Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DGL-4500 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DGL-4500. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

Transmission Rate: Select the transmit rate. It is strongly suggested to select **Best (Auto)** for best performance.

Channel Width: Select the Channel Width:
Auto 20/40 - Select if you are using both 802.11n and non-802.11n wireless devices.
20MHz - Select if you are not using any 802.11n wireless clients. This is the default setting.
40MHz - Select if you are using 802.11n wireless clients only.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DGL-4500. If Invisible is selected, the SSID of the DGL-4500 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DGL-4500 in order to connect to it.

Wireless Security: Refer to page 66 for more information regarding wireless security.

Network Settings

This section will allow you to change the local network settings of the router and to configure the DHCP settings.

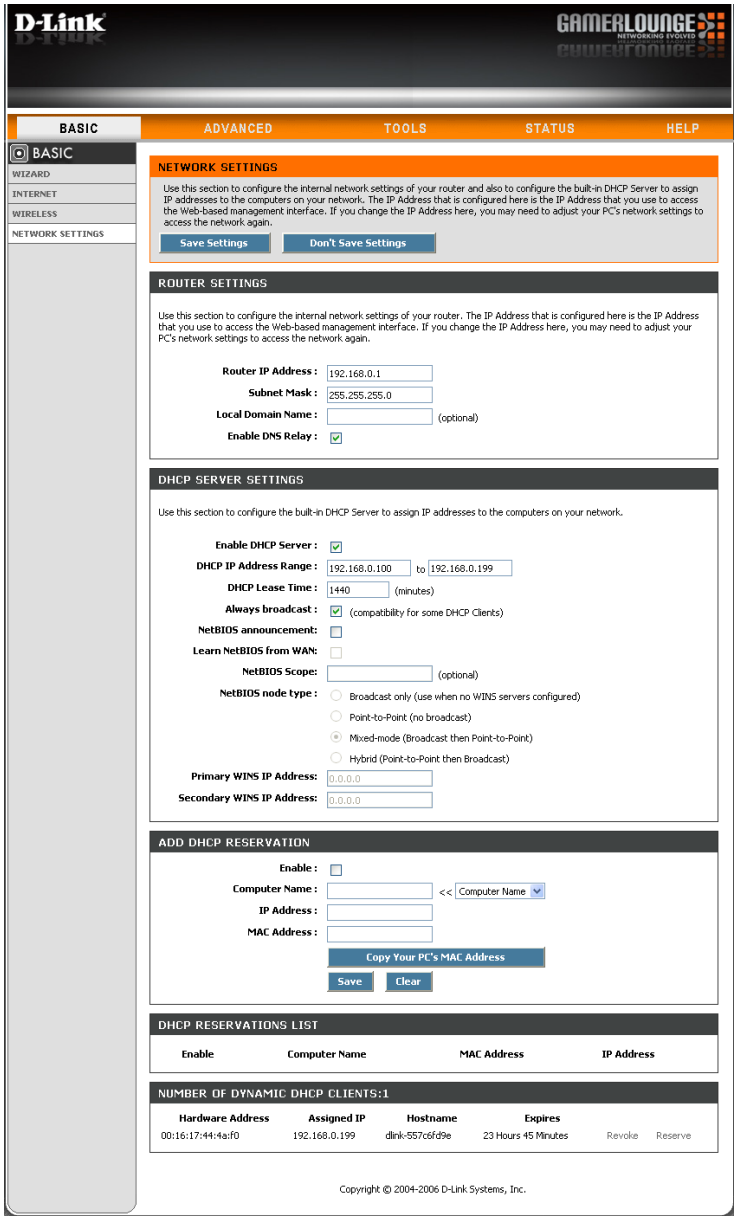
IP Address: Enter the IP address of the router. The default IP address is 192.168.0.1.

If you change the IP address, once you click Apply, you will need to enter the new IP address in your browser to get back into the configuration utility.

Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

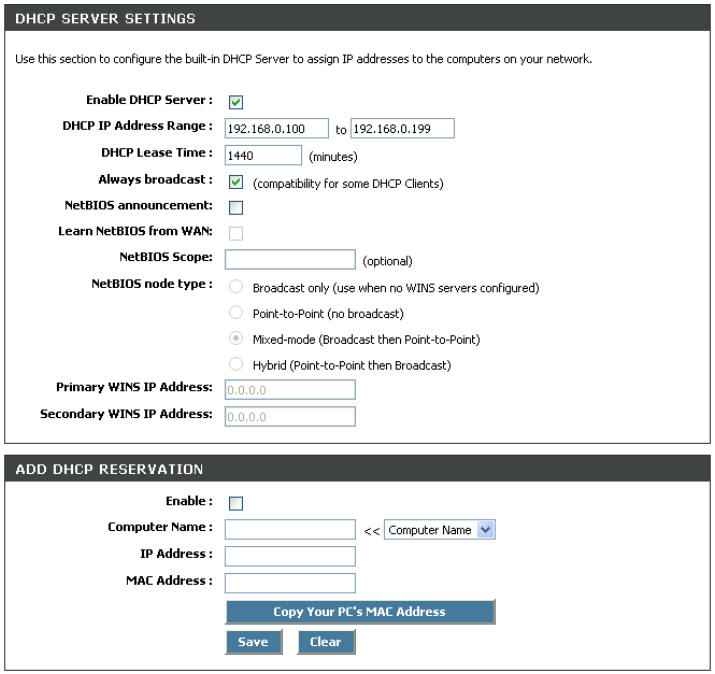
Local Domain: Enter the Domain name (Optional).

Enable DNS Relay: Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.



DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The router has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DGL-4500. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.



Enable DHCP Server: Check this box to enable the DHCP server on your router. Uncheck to disable this function.

DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

Note: If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.

DHCP Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

Always Broadcast: Enable this feature to broadcast your networks DHCP server to LAN/WLAN clients.

NetBIOS Announcement: NetBIOS allows LAN hosts to discover all other computers within the network, enable this feature to allow the DHCP Server to offer NetBIOS configuration settings.

Learn NetBIOS from WAN: Enable this feature to allow WINS information to be learned from the WAN side, disable to allow manual configuration.

NetBIOS Scope: This feature allows the configuration of a NetBIOS 'domain' name under which network hosts operates. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

NetBIOS Node: Select the different type of NetBIOS node; **Broadcast only**, **Point-to-Point**, **Mixed-mode**, and **Hybrid**.

WINS IP Address: Enter your WINS IP address

DHCP Reservation

If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

Note: This IP address must be within the DHCP IP Address Range.

Enable: Check this box to enable the reservation.

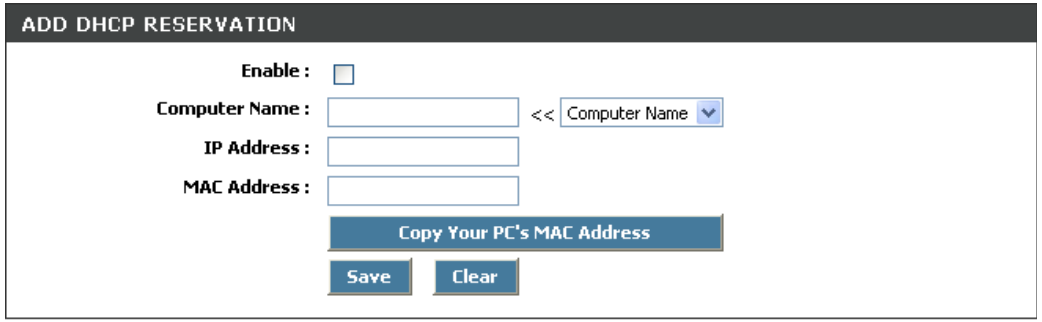
Computer Name: Enter the computer name or select from the drop-down menu and click **<<**.

IP Address: Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.

MAC Address: Enter the MAC address of the computer or device.

Copy Your PC's MAC Address: If you want to assign an IP address to the computer you are currently on, click this button to populate the fields.

Save: Click **Save** to save your entry. You must click **Save Settings** at the top to activate your reservations.



Virtual Server

The DGL-4500 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DGL-4500 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DGL-4500 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DGL-4500 redirects the external service request to the appropriate server within the LAN network.

The DGL-4500 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. There are pre-defined virtual services already in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

For a list of ports for common applications, please visit **http://support.dlink.com/faq/view.asp?prod_id=1191**.

This will allow you to open a single port. If you would like to open a range of ports, refer to page 35.

Enable: Check this box to enable the rule.

Name: Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

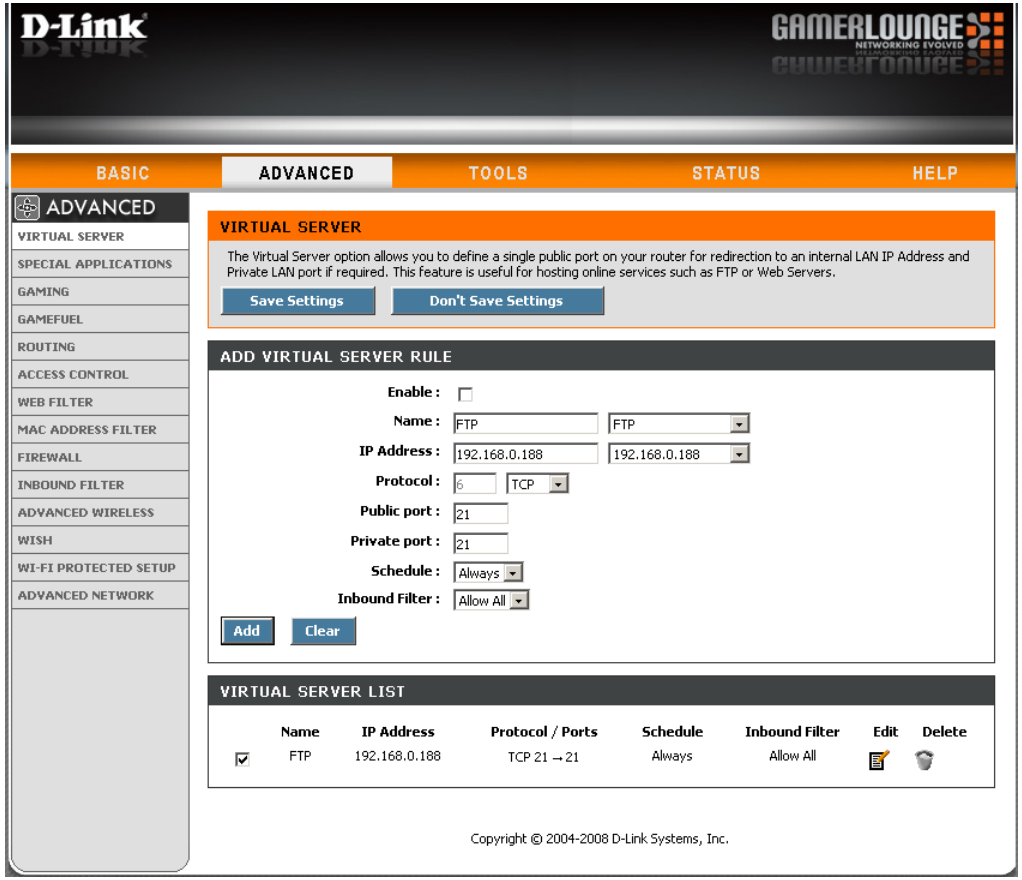
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click <<.

Protocol Type: Select **TCP**, **UDP**, or **Both** from the drop-down menu.

Private Port/ Public Port: Enter the port that you want to open next to Private Port and Public Port. The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.

Schedule: The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools** > **Schedules** section.

Inbound Filter: Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.



Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DGL-4500. If you need to run applications that require multiple connections, specify the port normally associated with an application in the “Trigger Port” field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DGL-4500 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

Enable: Check this box to enable the rule.

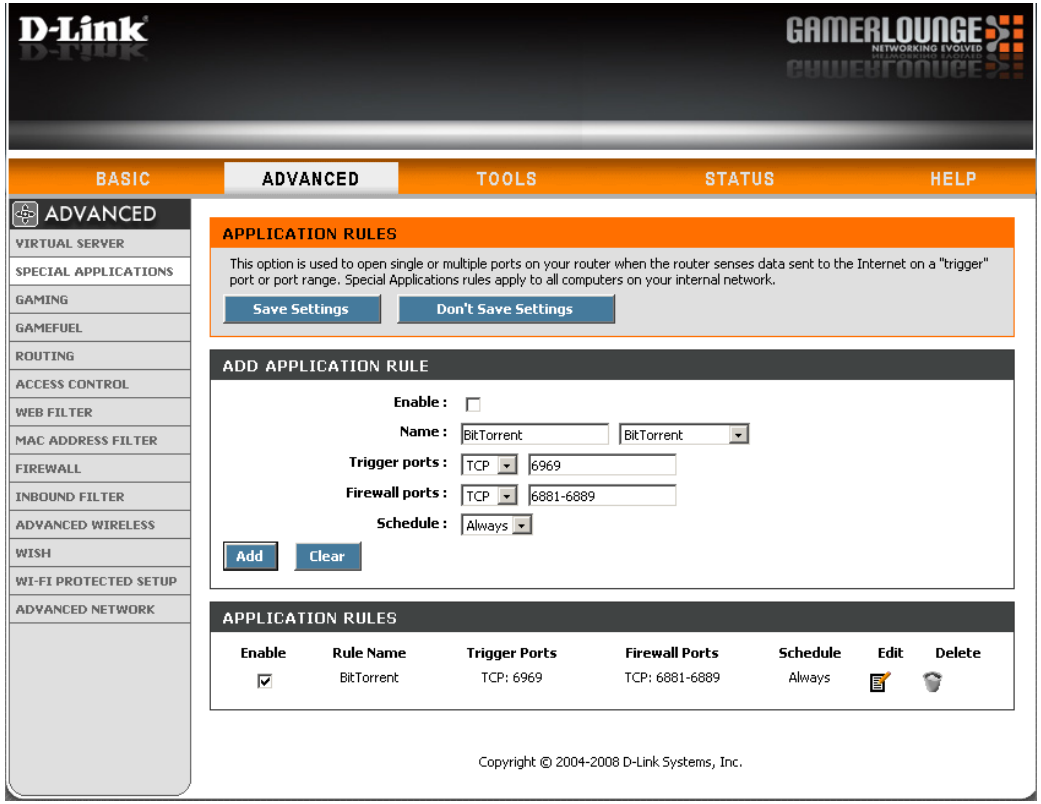
Name: Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click <<.

Trigger: This is the port used to trigger the application. It can be either a single port or a range of ports.

Traffic Type: Select the protocol of the trigger port (TCP, UDP, or Both).

Firewall: This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Traffic Type: Select the protocol of the firewall port (TCP, UDP, or Both).



Schedule: The schedule of time when the Application Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools** > **Schedules** section.

Gaming

This will allow you to open a single port or a range of ports.

Enable: Check this box to enable the rule.

Name: Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

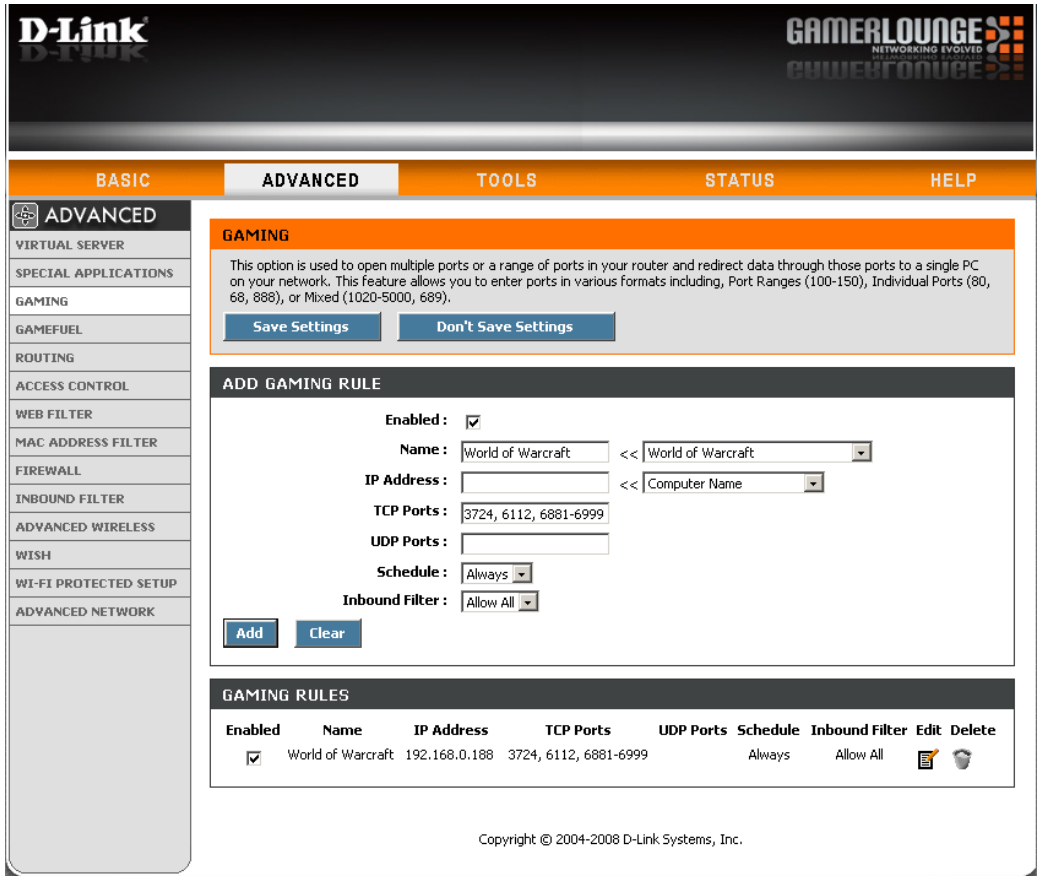
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click <<.

TCP/UDP: Enter the TCP and/or UDP port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common.

Example: 24,1009,3000-4000

Schedule: The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools** > **Schedules** section.

Inbound Filter: Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.



GameFuel

The GameFuel option helps improve your network gaming performance by prioritizing applications. By default the GameFuel settings are disabled and application priority is not classified automatically.

Enable GameFuel: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

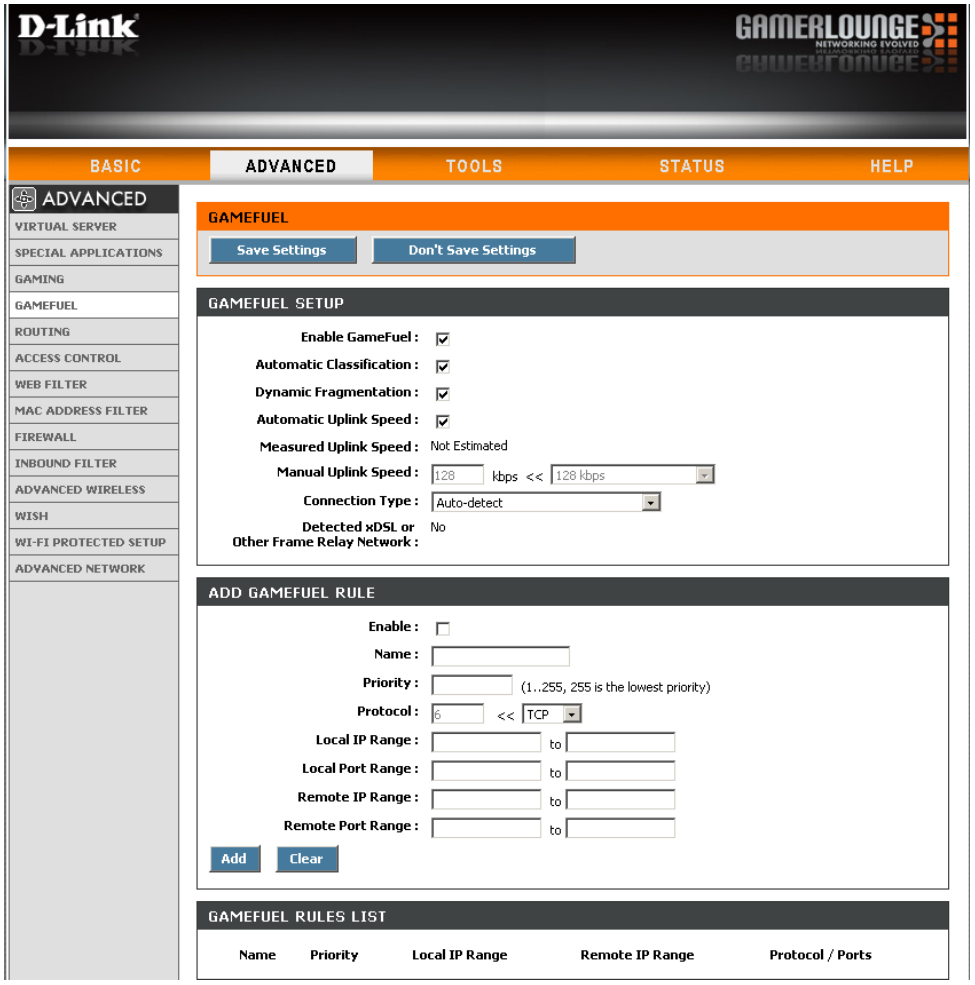
Automatic Classification: This option is enabled by default. This will allow your router to automatically determine the network priority of running programs.

Dynamic Fragmentation: This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones.

Automatic Uplink Speed: This option is enabled by default when the GameFuel option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

Measured Uplink Speed: This displays the detected uplink speed.

Manual Uplink Speed: The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.



Connection Type: By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either “Static” or “DHCP” in the Internet settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

Detected xDSL: When Connection Type is set to automatic, the automatically detected connection type is displayed here.

Routing

Use the routing option to define fixed routes to specific destinations.

Enable: Check this box to enable the rule.

Name: Enter a name for the rule.

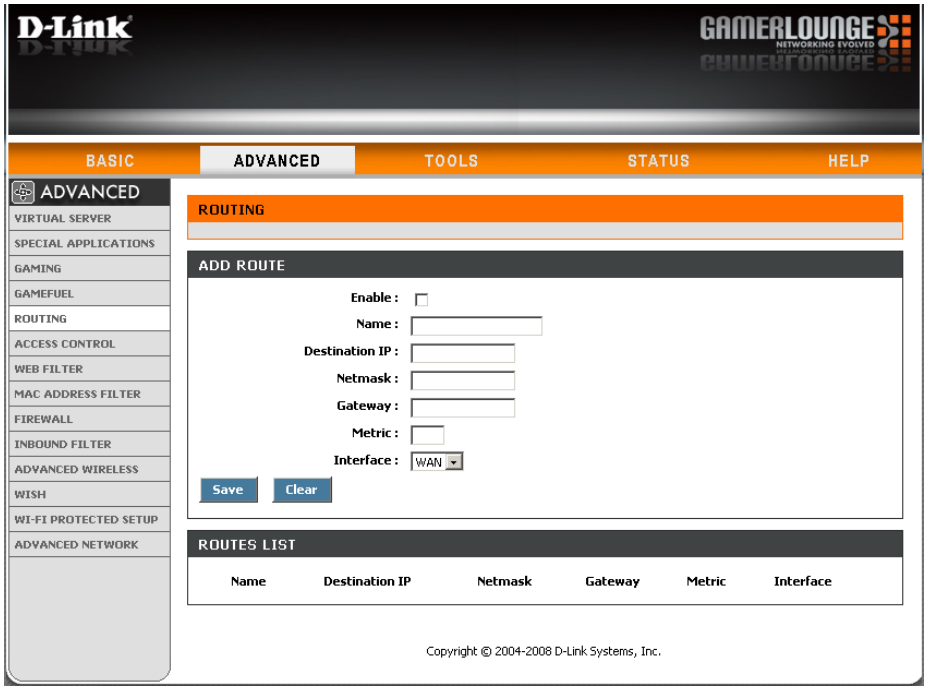
Destination IP: Enter the destination IP address or network address.

Netmask: Enter the destination subnet mask.

Gateway: Enter the destination's gateway IP address.

Metric: Enter the route's priority. The higher the number the lower the priority.

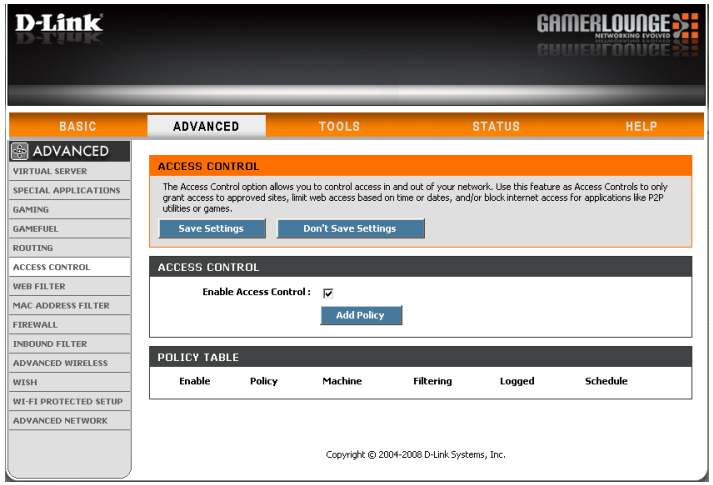
Interface: Select LAN or WAN from the drop-down menu.



Access Control

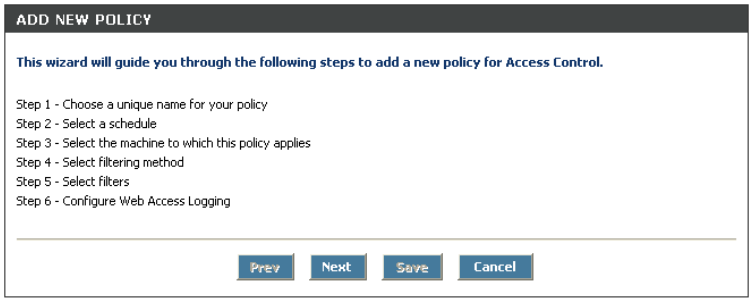
The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

Add Policy: Click the **Add Policy** button to start the Access Control Wizard.

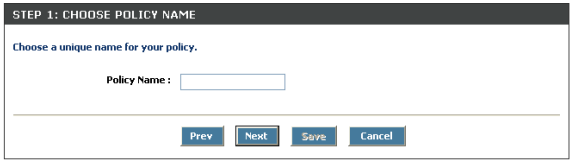


Access Control Wizard

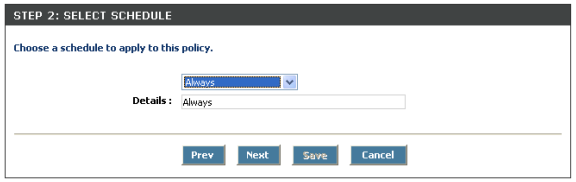
Click **Next** to continue with the wizard.



Enter a name for the policy and then click **Next** to continue.

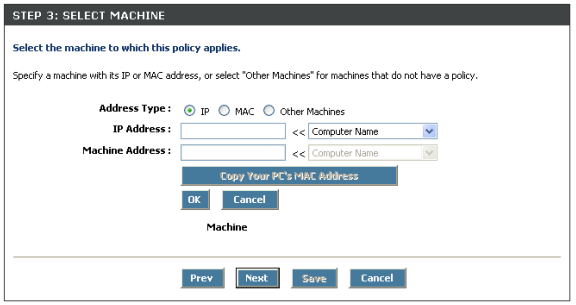


Select either **Always**, **Never**, or **Define a new schedule** from the drop-down menu and then click **Next** to continue.

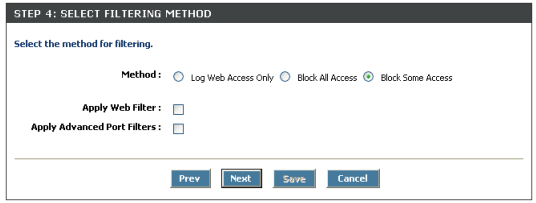


Enter the following information and then click **Next** to continue.

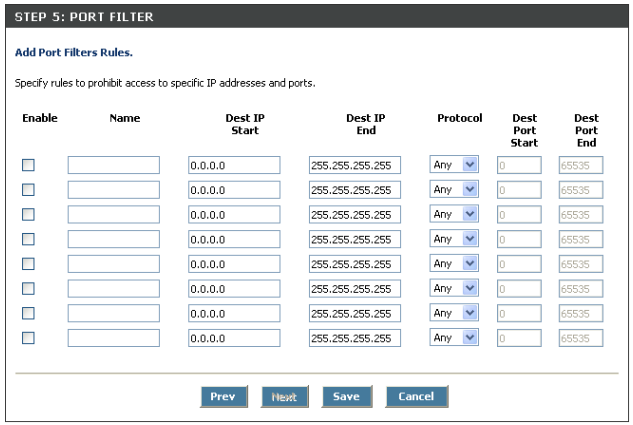
- **Address Type** - Select IP address, MAC address, or Other Machines.
- **IP Address** - Enter the IP address of the computer you want to apply the rule to.



Select the filtering method and then click **Next** to continue.



If you selected **Block Some Access** and **Apply Advanced Port Filter**, then the following screen will appear.

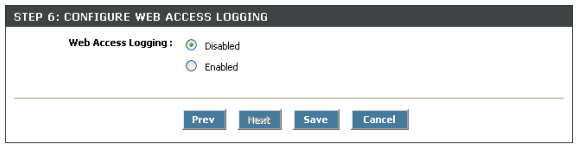


Enter the rule:

Enable - Check to enable the rule.
Name - Enter a name for your rule.
Dest IP Start - Enter the starting IP address.
Dest IP End - Enter the ending IP address.
Protocol - Select the protocol.
Dest Port Start - Enter the starting port number.
Dest Port End - Enter the ending port number.

To enable web logging, click **Enable**.

Click **Save** to save the access control rule.

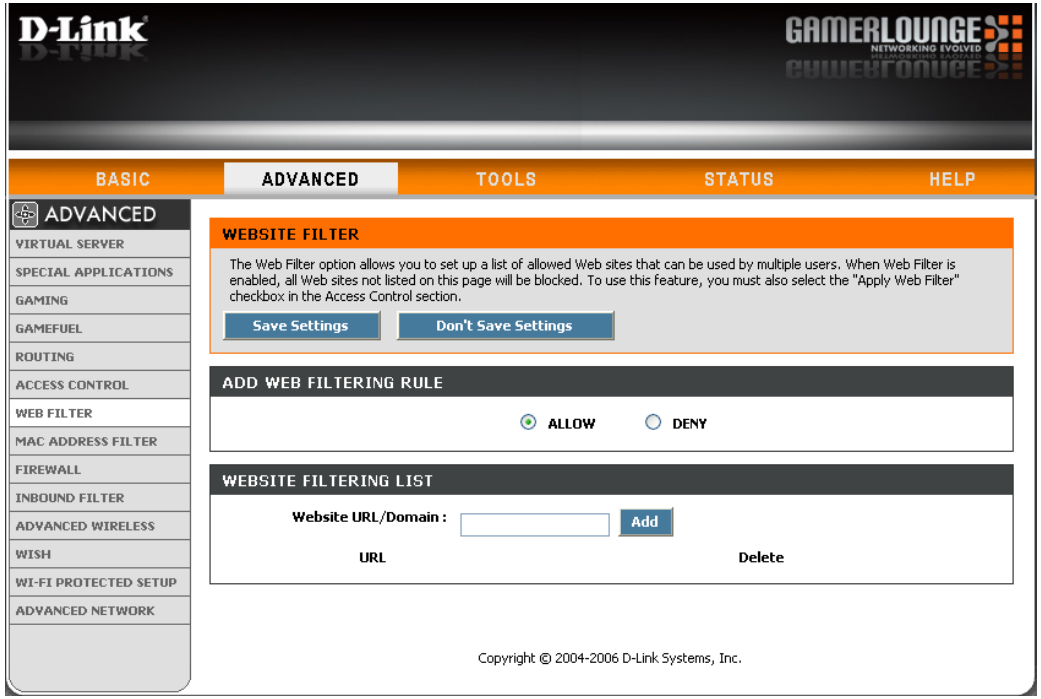


Website Filters

Website Filters are used to allow you to set up a list of allowed Web sites that can be used by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Add**, and then click **Save Settings**. You must also select **Apply Web Filter** under the Access Control section (page 40).

Add Website Filtering Rule: Select **Allow** or **Deny**.

Website Filtering List: Enter the keywords or URLs that you want to allow or deny and then click **Add**.



MAC Address Filters

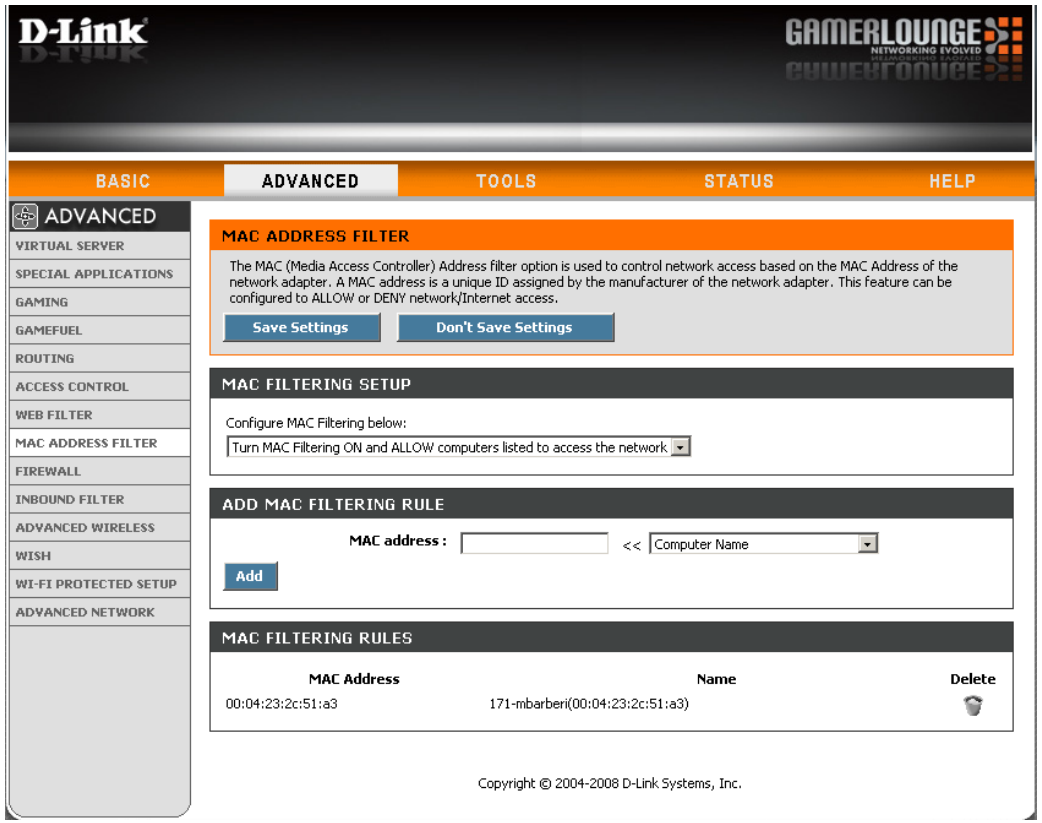
Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

Configure MAC Filtering: Select Turn MAC Filtering Off, allow MAC addresses listed below, or deny MAC addresses listed below from the drop-down menu.

MAC Address: Enter the MAC address you would like to filter. To find the MAC address on a computer, please refer to the Networking Basics section in this manual.

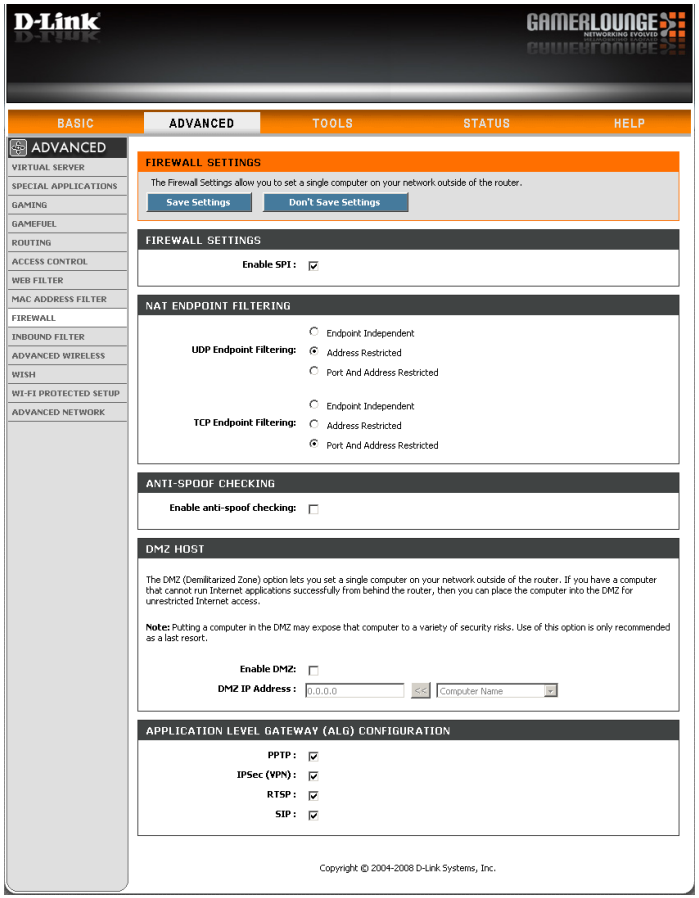
DHCP Client: Select a DHCP client from the drop-down menu and click << to copy that MAC Address.

Add: Click to add the rule.



Firewall Settings

A firewall protects your network from the outside world. The D-Link DGL-4500 offers a firewall type functionality.



Enable SPI: SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.

NAT Endpoint Filtering: Select one of the following for TCP and UDP ports:
Endpoint Independent - Any incoming traffic sent to an open port will be forwarded to the application that opened the port. The port will close if idle for 5 minutes.

Address Restricted - Incoming traffic must match the IP address of the outgoing connection.

Address and Port Restriction - Incoming traffic must match the IP address and port of the outgoing connection.

Anti-Spoofing: Click to enable Anti-Spoofing protection.

Enable DMZ Host: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer. **Note:** Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains it's IP address automatically using DHCP, be sure to make a static reservation on the **Basic** > **DHCP** page so that the IP address of the DMZ machine does not change.

Non-UDP/TCP/ICMP LAN Sessions: Enable this feature to allow the router' NAT to track application that uses protocols other than UDP, TCP or ICMP.

ALG: Check the PPTP, IPSec, RTSP, and SIP boxes to allow pass-through.

Inbound Filters

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range. Inbound Filters can be used with Virtual Server, Port Forwarding, or Remote Administration features.

Name: Enter a name for the inbound filter rule.

Action: Select **Allow** or **Deny**.

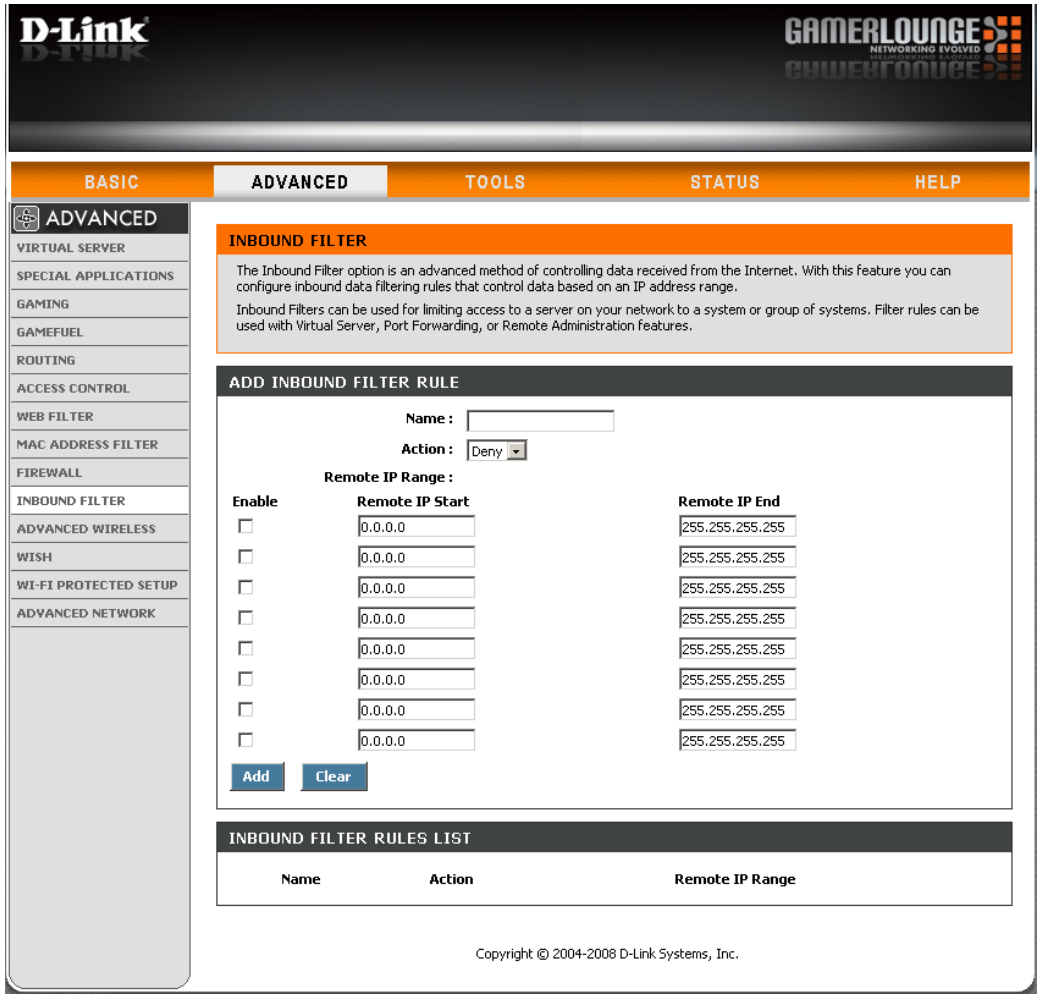
Enable: Check to enable rule.

Source IP Start: Enter the starting IP address. Enter 0.0.0.0 if you do not want to specify an IP range.

Source IP End: Enter the ending IP address. Enter 255.255.255.255 if you do not want to specify and IP range.

Add: Click the **Add** button to apply your settings. You must click **Save Settings** at the top to save the settings.

Inbound Filter Rules List: This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.



Advanced Wireless Settings

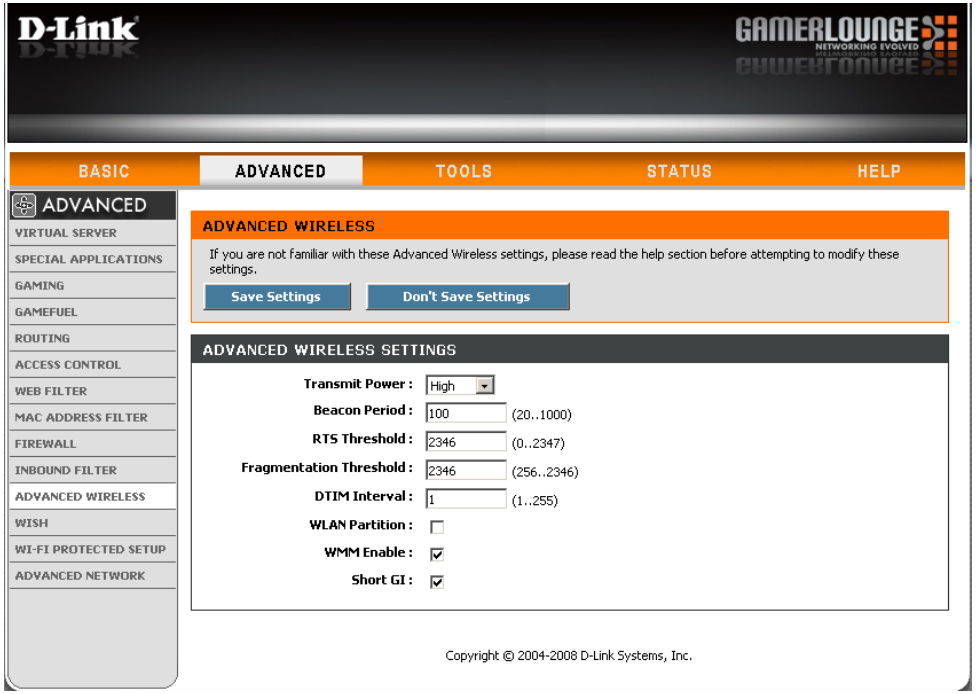
Transmit Power: Set the transmit power of the antennas.

Beacon Period: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

RTS Threshold: This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation Threshold: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

DTIM Interval: (Delivery Traffic Indication Message) 3 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.



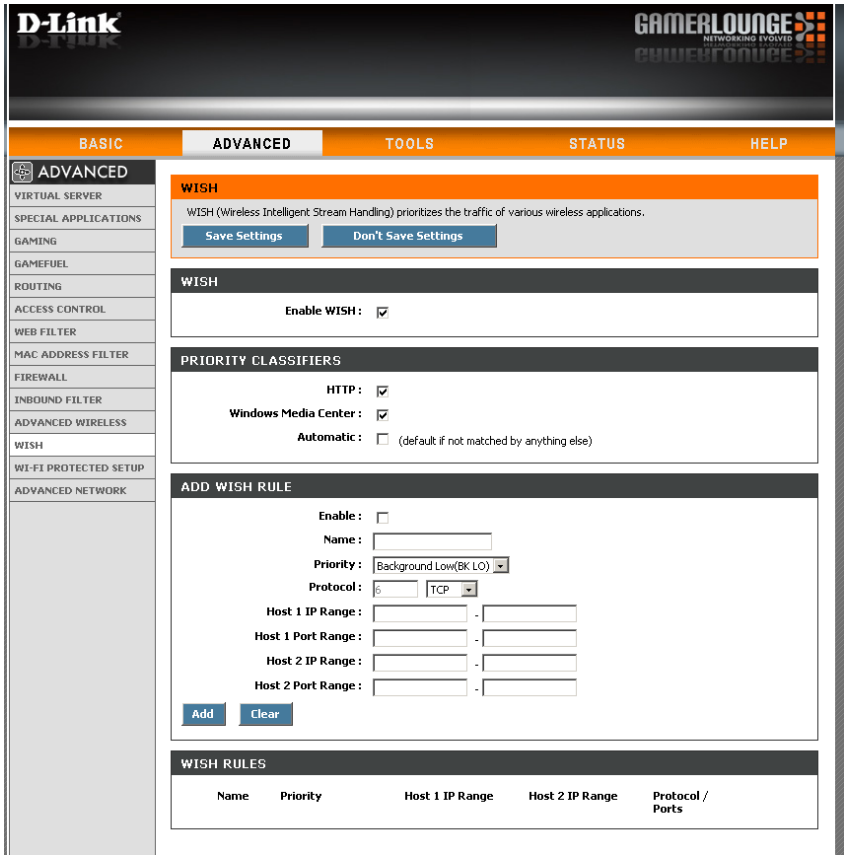
WLAN Partition: Enabling WLAN Partition prevents associated wireless clients from communicating with each other.

WMM Function: WMM is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

WISH Settings

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.



Enable WISH: Enable this option if you want to allow WISH to prioritize your traffic.

HTTP: Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Windows Media Center: Enables the router to recognize certain audio and video streams generated by a Windows® Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows® Media Extenders, such as the Xbox 360.

Automatic: When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

WISH Rules: A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

Name: Create a name for the rule that is meaningful to you.

Priority: The priority of the message flow is entered here. The four priorities are defined as:

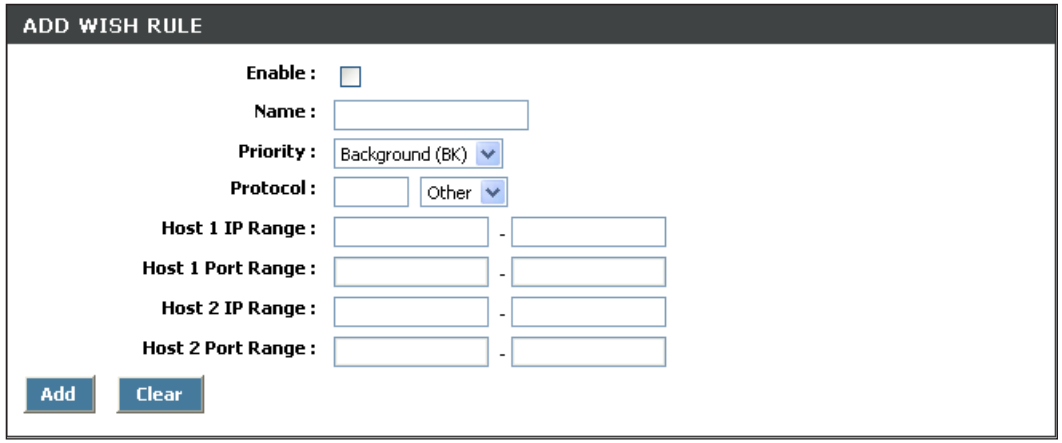
BK: Background (least urgent)
BE: Best Effort.
VI: Video
VO: Voice (most urgent)

Protocol: The protocol used by the messages.

Host IP Range: The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host Port Range: The rule applies to a flow of messages for which host's port number is within the range set here.

Add: Click to add the rule.



Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the “Initial setup” as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy, as depressing a button for the Push-Button Method or correctly entering the 8-digit code for the Pin-Code Method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

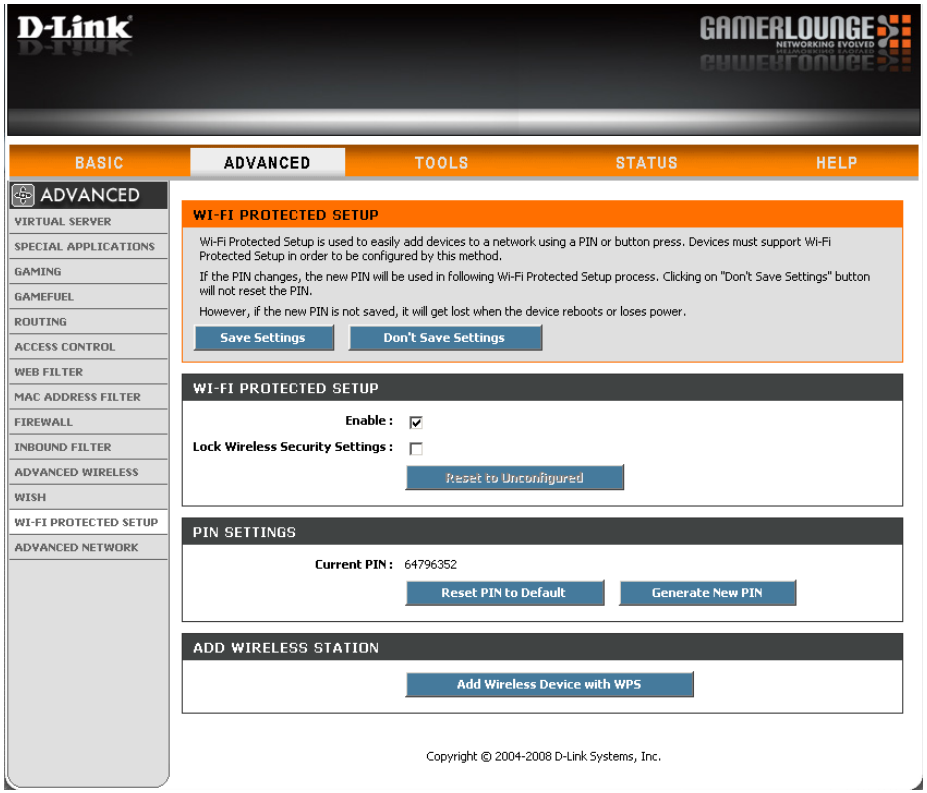
Enable: Enable the Wi-Fi Protected Setup feature.

Lock Wireless Security Settings: Locking the wireless security settings prevents the settings from being changed by the Wi-Fi Protected Setup feature of the router. Devices can still be added to the network using Wi-Fi Protected Setup. However, the settings of the network will not change once this option is checked.

PIN Settings: A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator (“admin” account) can change or reset the PIN.

Current PIN: Shows the current value of the router’s PIN.

Reset PIN to Default: Restore the default PIN of the router.



Generate New PIN: Create a random number that is a valid PIN. This becomes the router’s PIN. You can then copy this PIN to the user interface of the registrar.

Add Wireless Station: This Wizard helps you add wireless devices to the wireless network.

The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

Add Wireless Device Wizard: Start the wizard.

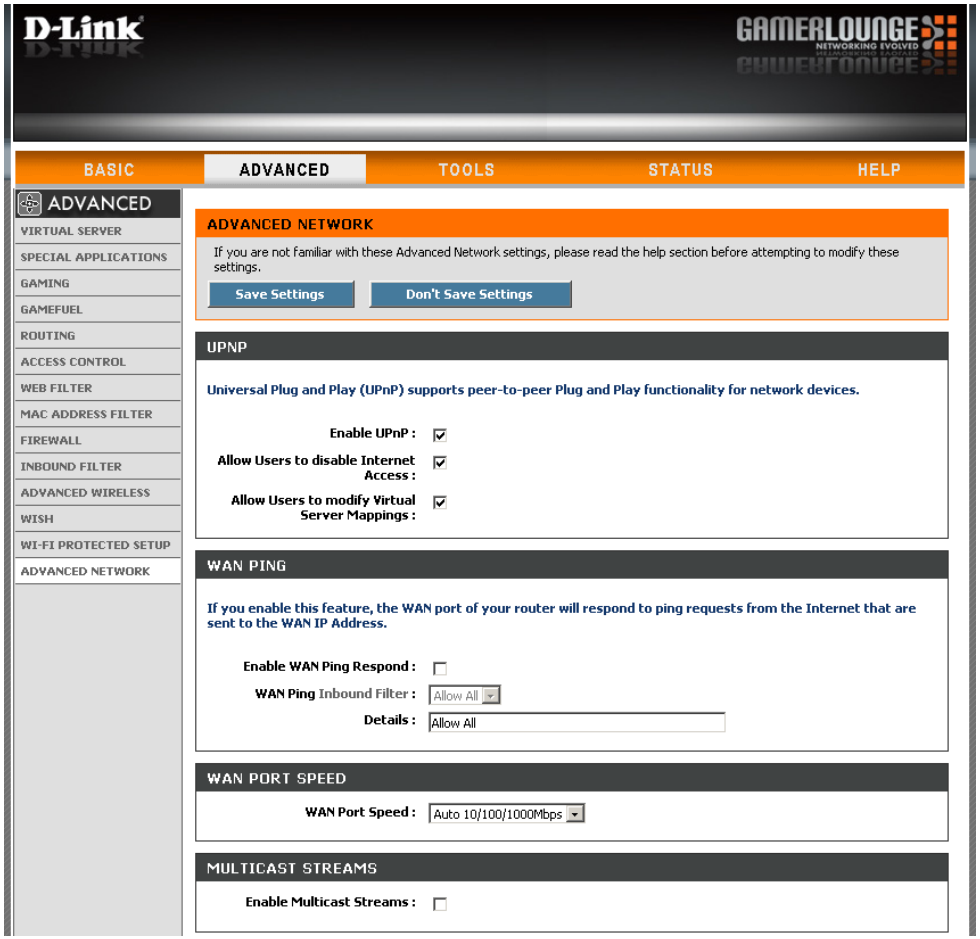
Advanced Network Settings

UPnP Settings: To use the Universal Plug and Play (UPnP™) feature click on **Enabled**. UPnP provides compatibility with networking equipment, software and peripherals.

WAN Ping: Unchecking the box will not allow the DGL-4500 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be “pinged”.

WAN Port Speed: You may set the port speed of the Internet port to 10Mbps, 100Mbps, or auto. Some older cable or DSL modems may require you to set the port speed to 10Mbps.

Multicast streams: Check the box to allow multicast traffic to pass through the router from the Internet.



Administrator Settings

This page will allow you to change the Administrator and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. **Admin** has read/write access while **User** has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.

Admin Password: Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

User Password: Enter the new password for the User login. If you login as the User, you can only see the settings, but cannot change them.

Gateway Name: Enter a name for the DGL-4500 router.

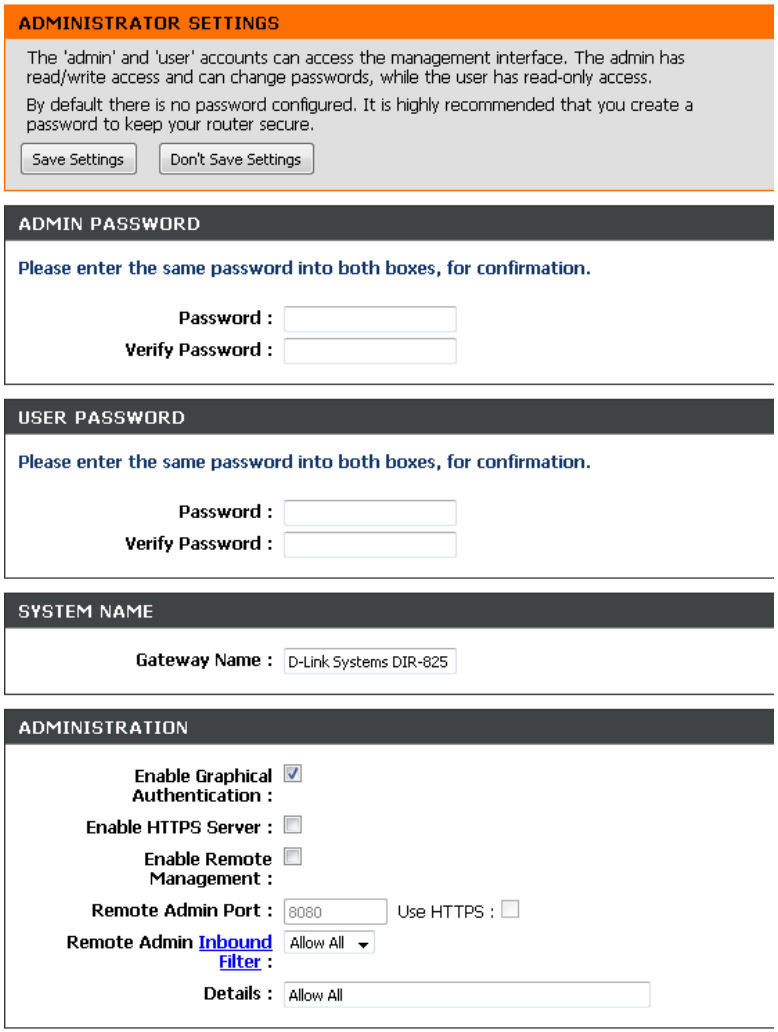
Enable Graphical Authentication: Enables a challenge-response test to require users to type letters or numbers from a distorted image displayed on the screen to prevent online hackers and unauthorized users from gaining access to your router's network settings.

Enable HTTPS Server: Check this option to enable HTTPS server through remote management.

Remote Management: Remote management allows the DGL-4500 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

Remote Admin Port: The port number used to access the DGL-4500.
Example: http://x.x.x.x:8080 whereas x.x.x.x is the Internet IP address of the DGL-4500 and 8080 is the port used for the Web Management interface.

Inbound Filter: This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.



Time Settings

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

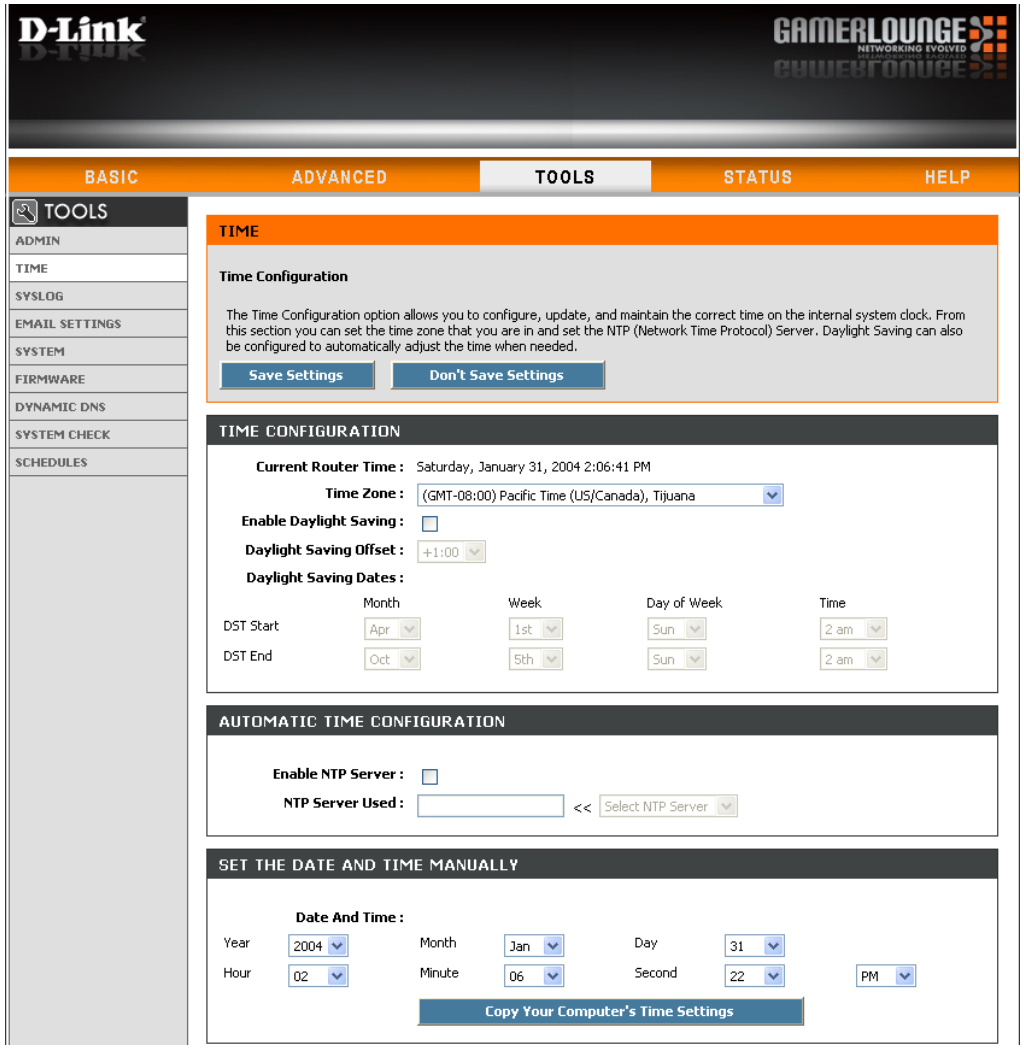
Time Zone: Select the Time Zone from the drop-down menu.

Daylight Saving: To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

Enable NTP Server: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

NTP Server Used: Enter the NTP server or select one from the drop-down menu.

Manual: To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Set Time**. You can also click **Copy Your Computer's Time Settings**.

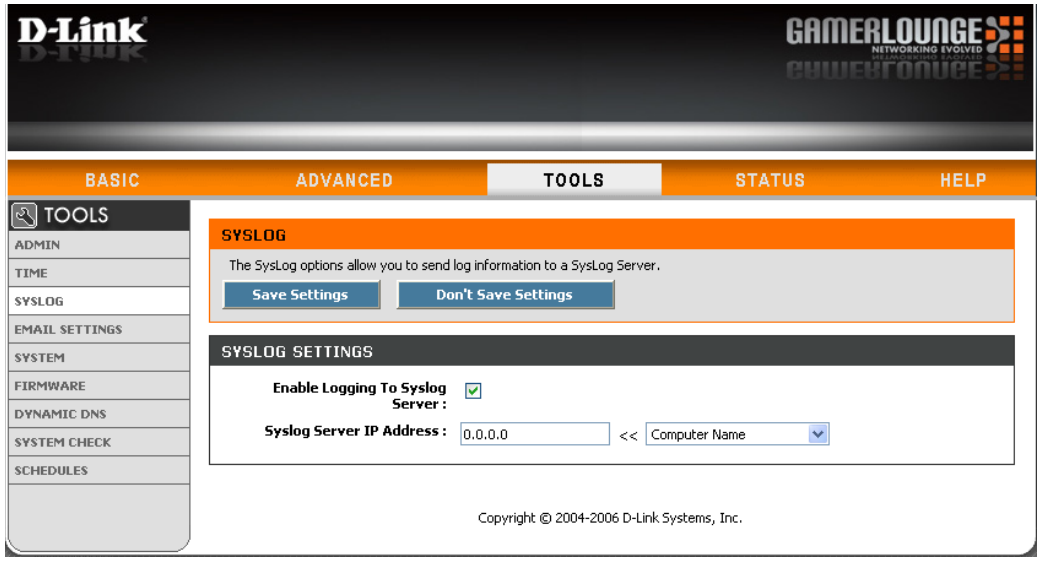


SysLog

The Broadband Router keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server on your network.

Enable Logging to SysLog Server: Check this box to send the router logs to a SysLog Server.

SysLog Server IP Address: The address of the SysLog server that will be used to send the logs. You may also select your computer from the drop-down menu (only if receiving an IP address from the router via DHCP).



Email Settings

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

Enable Email Notification: When this option is enabled, router activity logs are e-mailed to a designated email address.

From Email Address: This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

To Email Address: Enter the email address where you want the email sent.

SMTP Server Address: Enter the SMTP server address for sending email. If your SMTP server requires authentication, select this option.

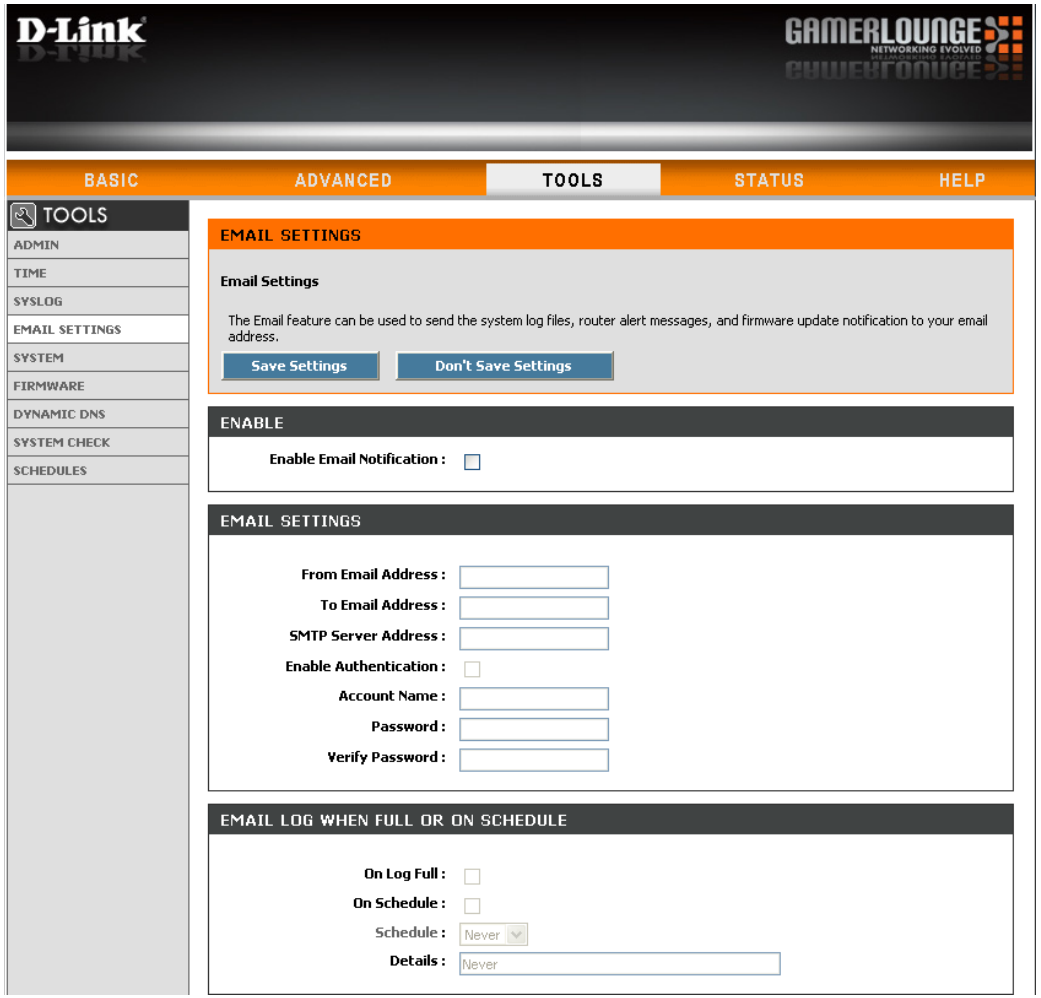
Enable Authentication: Check this box if your SMTP server requires authentication.

Account Name: Enter your account for sending email.

Password: Enter the password associated with the account. Re-type the password associated with the account.

On Log Full: When this option is selected, logs will be sent via email when the log is full.

On Schedule: Selecting this option will send the logs via email according to schedule.



Schedule: This option is enabled when On Schedule is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to **Tools > Schedules**.

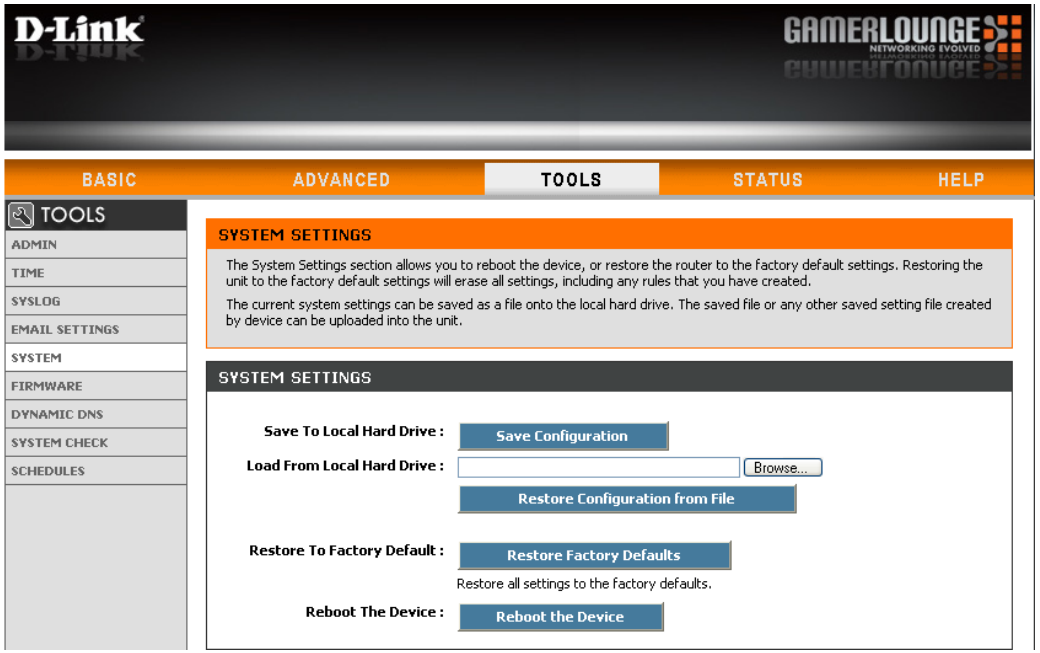
System Settings

Save Settings to Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the Save button. You will then see a file dialog, where you can select a location and file name for the settings.

Load Settings from Local Hard Drive: Use this option to load previously saved router configuration settings. First, use the Browse control to find a previously save file of configuration settings. Then, click the Load button to transfer those settings to the router.

Restore to Factory Default Settings: This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the Save button above.

Reboot Device: Click to reboot the router.



Update Firmware

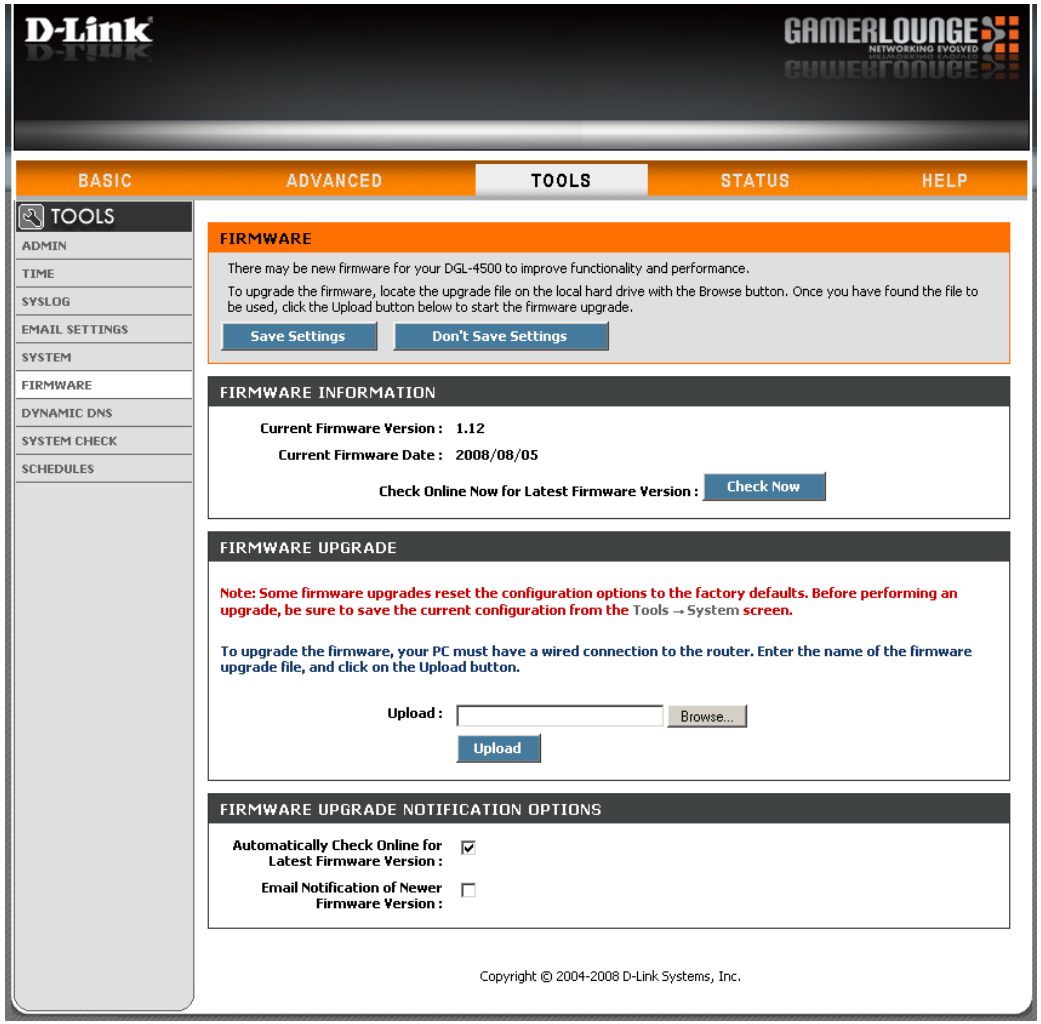
You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Upgrade: Click on **Check Online Now for Latest Firmware Version** to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

Browse: After you have downloaded the new firmware, click **Browse** to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade.

Notifications Options: Check **Automatically Check Online for Latest Firmware Version** to have the router check automatically to see if there is a new firmware upgrade.

Check **Email Notification of Newer Firmware Version** to have the router send an email when there is a new firmware available.



Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc…) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.

DDNS: Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.

Server Address: Choose your DDNS provider from the drop down menu.

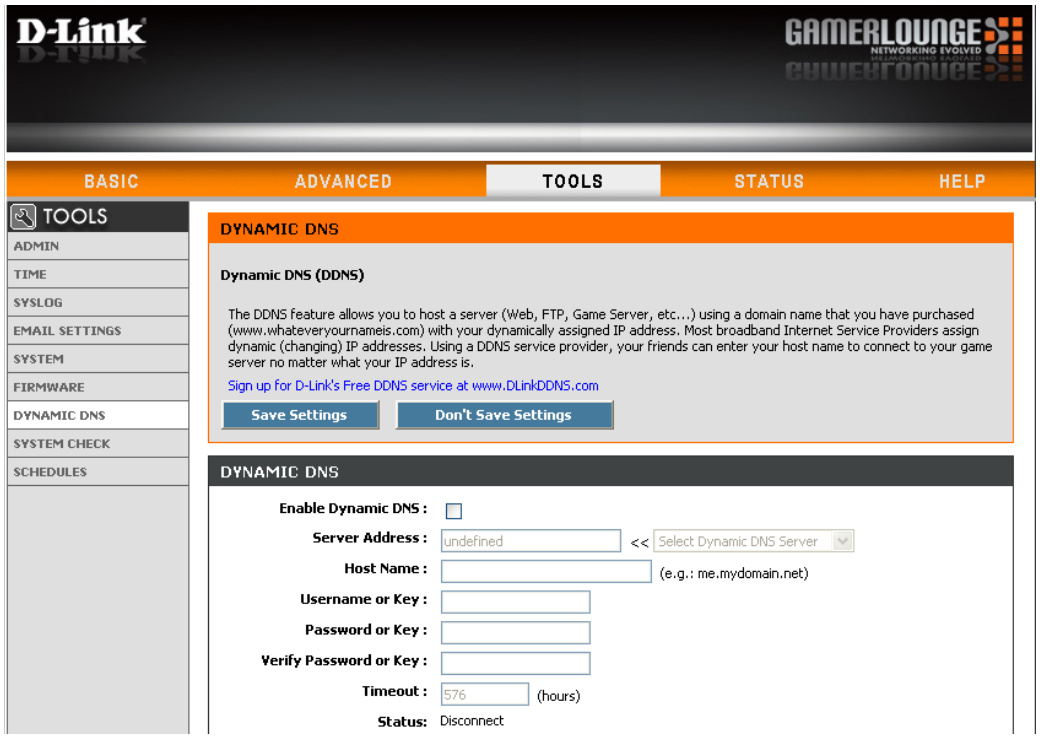
Host Name: Enter the Host Name that you registered with your DDNS service provider.

Username or Key: Enter the Username for your DDNS account.

Password or Key: Enter the Password for your DDNS account.

Timeout: Enter a time (in hours).

Status: Displays the current status.



System Check

Ping Test: The Ping Test is used to send Ping packets to test if a computer is on the Internet. Enter the IP Address that you wish to Ping, and click **Ping**.

Ping Results: The results of your ping attempts will be displayed here.