

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.

D-Link **GAMERLOUNGE**

BASIC **ADVANCED** **TOOLS** **STATUS** **HELP**

NETWORK SETTINGS

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP Server to assign IP addresses to the computers on your network. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Save Settings Don't Save Settings

ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address: 192.168.0.1
 Subnet Mask: 255.255.255.0
 Local Domain Name: (optional)
 Enable DNS Relay:

DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server:
 DHCP IP Address Range: 192.168.0.100 to 192.168.0.199
 DHCP Lease Time: 1440 (minutes)
 Always broadcast: (compatibility for some DHCP Clients)
 NetBIOS announcement:
 Learn NetBIOS from WAN:
 NetBIOS Scope: (optional)
 NetBIOS node type: Broadcast only (use when no WINS servers configured)
 Point-to-Point (no broadcast)
 Mixed-mode (Broadcast then Point-to-Point)
 Hybrid (Point-to-Point then Broadcast)
 Primary WINS IP Address: 0.0.0.0
 Secondary WINS IP Address: 0.0.0.0

ADD DHCP RESERVATION

Enable:
 Computer Name: << Computer Name
 IP Address:
 MAC Address:
 Copy Your PC's MAC Address
 Save Clear

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS:1

Hardware Address	Assigned IP	Hostname	Expires	Revoke	Reserve
00:16:17:44:4a:f0	192.168.0.199	dlink-957c6fd9e	23 Hours 45 Minutes		

Copyright © 2004-2006 D-Link Systems, Inc.

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 SERVER SETTINGS

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range : to

DHCP Lease Time : (minutes)

Always broadcast : (compatibility for some DHCP Clients)

NetBIOS announcement :

Learn NetBIOS from WAN :

NetBIOS Scope : (optional)

NetBIOS node type : Broadcast only (use when no WINS servers configured)
 Point-to-Point (no broadcast)
 Mixed-mode (Broadcast then Point-to-Point)
 Hybrid (Point-to-Point then Broadcast)

Primary WINS IP Address :

Secondary WINS IP Address :

ADD DHCP RESERVATION

Enable :

Computer Name : <<

IP Address :

MAC 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.

ADD DHCP RESERVATION

Enable:

Computer Name: << Computer Name ▾

IP Address:

MAC Address:

[Copy Your PC's MAC Address](#)

[Save](#) [Clear](#)

DHCP RESERVATIONS LIST			
Enable	Computer Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS:1					
Hardware Address	Assigned IP	Hostname	Expires	Revoke	Reserve
00:16:17:44:4a:f0	192.168.0.199	dlink-557c6fd9e	23 Hours 45 Minutes	Revoke	Reserve

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), your 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.

D-Link **GAMELOUNGE**
NETWORKING EVOLVED
GAMERLOUNGE

BASIC **ADVANCED** TOOLS STATUS HELP

ADVANCED

VIRTUAL SERVER

SPECIAL APPLICATIONS

GAMING

GAMEFUEL

ROUTING

ACCESS CONTROL

WEB FILTER

MAC ADDRESS FILTER

FIREWALL

INBOUND FILTER

ADVANCED WIRELESS

WISH

WI-FI PROTECTED SETUP

ADVANCED NETWORK

VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

ADD VIRTUAL SERVER RULE

Enable:

Name: FTP FTP

IP Address: 192.168.0.188 192.168.0.188

Protocol: 6 TCP

Public port: 21

Private port: 21

Schedule: Always

Inbound Filter: Allow All

Add Clear

VIRTUAL SERVER LIST

	Name	IP Address	Protocol / Ports	Schedule	Inbound Filter	Edit	Delete
<input checked="" type="checkbox"/>	FTP	192.168.0.188	TCP 21 → 21	Always	Allow All		

Copyright © 2004-2008 D-Link Systems, Inc.

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.

The screenshot shows the D-Link web interface for configuring Application Rules. The top navigation bar includes 'BASIC', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The left sidebar lists various configuration categories, with 'ADVANCED' selected. The main content area is titled 'APPLICATION RULES' and contains the following information:

APPLICATION RULES
This option is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.
[Save Settings] [Don't Save Settings]

ADD APPLICATION RULE

Enable:
 Name: BitTorrent [BitTorrent] [v]
 Trigger ports: TCP [6969]
 Firewall ports: TCP [6881-6889]
 Schedule: Always [v]

[Add] [Clear]

APPLICATION RULES

Enable	Rule Name	Trigger Ports	Firewall Ports	Schedule	Edit	Delete
<input checked="" type="checkbox"/>	BitTorrent	TCP: 6969	TCP: 6881-6889	Always	[Edit]	[Delete]

Copyright © 2004-2008 D-Link Systems, Inc.

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.

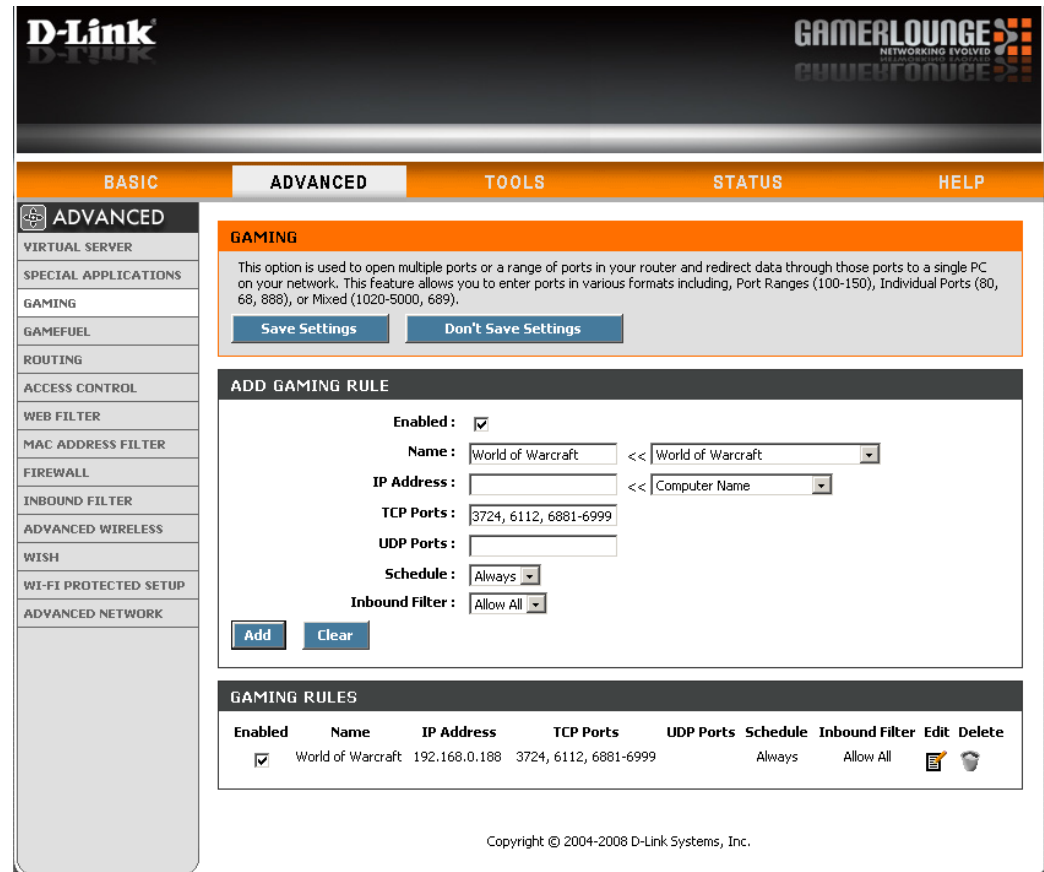
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the “Computer Name” drop-down menu. Select your computer and click 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

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.



D-Link **GAMERLOUNGE**
NETWORKING EVOLVED
ADVANCED NETWORKING

BASIC **ADVANCED** **TOOLS** **STATUS** **HELP**

ADVANCED

VIRTUAL SERVER
SPECIAL APPLICATIONS
GAMING
GAMEFUEL
ROUTING
ACCESS CONTROL
WEB FILTER
MAC ADDRESS FILTER
FIREWALL
INBOUND FILTER
ADVANCED WIRELESS
WISH
WI-FI PROTECTED SETUP
ADVANCED NETWORK

GAMING

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

[Save Settings](#) [Don't Save Settings](#)

ADD GAMING RULE

Enabled:

Name: World of Warcraft << World of Warcraft

IP Address: << Computer Name

TCP Ports: 3724, 6112, 6881-6999

UDP Ports:

Schedule: Always

Inbound Filter: Allow All

[Add](#) [Clear](#)

GAMING RULES

Enabled	Name	IP Address	TCP Ports	UDP Ports	Schedule	Inbound Filter	Edit	Delete
<input checked="" type="checkbox"/>	World of Warcraft	192.168.0.188	3724, 6112, 6881-6999		Always	Allow All	Edit	Delete

Copyright © 2004-2008 D-Link Systems, Inc.

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, 1.5Mbps/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.

The screenshot shows the D-Link GameFuel configuration page. The 'ADVANCED' tab is selected, and the 'GAMEFUEL' section is active. The 'GAMEFUEL SETUP' section includes the following options:

- Enable GameFuel:
- Automatic Classification:
- Dynamic Fragmentation:
- Automatic Uplink Speed:
- Measured Uplink Speed: Not Estimated
- Manual Uplink Speed: 128 kbps << 128 kbps
- Connection Type: Auto-detect
- Detected xDSL or Other Frame Relay Network: No

The 'ADD GAMEFUEL RULE' section includes the following fields:

- Enable:
- Name:
- Priority: (1..255, 255 is the lowest priority)
- Protocol: 6 << TCP
- Local IP Range: to
- Local Port Range: to
- Remote IP Range: to
- Remote Port Range: to

Buttons for 'Add' and 'Clear' are present. Below the configuration is a 'GAMEFUEL RULES LIST' table with columns for Name, Priority, Local IP Range, Remote IP Range, and Protocol / Ports.

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.

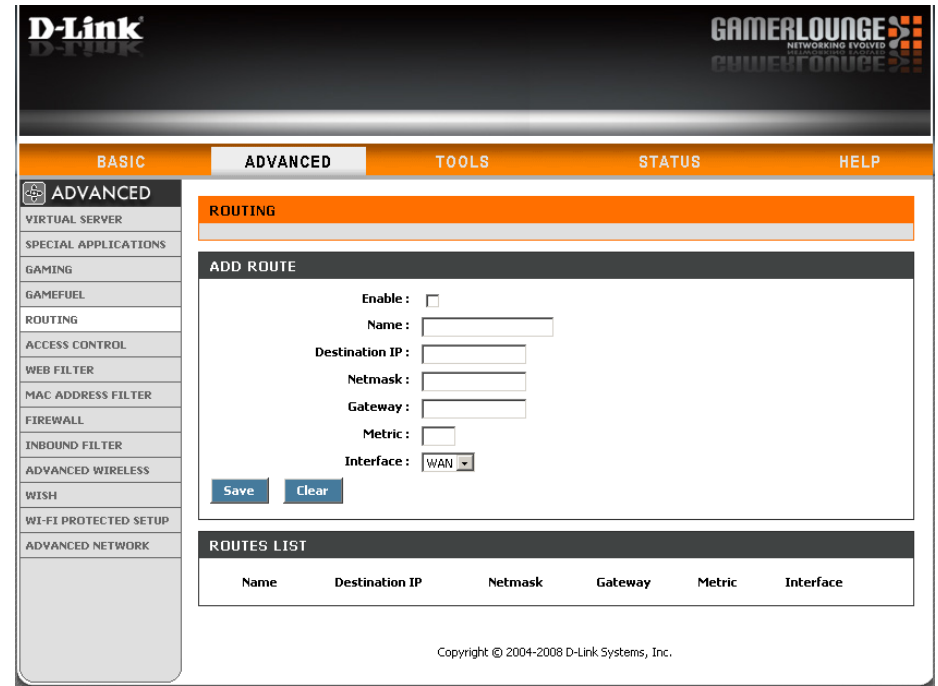
Destination IP: Enter the destination IP address or network address.

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.



D-Link **GAMERLOUNGE**
NETWORKING EVOLVED
ADVANCED NETWORKING
GAMERLOUNGE

BASIC **ADVANCED** TOOLS STATUS HELP

ADVANCED

VIRTUAL SERVER
SPECIAL APPLICATIONS
GAMING
GAMEFUEL
ROUTING
ACCESS CONTROL
WEB FILTER
MAC ADDRESS FILTER
FIREWALL
INBOUND FILTER
ADVANCED WIRELESS
WISH
WI-FI PROTECTED SETUP
ADVANCED NETWORK

ROUTING

ADD ROUTE

Enable:
Name:
Destination IP:
Netmask:
Gateway:
Metric:
Interface: WAN ▾

Save Clear

ROUTES LIST

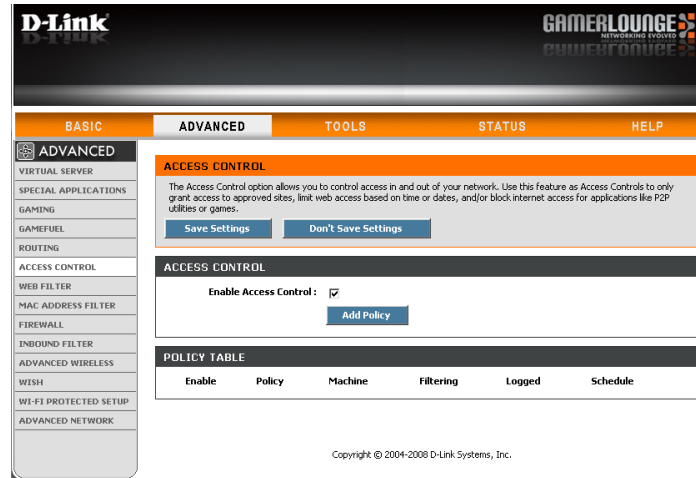
Name	Destination IP	Netmask	Gateway	Metric	Interface
------	----------------	---------	---------	--------	-----------

Copyright © 2004-2008 D-Link Systems, Inc.

Access Control

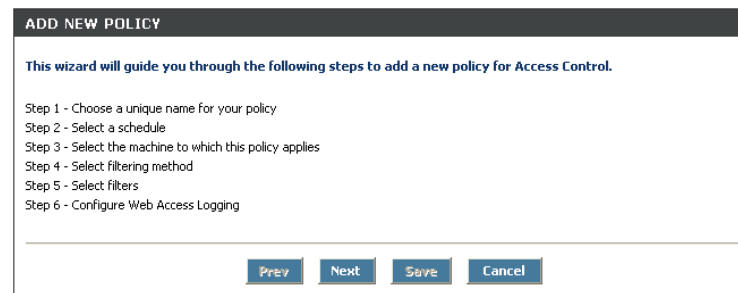
The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

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.

STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name:

Prev Next Save Cancel

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

STEP 2: SELECT SCHEDULE

Choose a schedule to apply to this policy.

Always

Details: Always

Prev Next Save Cancel

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.

STEP 3: SELECT MACHINE

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

Address Type: IP MAC Other Machines

IP Address: << Computer Name

Machine Address: << Computer Name

Copy Your PC's MAC Address

OK Cancel

Machine

Prev Next Save Cancel

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.

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	0	65535

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**.

D-Link **GAMERLOUNGE**
NETWORKING EVOLVED

BASIC **ADVANCED** **TOOLS** **STATUS** **HELP**

ADVANCED

- VIRTUAL SERVER
- SPECIAL APPLICATIONS
- GAMING
- GAMEFUEL
- ROUTING
- ACCESS CONTROL
- WEB FILTER
- MAC ADDRESS FILTER
- FIREWALL
- INBOUND FILTER
- ADVANCED WIRELESS
- WISH
- WI-FI PROTECTED SETUP
- ADVANCED NETWORK

WEBSITE FILTER

The Web Filter option allows you to set up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

Save Settings **Don't Save Settings**

ADD WEB FILTERING RULE

ALLOW **DENY**

WEBSITE FILTERING LIST

Website URL/Domain : **Add**

URL Delete

Copyright © 2004-2006 D-Link Systems, Inc.

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.

D-Link GAMERLOUNGE
NETWORKING EVOLVED
GAMERLOUNGE

BASIC **ADVANCED** **TOOLS** **STATUS** **HELP**

ADVANCED

- VIRTUAL SERVER
- SPECIAL APPLICATIONS
- GAMING
- GAMEFUEL
- ROUTING
- ACCESS CONTROL
- WEB FILTER
- MAC ADDRESS FILTER**
- FIREWALL
- INBOUND FILTER
- ADVANCED WIRELESS
- WISH
- WI-FI PROTECTED SETUP
- ADVANCED NETWORK

MAC ADDRESS FILTER

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

[Save Settings](#) [Don't Save Settings](#)

MAC FILTERING SETUP

Configure MAC Filtering below:

ADD MAC FILTERING RULE

MAC address : <<

[Add](#)

MAC FILTERING RULES

MAC Address	Name	Delete
00:04:23:2c:51:a3	171-mbarberi(00:04:23:2c:51:a3)	

Copyright © 2004-2008 D-Link Systems, Inc.

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 its 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's 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.

The screenshot shows the D-Link DGL-4500 web interface. The 'ADVANCED' tab is selected, and the 'FIREWALL SETTINGS' page is displayed. The page includes the following sections:

- FIREWALL SETTINGS:** A section with a description: "The Firewall Settings allow you to set a single computer on your network outside of the router." It contains two buttons: "Save Settings" and "Don't Save Settings".
- FIREWALL SETTINGS:** A section with a checkbox for "Enable SPI" which is checked.
- NAT ENDPOINT FILTERING:** A section with two sub-sections:
 - UDP Endpoint Filtering:** Radio buttons for "Endpoint Independent", "Address Restricted" (selected), and "Port And Address Restricted".
 - TCP Endpoint Filtering:** Radio buttons for "Endpoint Independent", "Address Restricted", and "Port And Address Restricted" (selected).
- ANTI-SPOOF CHECKING:** A section with a checkbox for "Enable anti-spoof checking" which is unchecked.
- DMZ HOST:** A section with a description: "The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access." It includes a note: "Note: Putting 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." It has a checkbox for "Enable DMZ" which is unchecked, and a text input field for "DMZ IP Address" with the value "0.0.0.0" and a dropdown menu for "Computer Name".
- APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION:** A section with checkboxes for "PPTP" (checked), "IPSec (VPN)" (checked), "RTSP" (checked), and "SIP" (checked).

Copyright © 2004-2008 D-Link Systems, Inc.

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 This section will list any rules that are created.

Rules List: You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.

D-Link **GAMERLOUNGE**
NETWORKING EVOLVED

BASIC **ADVANCED** **TOOLS** **STATUS** **HELP**

ADVANCED

- VIRTUAL SERVER
- SPECIAL APPLICATIONS
- GAMING
- GAMEFUEL
- ROUTING
- ACCESS CONTROL
- WEB FILTER
- MAC ADDRESS FILTER
- FIREWALL
- INBOUND FILTER**
- ADVANCED WIRELESS
- WISH
- WI-FI PROTECTED SETUP
- ADVANCED NETWORK

INBOUND FILTER

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 for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.

ADD INBOUND FILTER RULE

Name:

Action:

Enable	Remote IP Range	Remote IP Start	Remote IP End
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>		<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range
------	--------	-----------------

Copyright © 2004-2008 D-Link Systems, Inc.

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.

The screenshot shows the D-Link web interface for the 'Advanced Wireless Settings' page. The interface includes a navigation menu on the left with the following items: VIRTUAL SERVER, SPECIAL APPLICATIONS, GAMING, GAMEFUEL, ROUTING, ACCESS CONTROL, WEB FILTER, MAC ADDRESS FILTER, FIREWALL, INBOUND FILTER, ADVANCED WIRELESS (selected), WISH, WI-FI PROTECTED SETUP, and ADVANCED NETWORK. The main content area is titled 'ADVANCED WIRELESS' and contains a warning message: 'If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.' Below the warning are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'ADVANCED WIRELESS SETTINGS' section includes the following configuration options:

- Transmit Power:** High (dropdown menu)
- Beacon Period:** 100 (range: 20..1000)
- RTS Threshold:** 2346 (range: 0..2347)
- Fragmentation Threshold:** 2346 (range: 256..2346)
- DTIM Interval:** 1 (range: 1..255)
- WLAN Partition:**
- WMM Enable:**
- Short GI:**

Copyright © 2004-2008 D-Link Systems, Inc.

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.

The screenshot shows the D-Link router's configuration interface for WISH settings. The page is titled "WISH" and is part of the "ADVANCED" configuration section. The interface includes a navigation menu on the left with options like "VIRTUAL SERVER", "SPECIAL APPLICATIONS", "GAMING", "GAMEFUEL", "ROUTING", "ACCESS CONTROL", "WEB FILTER", "MAC ADDRESS FILTER", "FIREWALL", "INBOUND FILTER", "ADVANCED WIRELESS", "WISH", "WI-FI PROTECTED SETUP", and "ADVANCED NETWORK". The main content area is divided into several sections:

- WISH Overview:** A section with a description: "WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications." It includes "Save Settings" and "Don't Save Settings" buttons.
- WISH Section:** A section with a checkbox for "Enable WISH" which is checked.
- PRIORITY CLASSIFIERS:** A section with checkboxes for "HTTP" (checked), "Windows Media Center" (checked), and "Automatic" (unchecked). A note next to "Automatic" says "(default if not matched by anything else)".
- ADD WISH RULE:** A section for adding new rules. It includes an "Enable" checkbox (unchecked), a "Name" text field, a "Priority" dropdown menu (set to "Background Low(BK LO)"), a "Protocol" dropdown menu (set to "TCP"), and four input fields for "Host 1 IP Range", "Host 1 Port Range", "Host 2 IP Range", and "Host 2 Port Range". There are "Add" and "Clear" buttons at the bottom.
- WISH RULES:** A table with columns for "Name", "Priority", "Host 1 IP Range", "Host 2 IP Range", and "Protocol / Ports".

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.

The screenshot shows a configuration window titled "ADD WISH RULE". It contains the following elements:

- Enable:** A checkbox that is currently unchecked.
- Name:** A text input field.
- Priority:** A dropdown menu with "Background (BK)" selected.
- Protocol:** A dropdown menu with "Other" selected.
- Host 1 IP Range:** Two text input fields separated by a hyphen.
- Host 1 Port Range:** Two text input fields separated by a hyphen.
- Host 2 IP Range:** Two text input fields separated by a hyphen.
- Host 2 Port Range:** Two text input fields separated by a hyphen.
- Buttons:** "Add" and "Clear" buttons at the bottom left.

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.

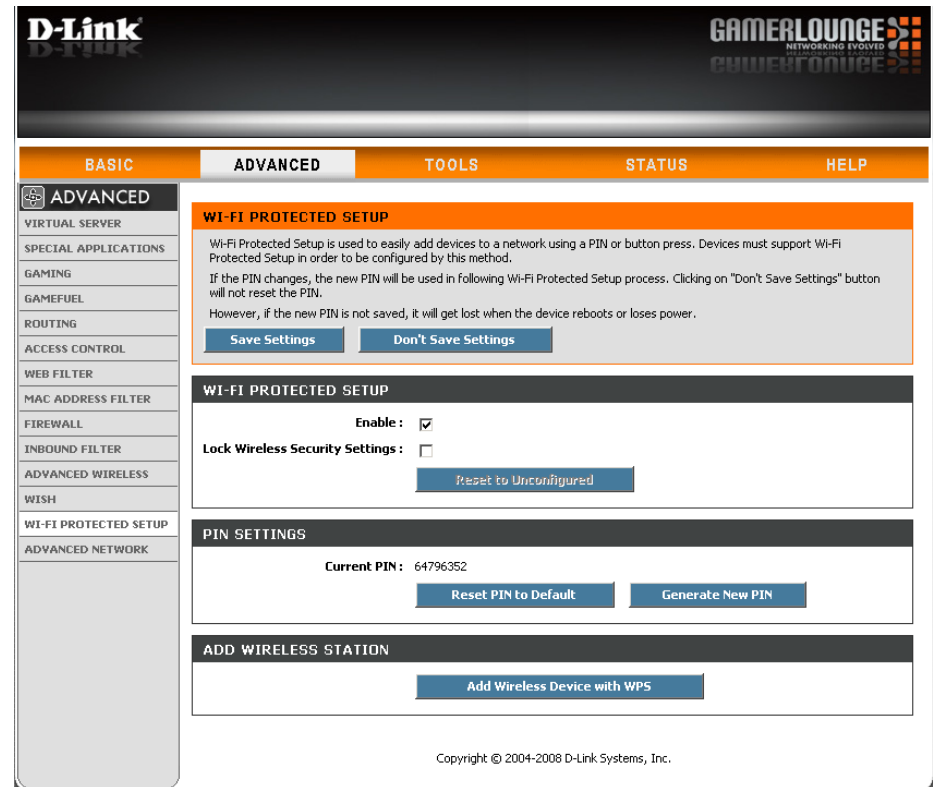
Lock Wireless Security Settings: Locking the wireless security settings prevents the settings from being changed by the Wi-Fi Protected Setup feature of the router. Devices can still be added to the network using Wi-Fi Protected Setup. However, the settings of the network will not change once this option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

Station:

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 Start the wizard.
Device 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.

The screenshot displays the D-Link router's configuration interface. At the top, there are navigation tabs: BASIC, ADVANCED (selected), TOOLS, STATUS, and HELP. The main content area is titled 'ADVANCED NETWORK' and includes a warning message: 'If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'.

The 'UPNP' section is expanded, showing the text: 'Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.' It contains three settings, all of which are checked: 'Enable UPnP', 'Allow Users to disable Internet Access', and 'Allow Users to modify Virtual Server Mappings'.

The 'WAN PING' section is also expanded, with the text: 'If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.' It includes three settings: 'Enable WAN Ping Respond' (unchecked), 'WAN Ping Inbound Filter' (set to 'Allow All' via a dropdown menu), and 'Details' (set to 'Allow All' via a text input field).

The 'WAN PORT SPEED' section is expanded, showing 'WAN Port Speed' set to 'Auto' from a dropdown menu with options 'Auto', '10/100/1000Mbps'.

The 'MULTICAST STREAMS' section is expanded, showing 'Enable Multicast Streams' (unchecked).

A sidebar on the left lists various configuration categories: VIRTUAL SERVER, SPECIAL APPLICATIONS, GAMING, GAMEFUEL, ROUTING, ACCESS CONTROL, WEB FILTER, MAC ADDRESS FILTER, FIREWALL, INBOUND FILTER, ADVANCED WIRELESS, WISH, WI-FI PROTECTED SETUP, and ADVANCED NETWORK (selected).

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.

ADMINISTRATOR SETTINGS

The 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :
 Verify Password :

USER PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :
 Verify Password :

SYSTEM NAME

Gateway Name :

ADMINISTRATION

Enable Graphical Authentication :
 Enable HTTPS Server :
 Enable Remote Management :
 Remote Admin Port : Use HTTPS :
 Remote Admin [Inbound Filter](#) :
 Details :

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**.

The screenshot displays the D-Link router's web interface for Time Configuration. The page is titled "TIME" and includes a navigation menu with options: BASIC, ADVANCED, TOOLS, STATUS, and HELP. The "TOOLS" menu is expanded, showing options like ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES.

The main content area is titled "TIME CONFIGURATION" and contains the following sections:

- Time Configuration:** A summary box explaining the purpose of the section and providing "Save Settings" and "Don't Save Settings" buttons.
- TIME CONFIGURATION:** A detailed configuration section showing:
 - Current Router Time: Saturday, January 31, 2004 2:06:41 PM
 - Time Zone: (GMT-08:00) Pacific Time (US/Canada), Tijuana
 - Enable Daylight Saving:
 - Daylight Saving Offset: +1:00
 - Daylight Saving Dates: A table for configuring DST start and end dates.

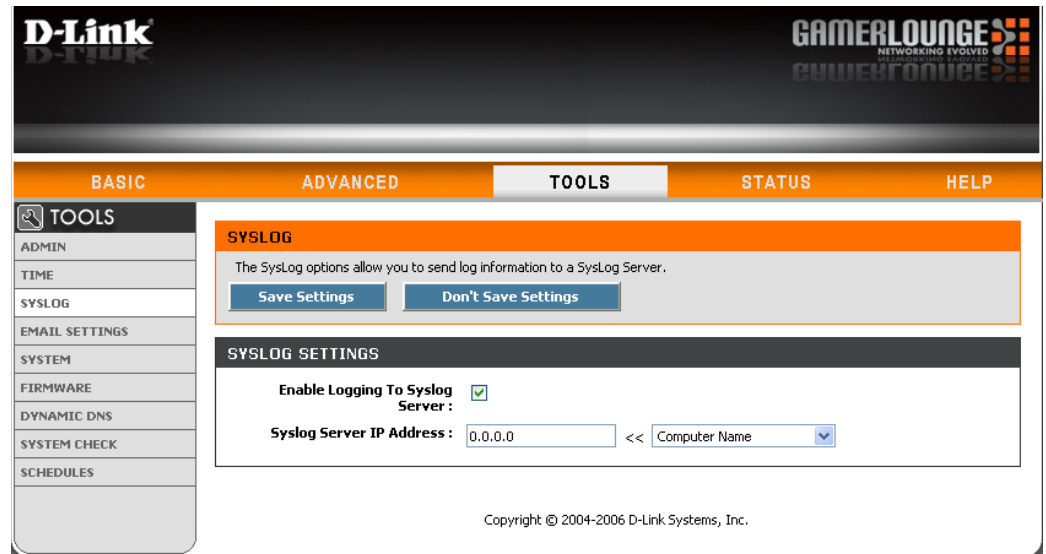
	Month	Week	Day of Week	Time
DST Start	Apr	1st	Sun	2 am
DST End	Oct	5th	Sun	2 am
- AUTOMATIC TIME CONFIGURATION:**
 - Enable NTP Server:
 - NTP Server Used: << Select NTP Server
- SET THE DATE AND TIME MANUALLY:**
 - Date And Time:
 - Year: 2004, Month: Jan, Day: 31, Hour: 02, Minute: 06, Second: 22, PM
 - 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).



The screenshot displays the D-Link router's configuration interface. At the top, there is a navigation bar with tabs for 'BASIC', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The 'TOOLS' tab is active, and a sub-menu on the left lists various tools including 'ADMIN', 'TIME', 'SYSLOG', 'EMAIL SETTINGS', 'SYSTEM', 'FIRMWARE', 'DYNAMIC DNS', 'SYSTEM CHECK', and 'SCHEDULES'. The 'SYSLOG' option is selected, leading to a configuration page. The page title is 'SYSLOG' and it includes a brief description: 'The SysLog options allow you to send log information to a SysLog Server.' Below this, there are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'SYSLOG SETTINGS' section contains a checkbox labeled 'Enable Logging To Syslog Server' which is checked. Underneath, there is a field for 'Syslog Server IP Address' containing '0.0.0.0' and a dropdown menu labeled 'Computer Name'.

Copyright © 2004-2006 D-Link Systems, Inc.

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**.

The screenshot shows the D-Link router's web interface. The top navigation bar includes 'BASIC', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The 'TOOLS' menu is expanded, showing options like 'ADMIN', 'TIME', 'SYSLOG', 'EMAIL SETTINGS', 'SYSTEM', 'FIRMWARE', 'DYNAMIC DNS', 'SYSTEM CHECK', and 'SCHEDULES'. The 'EMAIL SETTINGS' page is displayed, featuring a header with the D-Link logo and 'GAMERLOUNGE NETWORKING EVOLVED'. The main content area is titled 'EMAIL SETTINGS' and contains the following elements:

- An introductory text: "The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address." Below this are two buttons: "Save Settings" and "Don't Save Settings".
- An 'ENABLE' section with a checkbox for "Enable Email Notification".
- An 'EMAIL SETTINGS' section with the following fields:
 - From Email Address: [input field]
 - To Email Address: [input field]
 - SMTP Server Address: [input field]
 - Enable Authentication:
 - Account Name: [input field]
 - Password: [input field]
 - Verify Password: [input field]
- An 'EMAIL LOG WHEN FULL OR ON SCHEDULE' section with:
 - On Log Full:
 - On Schedule:
 - Schedule: [dropdown menu showing 'Never']
 - Details: [input field showing 'Never']

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.

The screenshot displays the D-Link router's web interface. At the top, there is a header with the D-Link logo and 'GAMERLOUNGE NETWORKING EVOLVED'. Below the header is a navigation bar with tabs for 'BASIC', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The 'TOOLS' tab is active, and a sidebar menu on the left lists various tool options: TOOLS, ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSTEM SETTINGS' and contains the following options:

- Save To Local Hard Drive:** A button labeled 'Save Configuration'.
- Load From Local Hard Drive:** A text input field followed by a 'Browse...' button, and a button labeled 'Restore Configuration from File'.
- Restore To Factory Default:** A button labeled 'Restore Factory Defaults' with the subtext 'Restore all settings to the factory defaults.'
- Reboot The Device:** A button labeled 'Reboot the Device'.

At the top of the main content area, there is a warning box: 'The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created. The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.'

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.

The screenshot shows the D-Link router's web interface. The top navigation bar includes tabs for BASIC, ADVANCED, TOOLS, STATUS, and HELP. The left sidebar lists various configuration options, with TOOLS selected. The main content area is titled 'FIRMWARE' and contains the following sections:

- FIRMWARE:** A message stating 'There may be new firmware for your DGL-4500 to improve functionality and performance. To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button below to start the firmware upgrade.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'.
- FIRMWARE INFORMATION:** Displays 'Current Firmware Version : 1.12' and 'Current Firmware Date : 2008/08/05'. It includes a 'Check Online Now for Latest Firmware Version : Check Now' button.
- FIRMWARE UPGRADE:** Contains a note: 'Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools → System screen.' Below the note, it says 'To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.' There is an 'Upload:' label, a text input field, a 'Browse...' button, and an 'Upload' button.
- FIRMWARE UPGRADE NOTIFICATION OPTIONS:** Includes two checkboxes: 'Automatically Check Online for Latest Firmware Version : ' and 'Email Notification of Newer Firmware Version : '.

At the bottom of the page, the copyright notice reads: 'Copyright © 2004-2008 D-Link Systems, Inc.'

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.

D-Link **GAMERLOUNGE**
NETWORKING EVOLVED

BASIC ADVANCED **TOOLS** STATUS HELP

TOOLS

ADMIN
TIME
SYSLOG
EMAIL SETTINGS
SYSTEM
FIRMWARE
DYNAMIC DNS
SYSTEM CHECK
SCHEDULES

DYNAMIC DNS

Dynamic DNS (DDNS)

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 your host name to connect to your game server no matter what your IP address is.

[Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com](http://www.DLinkDDNS.com)

Save Settings Don't Save Settings

DYNAMIC DNS

Enable Dynamic DNS :

Server Address : undefined << Select Dynamic DNS Server

Host Name : (e.g.: me.mydomain.net)

Username or Key :

Password or Key :

Verify Password or Key :

Timeout : 576 (hours)

Status: Disconnect

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.

