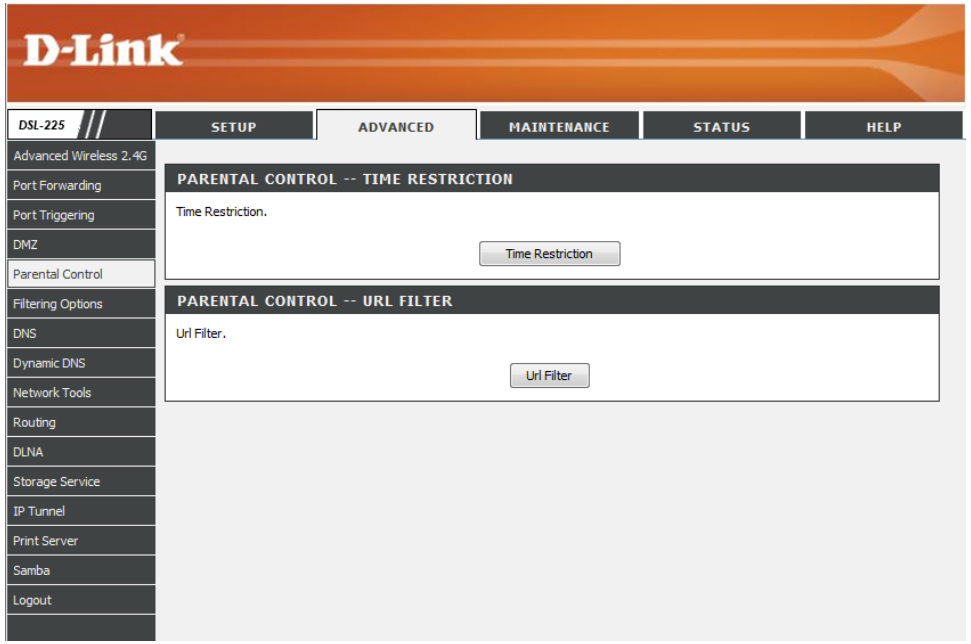
Click the **Cancel** button to discard the changes made and return to the main page.



Parental Control

To access the **Parental Control** page, click on the **Advanced** menu link, at the top, and then click on the **Parental Control** menu link, on the left.

On this page the user can configure services related to the parental control feature of this product.

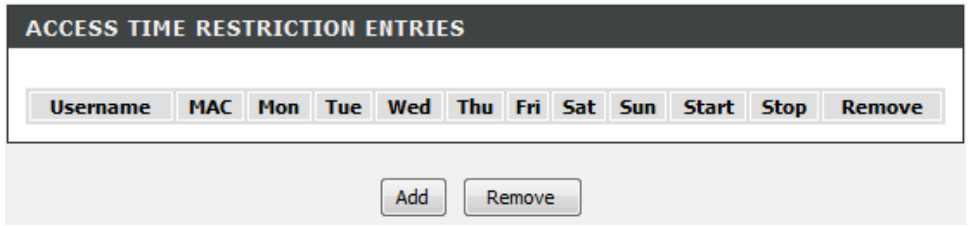


Time Restriction

Click the **Time Restriction** button to access the **Parental Control Time Restriction** configuration page.

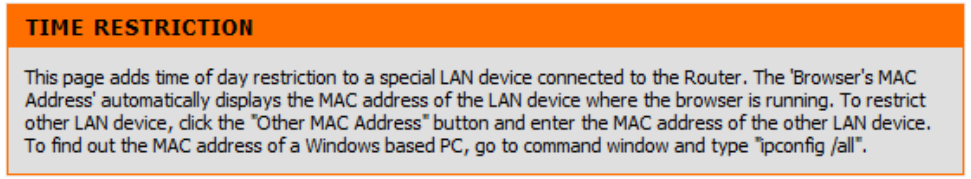
After clicking the **Time Restriction** button the following page is available.

In this section a list of Time Restriction entries will be displayed.



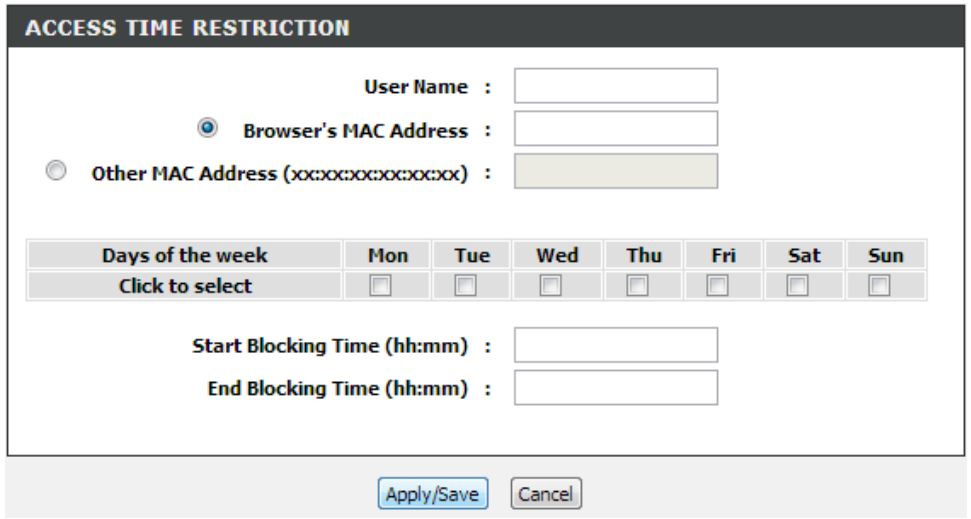
Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.

After clicking the **Add** button the following page is available.



In this section we can configure the **Access Time Restriction** settings for this router.

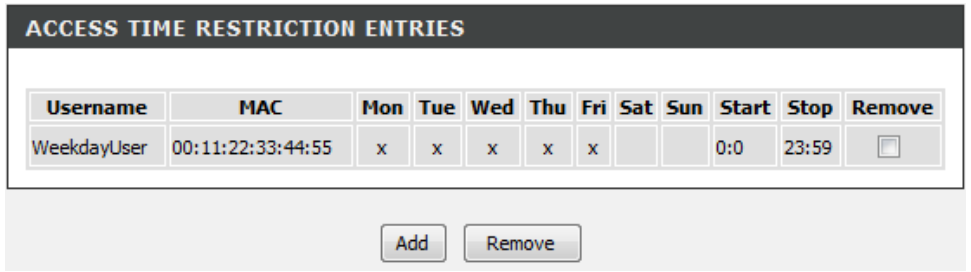
User Name: Enter the user name used here.
Browser's MAC Address: Enter the browser's MAC address here.
Other MAC Address: Enter the other MAC address here.
Days of the Week: Select which days of the week to include in this rule.
Start Blocking Time: Enter the time value that will be used to start blocking.
End Blocking Time: Enter the time value that will be used to end blocking.



Click the **Apply/Save** button to accept the changes made.
Click the **Cancel** button to discard the changes made and return to the main page.

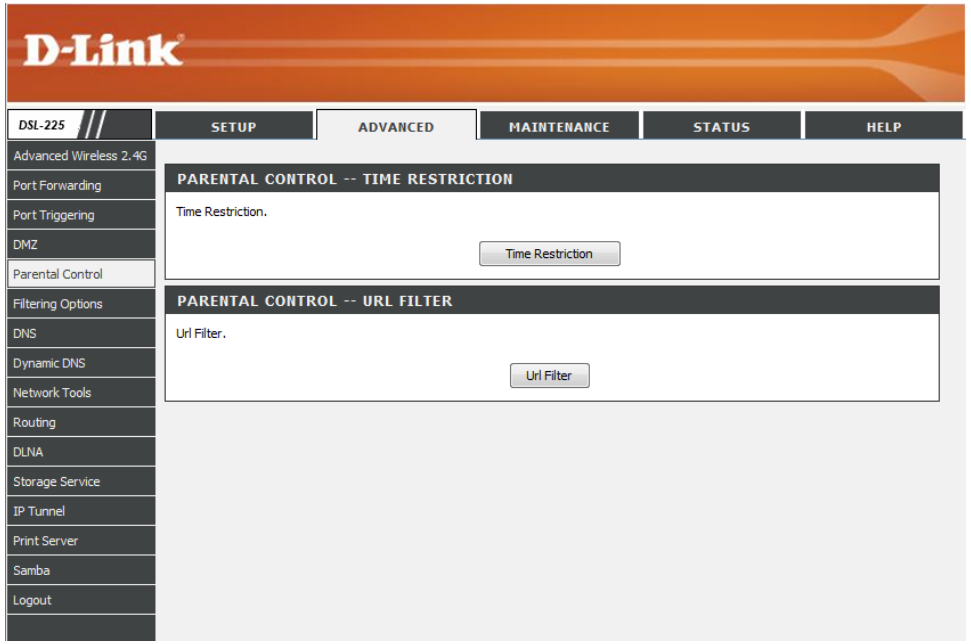
In this section a list of Time Restriction entries will be displayed.

Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.

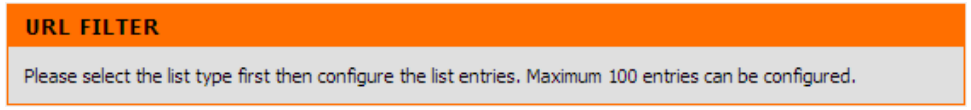


URL Filter

Click the **URL Filter** button to access the **Parental Control URL Filter** configuration page.

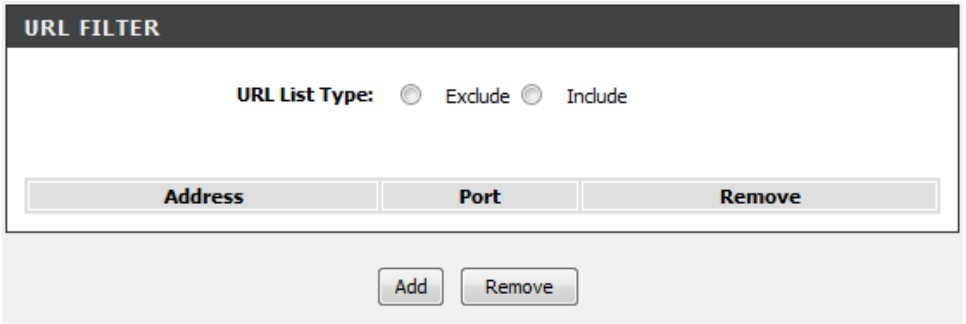


After clicking the **URL Filter** button the following page is available.

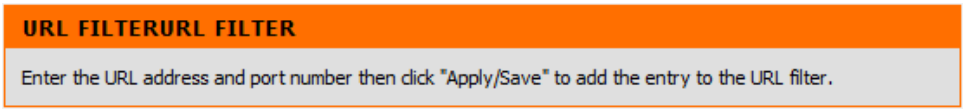


In this section a list of **URL Filter** entries will be displayed. Select to **Exclude** or **Include** these rules from the **URL List Type**.

Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.

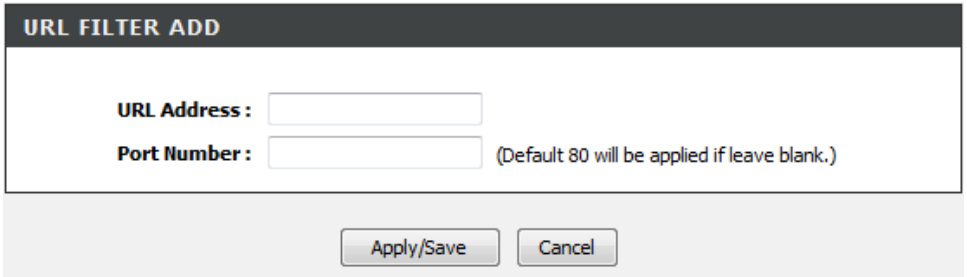


After clicking the **Add** button the following page is available.



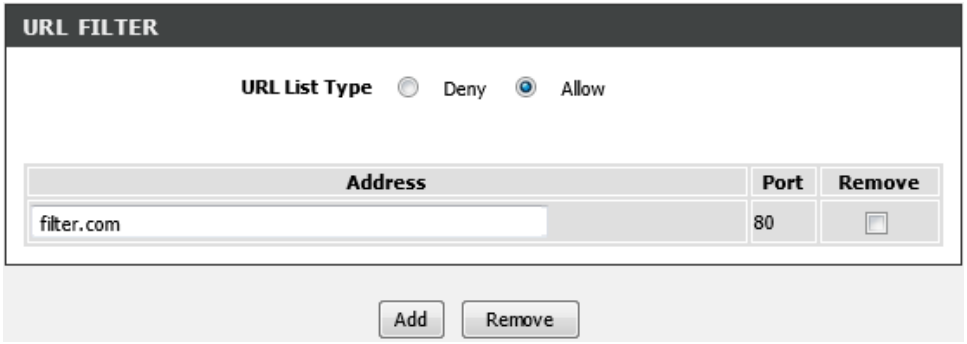
In this section we can create a new **URL Filter** rule by entering the **URL Address** and **Port Number**.

Click the **Apply/Save** button to accept the changes made.
Click the **Cancel** button to discard the changes made and return to the main page.



In this section a list of URL Filter entries will be displayed. Select to **Exclude** or **Include** these rules from the **URL List Type**.

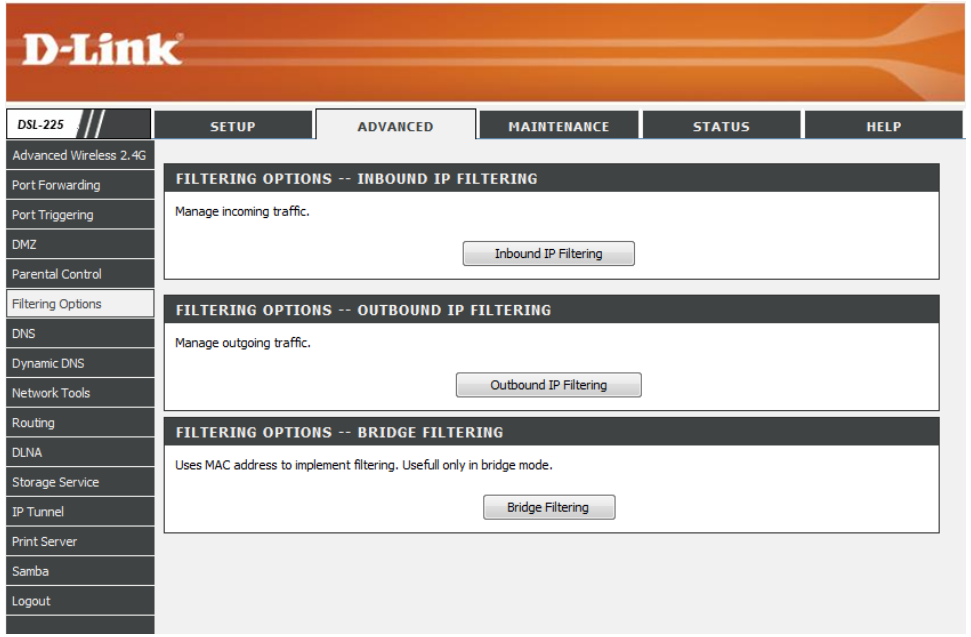
Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.



Filtering Options

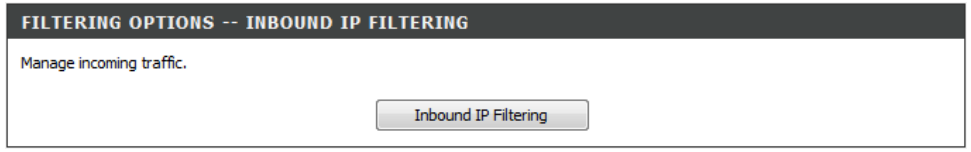
To access the **Filtering Options** page, click on the **Advanced** menu link, at the top, and then click on the **Filtering Options** menu link, on the left.

On this page the user can configure services related to the port triggering feature of this product.

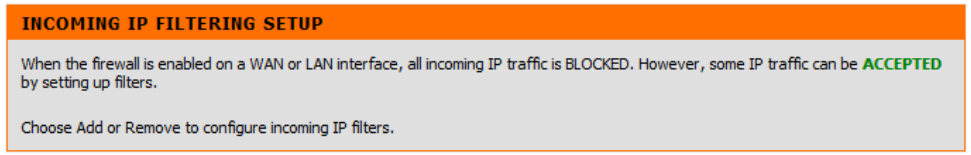


Inbound IP Filtering

Click the **Inbound IP Filtering** button to access the **Inbound IP Filtering** rule configuration page.

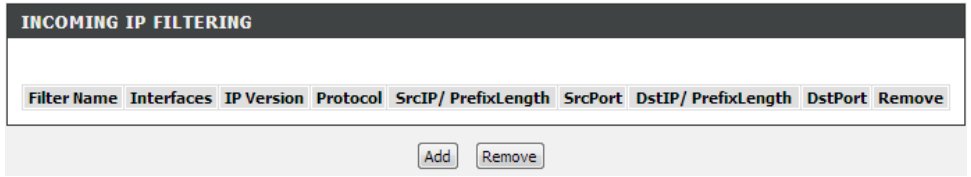


After clicking the **Inbound IP Filtering** button the following page is available.

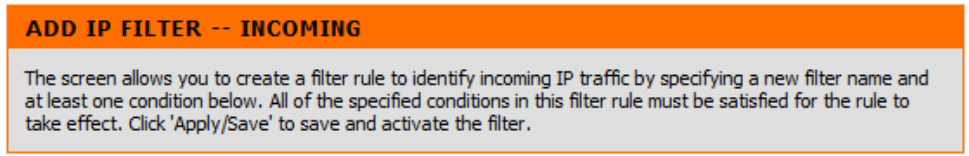


In this section a list of Inbound IP filtering rules will be displayed.

Click the **Add** button to add a new rule.
Select the **Remove** option and click the **Remove** button to remove the specific rule.



After clicking the **Add** button the following page is available.



In this section we can create a new Inbound Filtering rule.

Filter Name: Enter the Inbound filtering rule name here.

IP Version: Select the IP version from the list. Options to choose from are **IPv4** and **IPv6**.

Protocol: Select the protocol used from the list. Options to choose from are **TCP/UDP**, **TCP**, **UDP**, and **ICMP**.

Source IP address: Enter the source IP address here.

Source Port: Enter the source port number here.

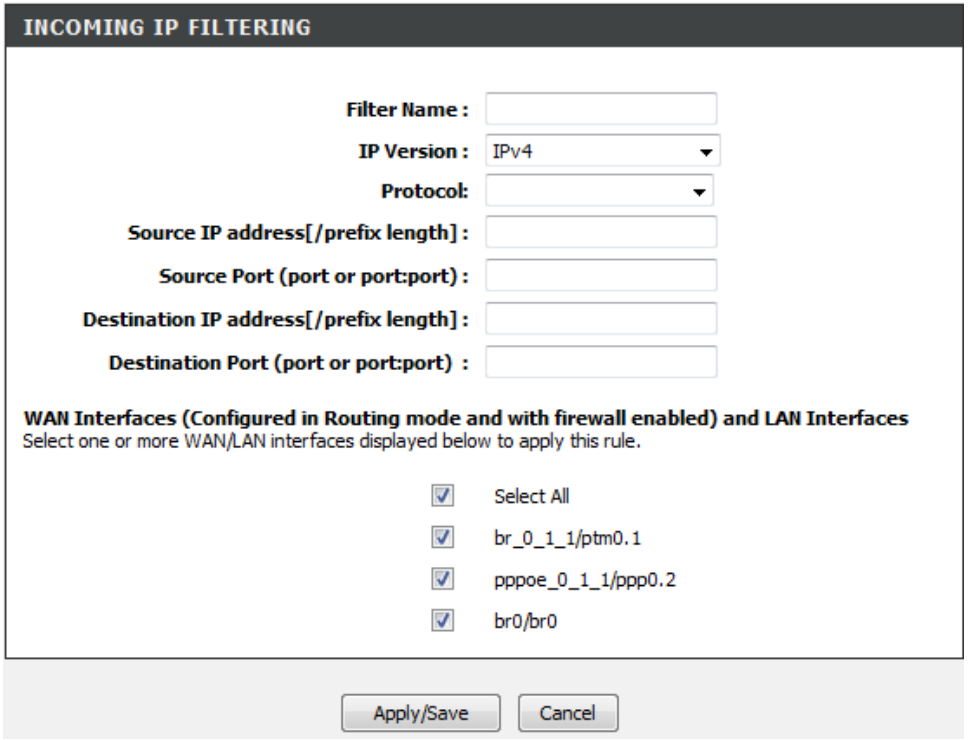
Destination IP address: Enter the destination IP address here.

Destination Port: Enter the destination port number here.

WAN Interfaces: Select the WAN interface that will be used for this incoming IP filter rule.

Click the **Apply/Save** button to accept the changes made.

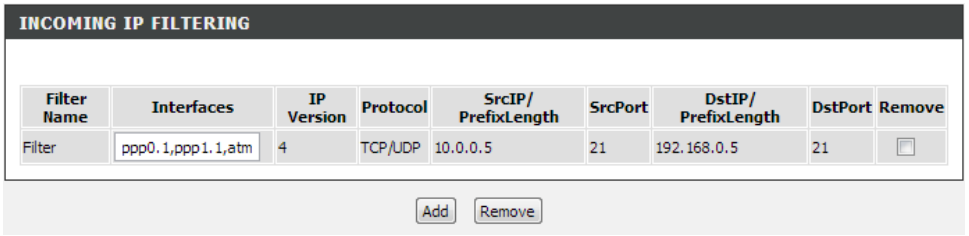
Click the **Cancel** button to discard the changes made and return to the main page.



In this section a list of Inbound IP filtering rules will be displayed.

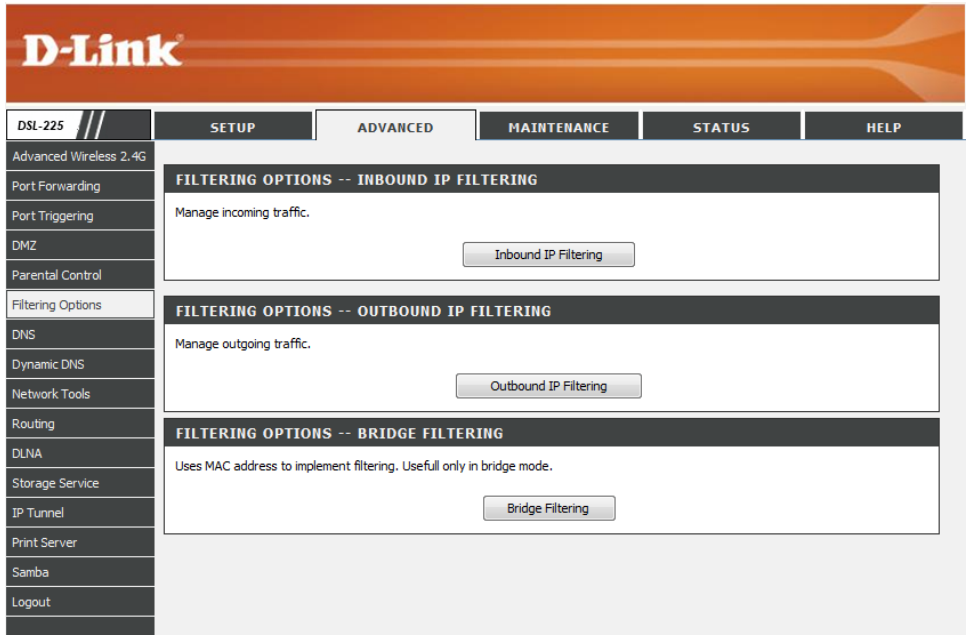
Click the **Add** button to add a new rule.

Select the **Remove** option and click the **Remove** button to remove the specific rule.

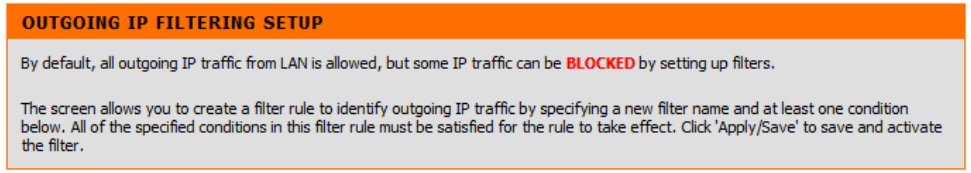


Outbound IP Filtering

Click the **Outbound IP Filtering** button to access the **Outbound IP Filtering** rule configuration page.

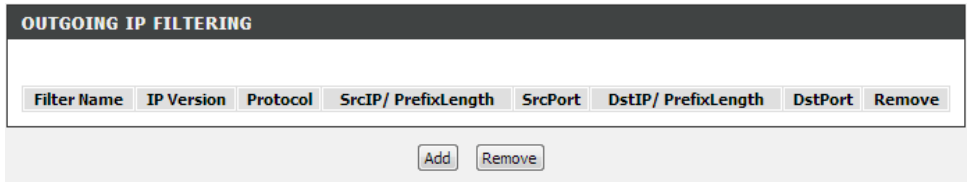


After clicking the **Outbound IP Filtering** button the following page is available.

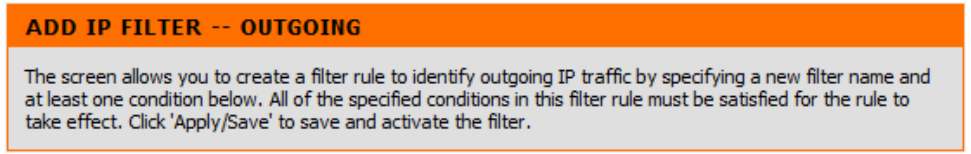


In this section a list of Outbound IP filtering rules will be displayed.

Click the **Add** button to add a new rule.
Select the **Remove** option and click the **Remove** button to remove the specific rule.



After clicking the **Add** button the following page is available.



In this section we can create a new Outbound IP filter rule.

Filter Name: Enter the Outbound filtering rule name here.

IP Version: Select the IP version from the list. Options to choose from are **IPv4** and **IPv6**.

Protocol: Select the protocol used from the list. Options to choose from are **TCP/UDP**, **TCP**, **UDP**, and **ICMP**.

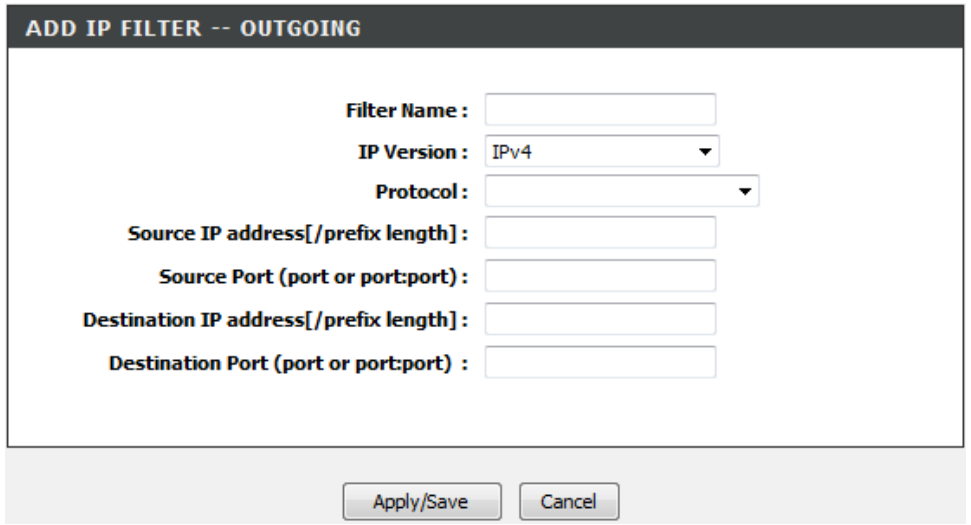
Source IP address: Enter the source IP address here.

Source Port: Enter the source port number here.

Destination IP address: Enter the destination IP address here.

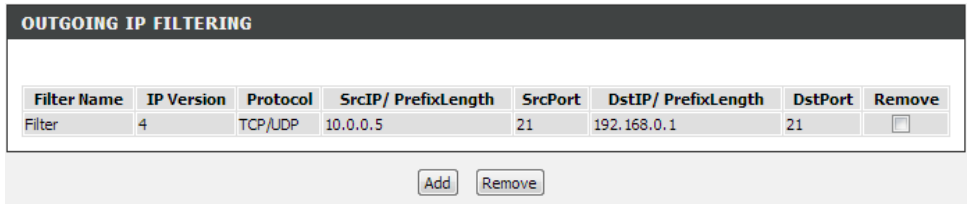
Destination Port: Enter the destination port number here.

Click the **Apply/Save** button to accept the changes made.
Click the **Cancel** button to discard the changes made and return to the main page.



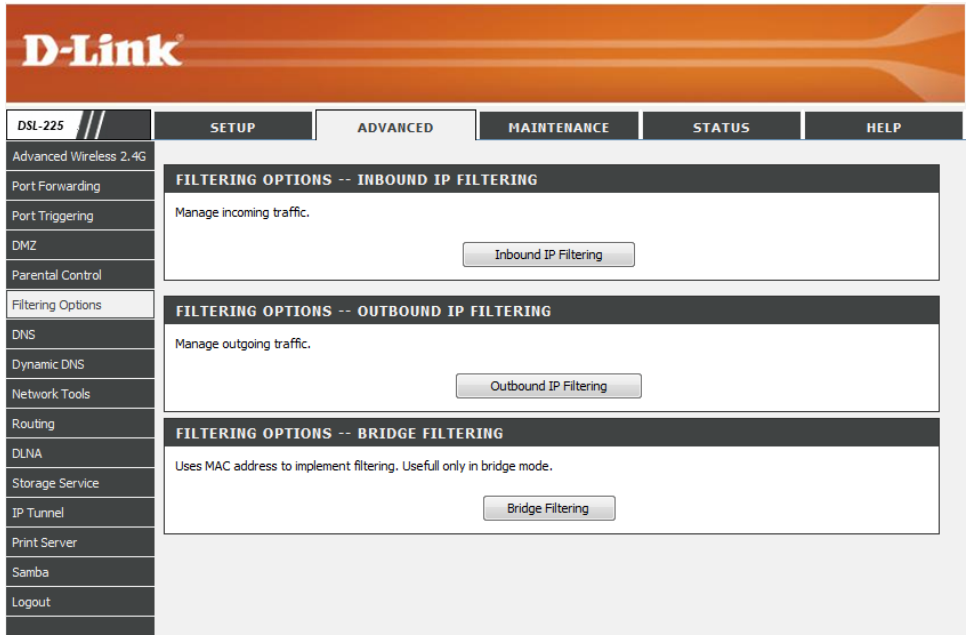
In this section a list of Outbound IP filtering rules will be displayed.

Click the **Add** button to add a new rule.
Select the **Remove** option and click the **Remove** button to remove the specific rule.

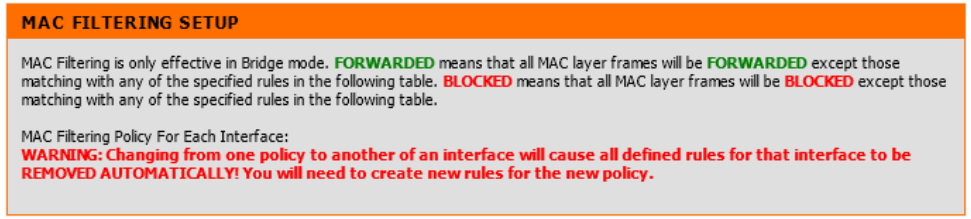


Bridge Filtering

Click the **Bridge Filtering** button to access the **Bridge Filtering** rule configuration page.



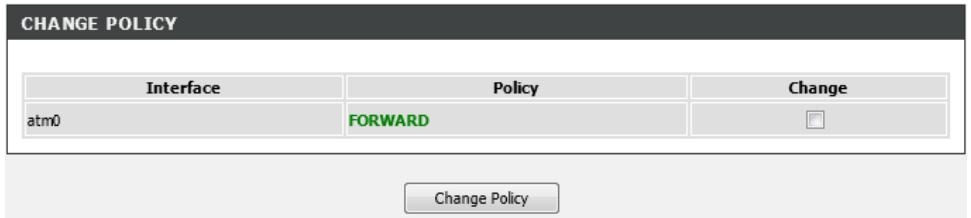
After clicking the **Bridge Filtering** button the following page is available.



MAC Filtering is only effective in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

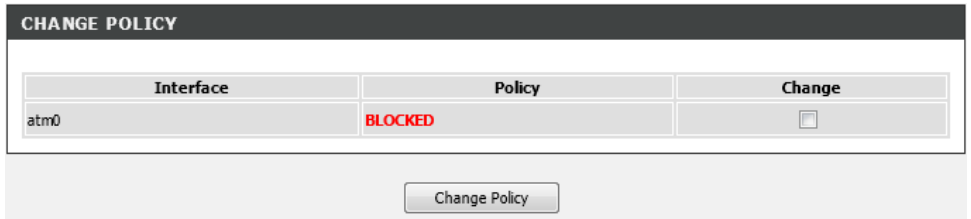
In this section we will find the current **Policy** status as well the option to change this option.

Select the **Change** tick box and click the **Change Policy** button, to change the Bridge MAC filtering policy.



After selecting the **Change** option and clicking the **Change Policy** button. The policy will be changed.

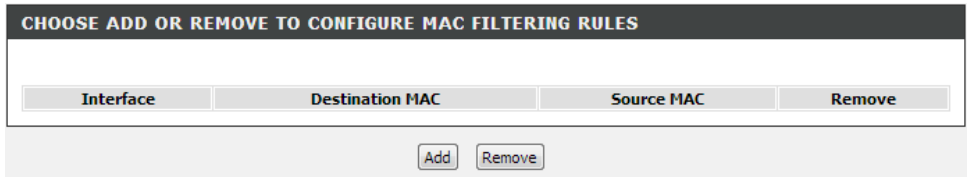
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be **REMOVED AUTOMATICALLY**! You will need to create new rules for the new policy.



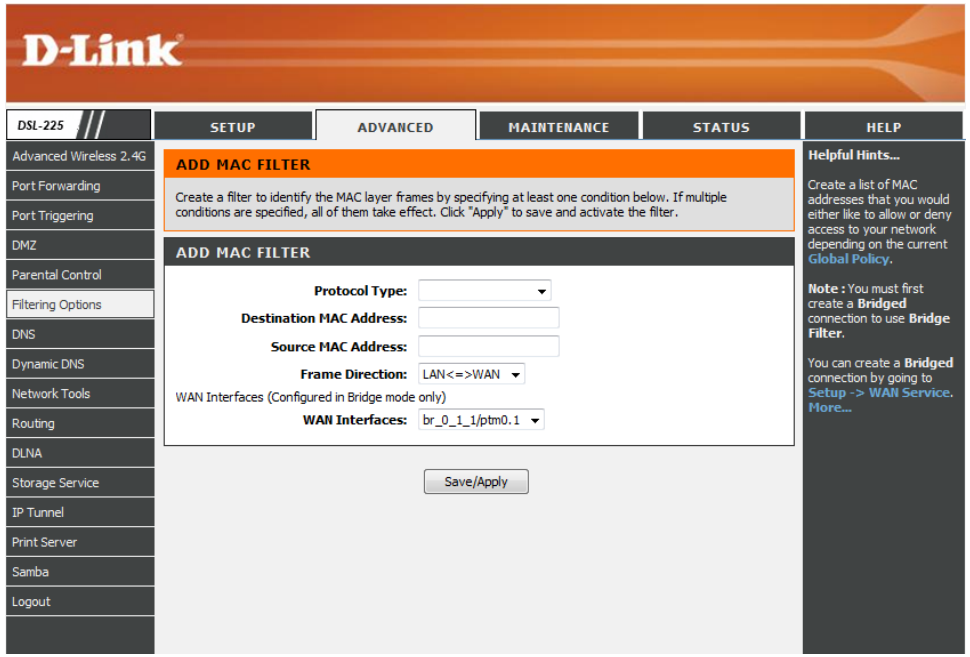
In this section we can see a list of MAC filtering rule created.

Click the **Add** button to add a new rule.

Select the **Remove** option and click the **Remove** button to remove the specific rule.



After clicking the **Add** button, the following page will be available.



In this section we can configure the MAC filtering rule.

Parameters available for configuration are:

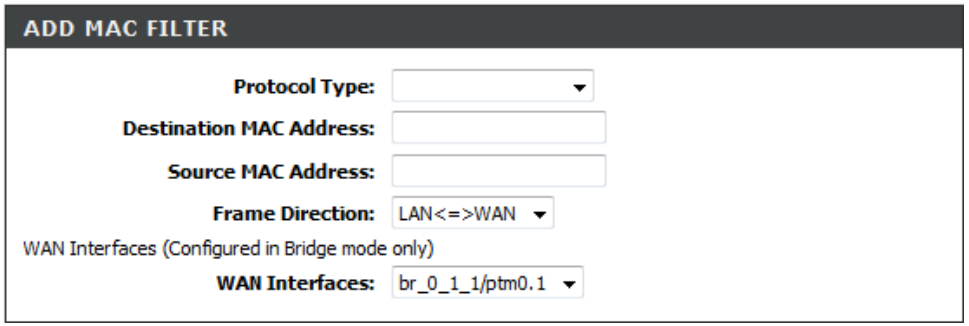
Protocol Type: Select the protocol type option that will be associated with this rule. Options to choose from are **PPPoE**, **IPv4**, **IPv6**, **IPX**, and **IGMP**.

Destination MAC Address: Enter the destination MAC address used here.

Source MAC Address: Enter the source MAC address used here.

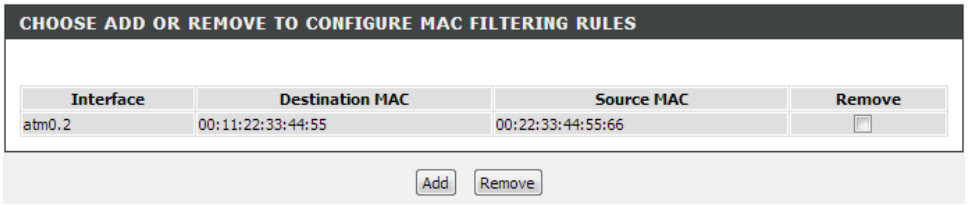
Frame Direction: Select the **Frame Direction** from the drop-down menu. Select between **LAN /WAN**, **WAN/LAN**, or **LAN to WAN**.

WAN Interface: Select the WAN interface that will be associated with this rule here.



Click the **Save/Apply** button to accept the changes made.

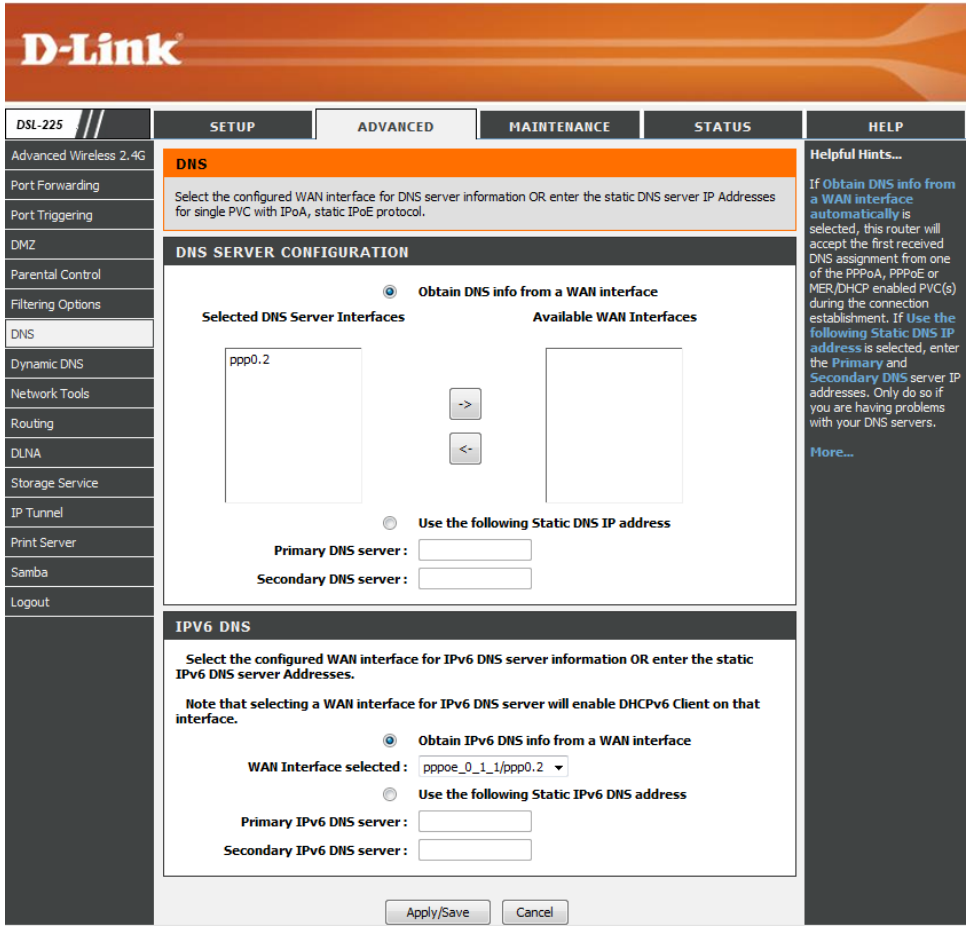
After the rule was added, it will be displayed in this section.



DNS

To access the **DNS** page, click on the **Advanced** menu link, at the top, and then click on the **DNS** menu link, on the left.

On this page the user can configure services related to the DNS feature of this product.



In this section we can configure the DNS Server Configuration.

Obtain DNS info from a WAN interface: Select this option to obtain DNS information from the WAN interface.

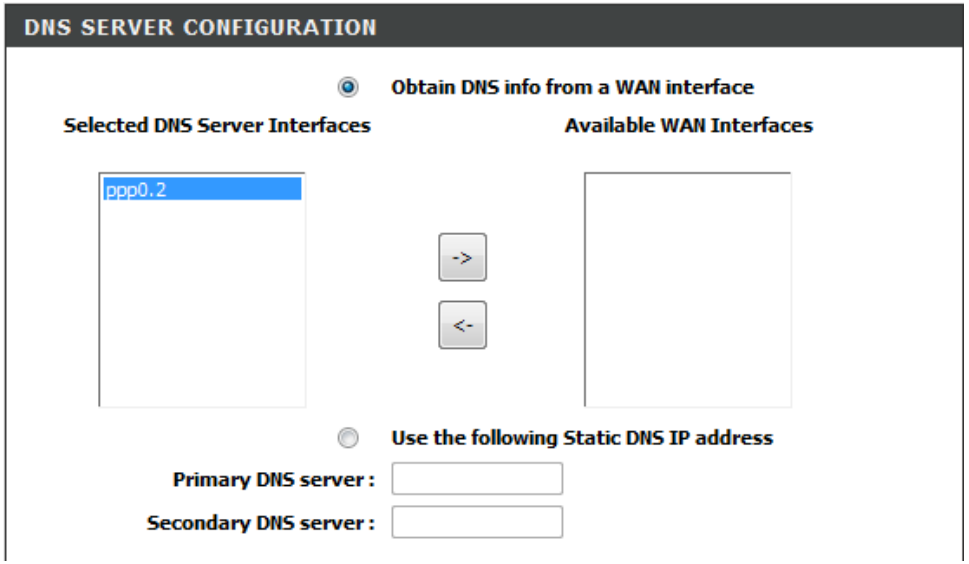
Selected DNS Server Interfaces: Select the DNS Server Interface from the available list in the left-hand column. Use the arrow button to move the selected DNS back and forth from the WAN Interfaces.

Available WAN Interfaces: If needed, add a WAN Interface.

Use the following Static DNS IP address: Select this option to us static DNS IP addresses.

Primary DNS server: Enter the primary DNS server IP address here.

Secondary DNS server: Enter the secondary DNS server IP address here.



In this section we can configure the IPv6 DNS Server Configuration.

Obtain IPv6 DNS info from a WAN interface: Select this option to obtain IPv6 DNS information from the WAN interface.

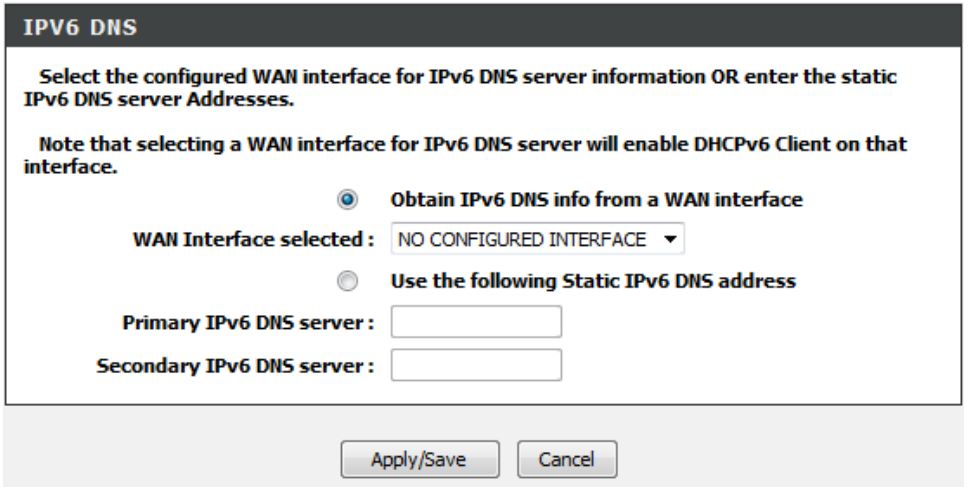
WAN Interface selected: Select the WAN interface, used to obtain the IPv6 DNS information, here.

Use the following Static IPv6 DNS address: Select this option to use static IPv6 DNS addresses.

Primary IPv6 DNS server: Enter the primary IPv6 DNS server address here.

Secondary IPv6 DNS server: Enter the secondary IPv6 DNS server address here.

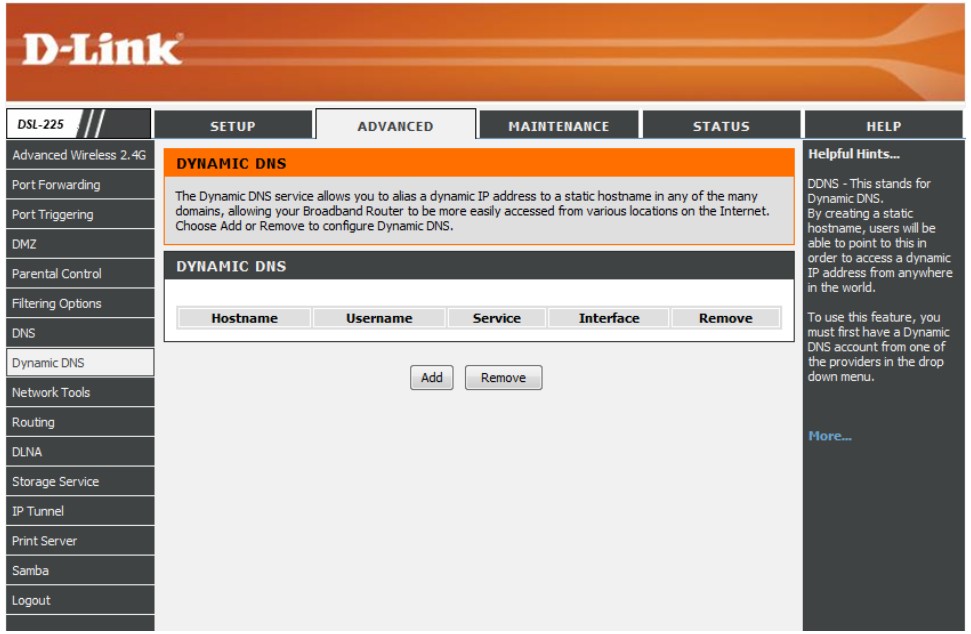
Click the **Apply/Save** button to accept the changes made.



Dynamic DNS

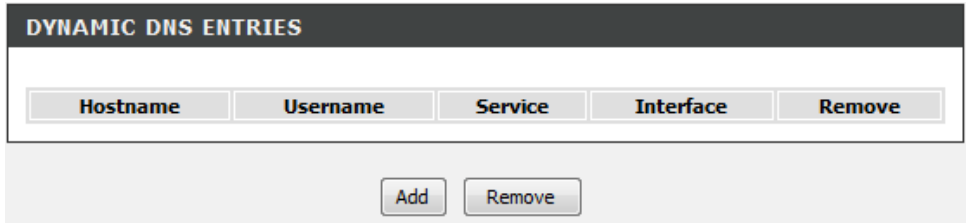
To access the **Dynamic DNS** page, click on the **Advanced** menu link, at the top, and then click on the **Dynamic DNS** menu link, on the left.

On this page the user can configure services related to the Dynamic DNS feature of this product.

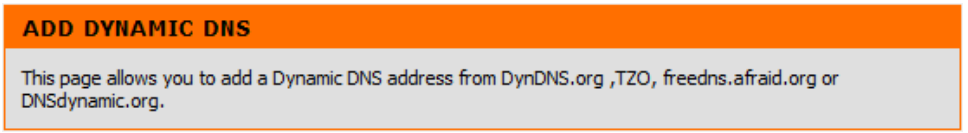


In this section a list of Dynamic DNS entries will be displayed.

Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.



After clicking the **Add** button, the following page is available.



In this section we can create a Dynamic DNS entry.

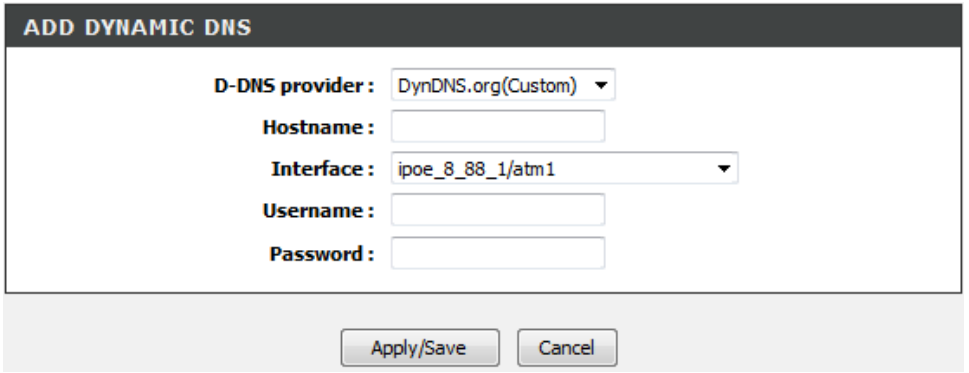
D-DNS provider: Select a Dynamic DNS provider from the list here. Options to choose from are **DynDNS.org** and **TZO**.

Hostname: Enter the hostname for this account here.

Interface: Select the interface that will be used together with this Dynamic DNS entry.

Username: Enter the Dynamic DNS account's username here.

Password: Enter the Dynamic DNS account's password here.



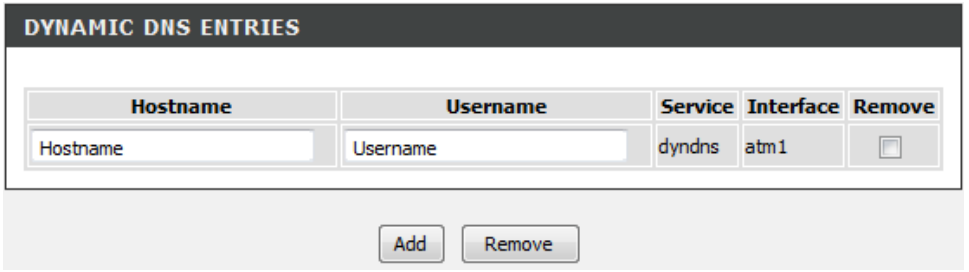
Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

In this section a list of Dynamic DNS entries will be displayed.

Click the **Add** button to add a new entry.

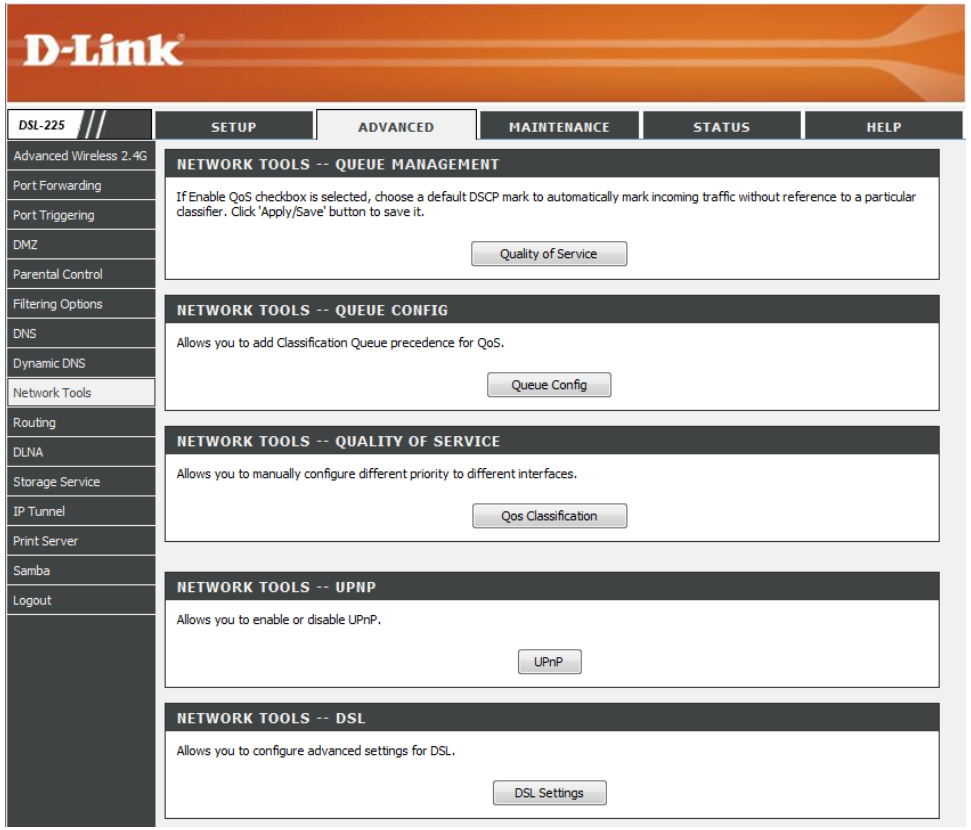
Select the **Remove** option and click the **Remove** button to remove the specific entry.



Network Tools

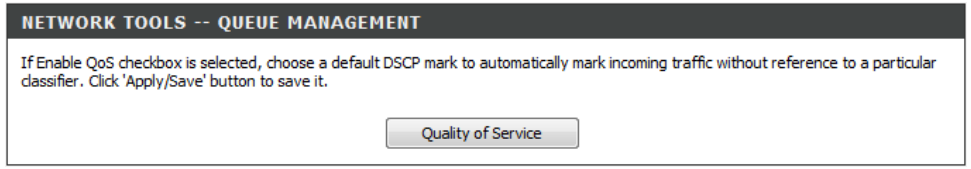
To access the **Network Tools** page, click on the **Advanced** menu link, at the top, and then click on the **Network Tools** menu link, on the left.

On this page the user can configure services related to the Network Tools available on this product.

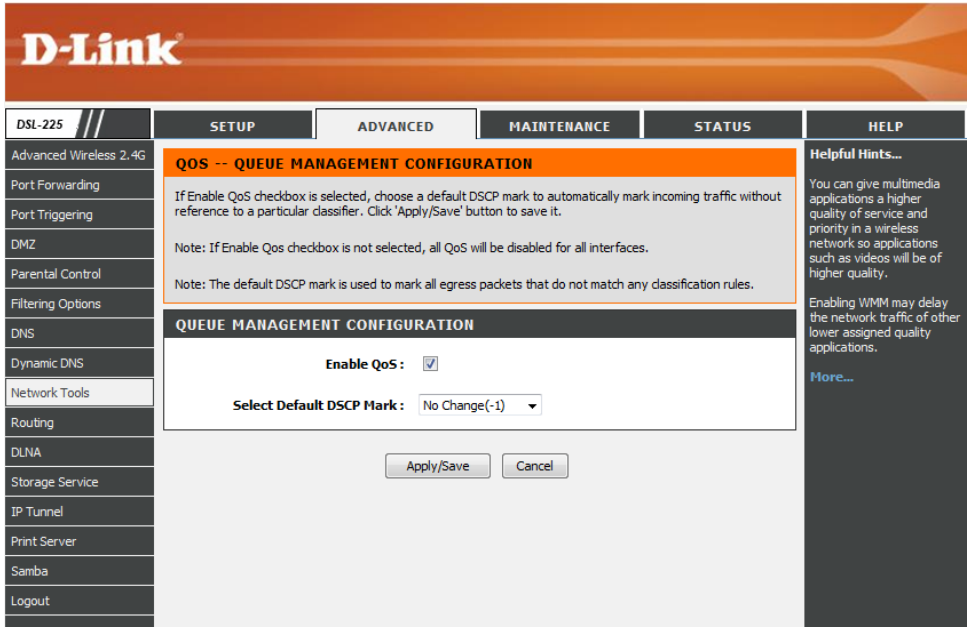


Queue Management

Click the **Quality of Service** button to access the **Queue Management** configuration page.



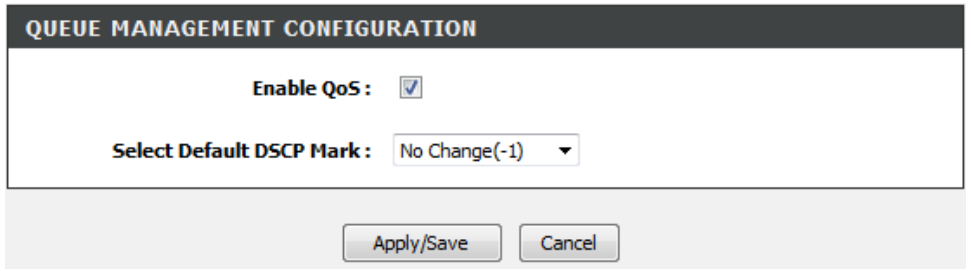
After clicking the **Quality of Service** button the following page is available.



In this section we can configure the Queue Management configuration.

Enable QoS: Select this option to enable the QoS queue management feature.

Select Default DSCP Mark: Select the default DSCP mark option here.

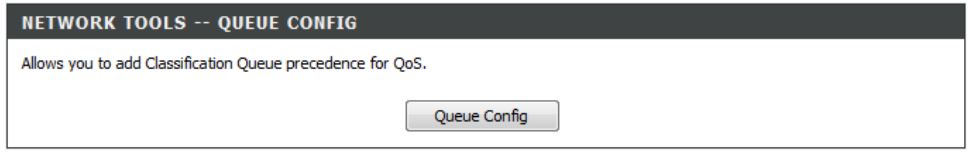


Click the **Apply/Save** button to accept the changes made.

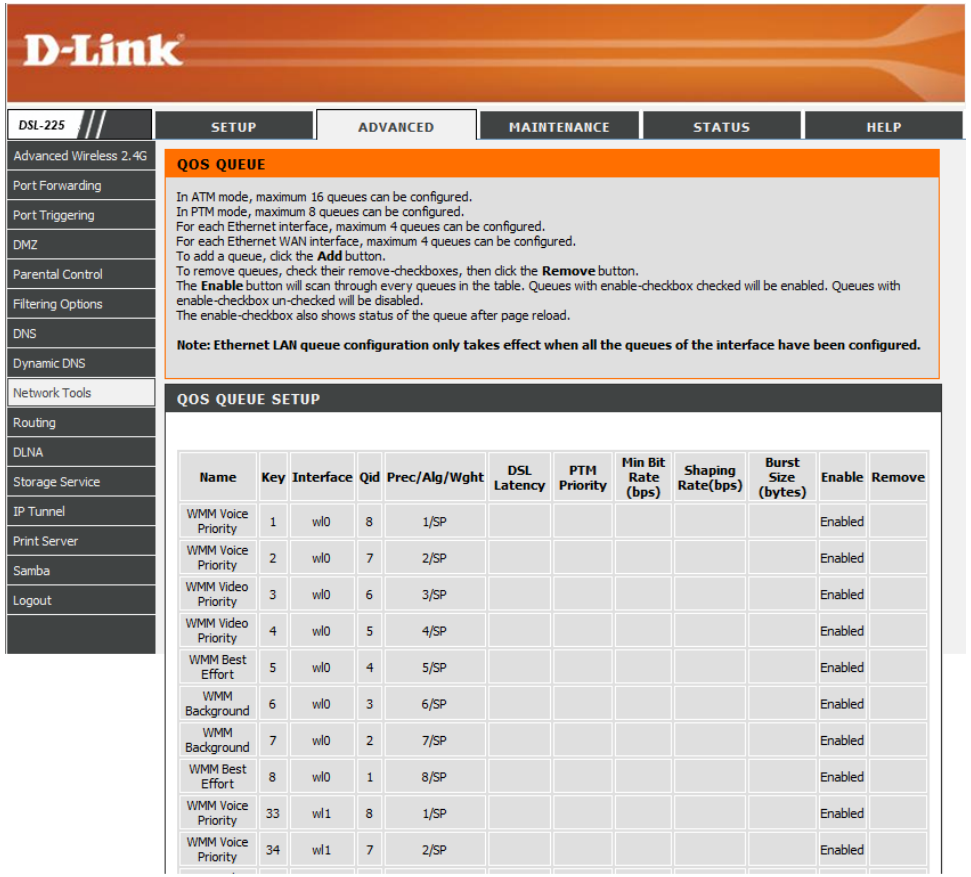
Click the **Cancel** button to discard the changes made and return to the main page.

Queue Config

Click the **Queue Config** button to access the **Queue** configuration page.

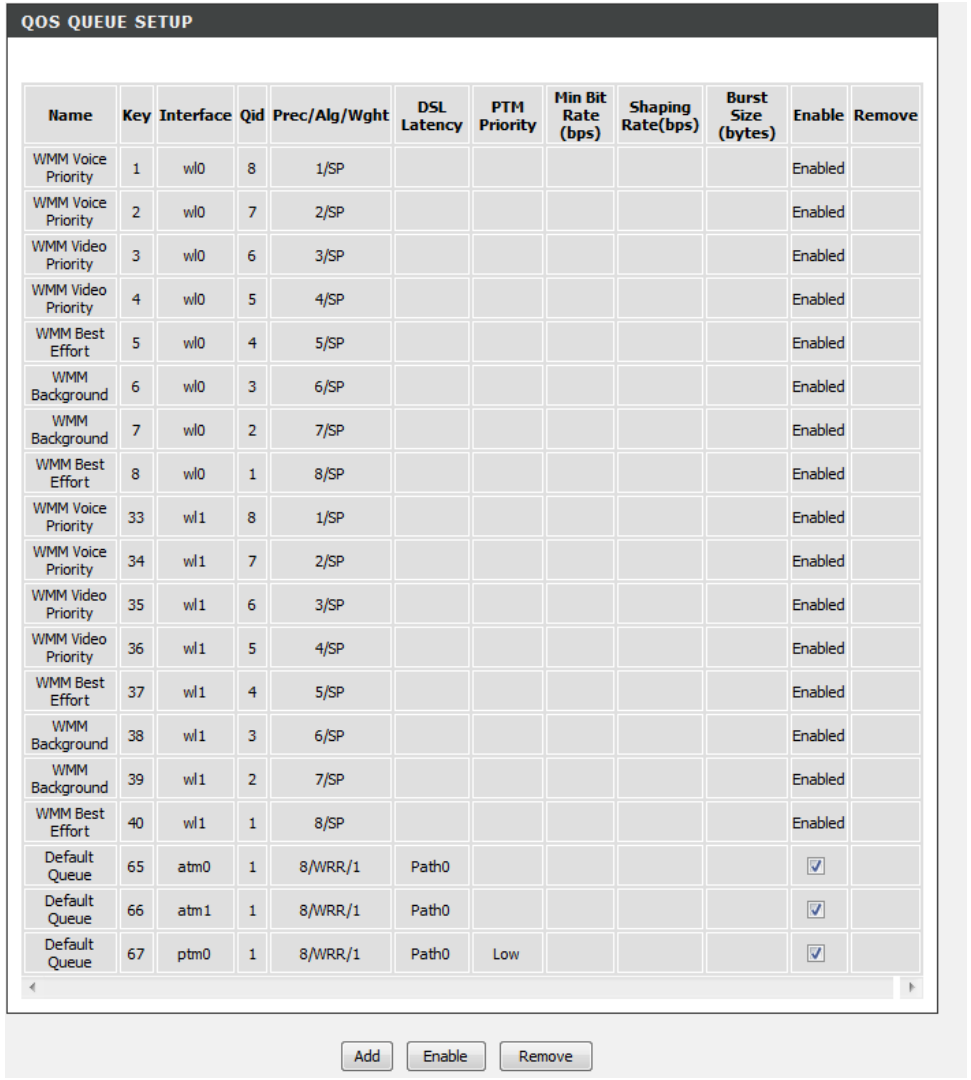


After clicking the **Queue Config** button the following page is available.

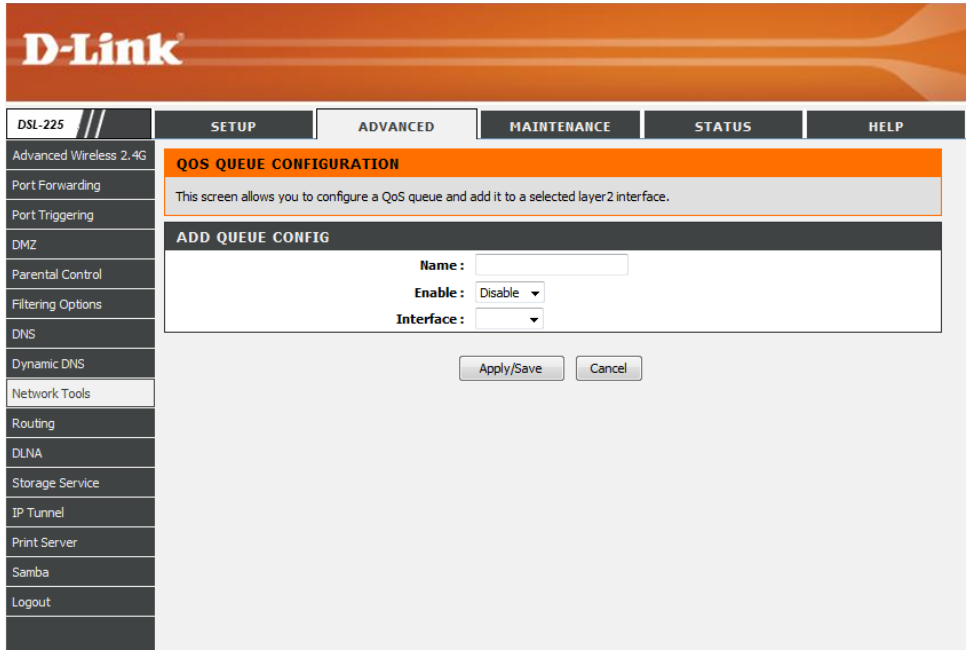


In this section a list of QoS queue configurations will be displayed.

Click the **Add** button to add a new entry.
Click the **Enable** button to enable an entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.



After clicking the **Add** button, the following page is available.

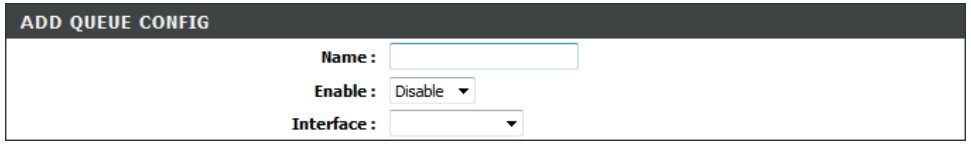


In this section we can create a QoS queue configuration entry.

Name: Enter the QoS queue configuration entry name here.

Enable: Select this option to enable or disable this entry. Options to choose from are **Enable** or **Disable**.

Interface: Select the interface that will be associated with this entry.



After selecting an **ATM** interface, the following parameters will be available.

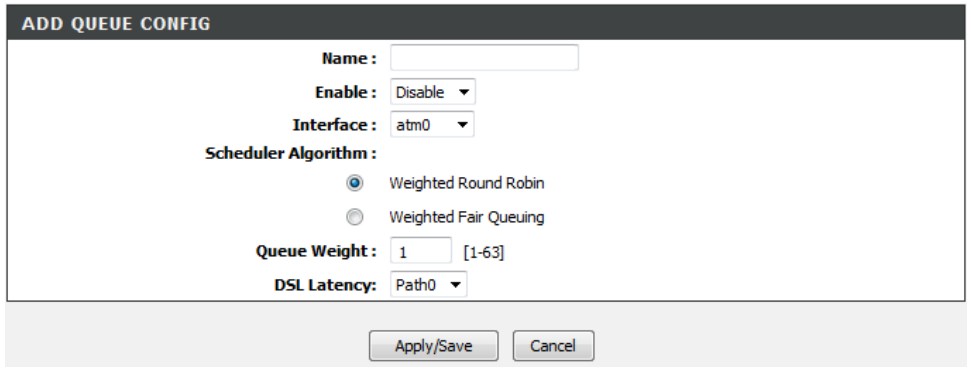
Scheduler Algorithm: Select the queue schedule method used here. Options to choose from are **Weighted Round Robin** and **Weighted Fair Queuing**.

Queue Weight: Enter the queue weight value used here.

DSL Latency: Select the DSL latency option here. The only option available is **Path0**.

Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.



After selecting an **Ethernet** interface, the following parameters will be available.

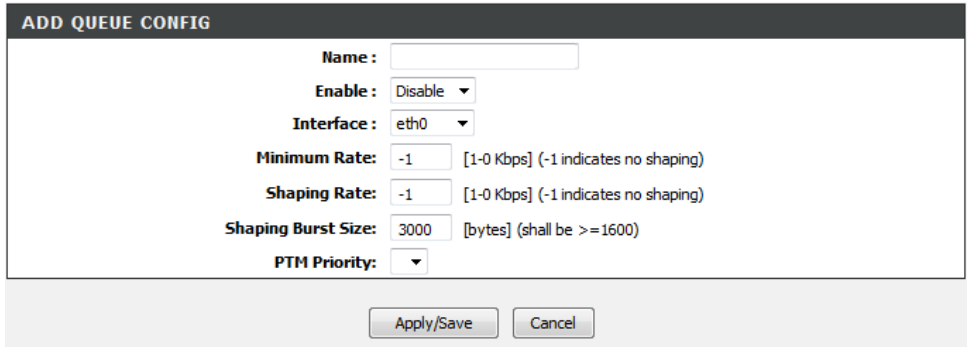
Minimum Rate: Enter the minimum rate value used here.

Shaping Rate: Enter the shaping rate value used here.

PTM Priority: Select the PTM priority option here.

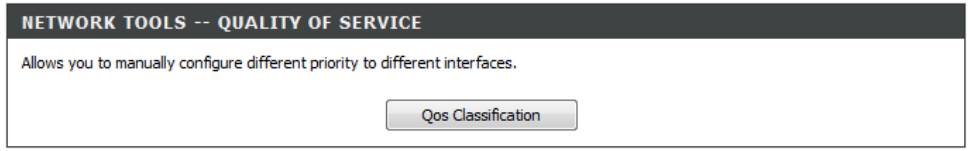
Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.

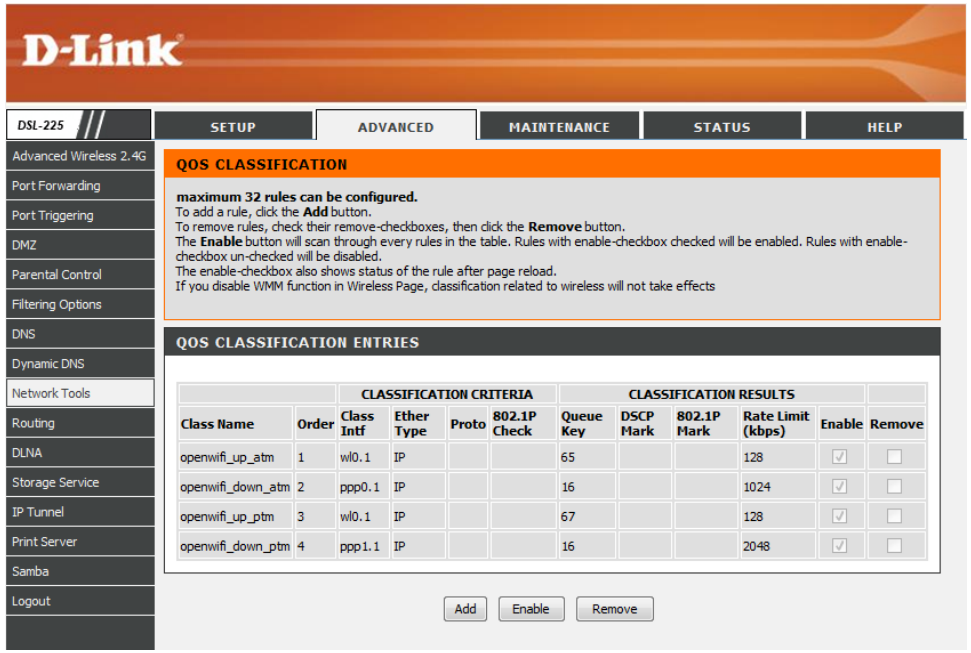


Quality of Service Classification

Click the **Qos Classification** button to access the **Quality of Service** configuration page.

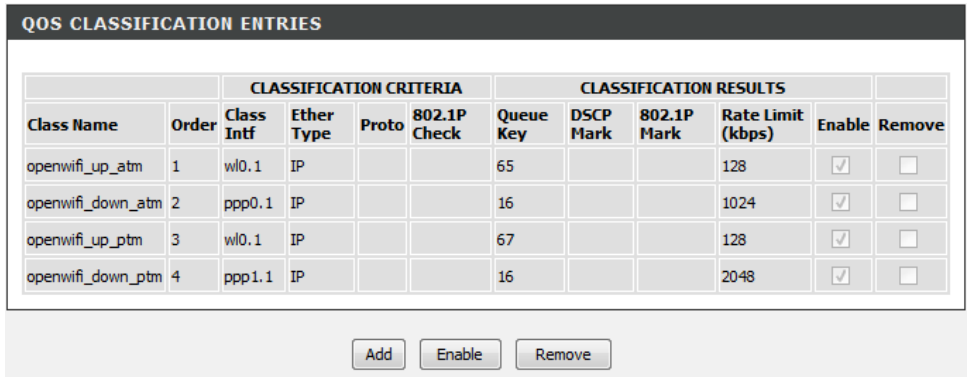


After clicking the **Qos Classification** button the following page is available.

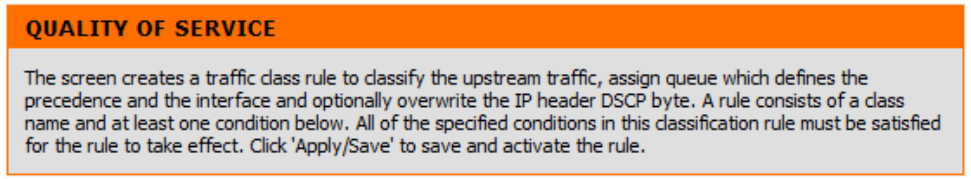


In this section a list of QoS classification entries will be displayed.

Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.



After clicking the **Add** button, the following page is available.

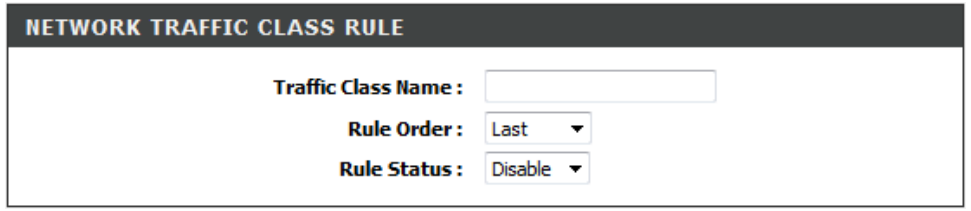


In this section we can create a QoS classification entry.

Traffic Class Name: Enter the traffic class name here.

Rule Order: Select the rule order option here. Options to choose from are **1** and **Last**.

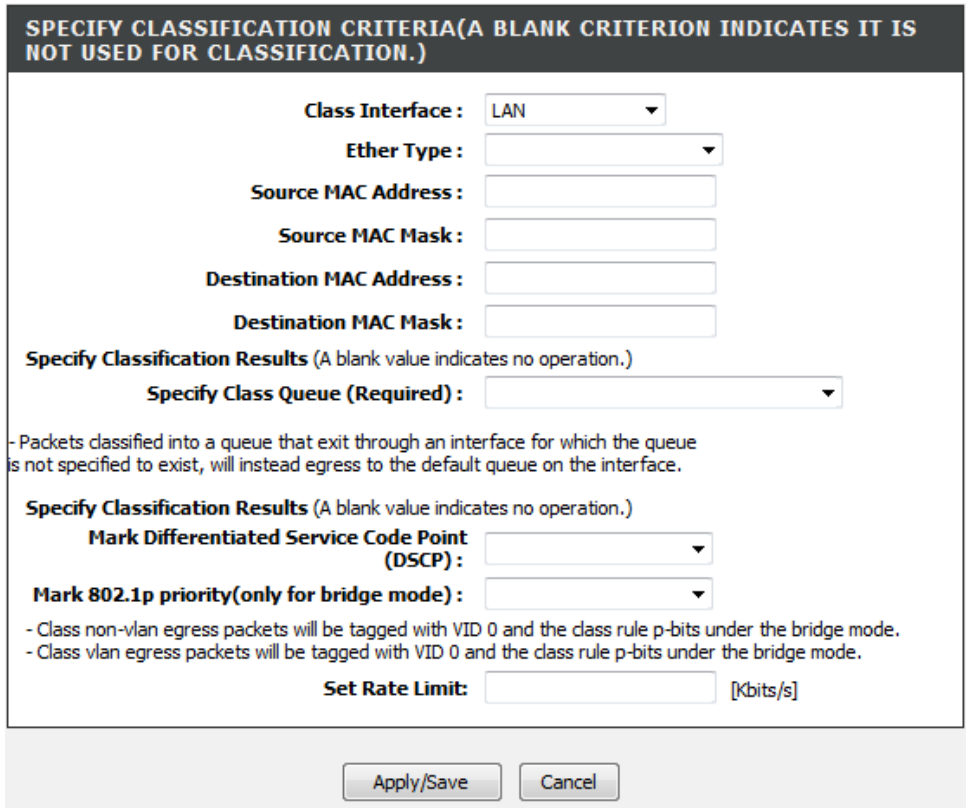
Rule Status: Select the rules state here. Options to choose from are **Enable** and **Disable**.



In this section we can specify the classification criteria for the QoS classification entry here. Make the appropriate modifications here.

Click the **Apply/Save** button to accept the changes made.

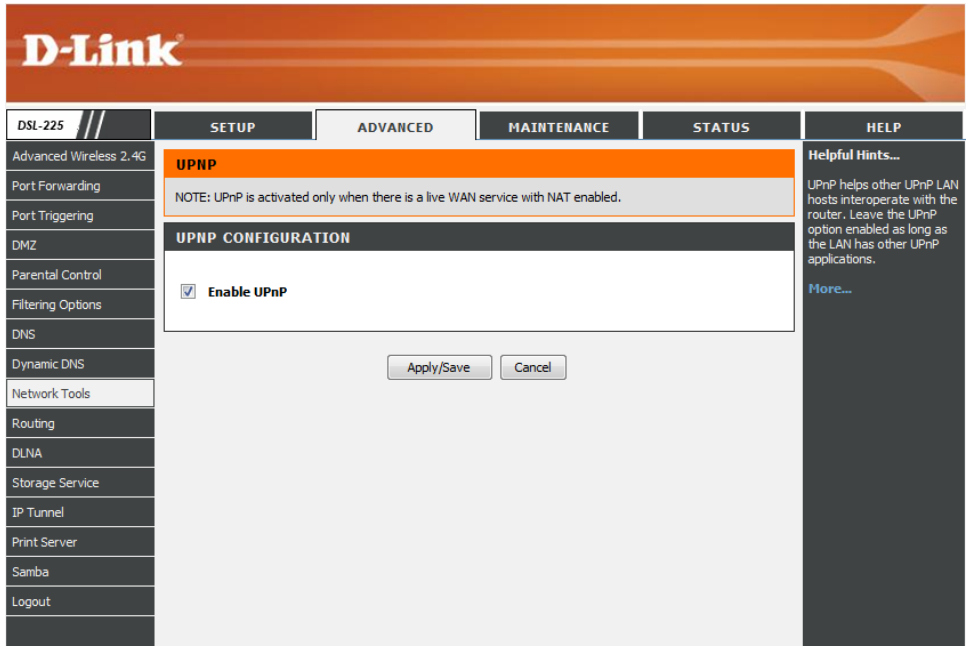
Click the **Cancel** button to discard the changes made and return to the main page.



UPnP

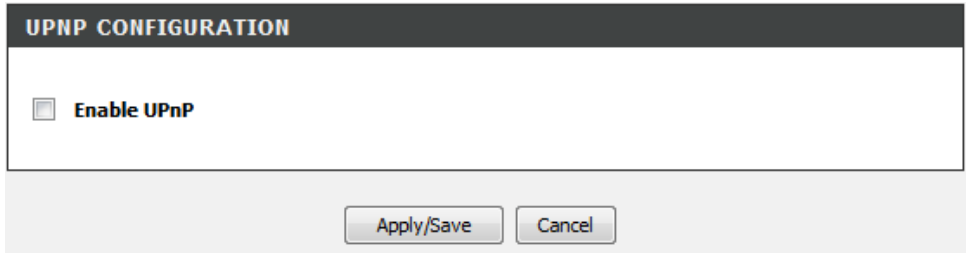
Click the **UPnP** button to access the **UPnP** configuration page.

After clicking the **UPnP** button the following page is available.



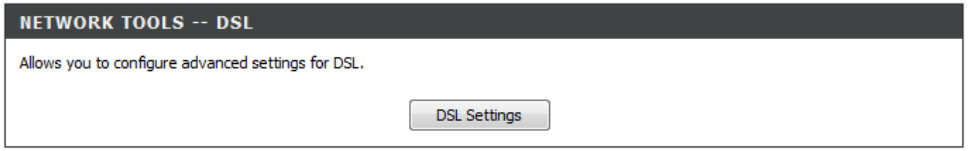
In this section we can **Enable** the UPnP protocol option by selecting this option or **Disable** the UPnP protocol by leaving this option blank.

Click the **Apply/Save** button to accept the changes made.

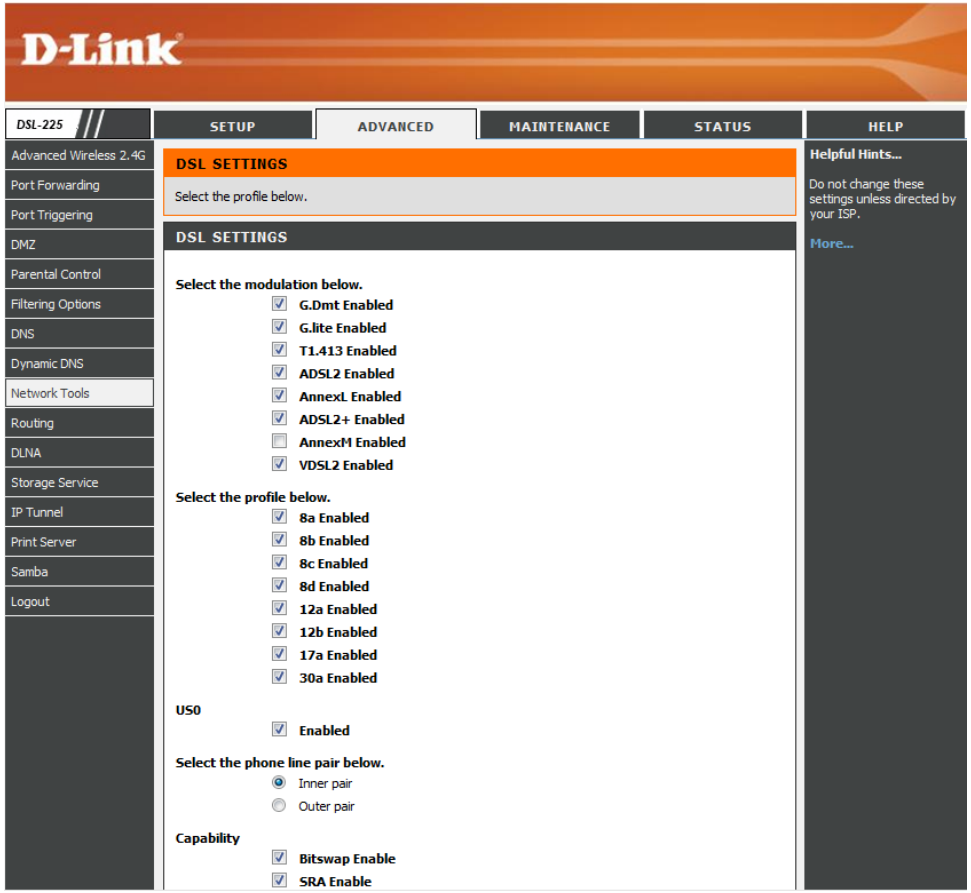


DSL Settings

Click the **DSL Settings** button to access the **DSL Settings** configuration page.



After clicking the **DSL Settings** button the following page is available.



In this section we can configure the DSL settings for this router.

Select the modulation below: To enable the DSL modulation type, tick the checkbox next to it. To disable the DSL modulation type, leave the checkbox next to it empty.

Select the profile below: To enable the specific profile, tick the checkbox next to it. To disable the specific profile, leave the checkbox next to it empty.

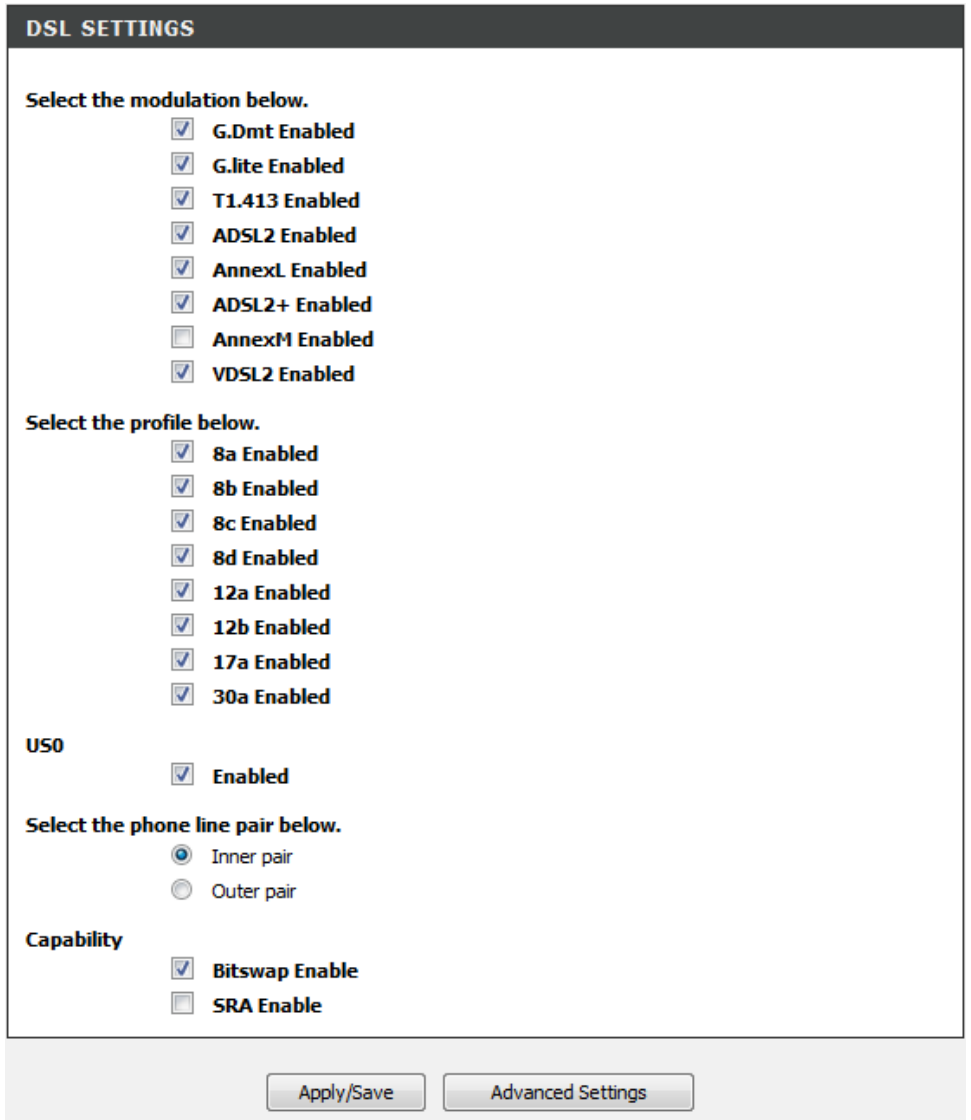
US0: To enable this option, tick the checkbox next to it. To disable this option, leave the checkbox next to it empty.

Select the phone line pair below: Select the phone line pair option here. Options to choose from are **Inner pair** and **Outer pair**.

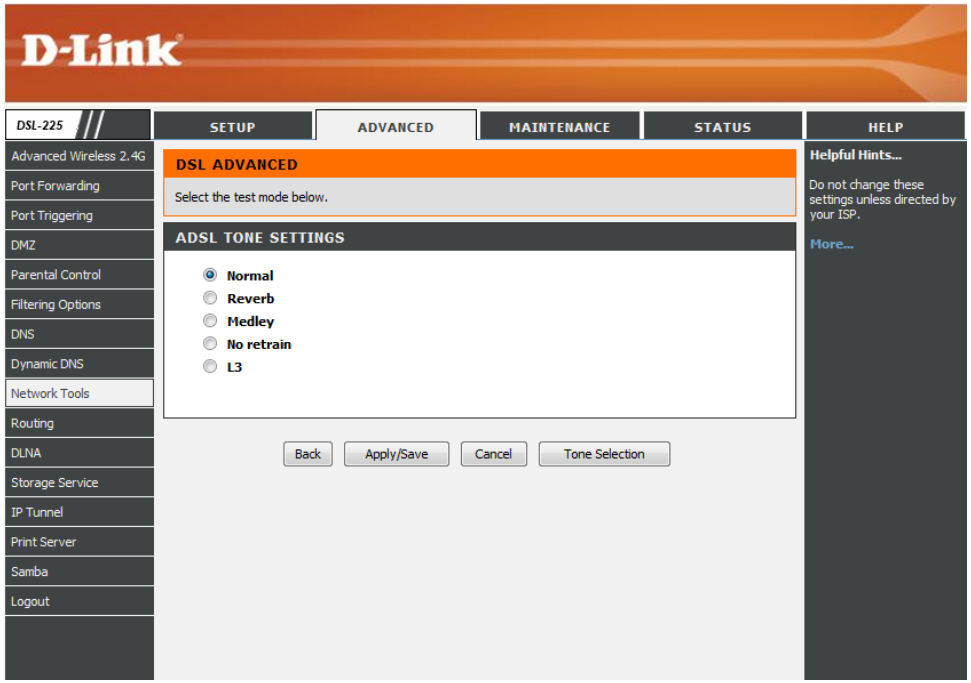
Capability: Select the DSL capability option here. Options to choose from are **Bitswap Enable** and **SRA Enable**.

Click the **Apply/Save** button to accept the changes made.

Click the **Advanced Settings** button to configure more advanced parameters, concerning the DSL settings.



After clicking the **Advanced Settings** button the following page is available.



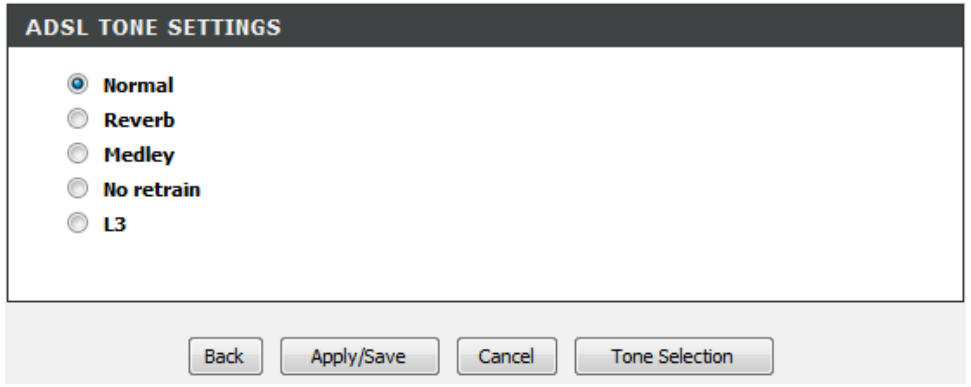
In this section we can configure the VDSL tone settings. Only one option can be selected. Options to choose from are **Normal**, **Reverb**, **Medley**, **No retrain**, and **L3**.

Click the **Back** button to return to the previous page.

Click the **Apply/Save** button to accept the changes made.

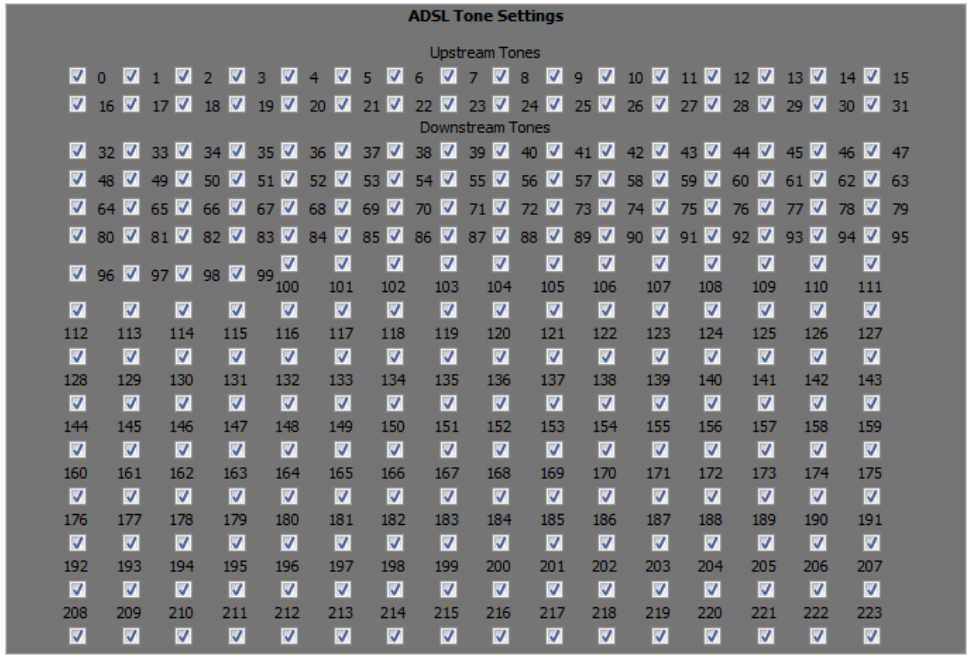
Click the **Cancel** button to discard the changes made and return to the main page.

Click the **Tone Selection** button to open a new page where we can manually select the tone.



After clicking the **Tone Selection** button the following page is available.

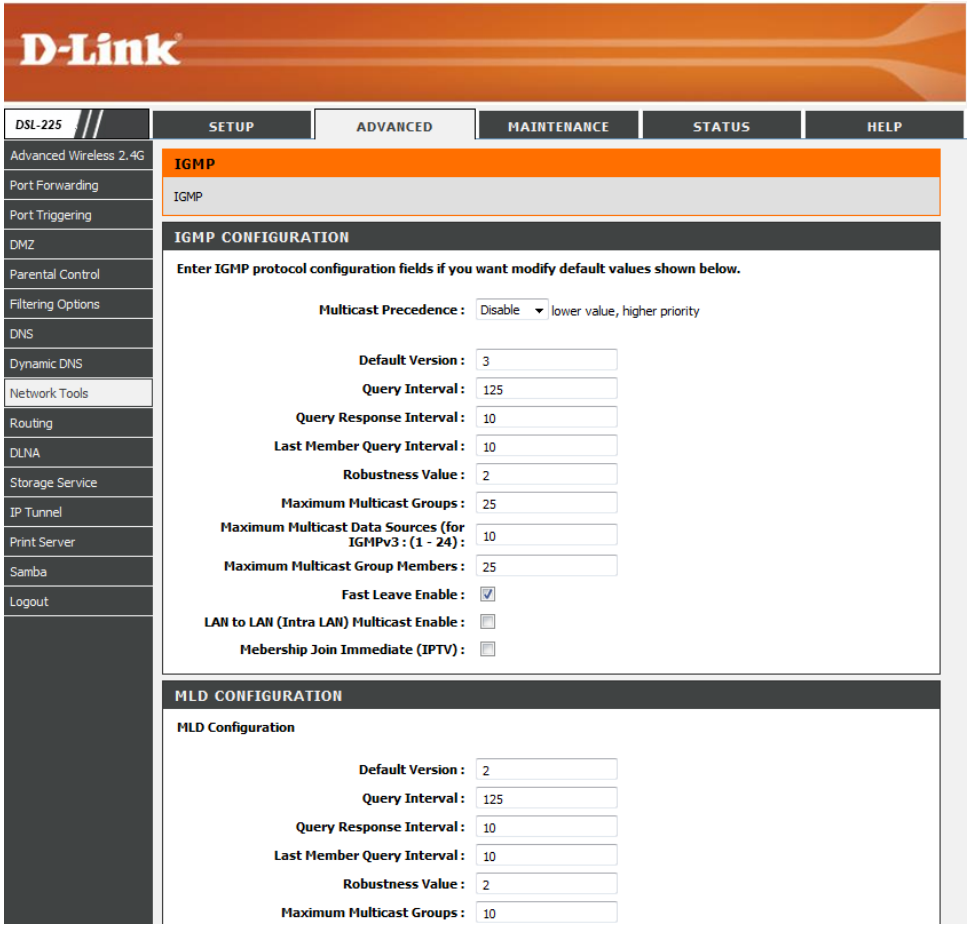
Here we can select the tone manually. Options to choose from are **Upstream Tones** and **Downstream Tones**.



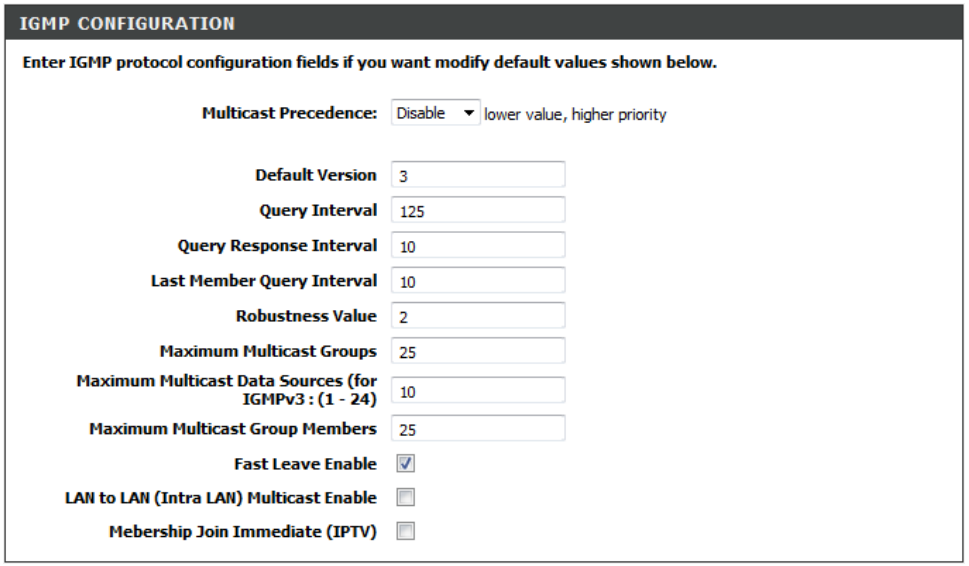
IGMP

Click the **IGMP** button to access the **IGMP** configuration page.

After clicking the **IGMP** button the following page is available.



In this section we can modify the **IGMP Configuration**.



Multicast Precedence: Select to enable or disable the multicast precedence feature here. Selecting a lower value assigns a higher priority.

Default Version: Enter the default IGMP version number here.

Query Interval: Enter the query interval value here.

Query Response Interval: Enter the query response interval value here.

Last Member Query Interval: Enter the last member query interval value here.

Robustness Value: Enter the robustness value here.

Maximum Multicast Groups: Enter the maximum multicast group value here.

Maximum Multicast Data Sources: Enter the maximum multicast data sources value here.

Maximum Multicast Group Members: Enter the maximum multicast group member value here.

Fast Leave Enable: Tick this option to enable the fast leave feature.

LAN to LAN (Intra LAN) Multicast Enable: Select this option to enable LAN to LAN (Intra LAN) multicasting.

Membership Join Immediate (IPTV): Tick this option to enable the membership join immediate (IPTV) feature.

In this section we can modify the **MLD Configuration**.

Default Version: Enter the default MLD version number here.

Query Interval: Enter the query interval value here.

Query Response Interval: Enter the query response interval value here.

Last Member Query Interval: Enter the last member query interval value here.

Robustness Value: Enter the robustness value here.

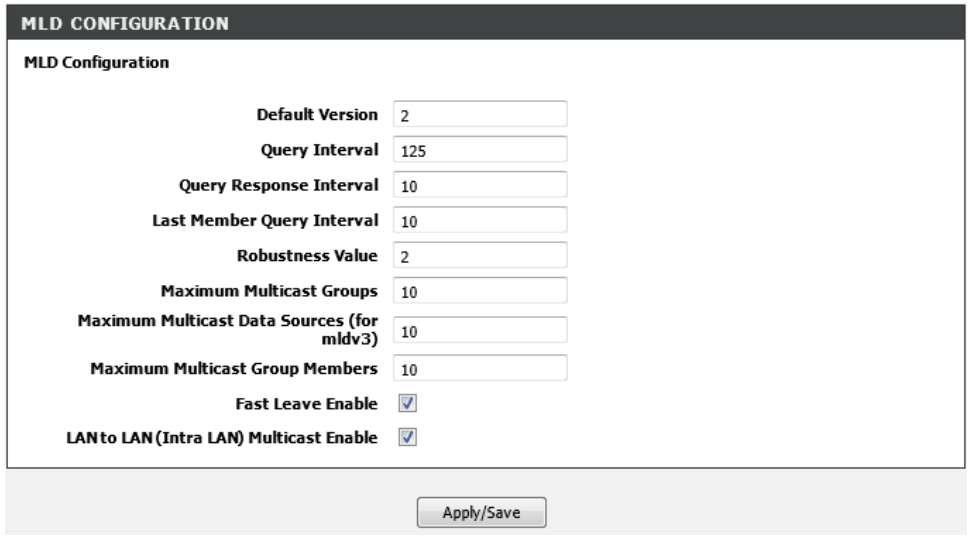
Maximum Multicast Groups: Enter the maximum multicast group value here.

Maximum Multicast Data Sources: Enter the maximum multicast data source value here.

Maximum Multicast Group Members: Enter the maximum multicast group member value here.

Fast Leave Enable: Tick this option to enable the fast leave feature.

LAN to LAN (Intra LAN) Multicast Enable: Select this option to enable LAN to LAN (Intra LAN) multicasting.

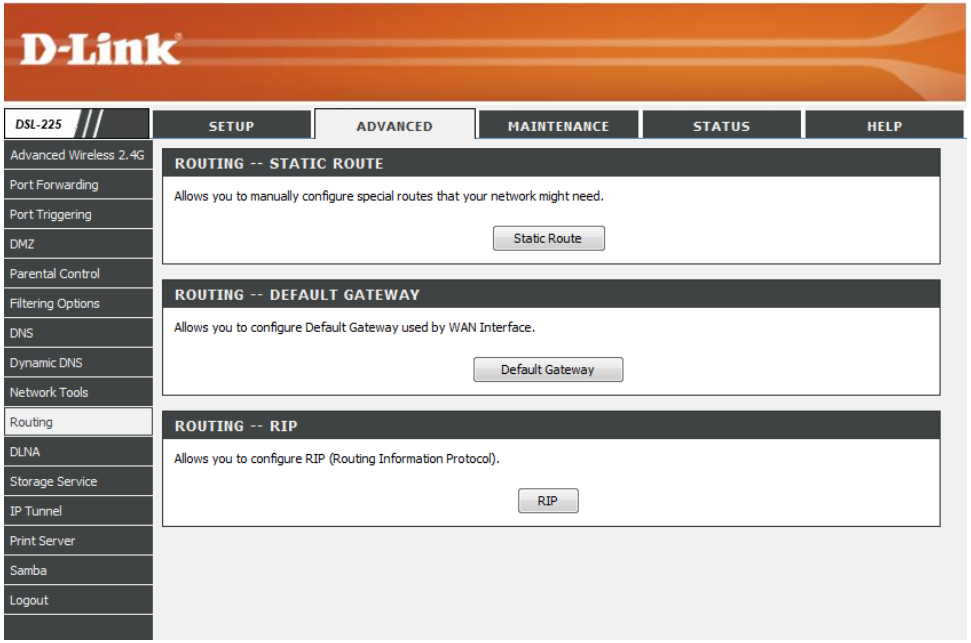


Click the **Apply/Save** button to accept the changes made.

Routing

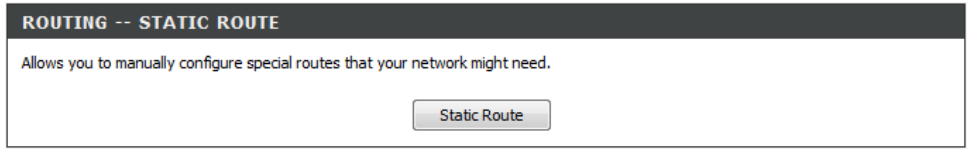
To access the **Routing** page, click on the **Advanced** menu link, at the top, and then click on the **Routing** menu link, on the left.

On this page the user can configure services related to the Routing feature of this product.

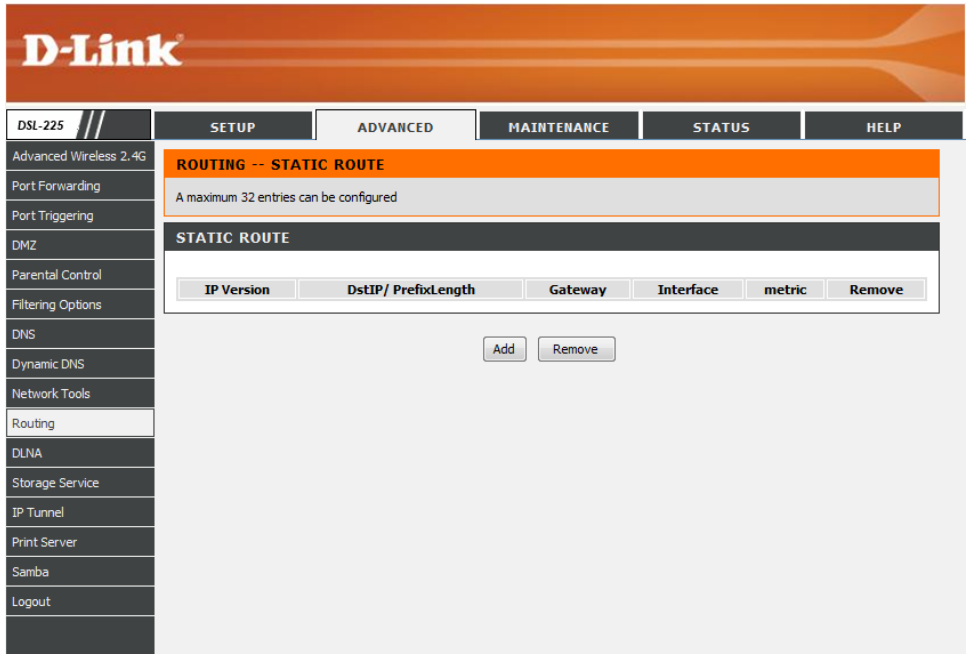


Static Route

Click the **Static Route** button to access the **Static Routing** configuration page.

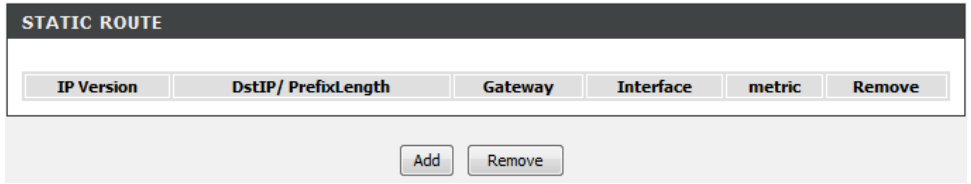


After clicking the **Static Route** button the following page is available.

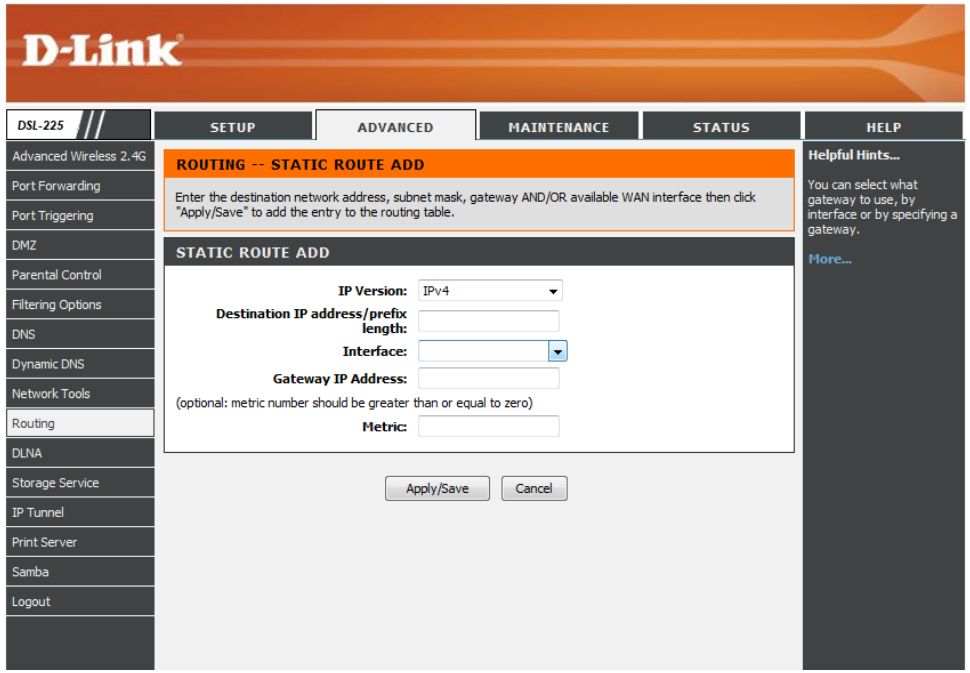


In this section a list of static route entries will be displayed.

Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.



After clicking the **Add** button, the following page is available.



In this section we can create a **Static Route** entry.

IP Version: Select the IP version used here. Options to choose from are **IPv4** and **IPv6**.

Destination IP address: Enter the destination IP address for this route entry here.

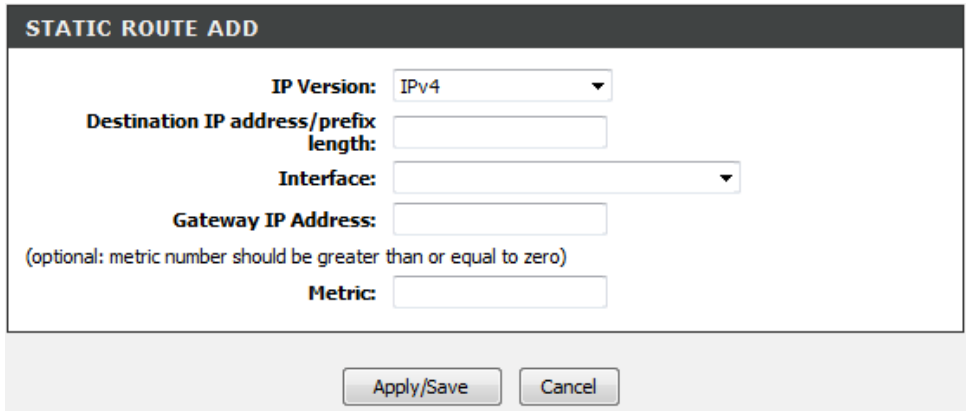
Interface: Select the interface this will be associated with this rule here.

Gateway IP Address: Enter the gateway IP address for this route entry here.

Metric: Enter the metric value, used by this route entry, here.

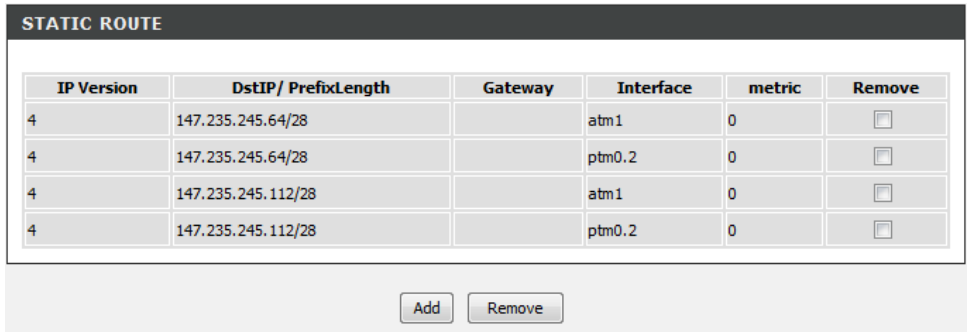
Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.



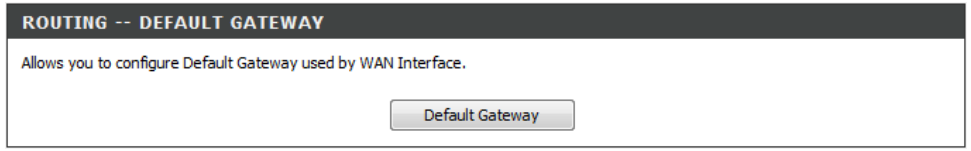
In this section a list of static route entries will be displayed.

Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry.

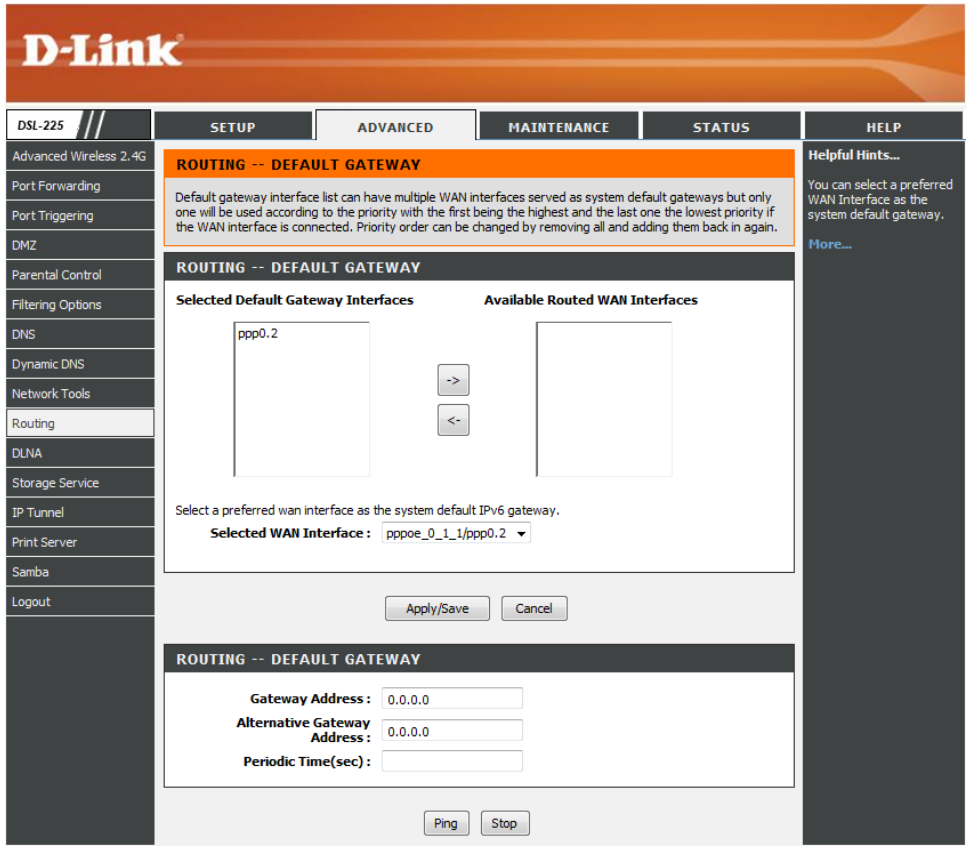


Default Gateway

Click the **Default Gateway** button to access the **Default Gateway** configuration page.



After clicking the **Default Gateway** button the following page is available.



In this section we can select the default gateway interface for this router.

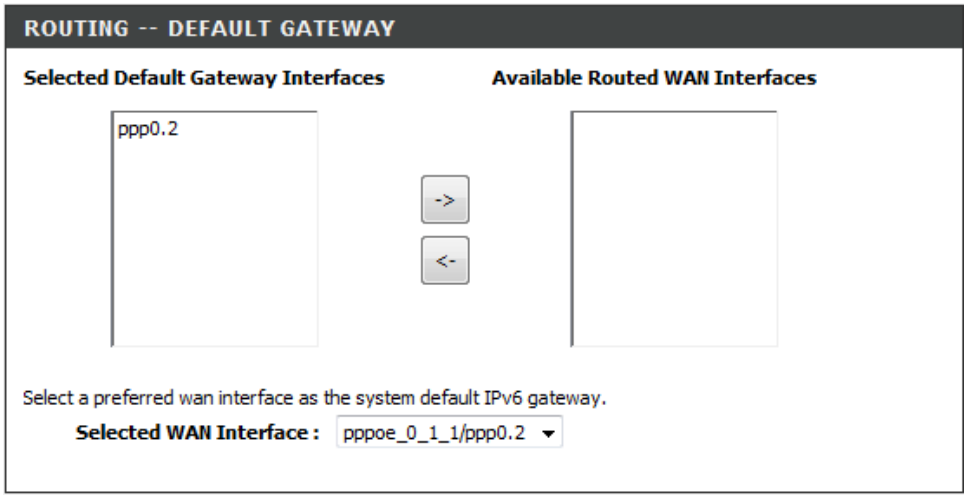
Selected WAN Interface: Select the IPv4 WAN interface that will be used here.

Selected Default Gateway Interfaces: Select the IPv6 WAN interface that will be used here.

Available Routed WAN Interfaces: Select a Routed WAN interface.

Click the **Apply/Save** button to accept the changes made.

Click the **Cancel** button to discard the changes made and return to the main page.



In this section we can configure the default gateway parameters for this router.

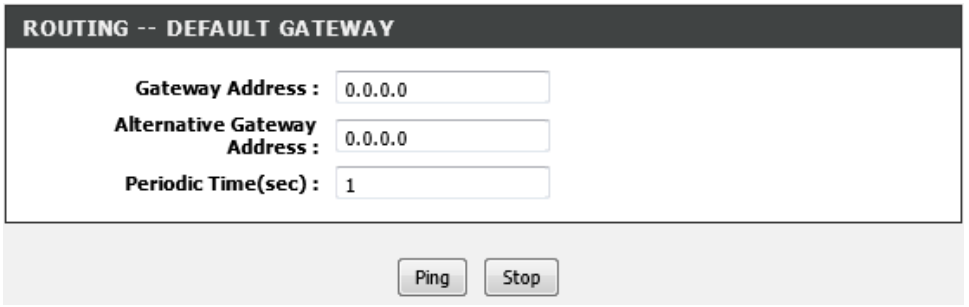
Gateway Address: Enter the primary gateway IP address used here.

Alternative Gateway: Enter the secondary gateway IP address used here.

Periodic Time: Enter the periodic time value here.

Click the **Ping** button to initiate the gateway IP check.

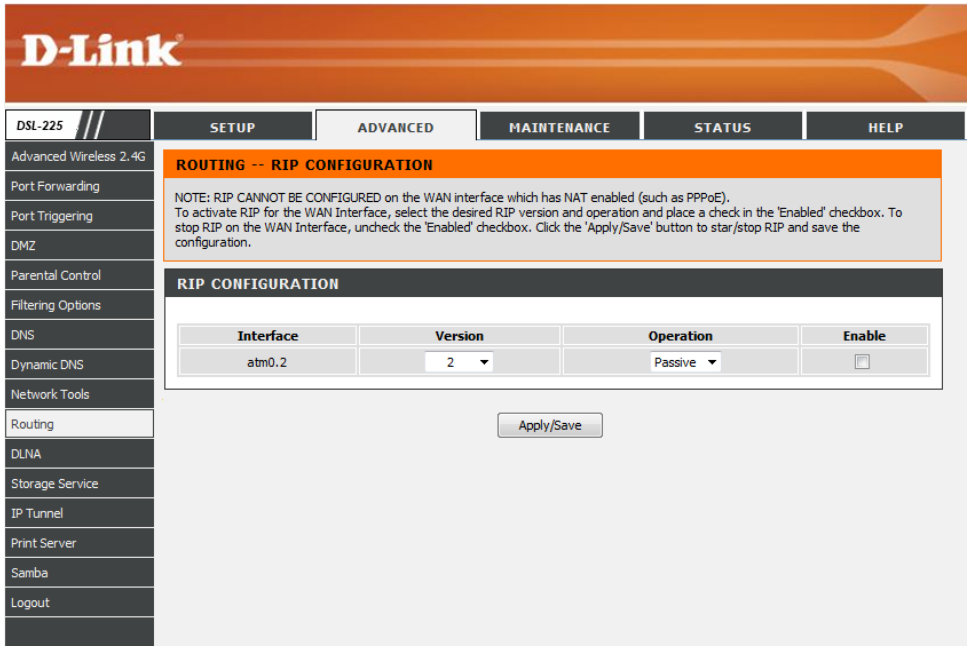
Click the **Stop** button to terminate the gateway IP check.



RIP

Click the **RIP** button to access the **RIP** configuration page.

After clicking the **RIP** button the following page is available.

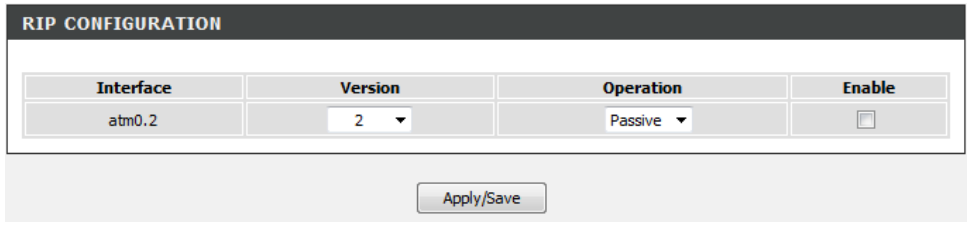


In this section we can configure the default gateway parameters for this router.

Version: Select the RIP version number here. Options to choose from are **1**, **2**, and **Both**.

Operation: Select the operation mode here. Options to choose from are **Active** and **Passive**.

Enable: Tick this option to enable the RIP configuration on the specified interface.

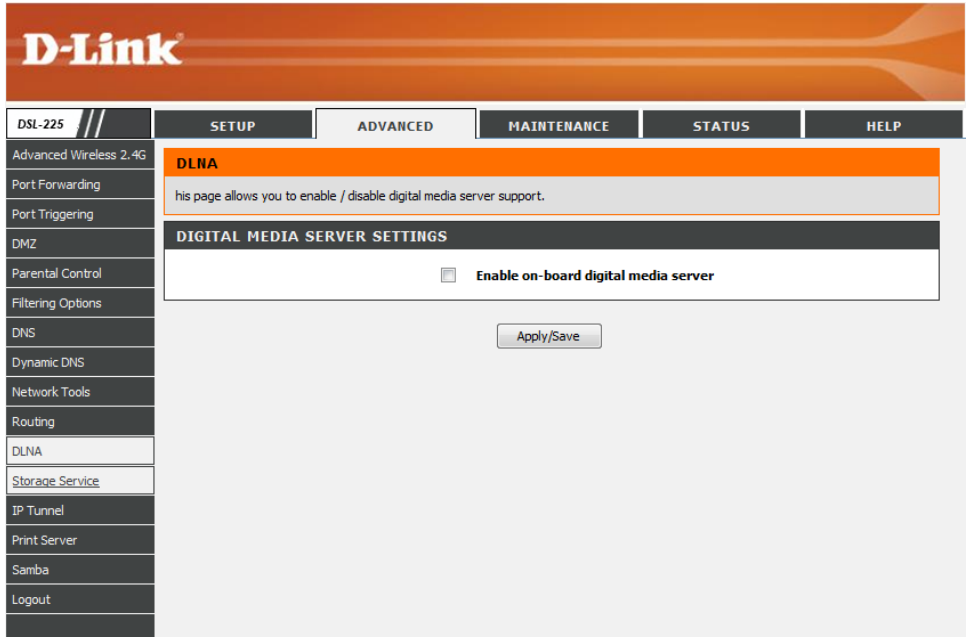


Click the **Apply/Save** button to accept the changes made.

DLNA

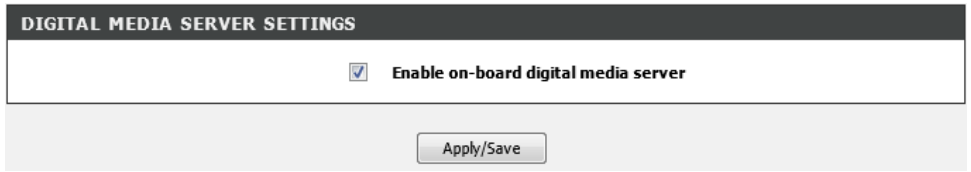
To access the **DLNA** page, click on the **Advanced** menu link, at the top, and then click on the **DLNA** menu link, on the left.

On this page the user can configure services related to the Digital Living Network Alliance (DLNA) feature of this product.



In this section we can configure the print server parameters for this router.

Enable on-board digital media server: Tick this option to enable the onboard digital media server.

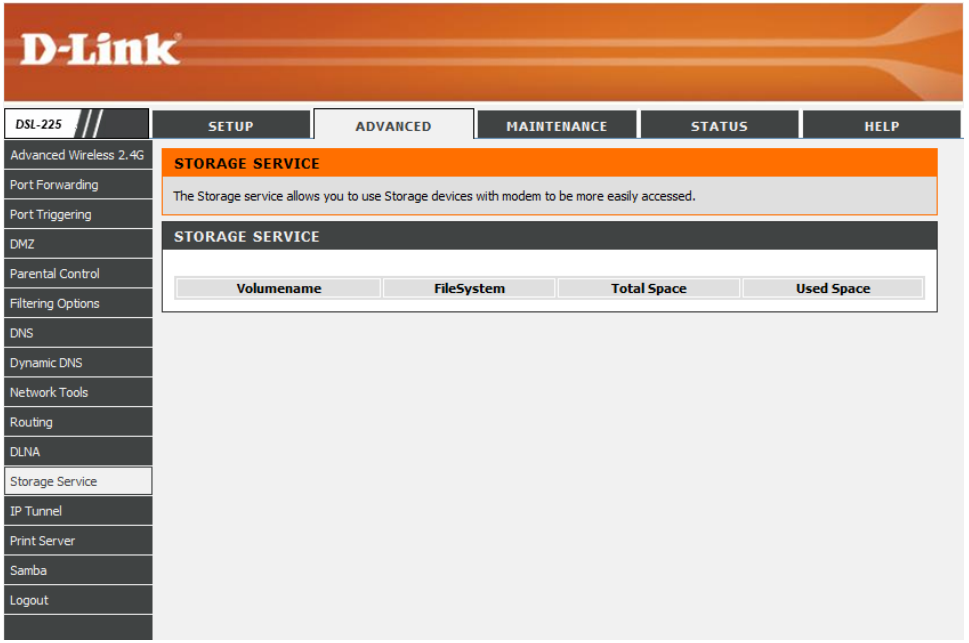


Click the **Apply/Save** button to accept the changes made.

Storage Service

To access the **Storage** page, click on the **Advanced** menu link, at the top, and then click on the **Storage Service** menu link, on the left.

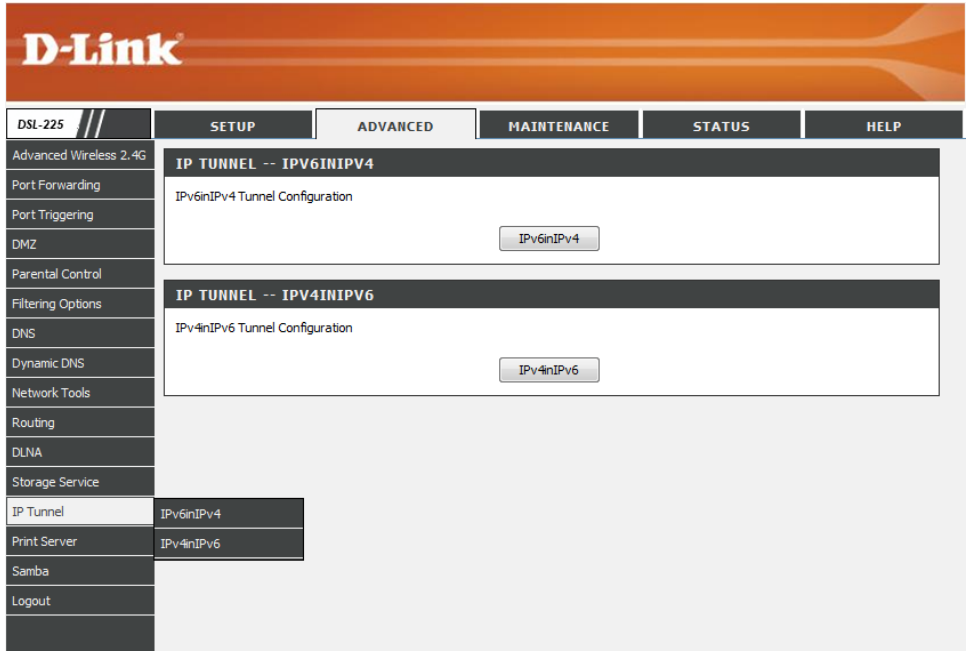
On this page the user can view information related to the **Storage Service** feature of this product.



IP Tunnel

To access the **IP Tunnel** page, click on the **Advanced** menu link, at the top, and then click on the **IP Tunnel** menu link, on the left.

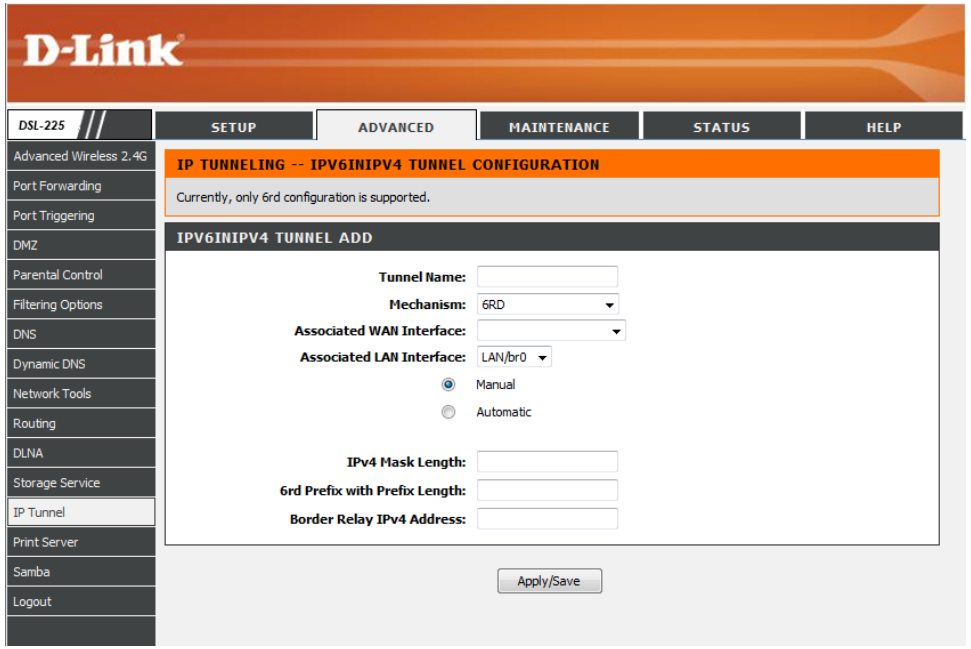
On this page the user can configure services related to IP Tunneling used on this product.



IPv6-in-IPv4

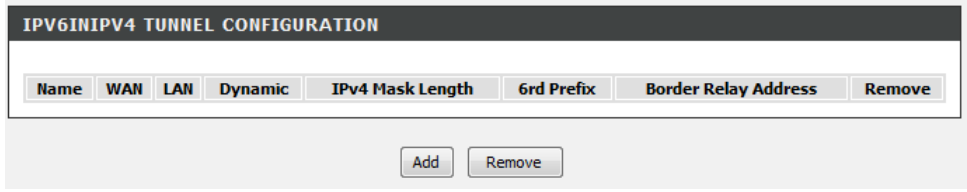
Click the **IPv6inIPv4** button to access the **IPv6-in-IPv4** configuration page.

After clicking the **IPv6inIPv4** button, the following page will be available.

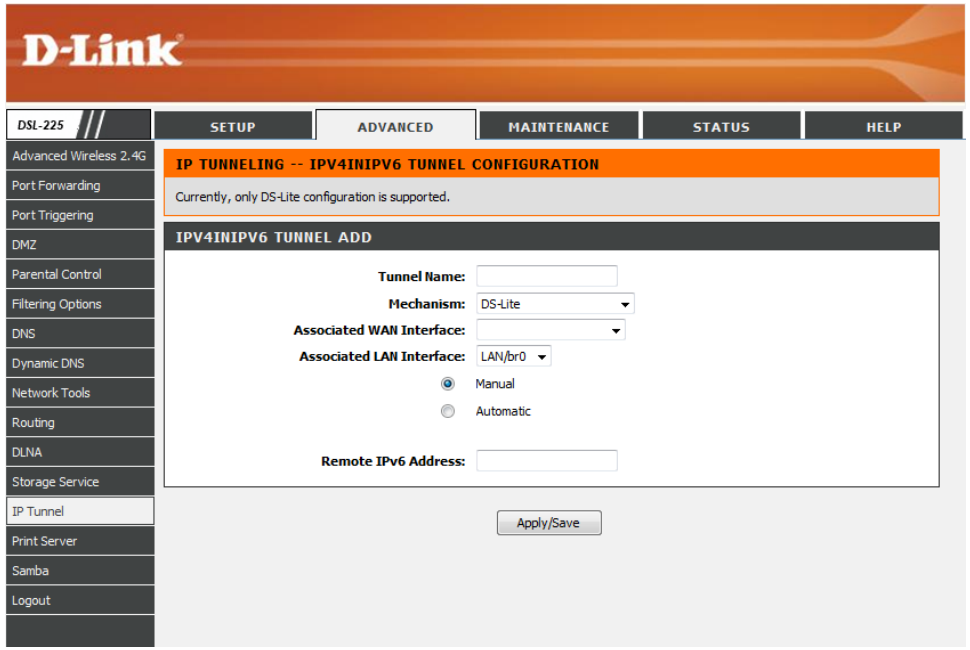


In this section a list of entries will be displayed.

Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry



After clicking the **Add** button, the following page will be available.



In this section, the following parameters can be configured:

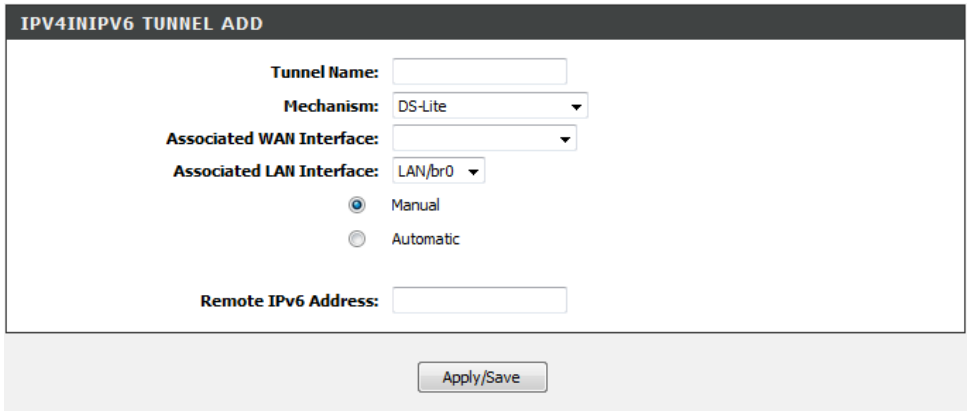
Tunnel Name: Enter the tunnel name here.

Mechanism: Select the tunnel mechanism option here. **6RD** is the only option available.

Associated WAN Interface: Select the WAN interface that will be associated with this entry here.

Associated LAN Interface: Select the LAN interface that will be associated with this entry here. Also select whether this interface will obtain the IPv4 mask length, 6rd prefix, and border relay IPv4 address information manually, by selecting **Manual**, or automatically, by selecting **Automatic**.

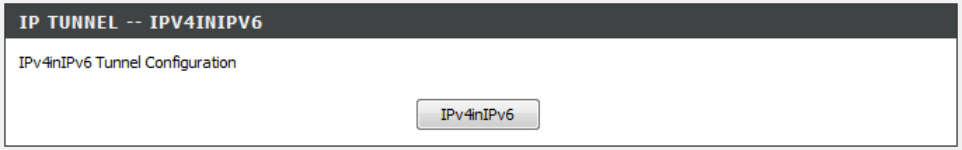
Remote IPv6 Address: After selecting **Manual**, enter the remote IPv6 address here.



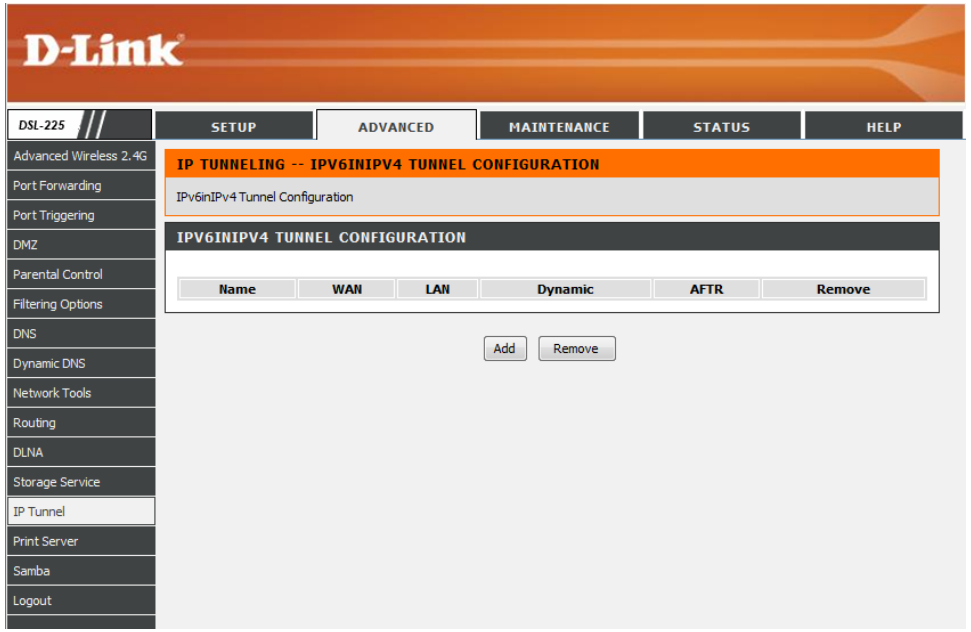
Click the **Apply/Save** button to accept the changes made.

IPv4-in-IPv6

Click the **IPv4inIPv6** button to access the **IPv4-in-IPv6** configuration page.

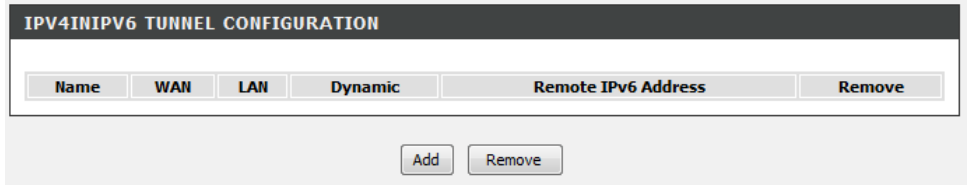


After click the **IPv4inIPv6** button, the following page will be available.

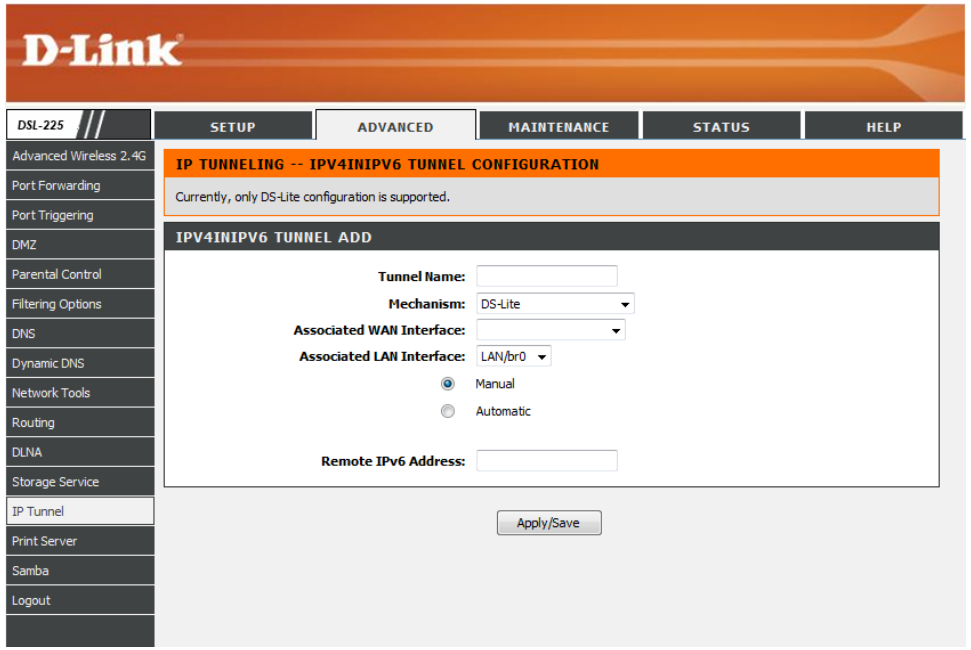


In this section a list of entries will be displayed.

Click the **Add** button to add a new entry.
Select the **Remove** option and click the **Remove** button to remove the specific entry



After click the **Add** button, the following page will be available.



In this section, the following parameters can be configured:

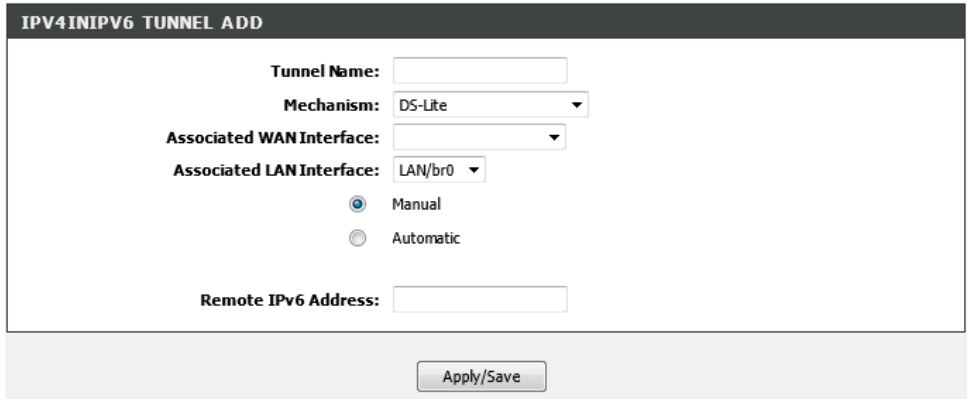
Tunnel Name: Enter the tunnel name here.

Mechanism: Select the mechanism option here. **DS-Lite** is the only option available.

Associated WAN Interface: Select the WAN interface will be associated with this entry here. Also select whether this interface will obtain the remote IPv6 address manually, by selecting **Manual**, or automatically, by selecting **Automatic**.

Associated LAN Interface: Select the LAN interface associated with this entry from the drop-down menu.

Remote IPv6 Address: After selecting **Manual**, enter the remote IPv6 address here.

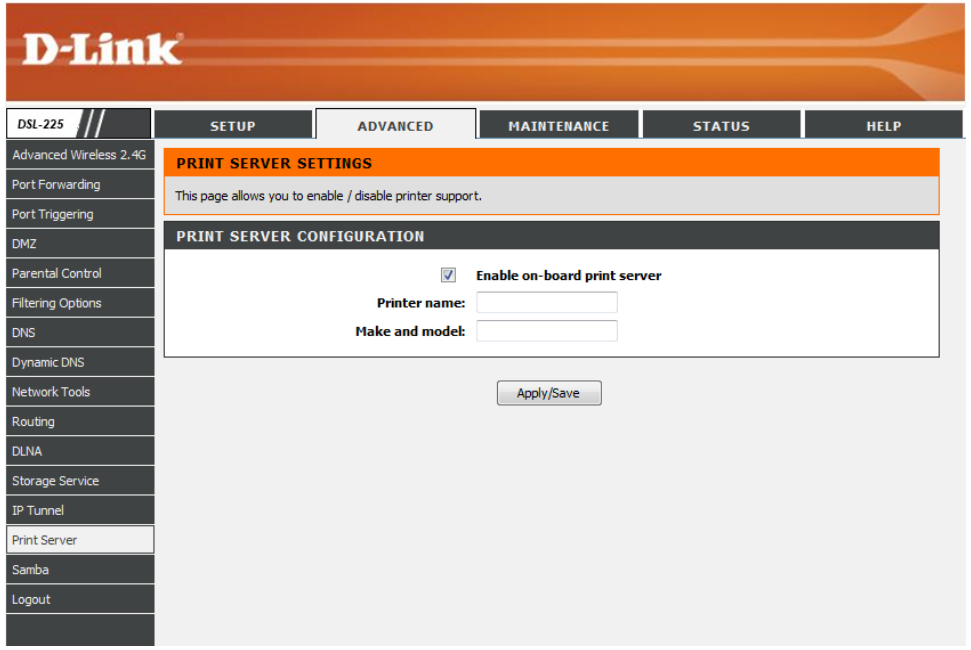


Click the **Apply/Save** button to accept the changes made.

Print Server

To access the **Print Server** page, click on the **Advanced** menu link, at the top, and then click on the **Print Server** menu link, on the left.

On this page the user can configure services related to the print server on this product.

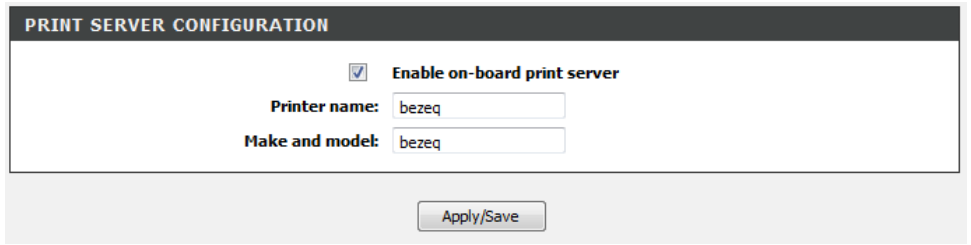


In this section, the following parameters can be configured:

Enable on-board print server: Tick this option to enable the onboard print server feature.

Printer name: Enter the printer name here.

Make and model: Enter the printer's make and model description here.

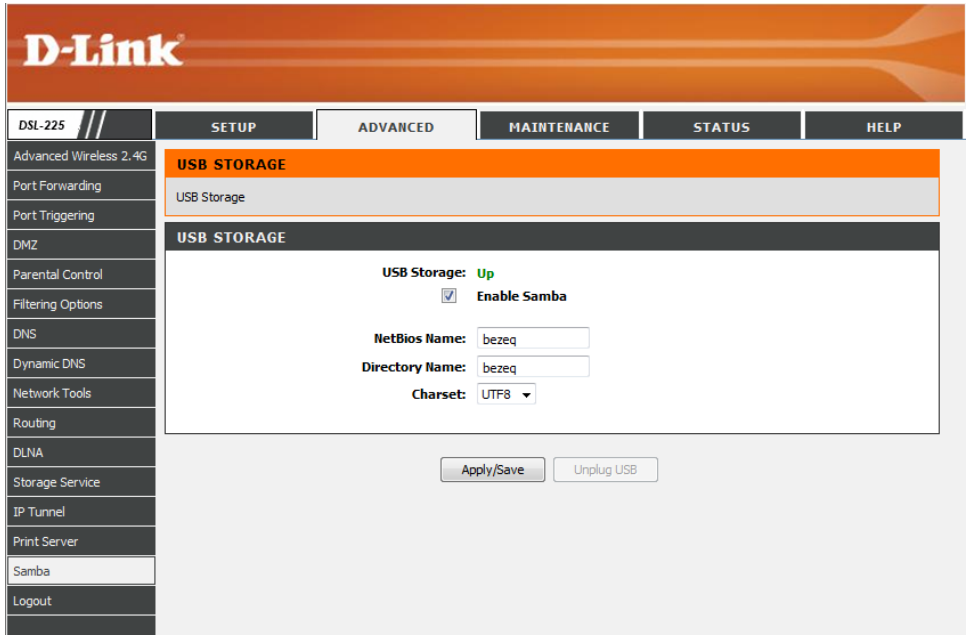


Click the **Apply/Save** button to accept the changes made.

Samba

To access the **Samba** page, click on the **Advanced** menu link, at the top, and then click on the **Samba** menu link, on the left.

On this page the user can configure services related to the Samba connectivity of this product.



In this section, the following parameters can be configured:

USB Storage: This parameter will display the USB storage device's status.

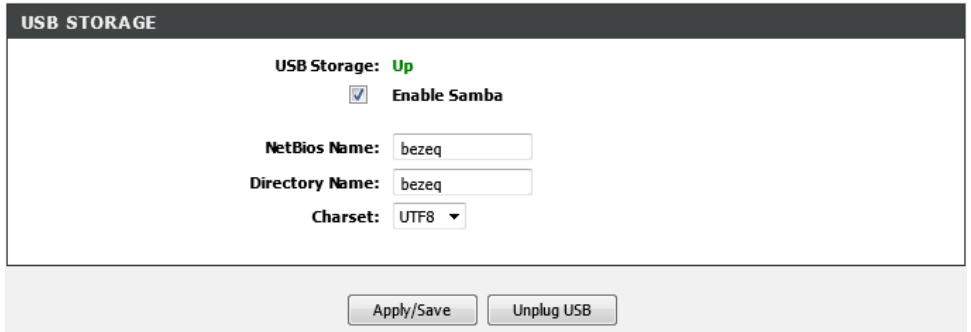
Enable Samba: Tick this option to enable the Samba feature.

NetBios Name: Enter the NetBIOS name here.

Directory Name: Enter the directory name here.

Charset: Select the character set option here. The only option available for selection is **UTF8**.

Click the **Apply/Save** button to accept the changes made.

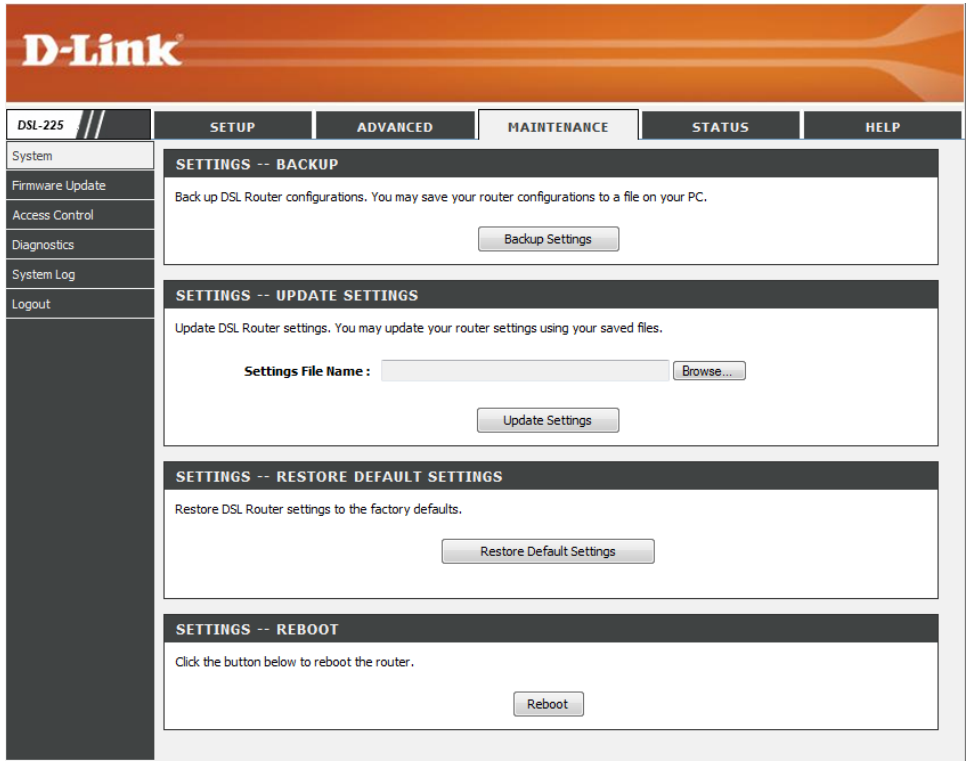


Maintenance Category

The **Maintenance** category is designed to assist the user with maintenance configurations for this product.

The following pages can be found in the **Maintenance** category:

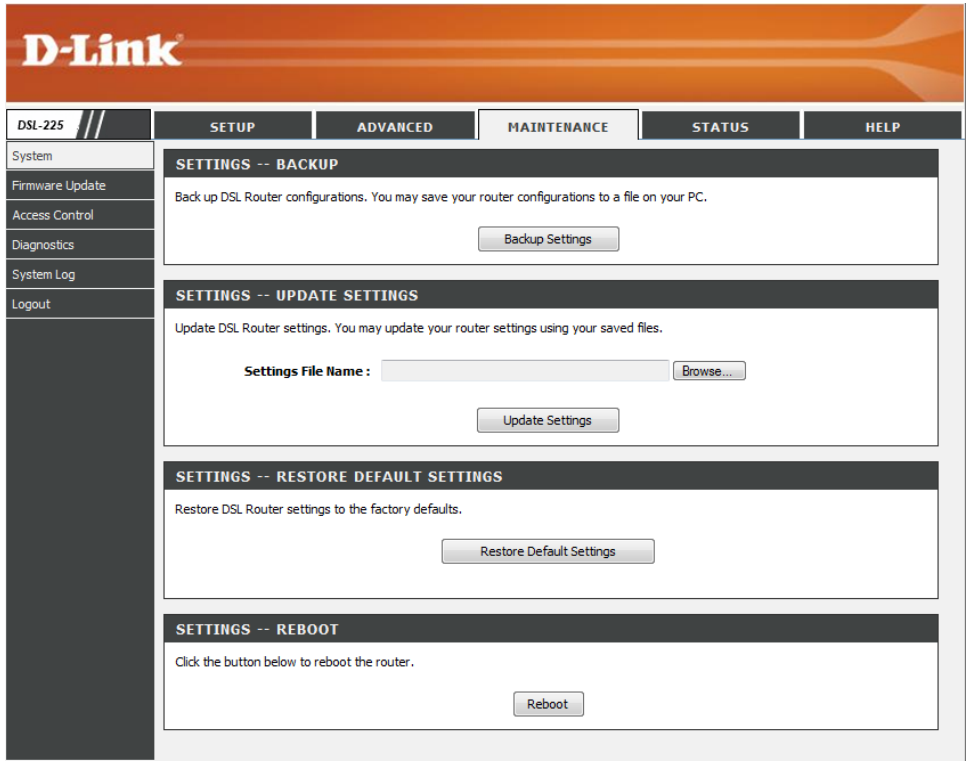
- **System** – On this page the user can perform maintenance concerning the System. Services available for configuration are **Backup and Restore Settings**, **Restore to Factory Default Settings**, and a **System Reboot**.
- **Firmware Update** – On this page the user can update the running firmware for this product.
- **Access Control** – On this page the user can configure the login username and password for the web user interface of this product.
- **Diagnostics** – On this page the user can run a diagnostics test that includes testing the **Ethernet**, **USB**, **Wireless**, and **DSL Connection** of this product.
- **System Log** – On this page the user can **View** and **Configure** the **System Log** used by this product.



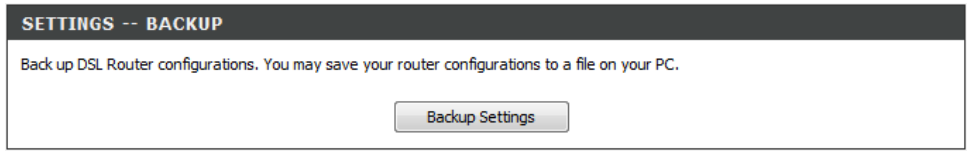
System

To access the **System** page, click on the **Maintenance** menu link, at the top, and then click on the **System** menu link, on the left.

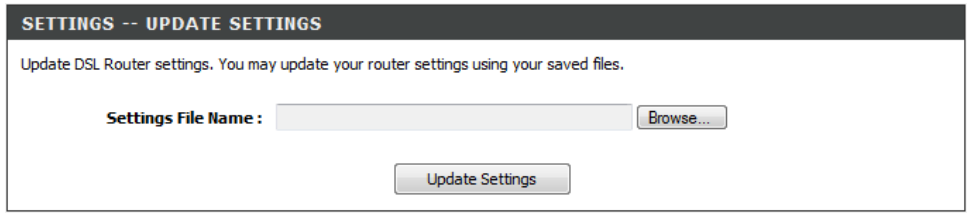
On this page the user can perform maintenance concerning the System. Services available for configuration are **Backup and Restore Settings**, **Restore to Factory Default Settings**, and a **System Reboot**.



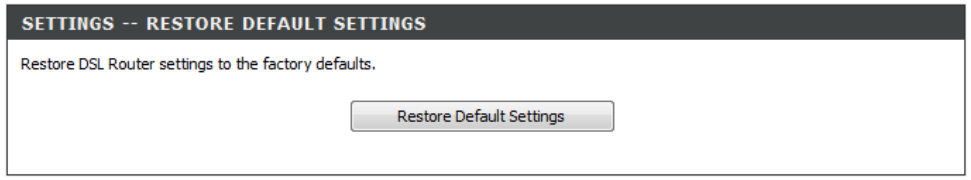
In this section we can initiate the configuration backup feature. Once you have configured the router to your satisfaction, it is a good idea to back up the configuration file to your computer. To save the current configuration settings to your computer, click the **Backup Settings** button. You will 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.



In this section we can restore the configuration backup from a saved file. To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Update 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.



In this section we can perform a factory reset on this router. 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.

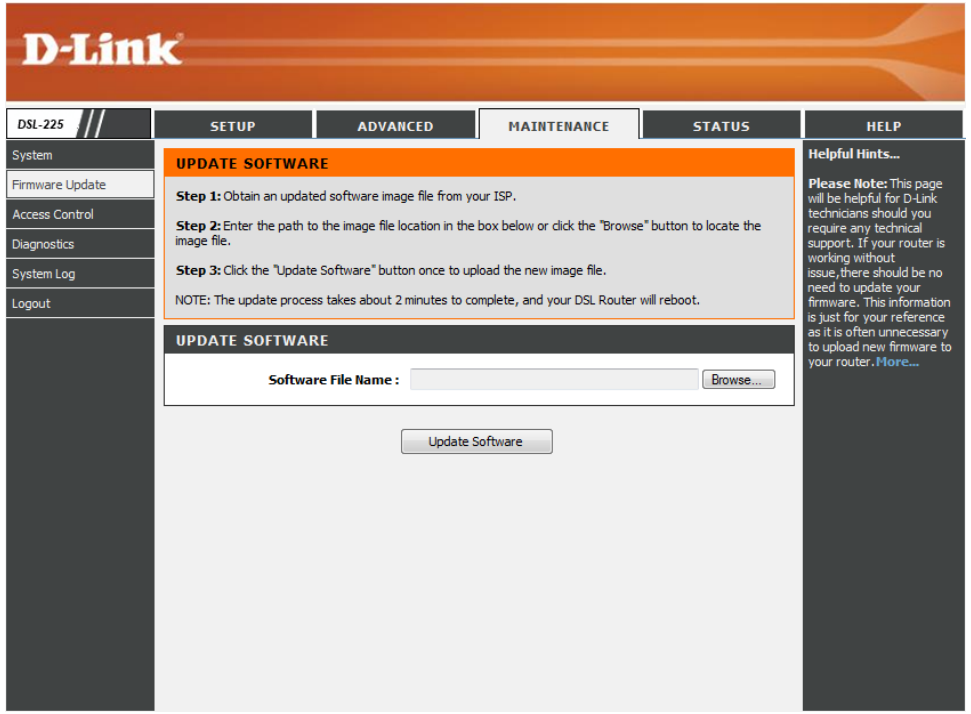


In this section we can reboot the router. Click the **Reboot** button to initiate the reboot procedure.

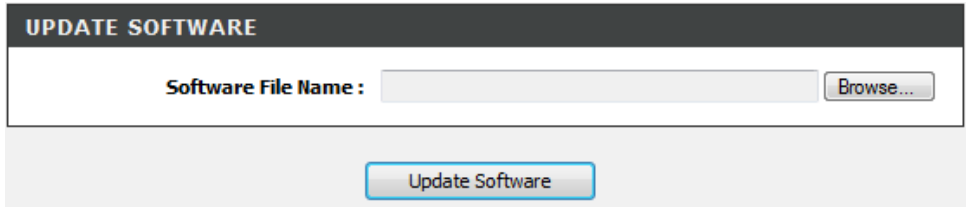
Firmware Update

To access the **Firmware Update** page, click on the **Maintenance** menu link, at the top, and then click on the **Firmware Update** menu link, on the left.

On this page the user can update the running firmware for this product. From time to time a software update will be available for this product. Keep an eye on the D-Link website for possible software updates that might be available in the future.



In this section we can load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings.

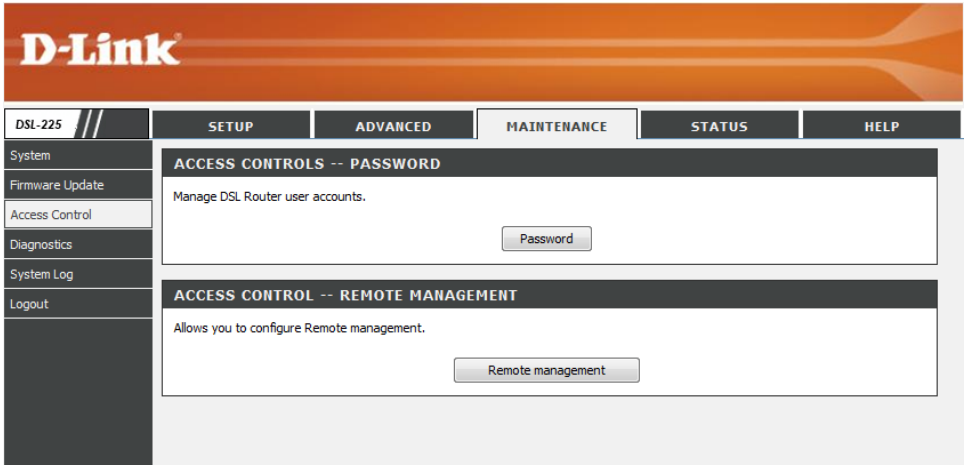


To upgrade the firmware, type in the name and path of the file in the **Software File Name** field or click on the **Browse** button to search for the file. Click the **Update Software** button to begin copying the file. The file will load and restart the router automatically.

Access Control

To access the **Access Control** page, click on the **Maintenance** menu link, at the top, and then click on the **Access Control** menu link, on the left.

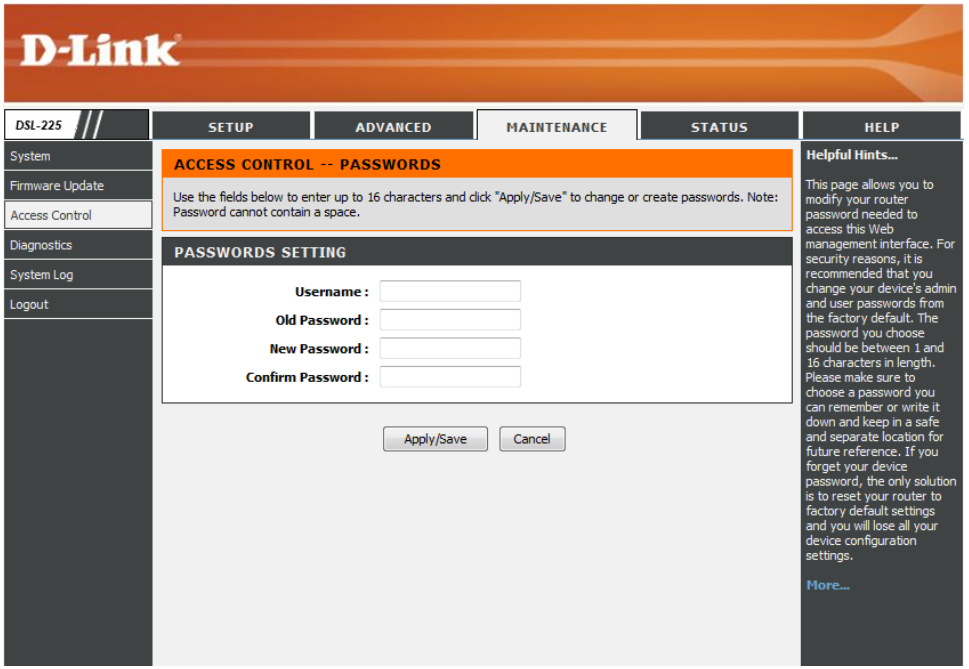
On this page the user can configure the login username and password for the web user interface of this product.



Passwords

Click the **Password** button to access the **Password** configuration page.

After clicking the **Password** button the following page is available.



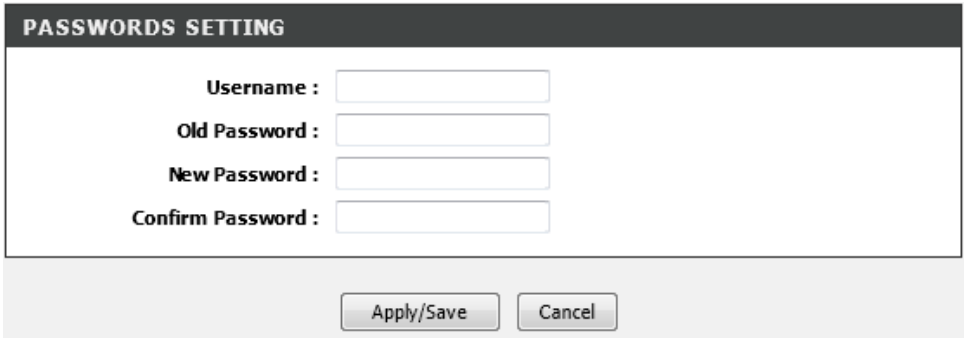
In this section we can configure the access control account information.

Username: Enter the new login username for this router here. The default username is **Admin**.

Old Password: Enter the old login password for this router here. The default password is **Admin**.

New Password: Enter the new login password for this router here.

Confirm Password: Enter the new login password for this router here again.

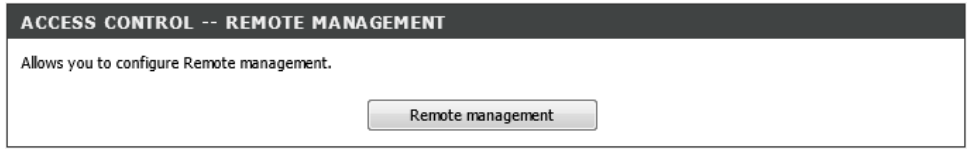


Click the **Apply/Save** button to accept the changes made.

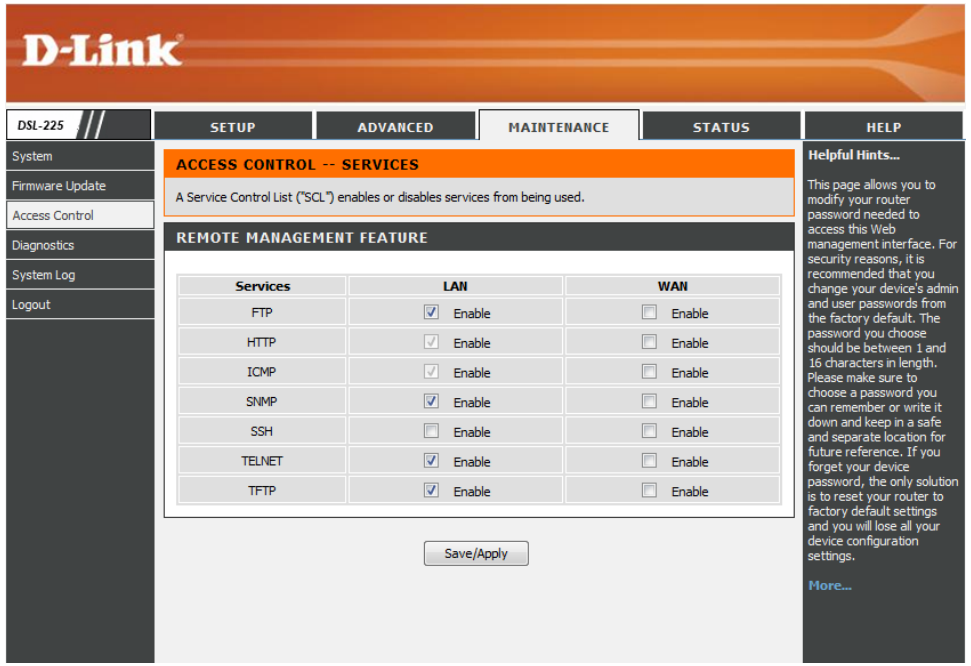
Click the **Cancel** button to discard the changes made and return to the main page.

Remote Management

Click the **Remote management** button to access the **Remote Management** configuration page.



After clicking the **Remote management** button the following page is available.



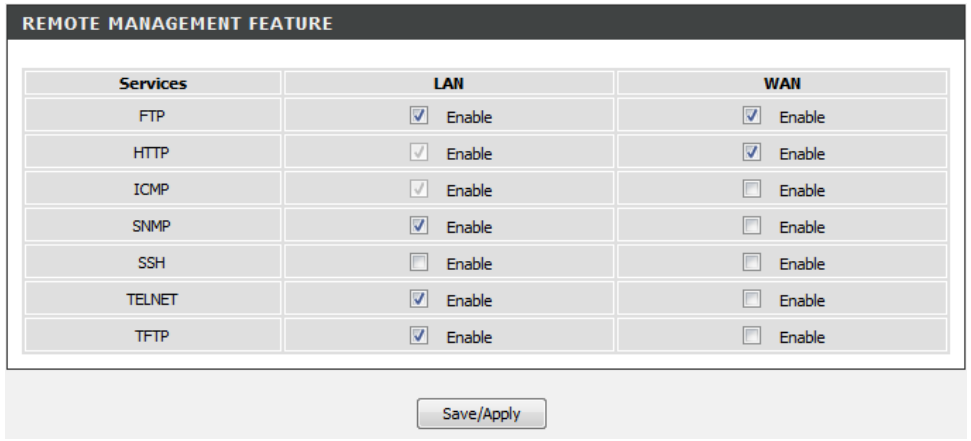
In this section we can configure the following information:

Service: In this column a list of service is be displayed that can be enabled or remote access.

LAN: Tick the **Enable** option to enable the related service on the LAN interface.

WAN: Tick the **Enable** option to enable the related service on the WAN interface.

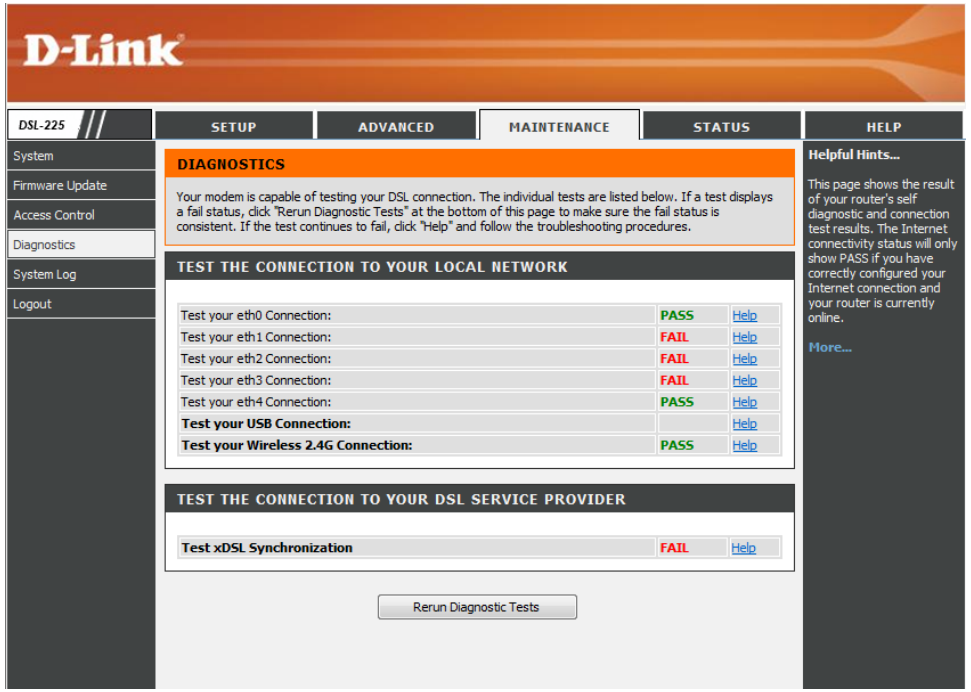
Click the **Save/Apply** button to accept the changes made.



Diagnostics

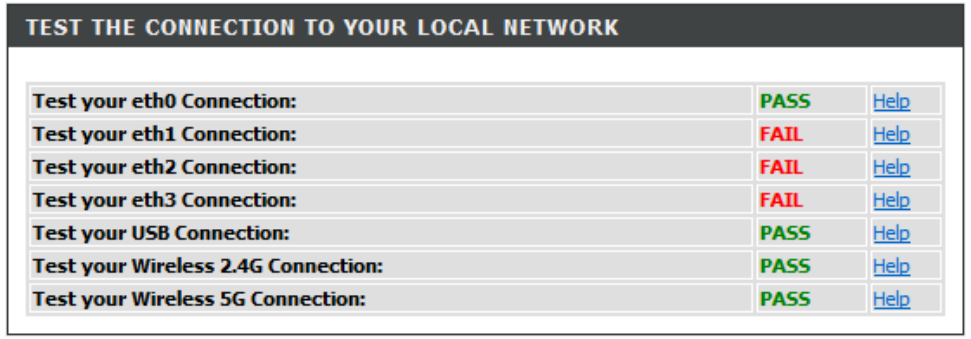
To access the **Diagnostics** page, click on the **Maintenance** menu link, at the top, and then click on the **Diagnostics** menu link, on the left.

On this page the user can run a diagnostics test that includes testing the Ethernet, USB, Wireless, and DSL Connection of this product.



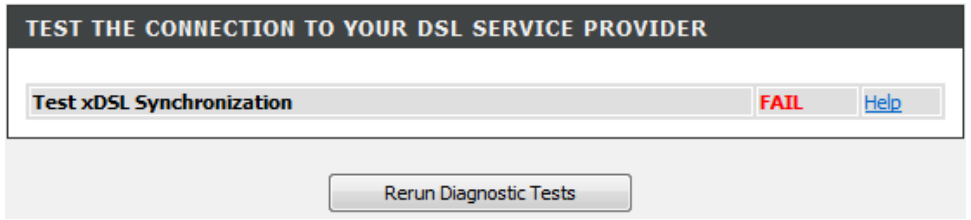
In this section diagnostic tests are performed to test the connection to the **Local Network** interface. This test will include testing the **Ethernet**, **USB**, and **Wireless** connections of this router.

If a connection does not pass the test, a **Help** link is available for a more detailed description about the connection test and the possible solutions that can be performed to solve the problem.



In this section diagnostic tests are performed to test the connection to the **DSL Service Provider**. This test will include testing the **xDSL Synchronization**.

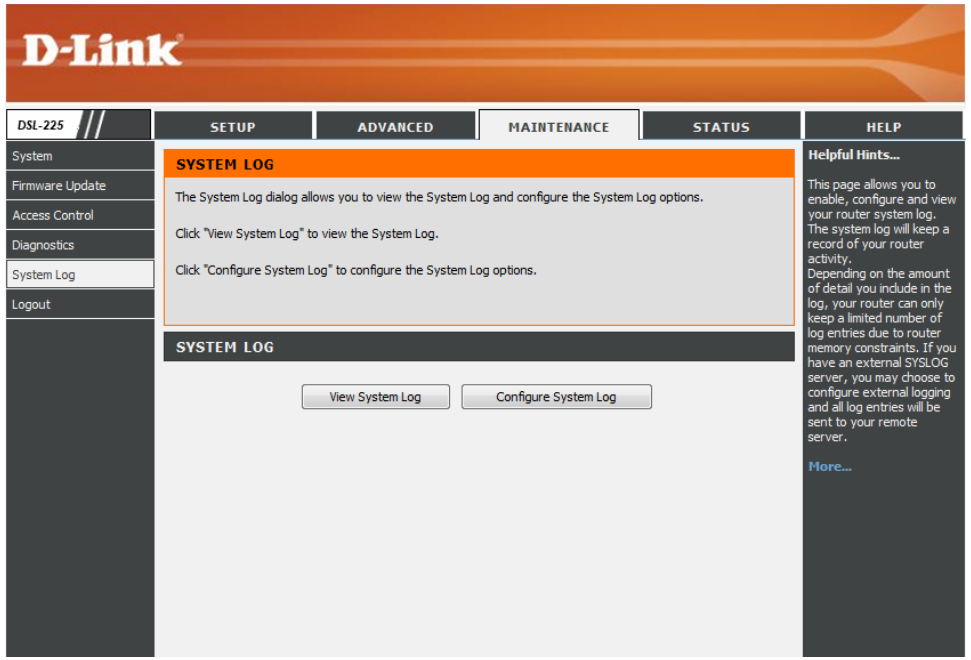
If a connection does not pass the test, a **Help** link is available for a more detailed description about the connection test and the possible solutions that can be performed to solve the problem.



System Log

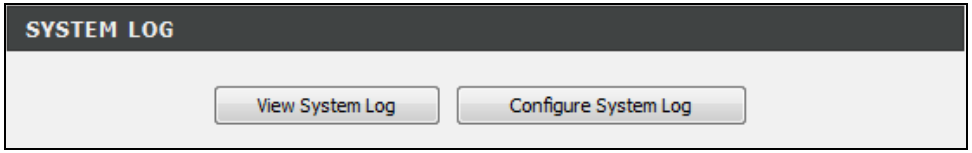
To access the **System Log** page, click on the **Maintenance** menu link, at the top, and then click on the **System Log** menu link, on the left.

On this page the user can view and configure the System Log used by this product.

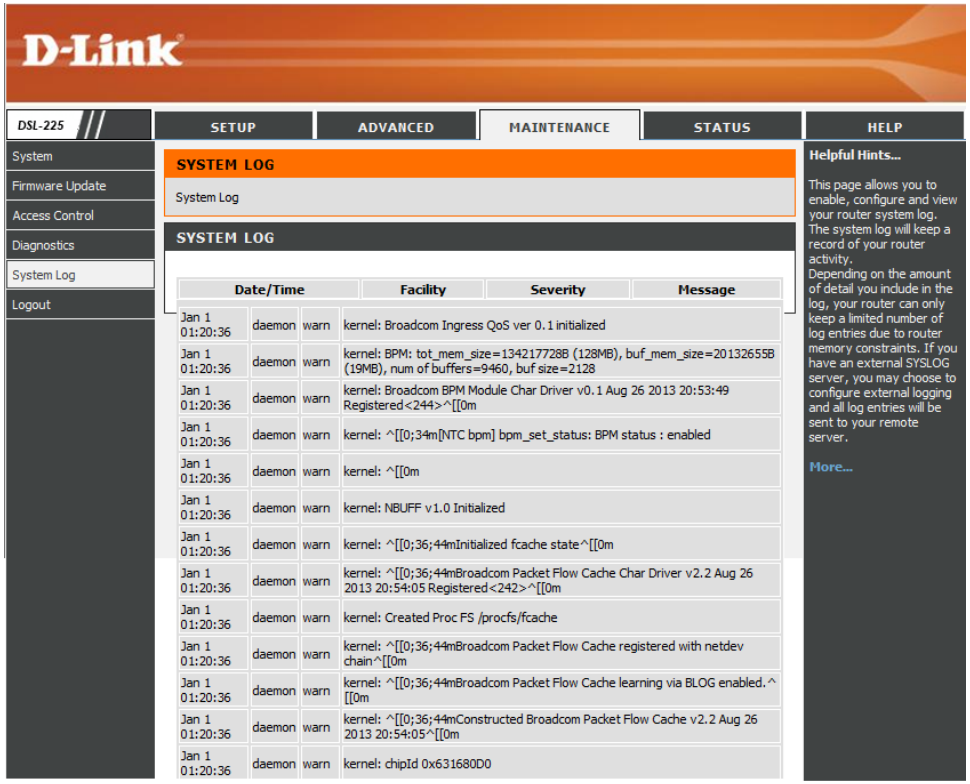


Click the **View System Log** button to access the **System Log Display** page.

Click the **Configure System Log** button to access the **System Log Configuration** page.

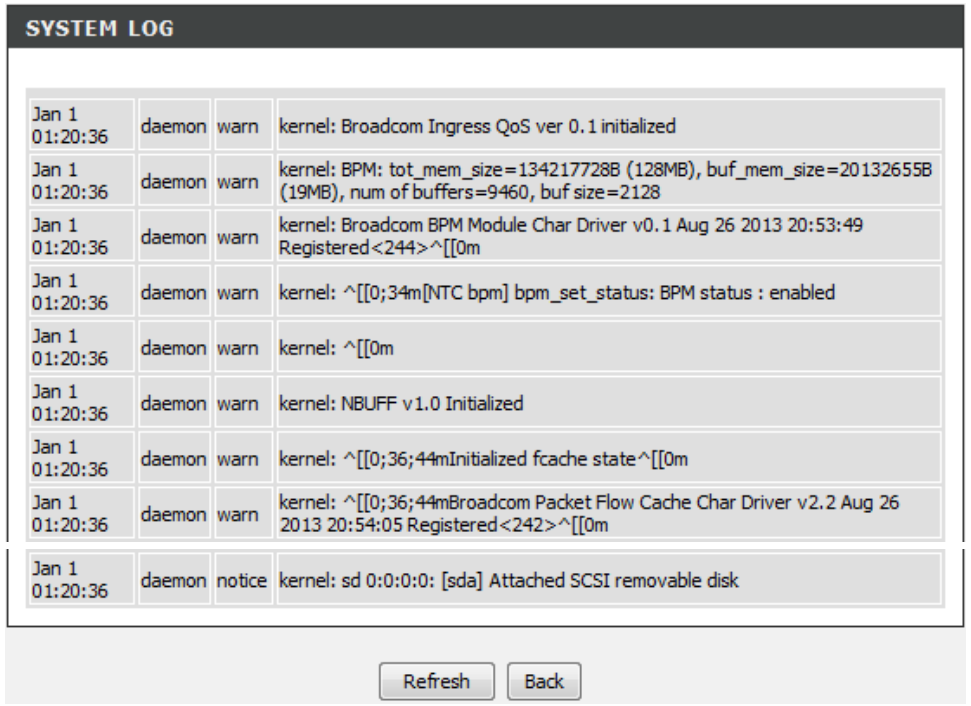


After clicking the **View System Log** button, the following page is available.

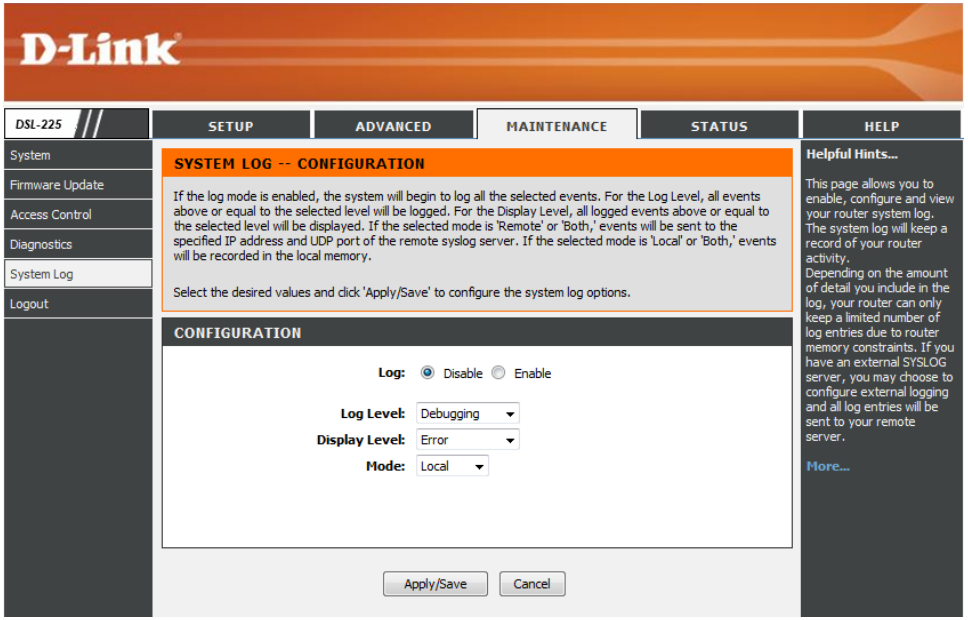


In this section a list of system log entries will be displayed.

Click the **Refresh** button to refresh the information in this table.
Click the **Back** button to return to the previous page.



After clicking the **Configure System Log** button, the following page is available.



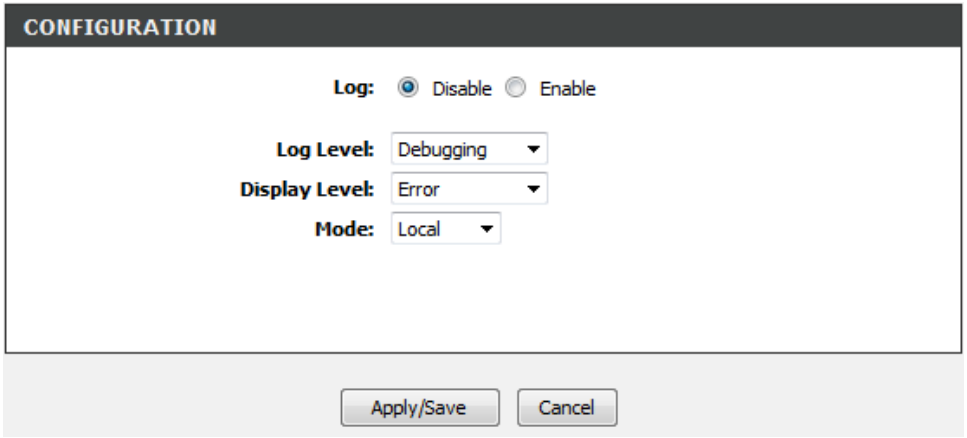
In this section we can configure the System Log parameters for this router.

Log: Select the log state here. Options to choose from are **Disable** and **Enable**.

Log Level: Select the log level option here. Options to choose from are **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Information**, and **Debugging**.

Display Level: Select the display level option here. Options to choose from are **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Information**, and **Debugging**.

Mode: Select the mode option here. Options to choose from are **Local**, **Remote**, and **Both**.



Click the **Apply/Save** button to accept the changes made.

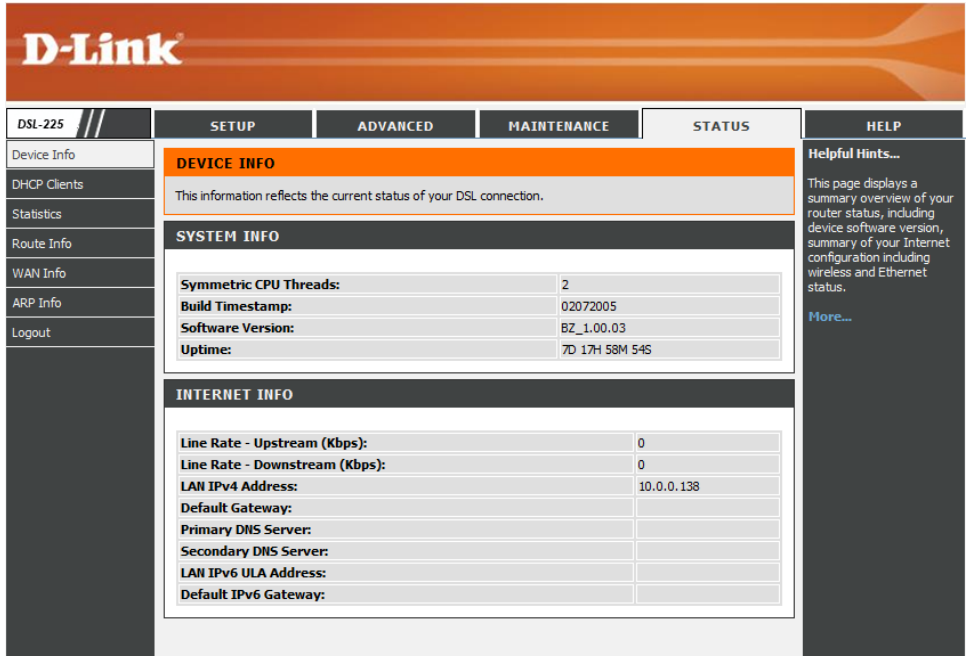
Click the **Cancel** button to discard the changes made and return to the main page.

Status Category

The **Status** category is designed to assist the user with information display pages, concerning the configuration and behavior of this product.

The following pages can be found in the **Status** category:

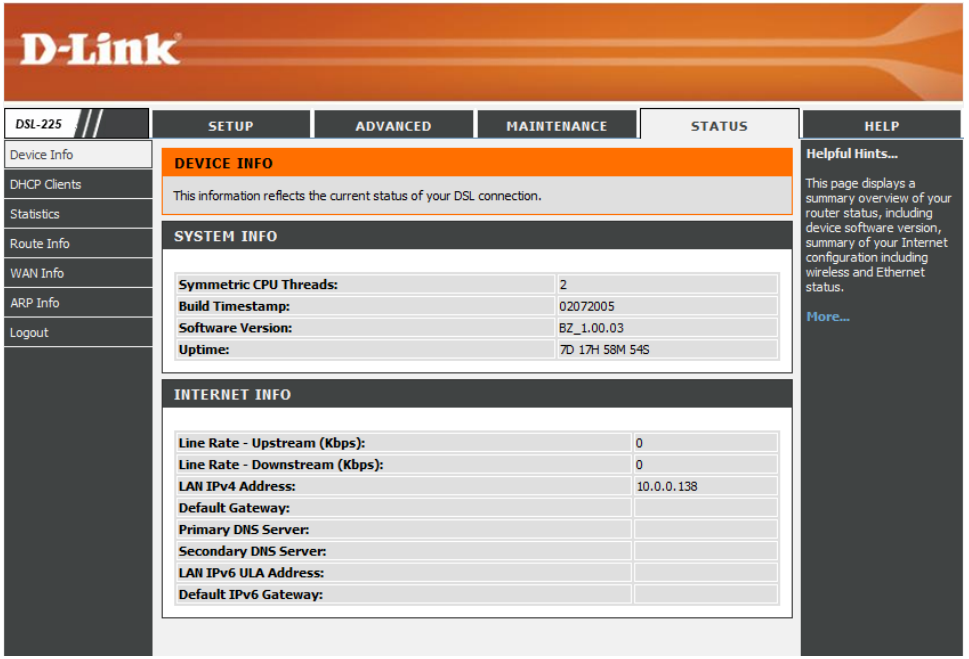
- **Device Info** – On this page the user can view information regarding the System and Internet Connectivity.
- **DHCP Clients** – On this page the user can view a list of **DHCP clients** that are currently connected to this product.
- **Statistics** – On this page the user can view statistical information about the LAN, WAN, xTM, and xDSL interfaces.
- **Route Info** – On this page the user can view information about routes used by this product.
- **WAN Info** – On this page the user can view information about WAN interfaces used by this product.
- **ARP Info** – On this page the user can view information about ARP interfaces used by this product.



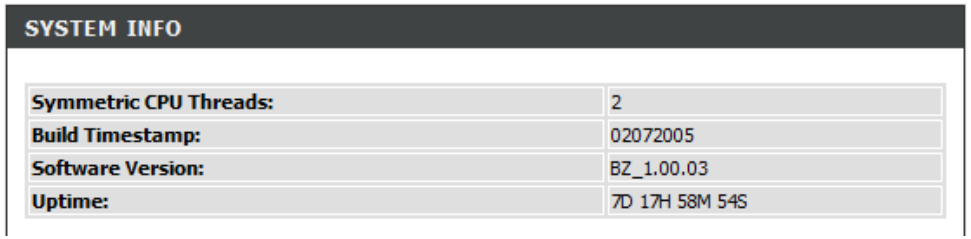
Device Info

To access the **Device Info** page, click on the **Status** menu link, at the top, and then click on the **Device Info** menu link, on the left.

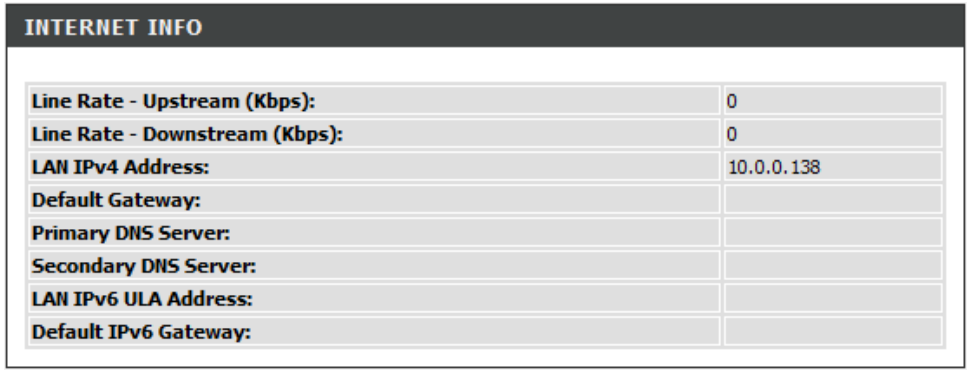
On this page the user can view System and Internet information.



In this section we can view **System Information**.



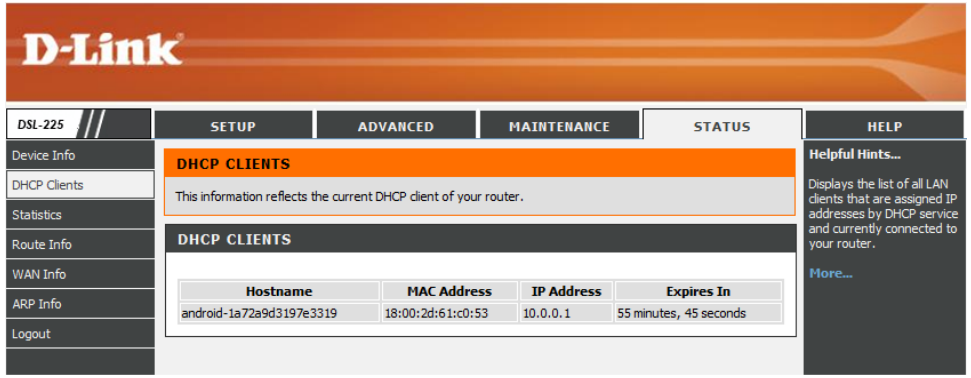
In this section we can view **Internet Information**.



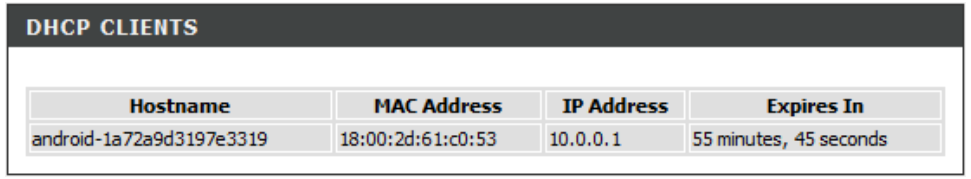
DHCP Clients

To access the **DHCP Clients** page, click on the **Status** menu link, at the top, and then click on the **DHCP Clients** menu link, on the left.

On the page the user can view a list of DHCP clients that are currently connected to this product.



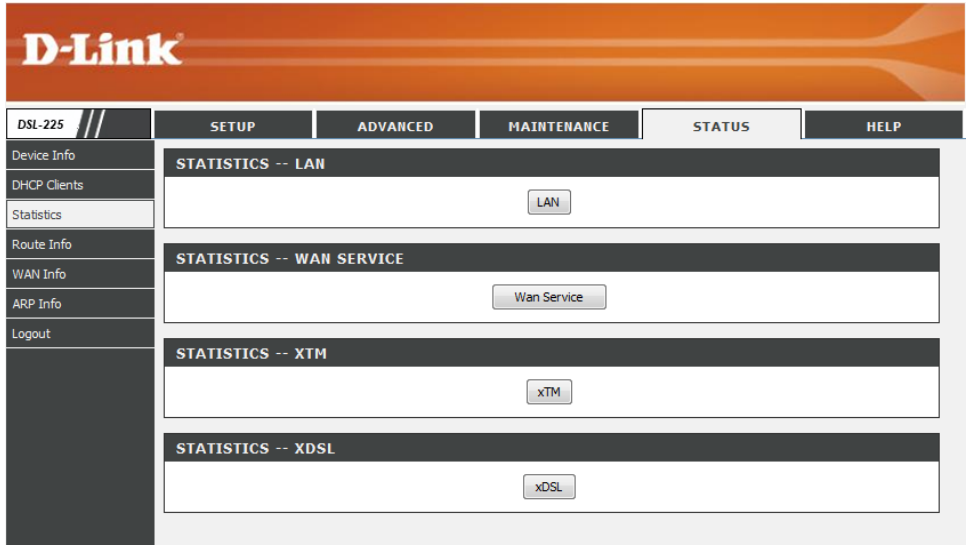
In this section we can view a list of **DHCP Clients**.



Statistics

To access the **Statistics** page, click on the **Status** menu link, at the top, and then click on the **Statistics** menu link, on the left.

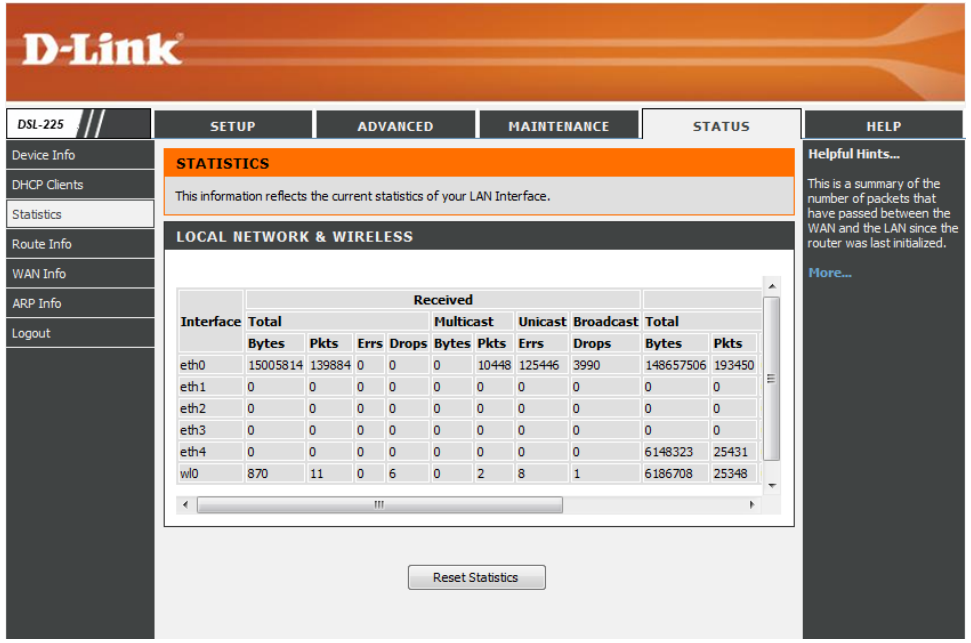
On this page the user can view statistical information about various interfaces used by this product.



LAN

Click the **LAN** button to access the **Local Network** and **Wireless Statistics** page.

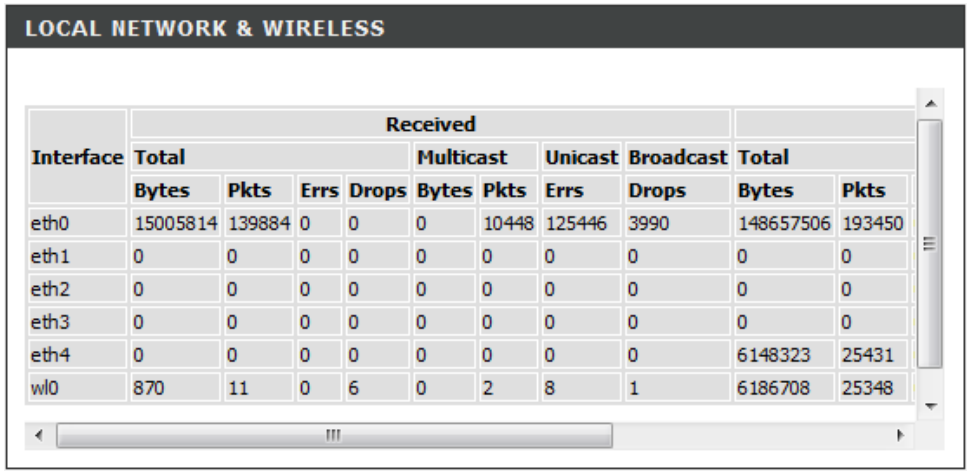
After clicking the **LAN** button, the following page is available.



Interface	Received				Multicast		Unicast	Broadcast	Total	
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	Bytes	Pkts
eth0	15005814	139884	0	0	0	10448	125446	3990	148657506	193450
eth1	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0
eth4	0	0	0	0	0	0	0	0	6148323	25431
wl0	870	11	0	6	0	2	8	1	6186708	25348

In this section we can view **Local Network** and **Wireless Statistics**.

Click the **Reset Statistics** button to reset the information in this section.

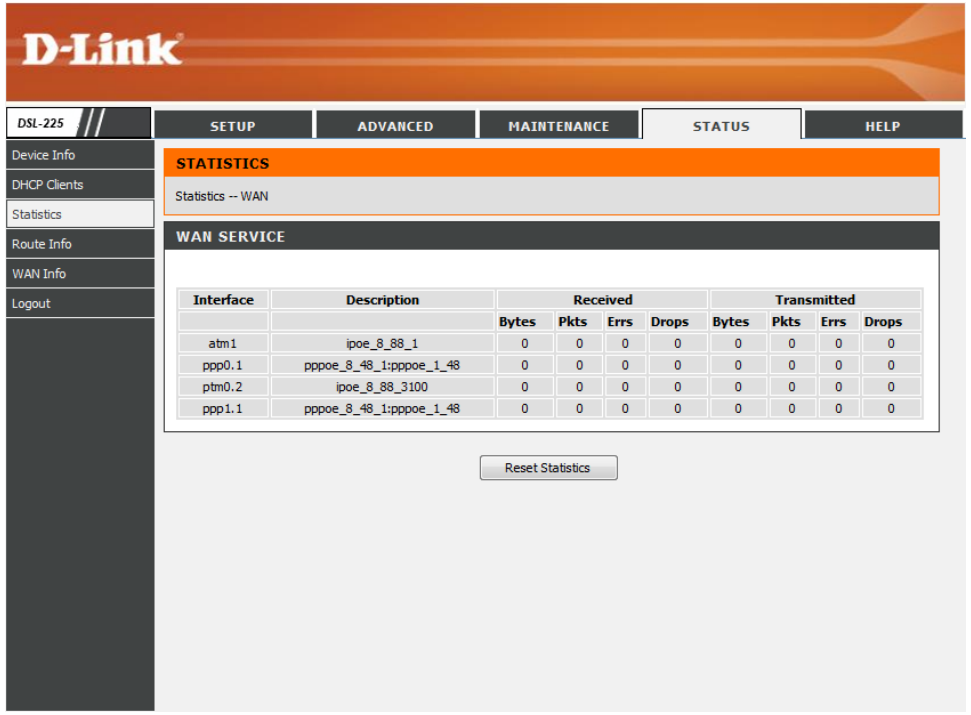


Interface	Received									
	Total				Multicast		Unicast	Broadcast	Total	
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	Bytes	Pkts
eth0	15005814	139884	0	0	0	10448	125446	3990	148657506	193450
eth1	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0
eth4	0	0	0	0	0	0	0	0	6148323	25431
wl0	870	11	0	6	0	2	8	1	6186708	25348

WAN Service

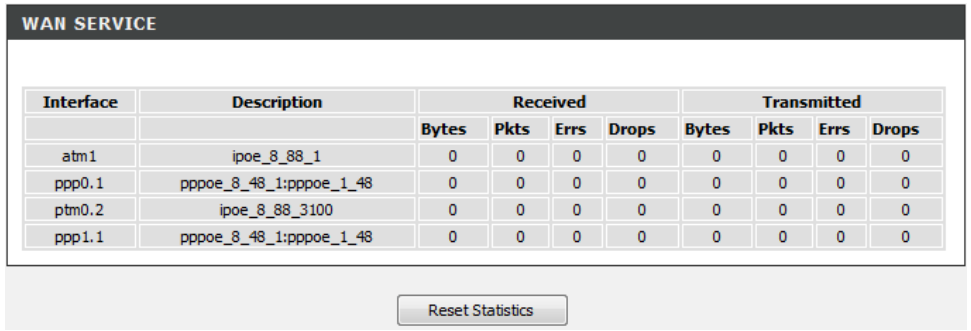
Click the **WAN Service** button to access the **WAN Statistics** page.

After clicking the **WAN Service** button, the following page is available.



In this section we can view **WAN Statistics**.

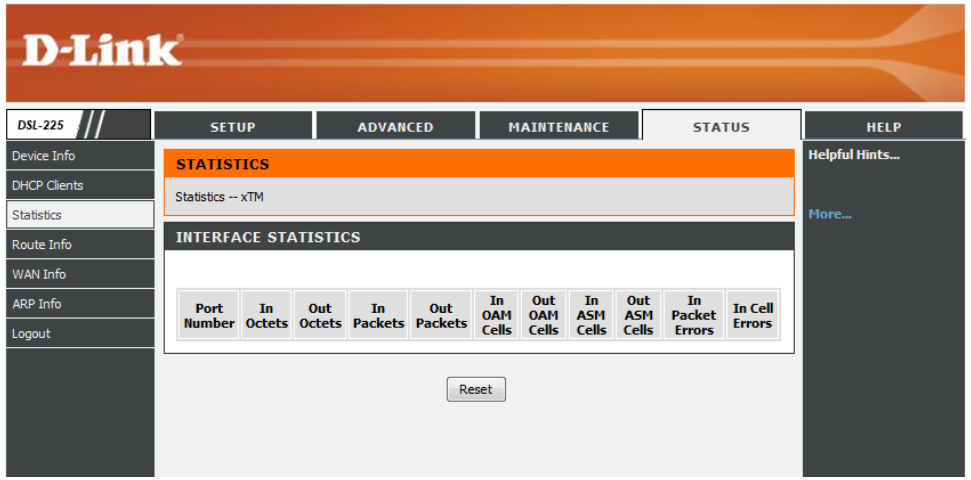
Click the **Reset Statistics** button to reset the information in this section.



xTM

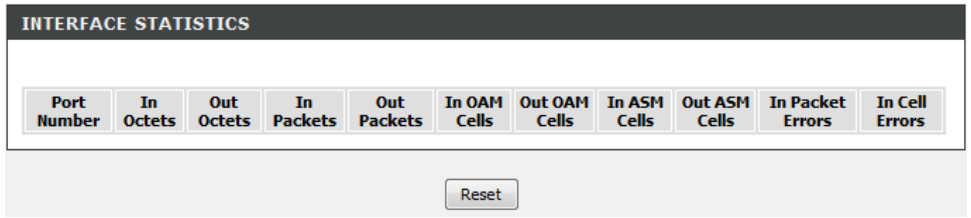
Click the **xTM** button to access the **xTM Statistics** page.

After clicking the **xTM** button, the following page is available.



In this section we can view **xTM Inteface Statistics**.

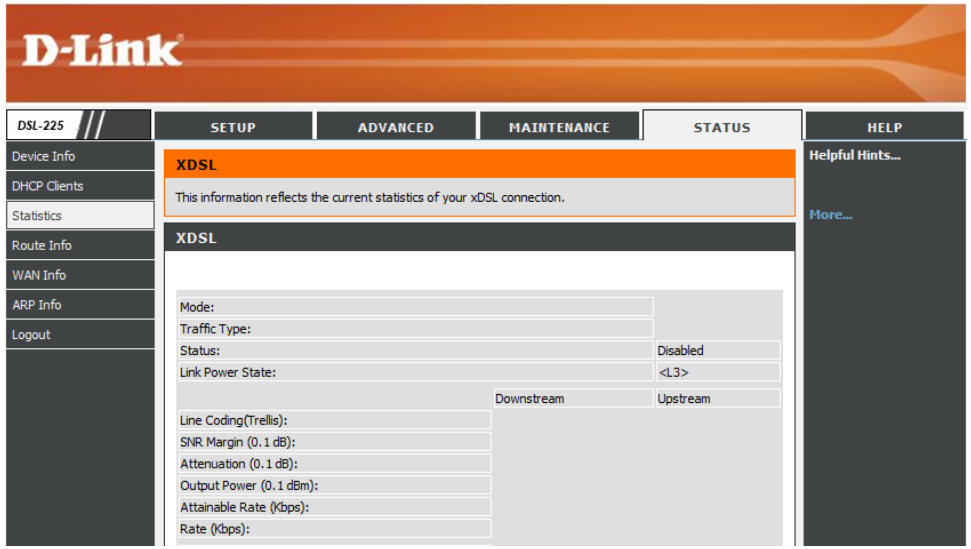
Click the **Reset** button to reset the information in this section.



xDSL

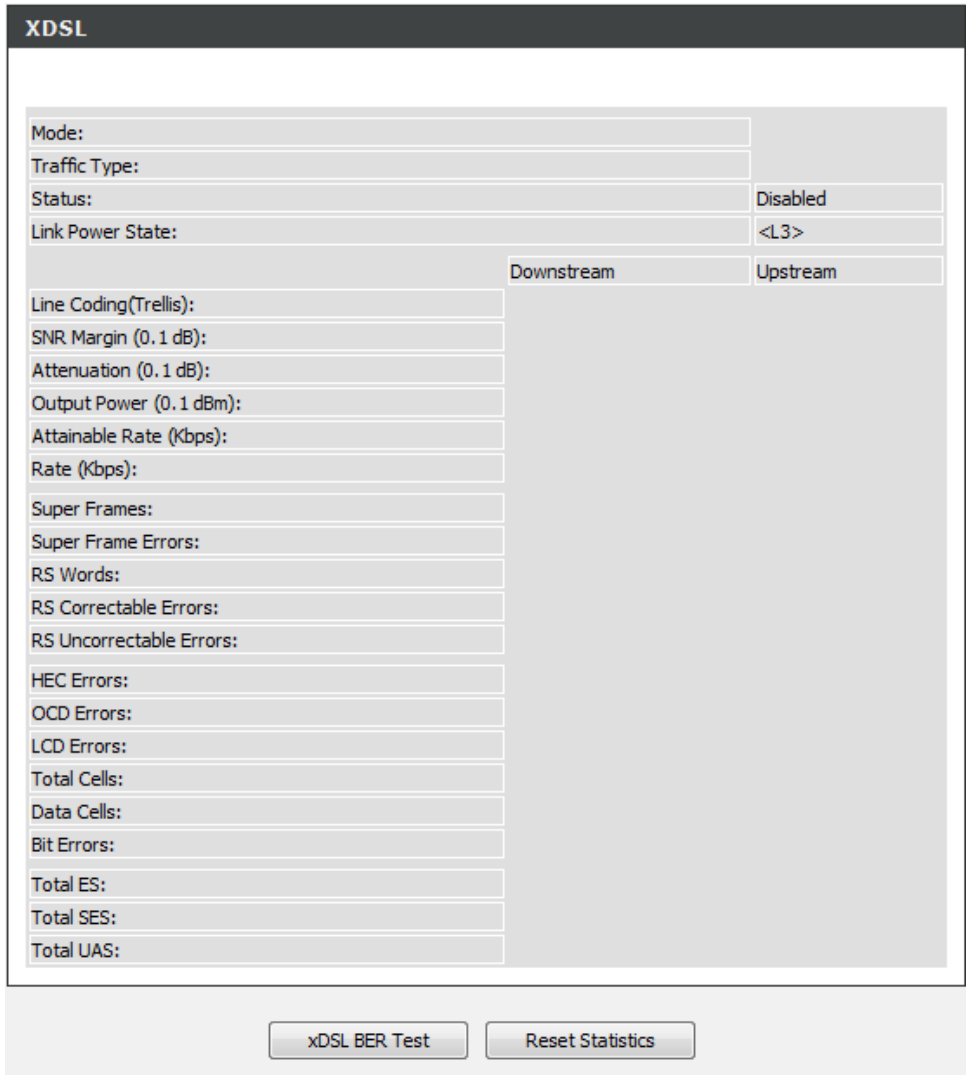
Click the **xDSL** button to access the **xDSL Statistics** page.

After clicking the **xDSL** button, the following page is available.

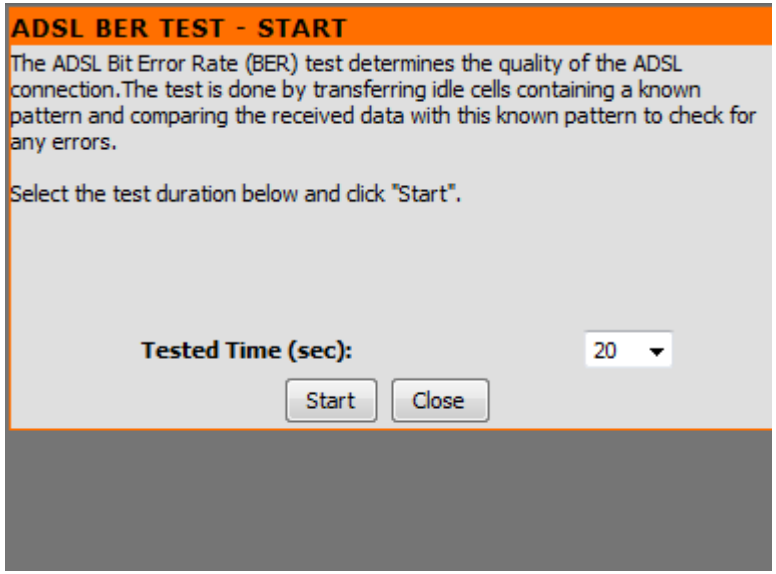


In this section we can view **xDSL Statistics**.

Click the **xDSL BER Test** button to initiate the ADSL BER Test.
Click the **Reset Statistics** button to reset the information in this section.



After clicking the **xDSL BER Test** button, the following page is available.

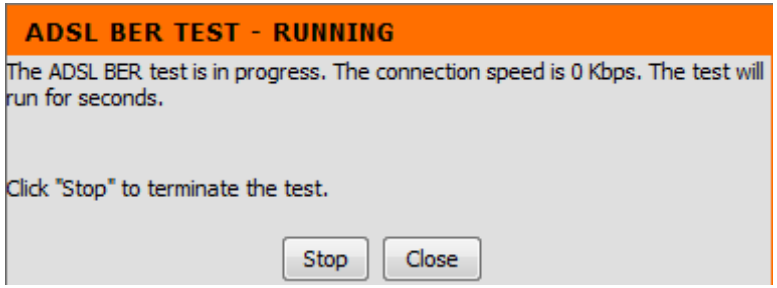


In this section we can initiate the ADSL BER Test.

Tested Time: Select the testing time value here. Options to choose from are **1**, **5**, **10**, **20**, **60**, **120**, **180**, **240**, **300**, and **360** seconds. By default this value is 20 seconds.

Click the **Start** button to start the ADSL BER Test.
Click the **Close** button to close the window.

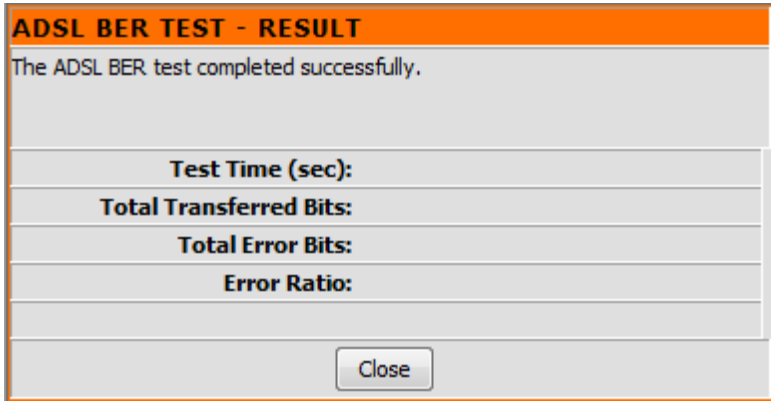
After clicking the **Start** button to the ADSL BER Test will run the test.



Click the **Stop** button to the stop the test.
Click the **Close** button to close the window.

After the completion of the test, the **ADSL BER Test Result** will be displayed.

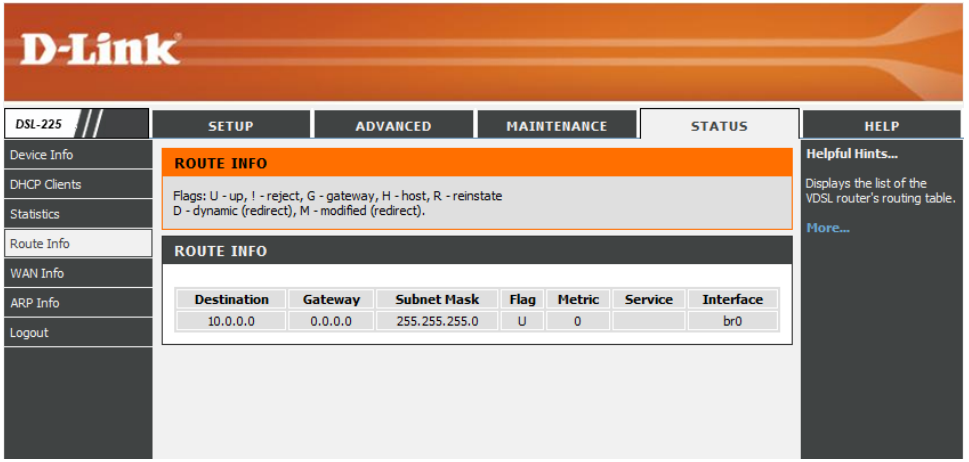
Click the **Close** button to close the window.



Route Info

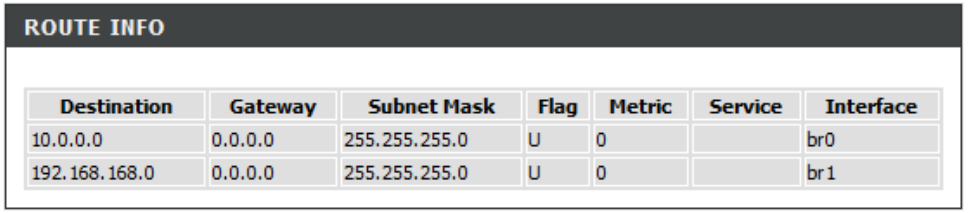
To access the **Route Info** page, click on the **Status** menu link, at the top, and then click on the **Route Info** menu link, on the left.

On this page the user can view information about routes used by this product.



In this section we can view **Route Information**.

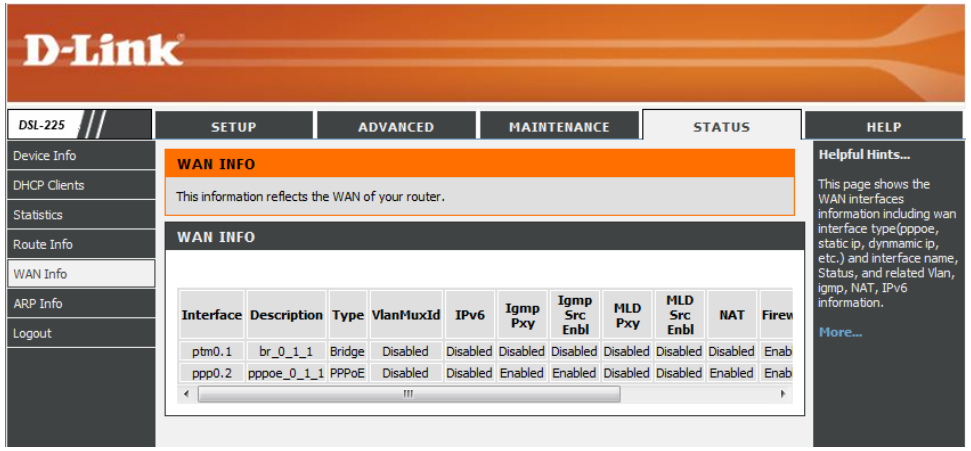
The information available in the **Flag** field can be translated to the following:
U means Up. **!** means Reject. **G** means Gateway. **H** means Host. **R** means Reinstate.
D means Dynamic or Redirect. **M** means Modified or also Redirect.



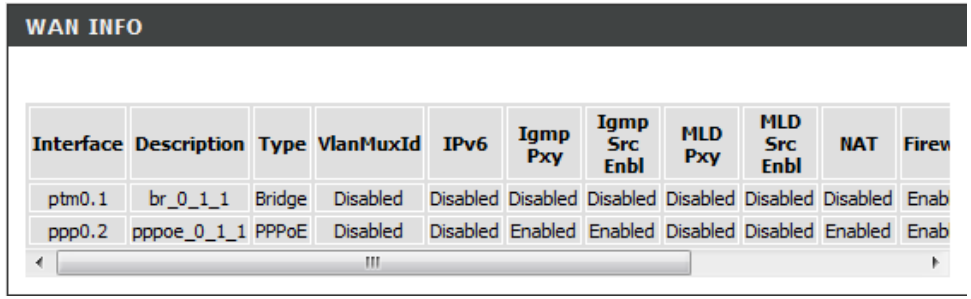
WAN Info

To access the **WAN Info** page, click on the **Status** menu link, at the top, and then click on the **WAN Info** menu link, on the left.

On this page the user can view information about WAN interfaces used by this product.



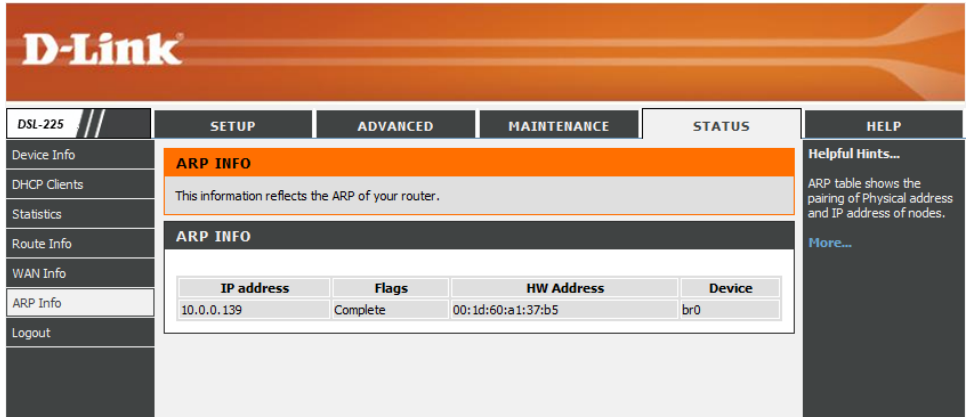
In this section we can view **WAN Information**.



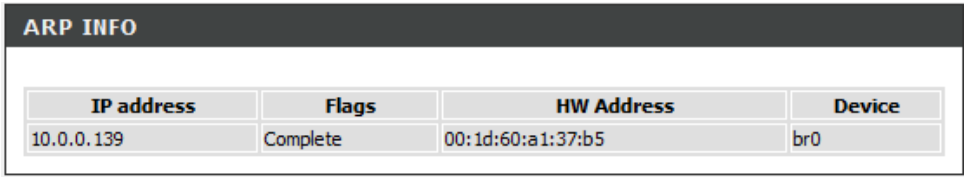
ARP Info

To access the **ARP Info** page, click on the **Status** menu link, at the top, and then click on the **ARP Info** menu link, on the left.

On this page the user can view information about ARP interfaces used by this product.



In this section we can view **ARP Information**.

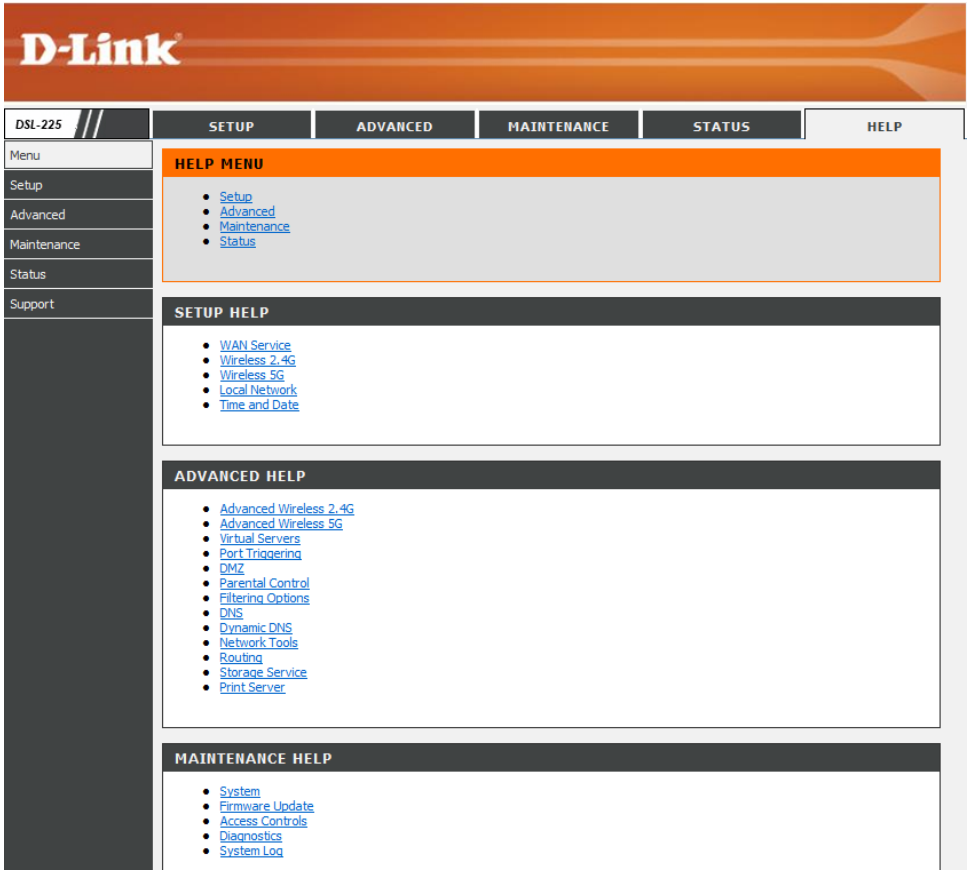


Help Category

The **Help** category is designed to assist the user with helpful information about every topic found on the web user interface of this product.

The following pages can be found in the **Help** category:

- **Menu** – On this page the user can navigate easily to any page throughout the menu structure to access help information.
- **Setup** – On this page the user can read more about topics discussed in the Setup category.
- **Advanced** – On this page the user can read more about topics discussed in the Advanced category.
- **Maintenance** – On this page the user can read more about topics discussed in the Maintenance category.
- **Status** – On this page the user can read more about topics discussed in the Status category.



Knowledge Base

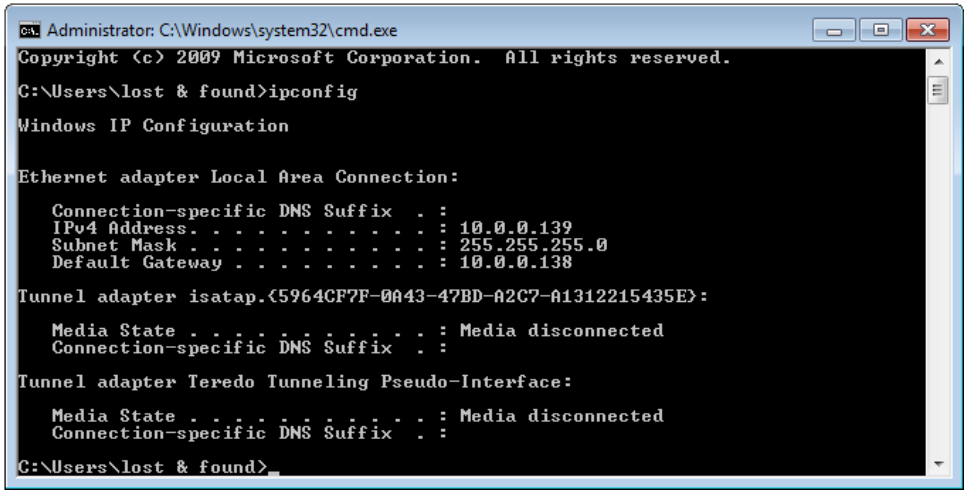
Networking Basics

Check your IP address

After you installed your new network or wireless adapter, by default, the TCP/IP settings should be set to obtain an IP address automatically from a DHCP server. By default the DHCP server option on your router is enabled.

To verify your IP address, please follow the steps below:

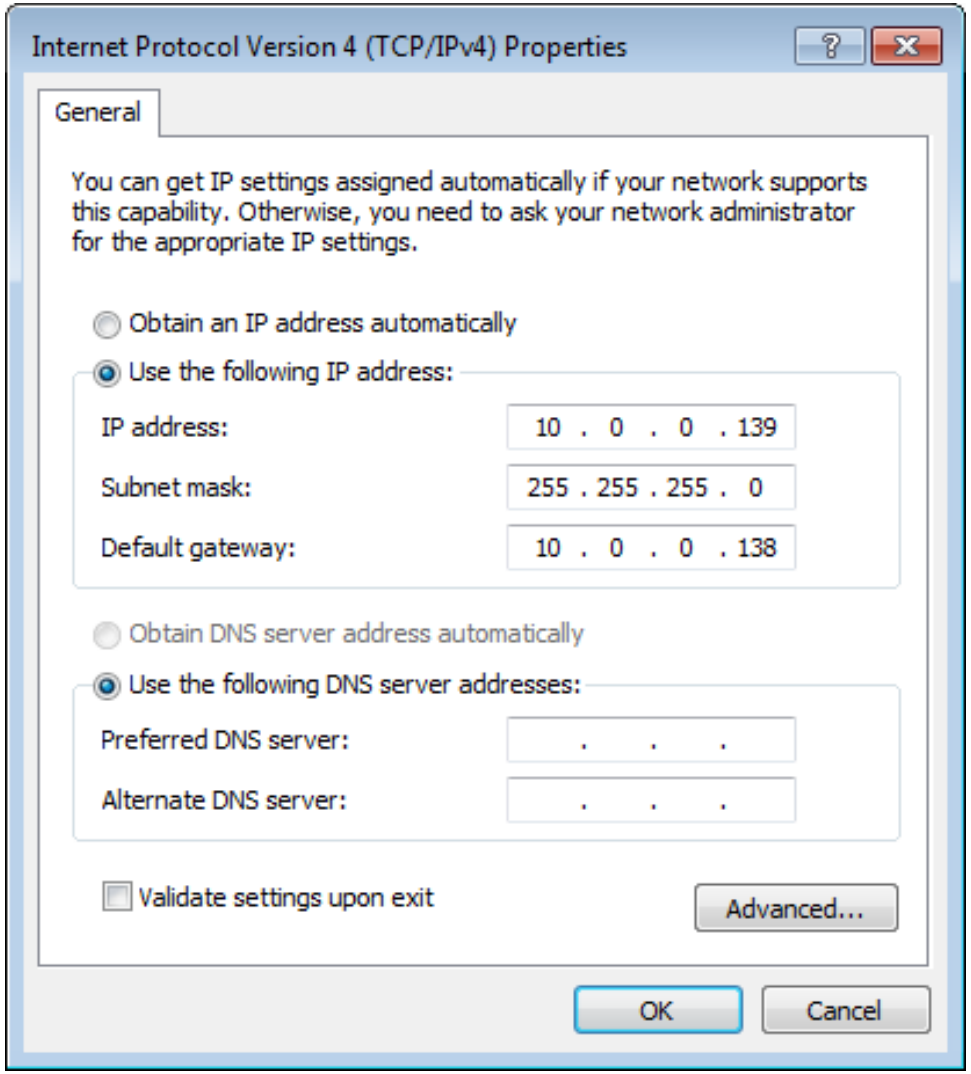
- Click on the Windows **Start** button and open the **Run** application.
- In the **Open** box type *cmd* and click **OK**.
- At the command prompt, type in the command *ipconfig* and press **Enter**. This will display the **IP address**, **Subnet Mask**, and the **Default Gateway** of your adapter. If the address is *0.0.0.0*, it means that your network adapter did not receive an IP address from the DHCP server. Check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

- Click on the Windows **Start** button and navigate to the **Control Panel** > **Network and Sharing Center** and click on the **Change Adapter Settings** option on the left panel.
- Right-click on the **Local Area Connection**, which represents your network adapter, and select **Properties**.
- Select the **Internet Protocol Version 4 (TCP/IPv4)** option and click on the **Properties** button.
- Select **Use the following IP address** and enter an IP address that is on the same subnet as your router. For example: If your router is running on the IP address of **10.0.0.138**, use any IP address from **10.0.0.1** to **10.0.0.254**, **except 10.0.0.138**. Use the Subnet Mask of **255.255.255.0**. Set Default Gateway the same as the LAN IP address of your router. Set Preferred DNS server IP address the same as the LAN IP address of your router. The Secondary DNS is not needed at this stage.
- Click the **OK** button twice to return to the **Network Connections** window.



Wireless Basics

Wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

How does Wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away. Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn’t use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, whether it's for home, office, business, we have a wireless solution for it.

Home

- Gives everyone at home broadband access.
- Surf the web, check email, instant message, etc…
- Gets rid of the cables around the house.
- Simple and easy to use.

Small Office and Home Office

- Stay on top of everything at home as you would at office.
- Remotely access your office network from home.
- Share Internet connection and printer with multiple computers.
- No need to dedicate office space.

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a Wireless Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let your next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless Cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The router offers wireless security options like WPA/WPA2 PSK/EAP.

What is WPA?

WPA (Wi-Fi Protected Access) is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Frequently Asked Questions

What can I do if my Router is not working correctly?

There are a few quick steps you can take to try and resolve any issues:

- Check that all the cables are firmly connected at both ends.
- Check that all the corresponding LED indicators are on, especially the Power, DSL, and LAN LED indicators.
- Ensure that the settings on the WAN Service page in the Web User Interface are the same as the settings that have been provided to you by your ISP.

Why can't I get an Internet connection?

For VDSL ISP users, please contact your ISP to make sure the service has been enabled/connected by your ISP and that your ISP username and password are correct.

What can I do if I forgot my web UI login password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10-15 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is **10.0.0.138**. When logging in, the username is '**Admin**' and the password is '**Admin**'.

Technical Specifications

Hardware Specifications

- LAN Interface: Four 10/100Mbps LAN ports
- DSL Interface: One RJ11 Internet port
- Wireless Interface (2.4Ghz): IEEE 802.11b/g/n
- USB Interface: Complaint USB 2.0

Operating Voltage

- Input: 100~240V (±10%), 50~60Hz
- Output: 12VDC, 1A EU

Temperature

- Operating: 32°F~104°F (0°C~40°C)
- Non-Operating: -4°F~149°F (-20°C~65°C)

Humidity

- Operating: 10%~90% non-condensing
- Non-Operating: 5%~95% non-condensing

ADSL2 Standards

- ITU-T G.992.3 (G.dmt.bis) Annex A/J/K/L/M)

VDSL2 Standards

- ITU G.992.3 (G.dmt.bis) Annex A/J/K/L/M
- Annex A, B over POTS
- G.998.4 (G.INP)
- G.993.5 (G.Vector)
- ITU-T G.992.5 Annex A/L/M

Wireless Security

- 64/128bit WEP, WPA/WPA2-Personal, WPA/WPA2-Mixed Mode, WPS (PIN & PBC)

VDSL2+ Standards

- ITU G.992.5 Annex A/L/M

VDSL Data Transfer Rate

- VDSL2 up to 100M/50M

Wireless Frequency Range

- IEEE 802.11b: 2400 MHz~2497 MHz
- IEEE 802.11g: 2400 MHz~2497 MHz
- IEEE 802.11n: 2400 MHz~2497 MHz

Wireless Bandwidth Rate

- IEEE 802.11b: 11, 5.5, 2, and 1 Mbps
- IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps
- IEEE 802.11n: 6.5 to 300 Mbps

Wireless Channel Numbers

- IEEE 802.11b: Channels 1~11 (USA), 1~13 (Europe), 1~14 (Japan)
- IEEE 802.11g: Channels 1~11 (USA), 1~13 (Europe), 1~14 (Japan)
- IEEE 802.11n: Channels 1~11 (USA), 1~13 (Europe), 1~14 (Japan)

Antenna Type

- 2X2 PCB Antenna

Certifications

- CE

Dimensions & Weight

- 195 x 123 x 34 mm (7.68 x 4.84 x 1.34 in) (Length x Width x Height)
- 314.97 grams (0.694 lbs)