Network Settings

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

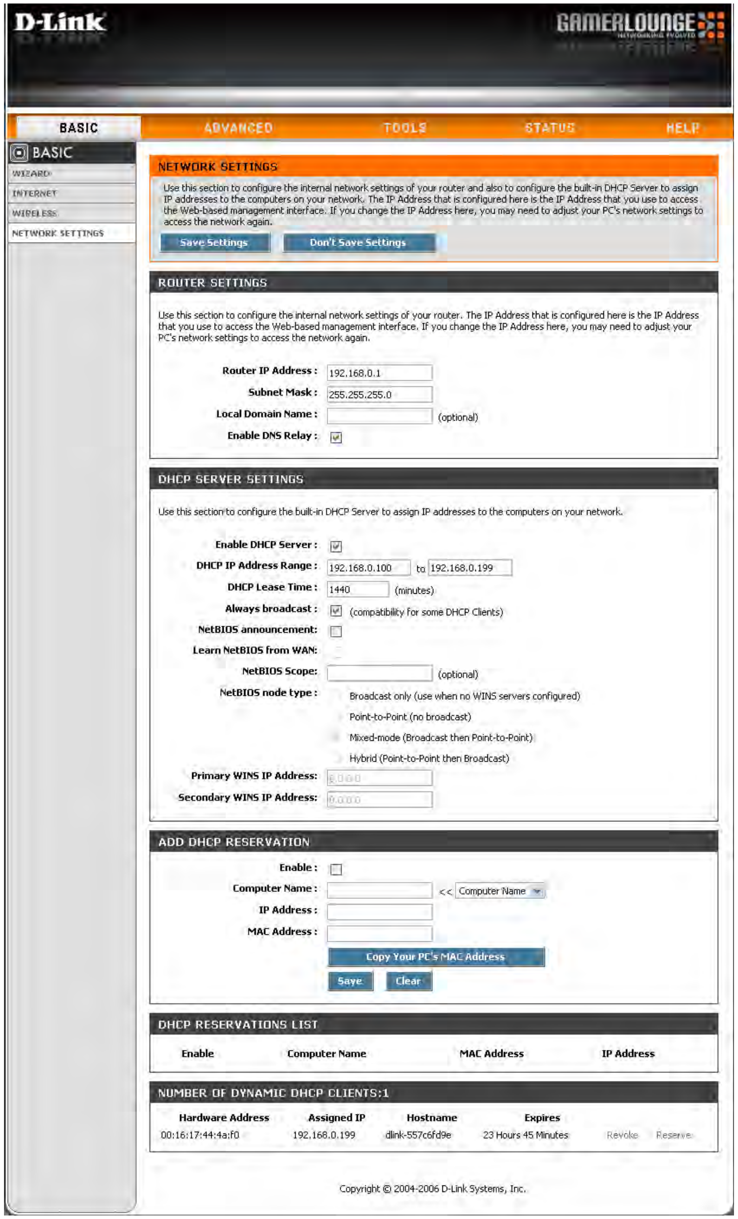
IP Address: Enter the IP address of the router. The default IP address is 192.168.0.1.

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.



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.

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 :

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address

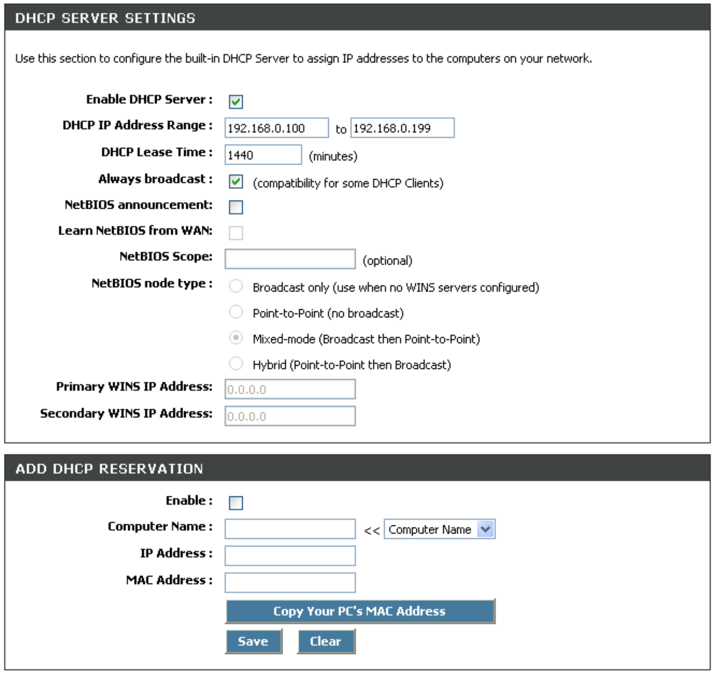
NUMBER OF DYNAMIC DHCP CLIENTS:1

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

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.



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 :

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.

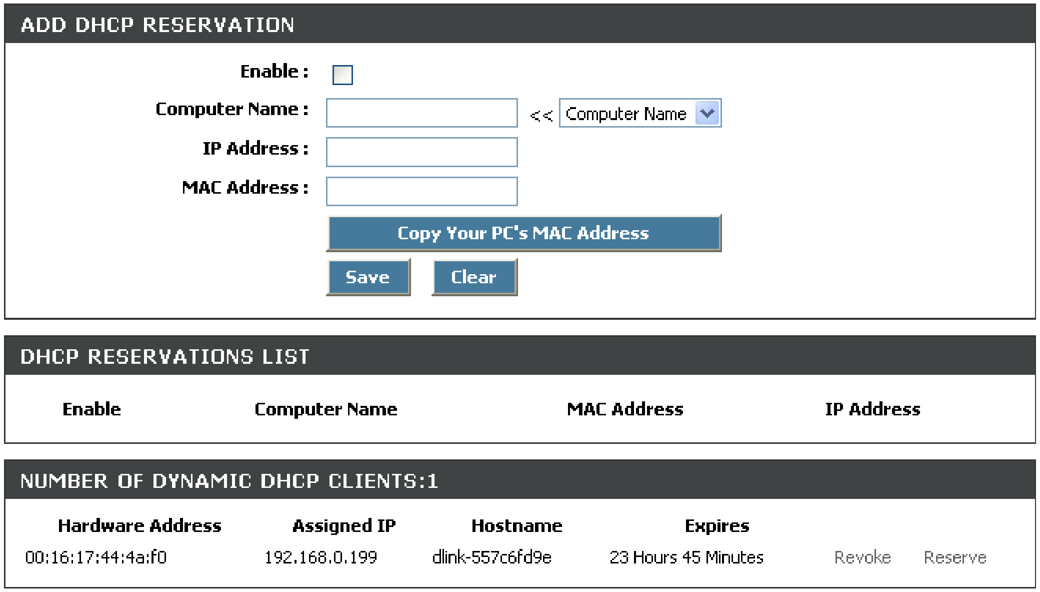
Computer Name: Enter the computer name or select from the drop-down menu and click **<<**.

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.



ADD DHCP RESERVATION

Enable : □

Computer Name : ________ <<

IP Address : ________

MAC Address : ________

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS:1

Hardware Address	Assigned IP	Hostname	Expires		
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.

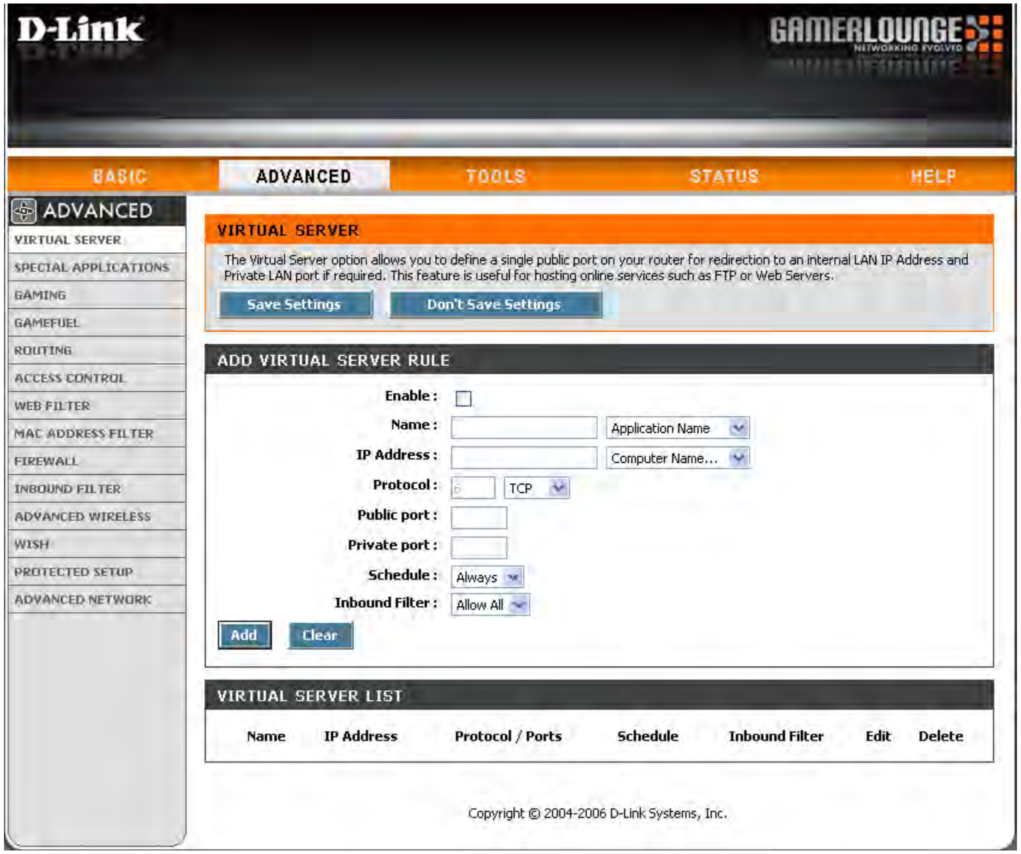
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the “Computer Name” drop-down menu. Select your computer and click **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

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.



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.

ADD VIRTUAL SERVER RULE

Enable : □
Name : ______ Application Name
IP Address : ______ Computer Name...
Protocol : 6 TCP
Public port : ______
Private port : ______
Schedule : Always
Inbound Filter : Allow All

VIRTUAL SERVER LIST

Name	IP Address	Protocol / Ports	Schedule	Inbound Filter	Edit	Delete

Copyright © 2004-2006 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.

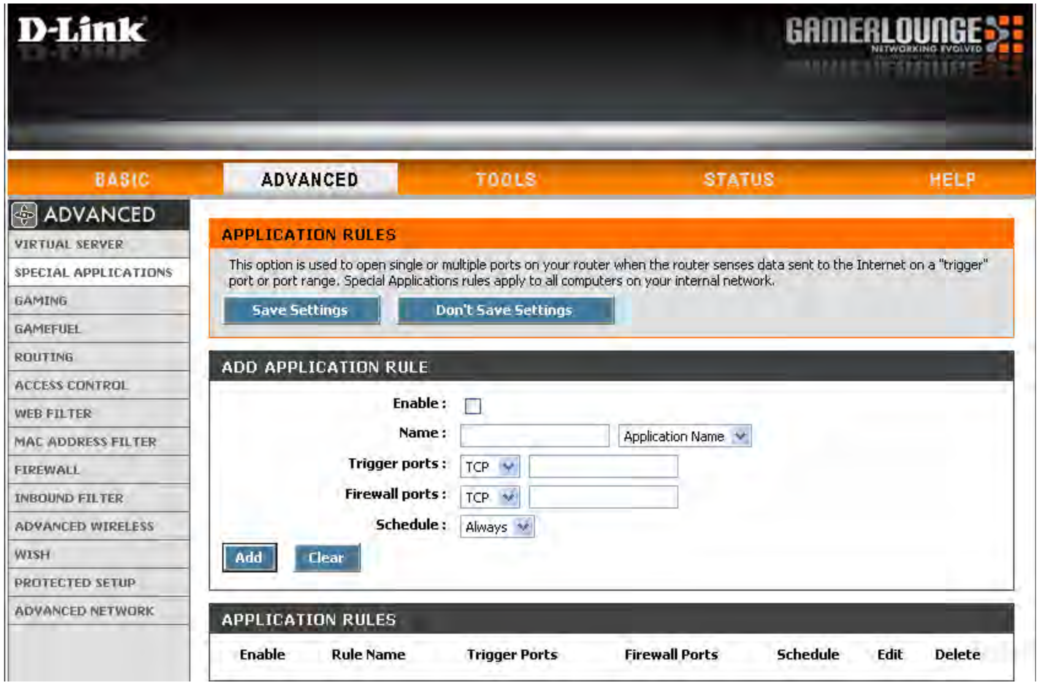
Enable: Check this box to enable the rule.

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.



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.

ADD APPLICATION RULE

Enable : □

Name : Application Name

Trigger ports : TCP

Firewall ports : TCP

Schedule : Always

APPLICATION RULES

Enable	Rule Name	Trigger Ports	Firewall Ports	Schedule	Edit	Delete

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.

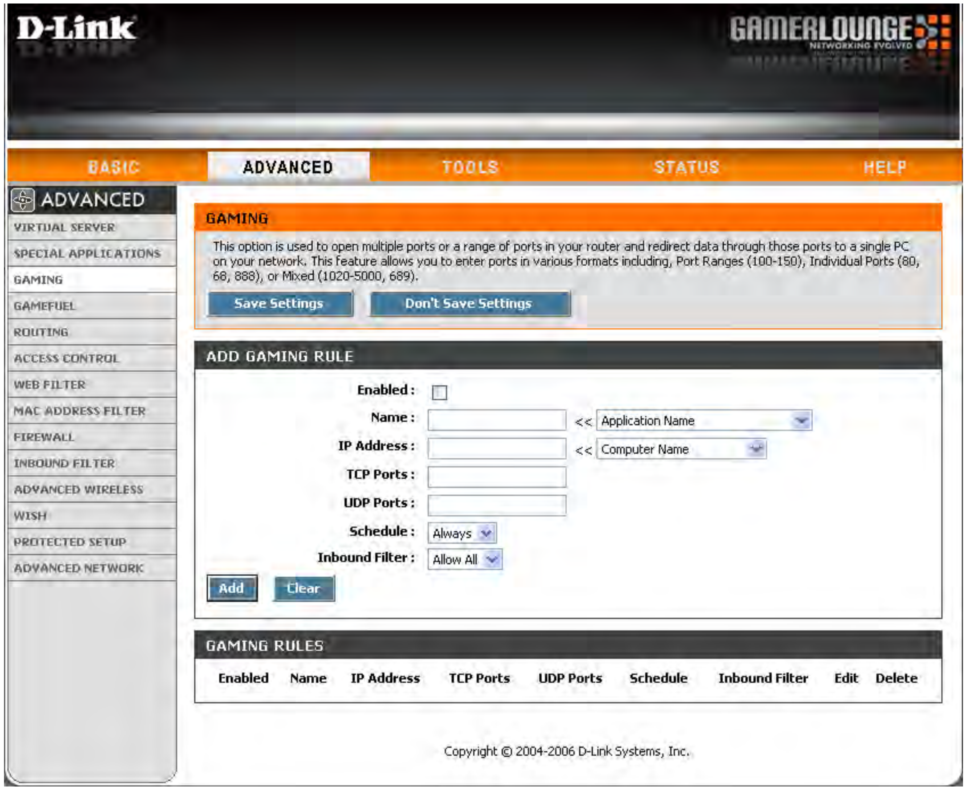
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click **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

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.



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).

ADD GAMING RULE

Enabled : □

Name : << Application Name

IP Address : << Computer Name

TCP Ports :

UDP Ports :

Schedule : Always

Inbound Filter : Allow All

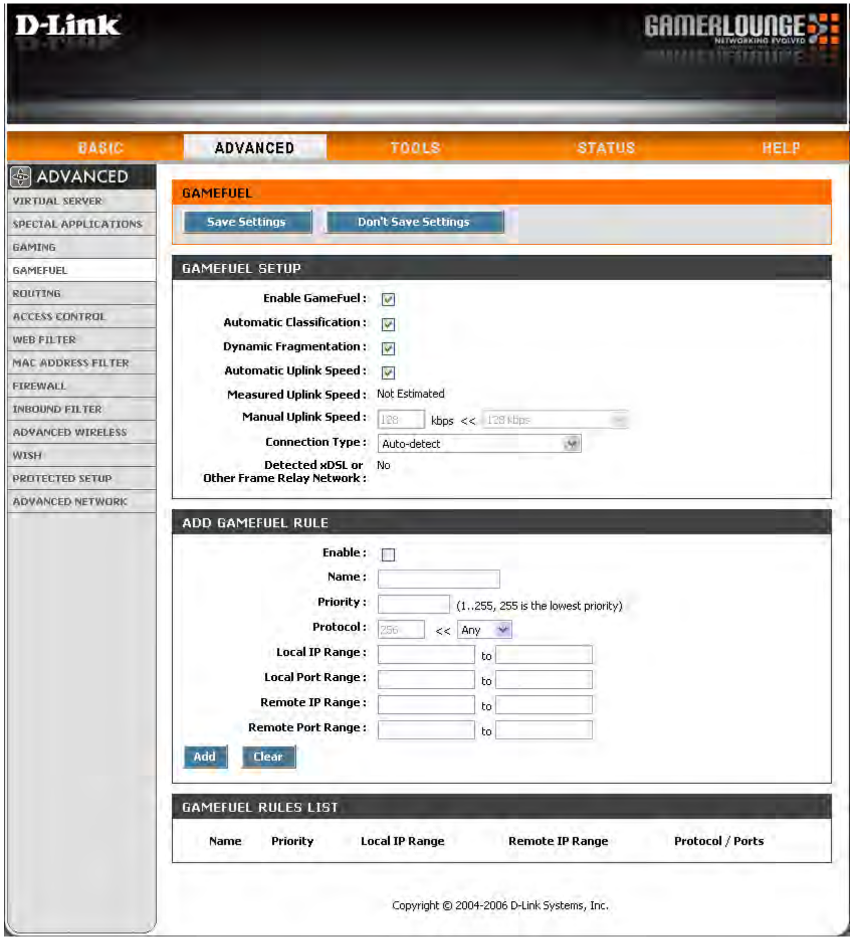
GAMING RULES

Enabled	Name	IP Address	TCP Ports	UDP Ports	Schedule	Inbound Filter	Edit	Delete

Copyright © 2004-2006 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.



GAMEFUEL

GAMEFUEL SETUP

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

ADD GAMEFUEL RULE

Enable : □
Name :
Priority : (1..255, 255 is the lowest priority)
Protocol : 256 << Any
Local IP Range : to
Local Port Range : to
Remote IP Range : to
Remote Port Range : to

GAMEFUEL RULES LIST

Name	Priority	Local IP Range	Remote IP Range	Protocol / Ports

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

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.

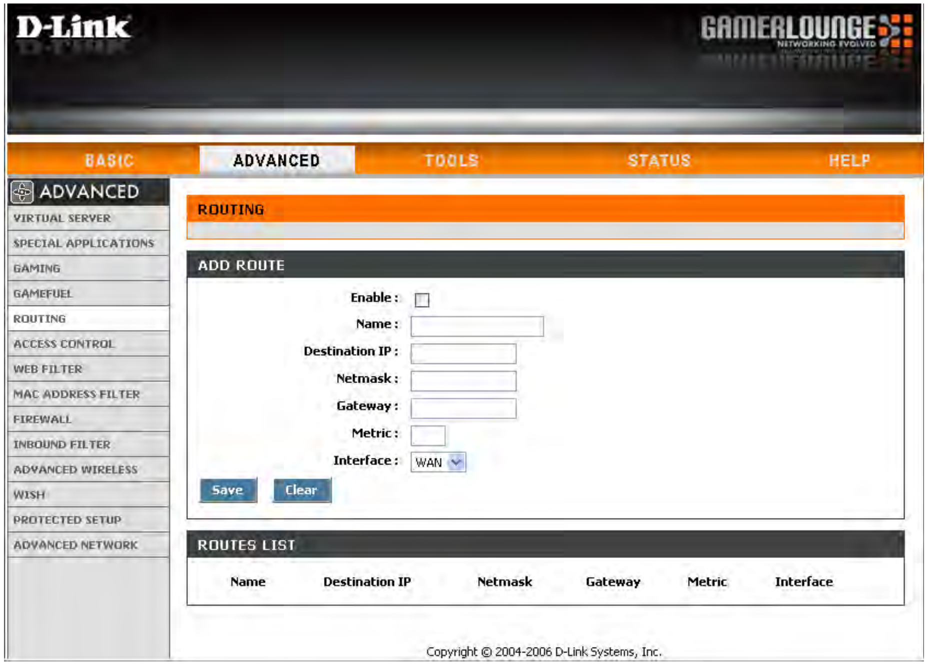
Destination IP: Enter the destination IP address or network address.

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.



ROUTING

ADD ROUTE

Enable : □

Name :

Destination IP :

Netmask :

Gateway :

Metric :

Interface : WAN

ROUTES LIST

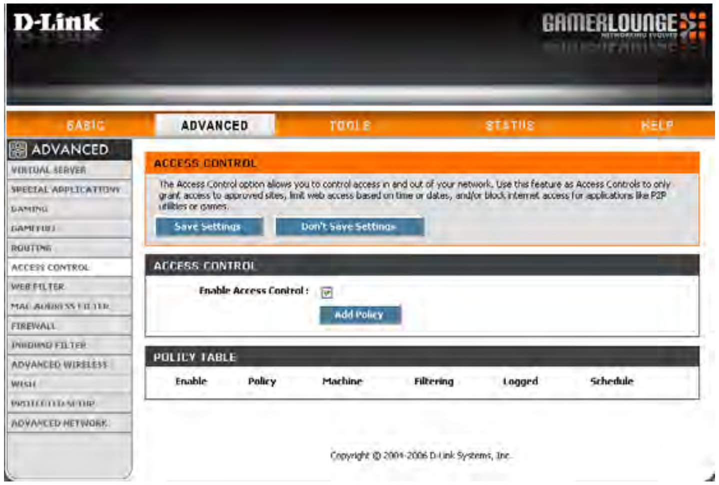
Name	Destination IP	Netmask	Gateway	Metric	Interface

Copyright © 2004-2006 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

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

ACCESS CONTROL

Enable Access Control : ☑

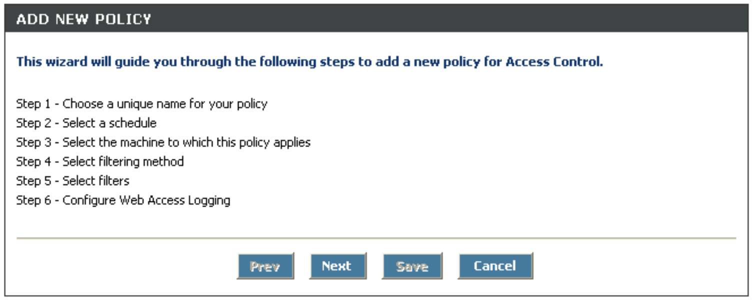
POLICY TABLE

Enable	Policy	Machine	Filtering	Logged	Schedule

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

Access Control Wizard

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



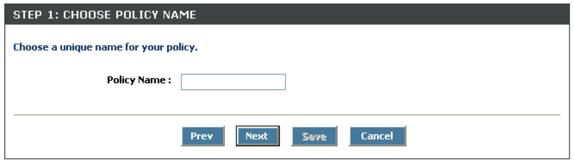
ADD NEW POLICY

This wizard will guide you through the following steps to add a new policy for Access Control.

Step 1 - Choose a unique name for your policy
Step 2 - Select a schedule
Step 3 - Select the machine to which this policy applies
Step 4 - Select filtering method
Step 5 - Select filters
Step 6 - Configure Web Access Logging

Access Control Wizard (continued)

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

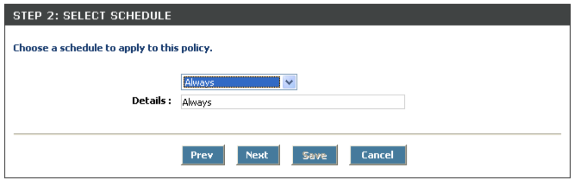


STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name :

Select a schedule (I.E. Always) from the drop-down menu and then click **Next** to continue.



STEP 2: SELECT SCHEDULE

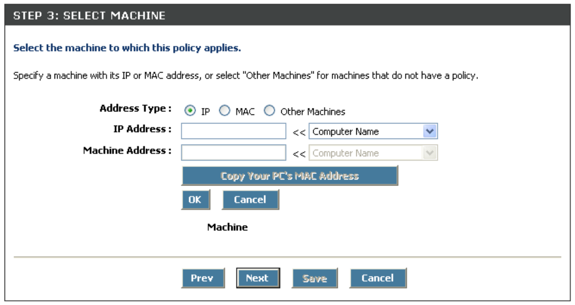
Choose a schedule to apply to this policy.

Always

Details : Always

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.

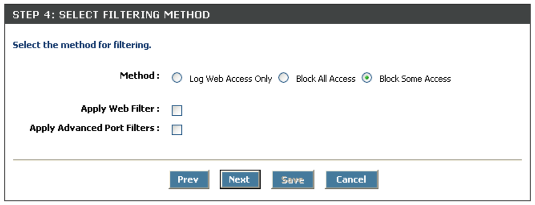
Address Type : ● IP ○ MAC ○ Other Machines

IP Address : << Computer Name

Machine Address : << Computer Name

Access Control Wizard (continued)

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



STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

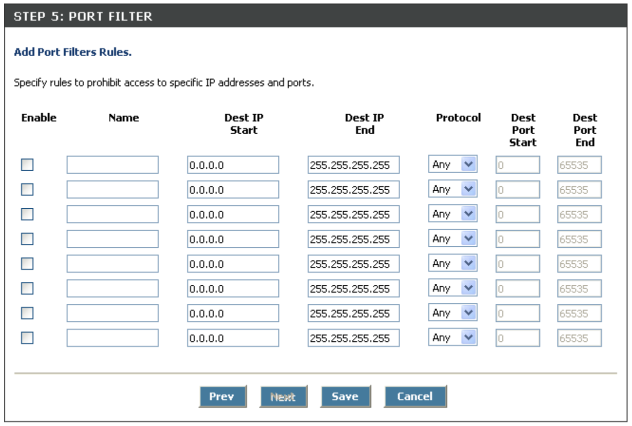
Method : ○ Log Web Access Only ○ Block All Access ● Block Some Access

Apply Web Filter : □

Apply Advanced Port Filters : □

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.



STEP 5: PORT FILTER

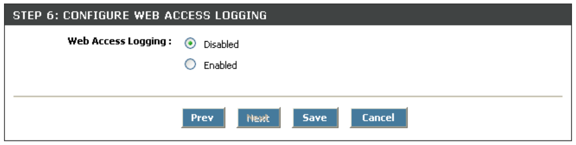
Add Port Filters Rules.

Specify rules to prohibit access to specific IP addresses and ports.

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		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.



STEP 6: CONFIGURE WEB ACCESS LOGGING

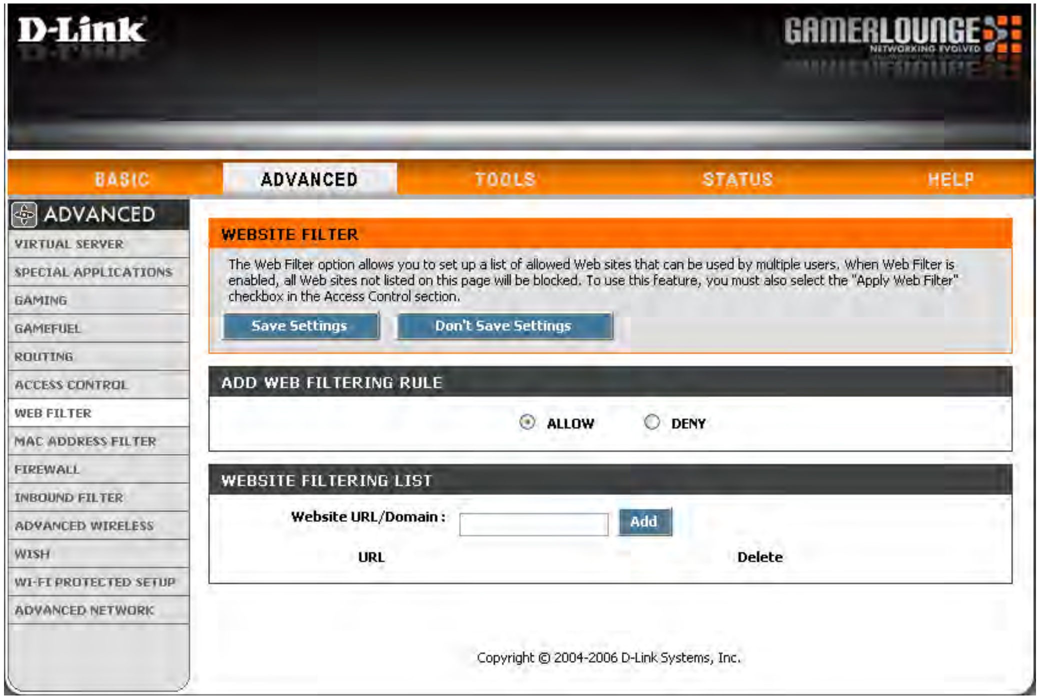
Web Access Logging : ● Disabled ○ Enabled

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 39).

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**.



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.

ADD WEB FILTERING RULE

● ALLOW ○ DENY

WEBSITE FILTERING LIST

Website URL/Domain :

URL	Delete

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

MAC Address Filters

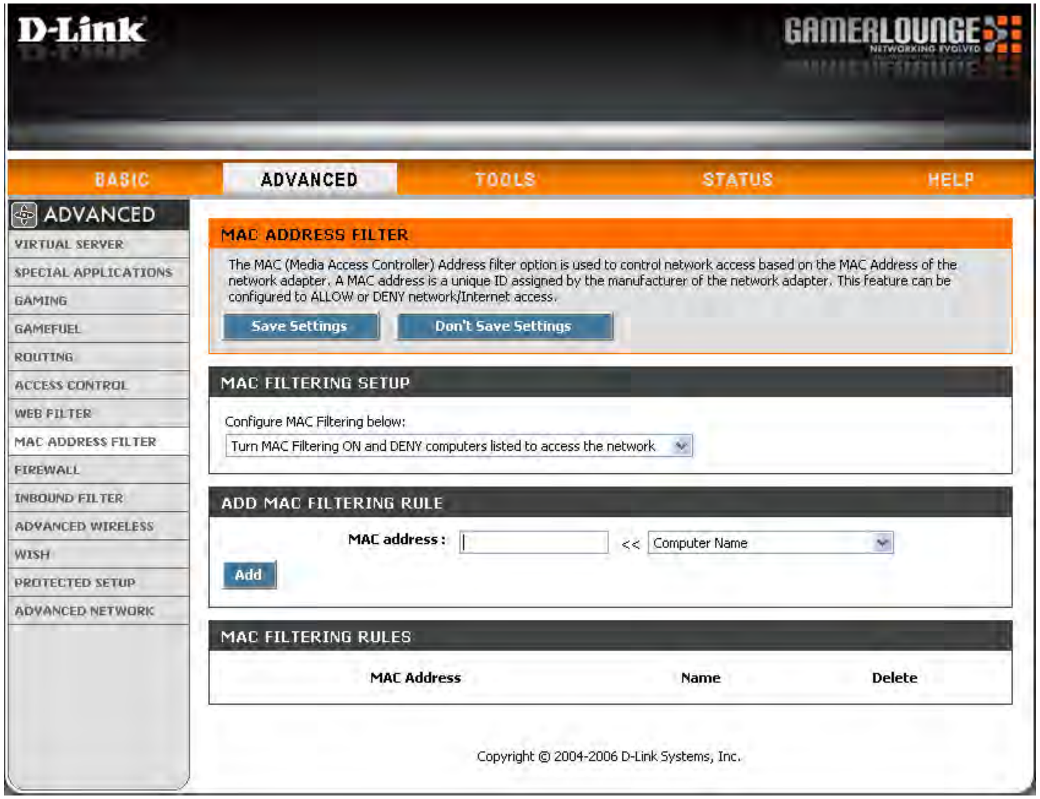
Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

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.



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.

MAC FILTERING SETUP

Configure MAC Filtering below:
Turn MAC Filtering ON and DENY computers listed to access the network

ADD MAC FILTERING RULE

MAC address : << Computer Name

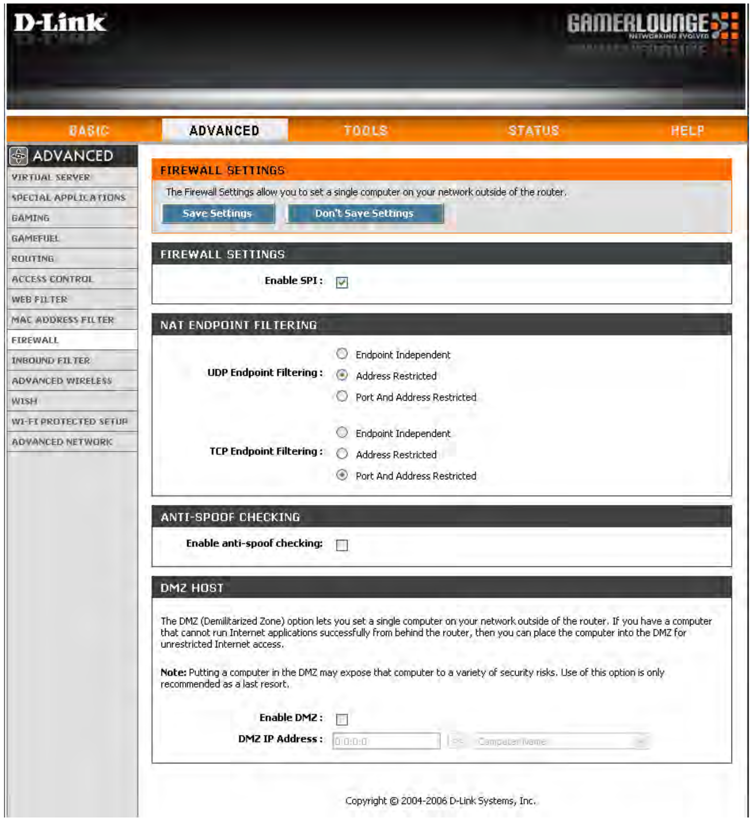
MAC FILTERING RULES

MAC Address	Name	Delete

Copyright © 2004-2006 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.



FIREWALL SETTINGS

The Firewall Settings allow you to set a single computer on your network outside of the router.

FIREWALL SETTINGS

Enable SPI : ☑

NAT ENDPOINT FILTERING

UDP Endpoint Filtering : ○ Endpoint Independent ● Address Restricted ○ Port And Address Restricted

TCP Endpoint Filtering : ○ Endpoint Independent ○ Address Restricted ● Port And Address Restricted

ANTI-SPOOF CHECKING

Enable anti-spoof checking: □

DMZ HOST

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.

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.

Enable DMZ : □

DMZ IP Address : 0.0.0.0 << Computer Name

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

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.

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**.

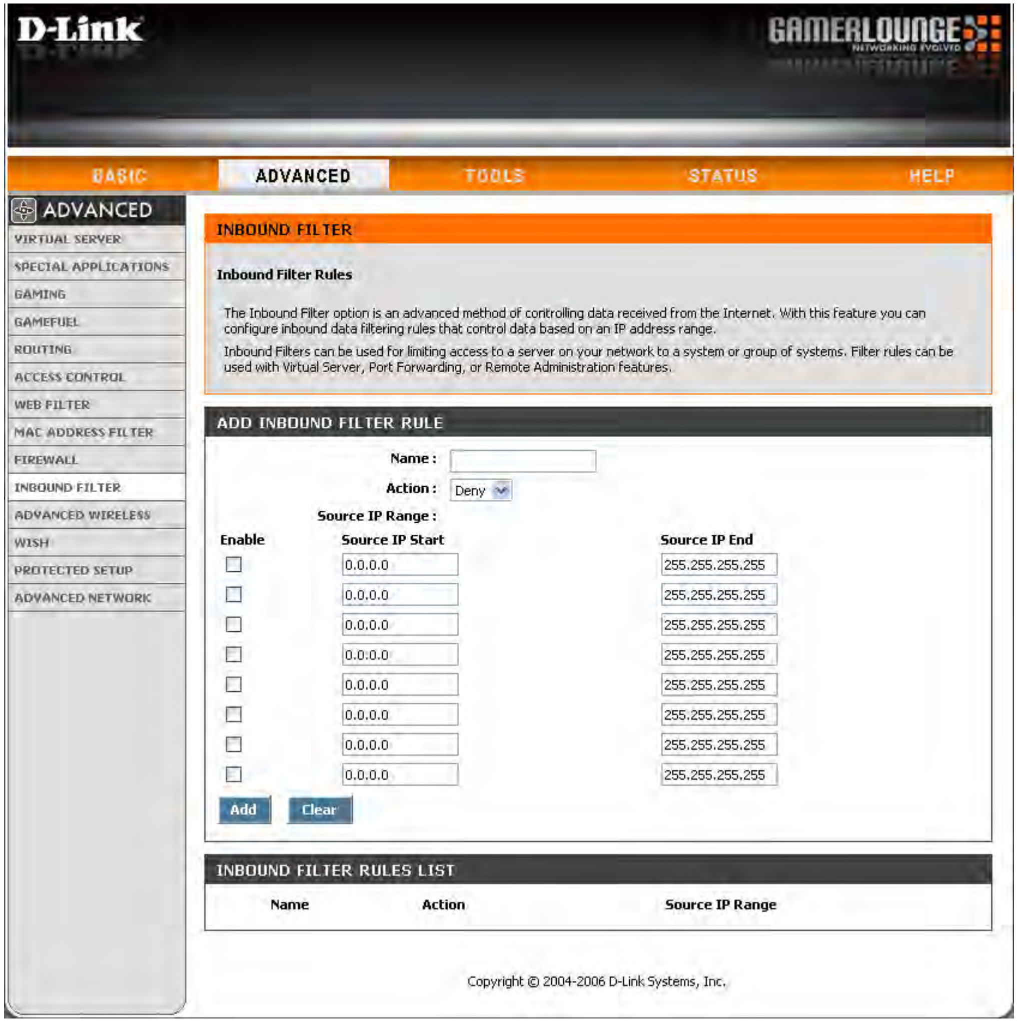
Enable: Check to enable rule.

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.



INBOUND FILTER

Inbound Filter Rules

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 : Deny

Source IP Range :

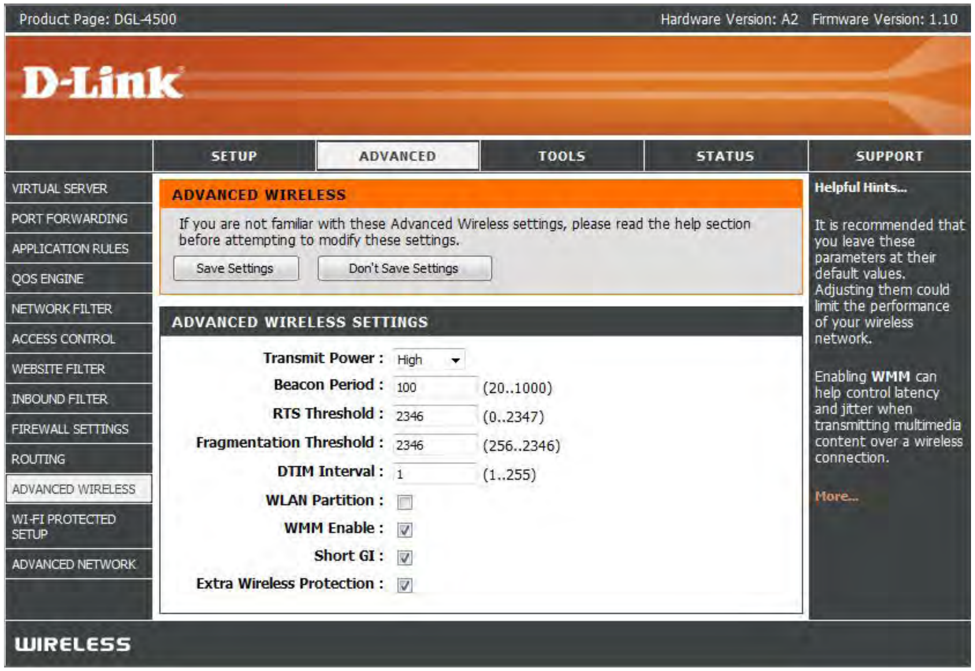
Enable	Source IP Start	Source IP End
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255

INBOUND FILTER RULES LIST

Name	Action	Source IP Range

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

Advanced Wireless Settings



ADVANCED WIRELESS

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

ADVANCED WIRELESS SETTINGS

Transmit Power :	High	
Beacon Period :	100	(20..1000)
RTS Threshold :	2346	(0..2347)
Fragmentation Threshold :	2346	(256..2346)
DTIM Interval :	1	(1..255)
WLAN Partition :	□	
WMM Enable :	☑	
Short GI :	☑	
Extra Wireless Protection :	☑	

Helpful Hints...

It is recommended that you leave these parameters at their default values. Adjusting them could limit the performance of your wireless network.

Enabling **WMM** can help control latency and jitter when transmitting multimedia content over a wireless connection.

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.

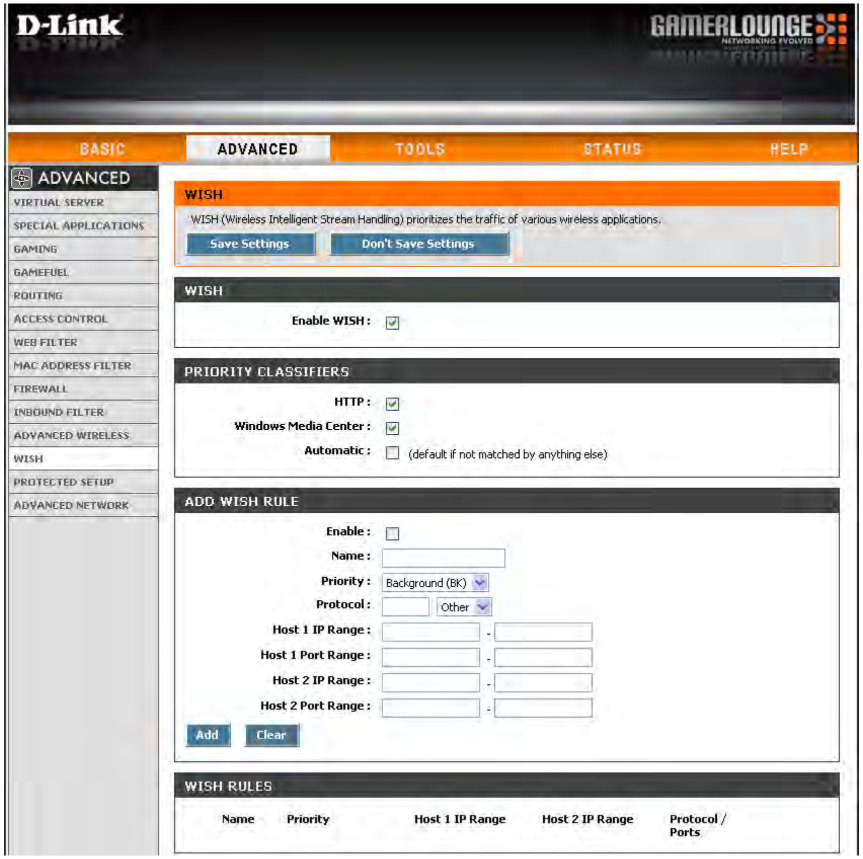
DTIM Interval: (Delivery Traffic Indication Message) 3 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

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.



WISH

WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications.

WISH

Enable WISH : ☑

PRIORITY CLASSIFIERS

HTTP : ☑

Windows Media Center : ☑

Automatic : □ (default if not matched by anything else)

ADD WISH RULE

Enable : □

Name :

Priority : Background (BK)

Protocol : Other

Host 1 IP Range : -

Host 1 Port Range : -

Host 2 IP Range : -

Host 2 Port Range : -

WISH RULES

Name	Priority	Host 1 IP Range	Host 2 IP Range	Protocol / Ports

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

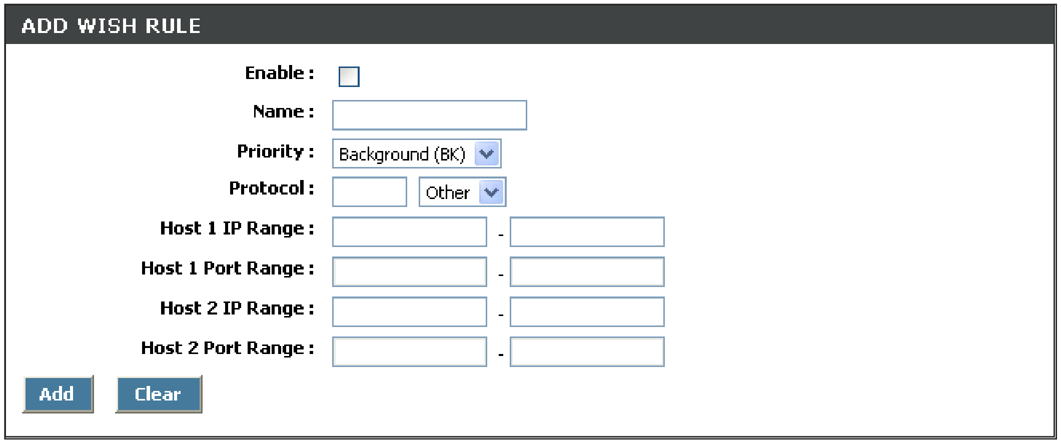
VO: Voice (most urgent)

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.



ADD WISH RULE

Enable : □

Name :

Priority : Background (BK)

Protocol : Other

Host 1 IP Range : -

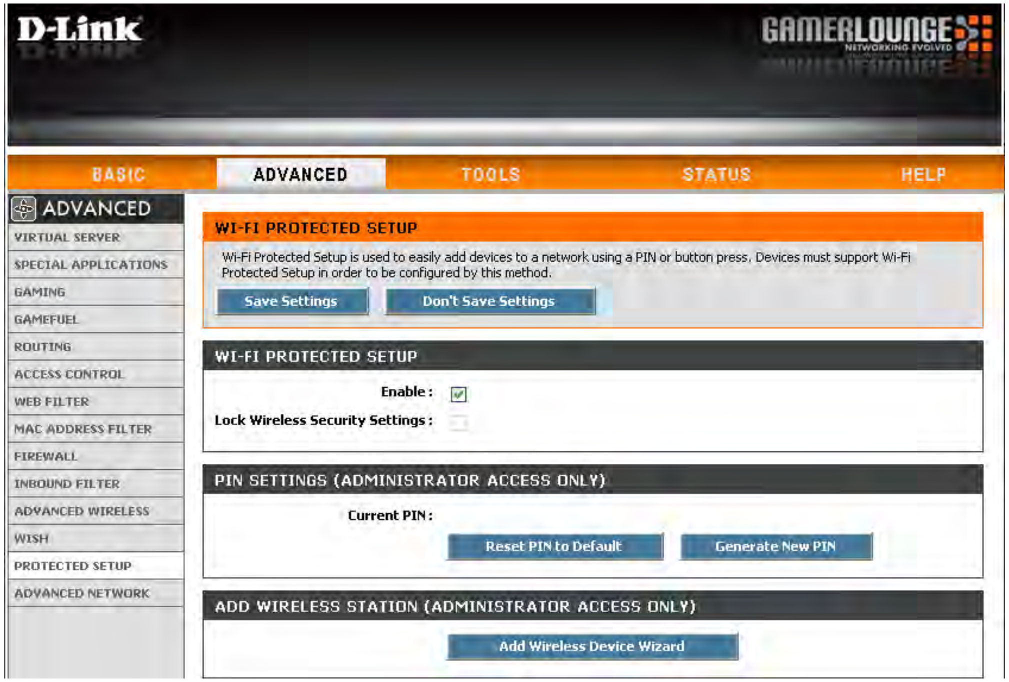
Host 1 Port Range : -

Host 2 IP Range : -

Host 2 Port Range : -

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.



WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

WI-FI PROTECTED SETUP

Enable : ☑

Lock Wireless Security Settings : □

PIN SETTINGS (ADMINISTRATOR ACCESS ONLY)

Current PIN :

ADD WIRELESS STATION (ADMINISTRATOR ACCESS ONLY)

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.

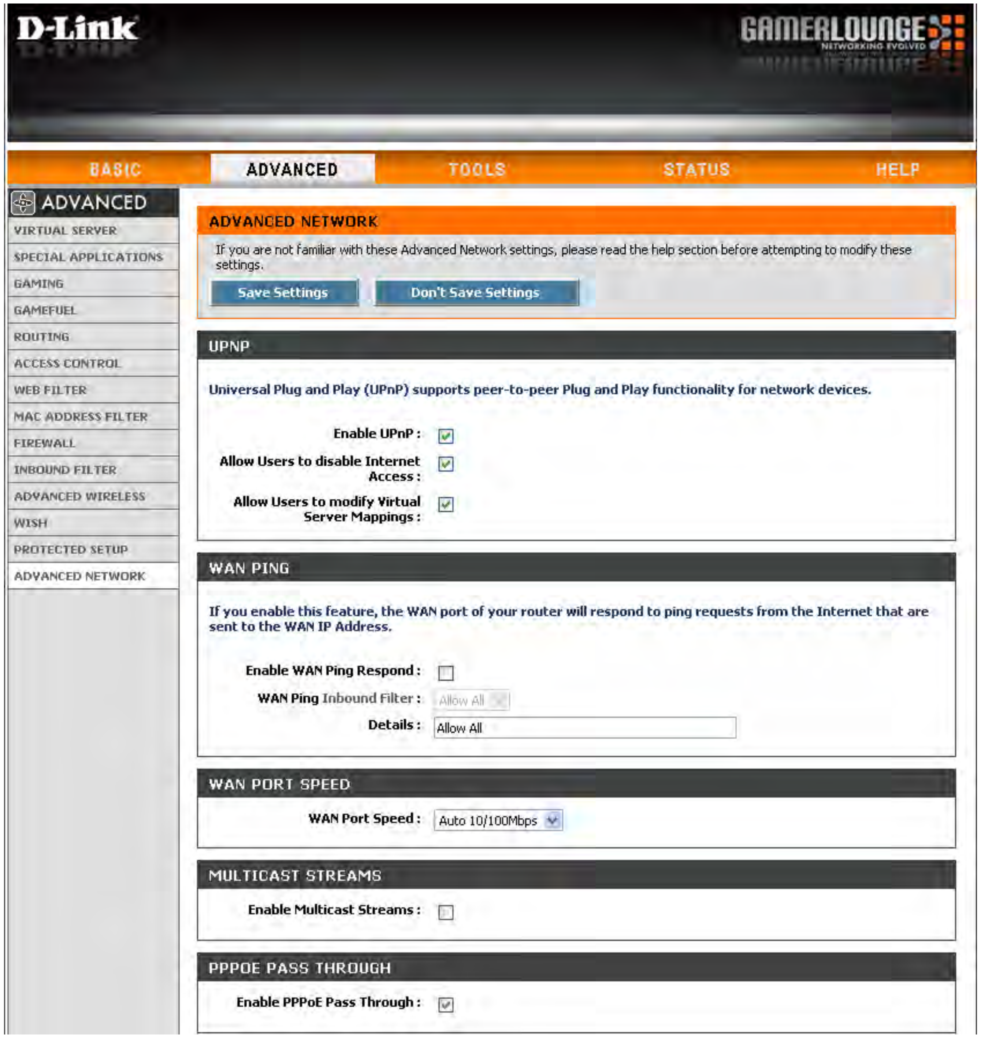
Advanced Network Settings

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.



ADVANCED NETWORK

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

UPNP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP : ☑
Allow Users to disable Internet Access : ☑
Allow Users to modify Virtual Server Mappings : ☑

WAN PING

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.

Enable WAN Ping Respond : □
WAN Ping Inbound Filter : Allow All
Details : Allow All

WAN PORT SPEED

WAN Port Speed : Auto 10/100Mbps

MULTICAST STREAMS

Enable Multicast Streams : □

PPPOE PASS THROUGH

Enable PPPoE Pass Through : ☑

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.

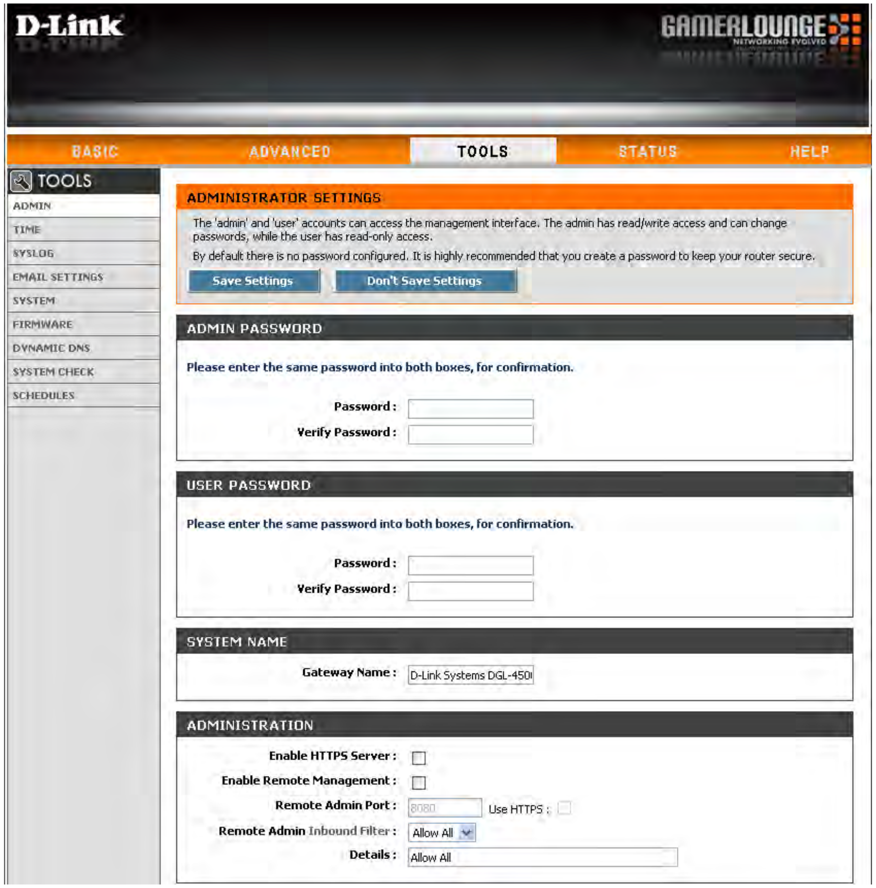
User Password: Enter the new password for the User login. If you login as the User, you can only see the settings, but cannot change them.

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

Enable 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.



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 : D-Link Systems DGL-450

ADMINISTRATION

Enable HTTPS Server : □

Enable Remote Management : □

Remote Admin Port : 8080 Use HTTPS : □

Remote Admin Inbound Filter : Allow All

Details : Allow All

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.

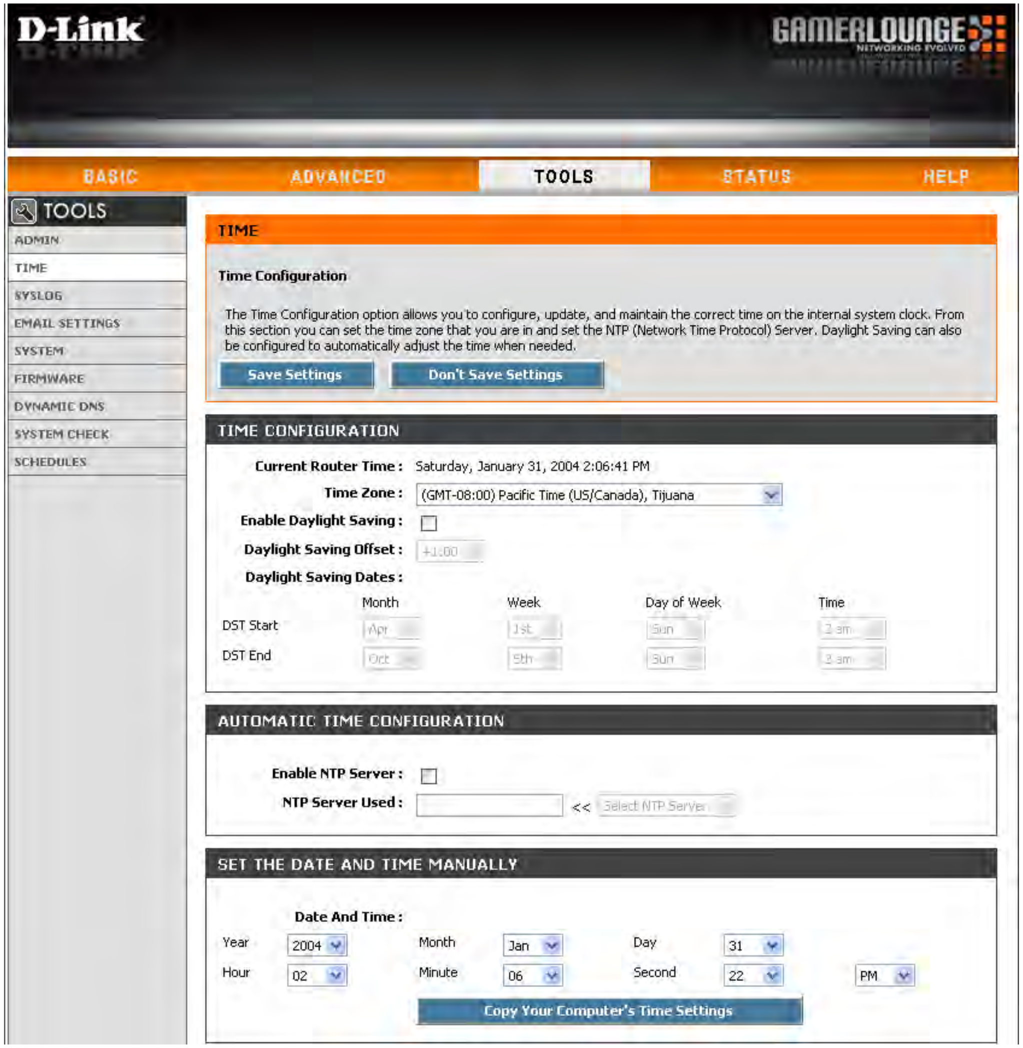
Time Zone: Select the Time Zone from the drop-down menu.

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**.



TIME

Time Configuration

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 NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME CONFIGURATION

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 :

	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 :

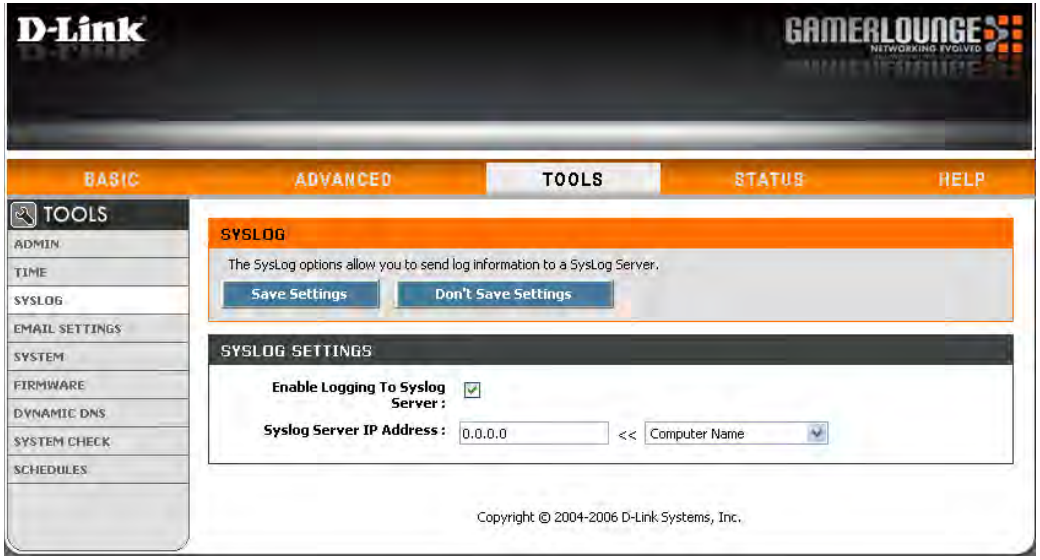
Year	2004	Month	Jan	Day	31	
Hour	02	Minute	06	Second	22	PM

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).



SYSLOG

The SysLog options allow you to send log information to a SysLog Server.

SYSLOG SETTINGS

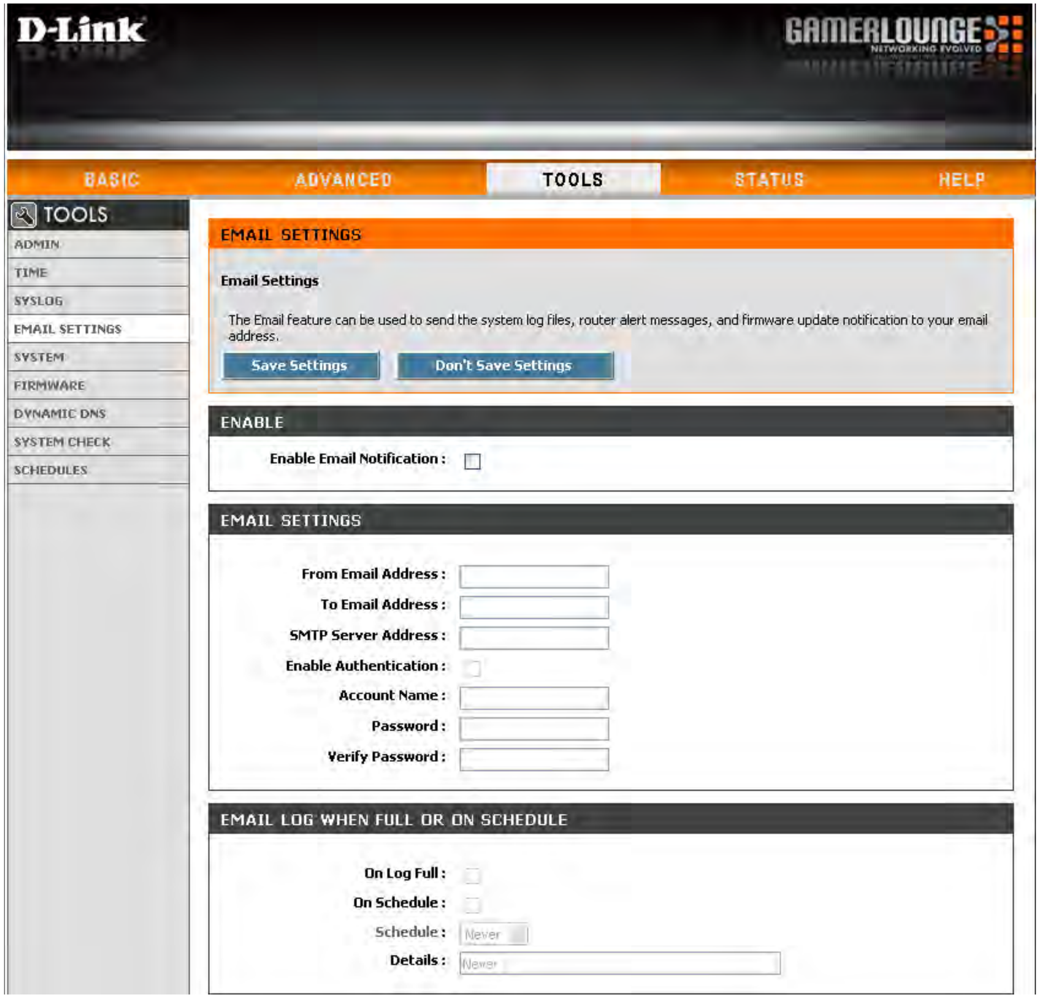
Enable Logging To Syslog Server : ☑

Syslog Server IP Address : 0.0.0.0 << 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.



EMAIL SETTINGS

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

Enable Email Notification : □

EMAIL SETTINGS

From Email Address :

To Email Address :

SMTP Server Address :

Enable Authentication : □

Account Name :

Password :

Verify Password :

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full : □

On Schedule : □

Schedule : Never

Details : Never

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**.

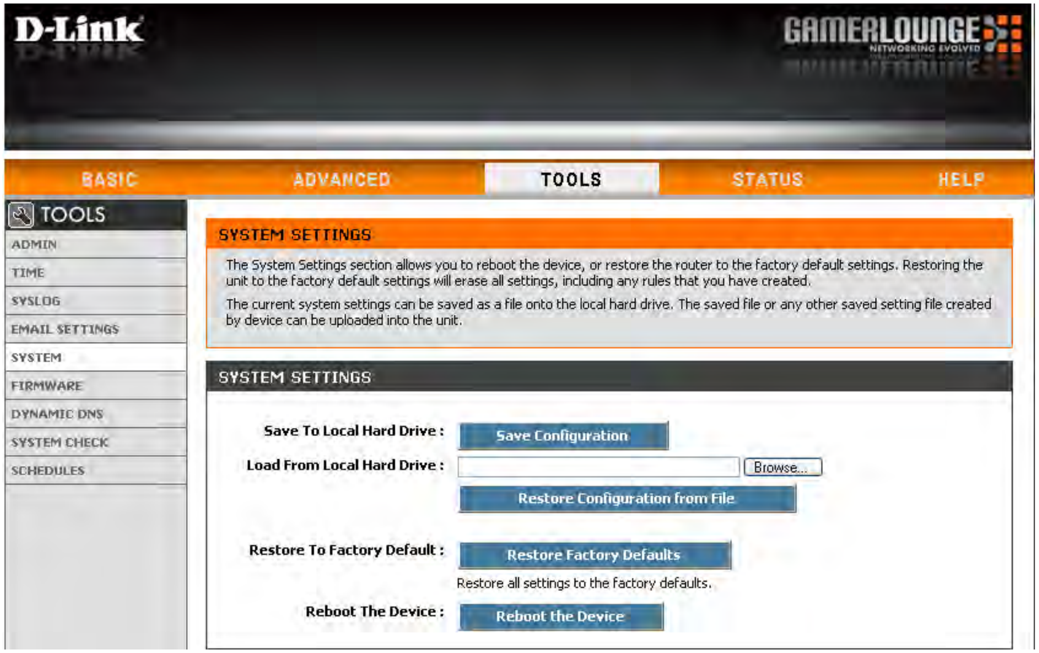
System Settings

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.



SYSTEM SETTINGS

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.

SYSTEM SETTINGS

Save To Local Hard Drive : Save Configuration

Load From Local Hard Drive : Browse...

Restore Configuration from File

Restore To Factory Default : Restore Factory Defaults

Restore all settings to the factory defaults.

Reboot The Device : Reboot the Device

Update Firmware

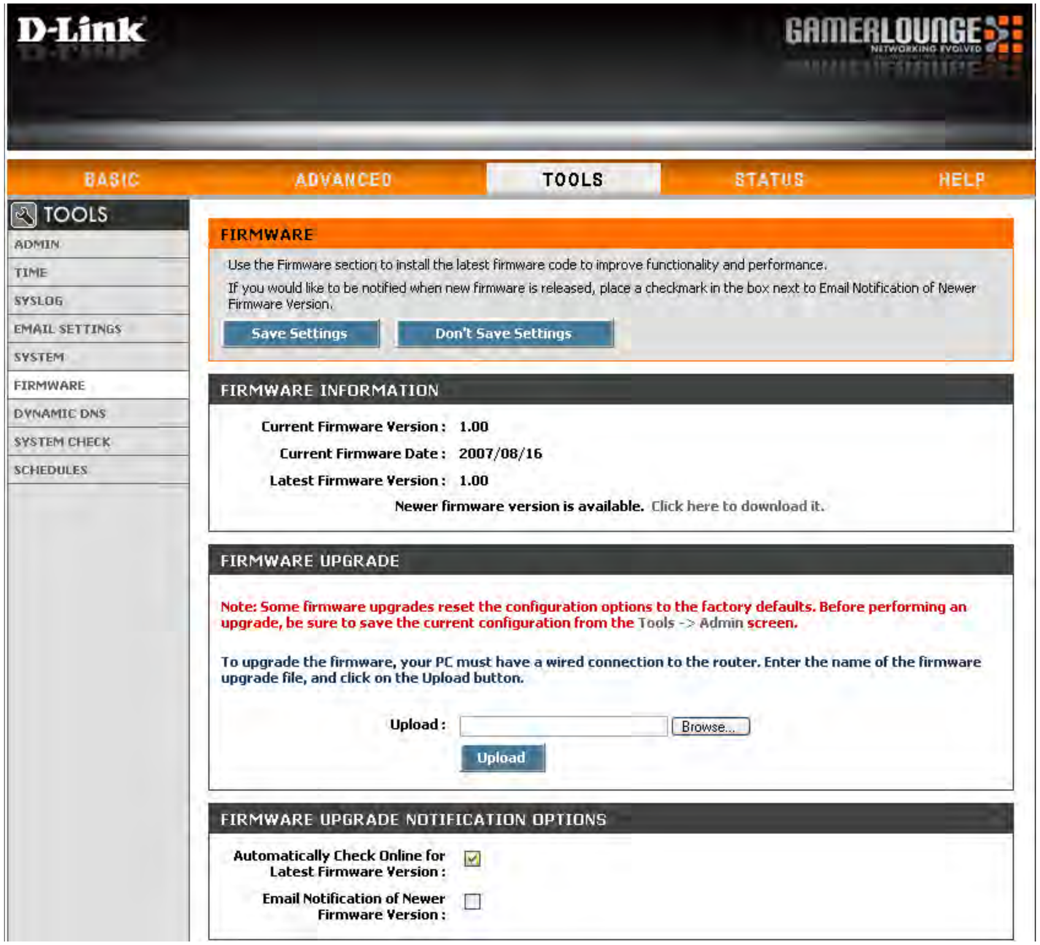
You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can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



FIRMWARE

Use the Firmware section to install the latest firmware code to improve functionality and performance.

If you would like to be notified when new firmware is released, place a checkmark in the box next to Email Notification of Newer Firmware Version.

FIRMWARE INFORMATION

Current Firmware Version : 1.00

Current Firmware Date : 2007/08/16

Latest Firmware Version : 1.00

Newer firmware version is available. Click here to download it.

FIRMWARE UPGRADE

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 -> Admin screen.

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.

Upload :

FIRMWARE UPGRADE NOTIFICATION OPTIONS

Automatically Check Online for Latest Firmware Version : ☑

Email Notification of Newer Firmware Version : □

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.

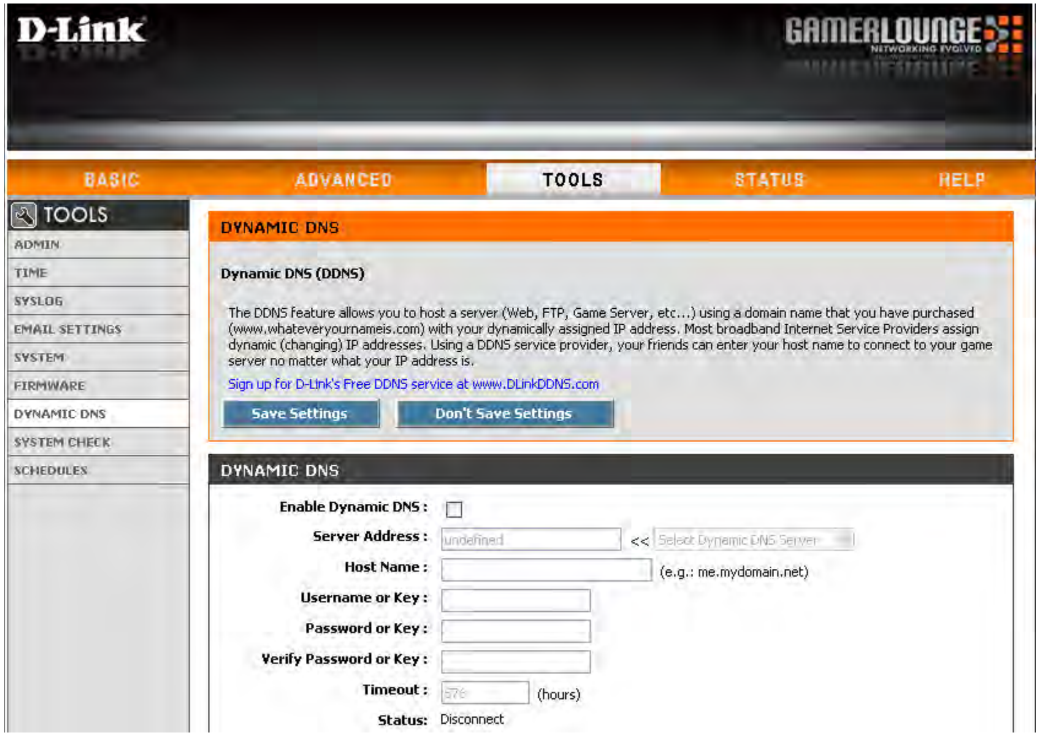
Host Name: Enter the Host Name that you registered with your DDNS service provider.

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.



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

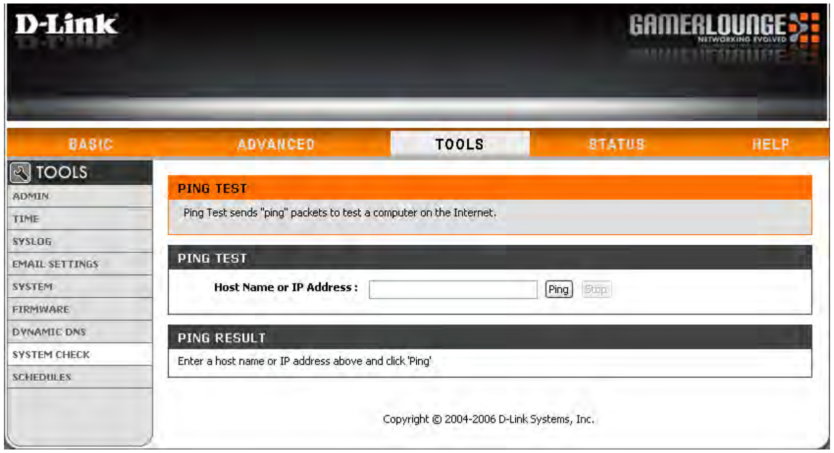
DYNAMIC DNS

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.



PING TEST

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

Host Name or IP Address :

PING RESULT

Enter a host name or IP address above and click 'Ping'

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

Schedules

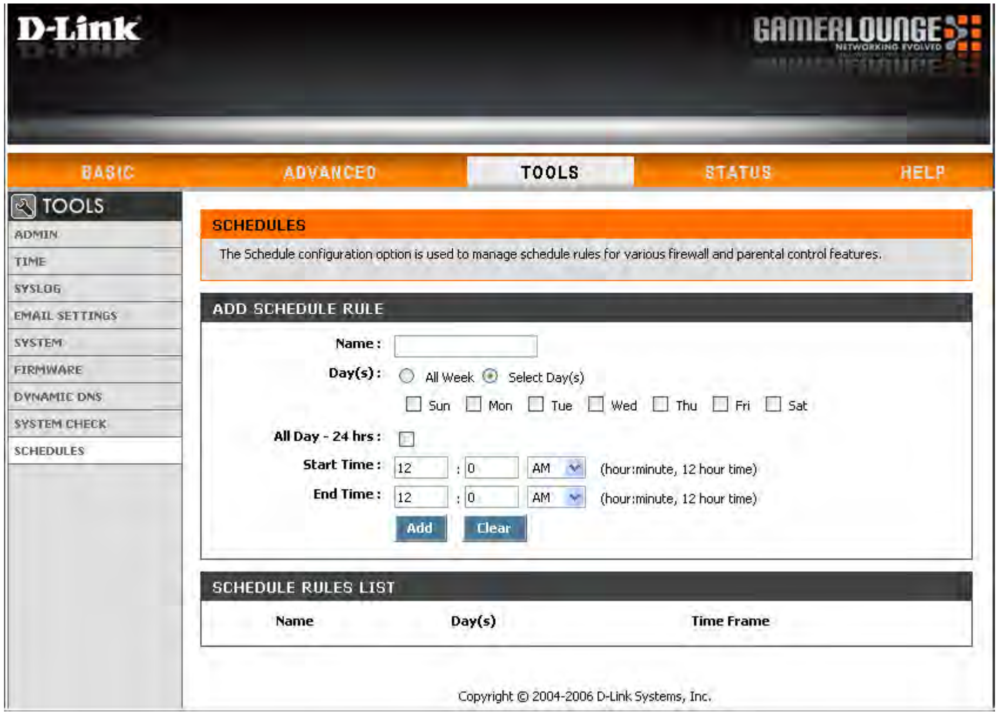
Name: Enter a name for your new schedule.

Days: Select a day, a range of days, or All Week to include every day.

Time: Check **All Day - 24hrs** or enter a start and end time for your schedule.

Add: Click **Add** to save your schedule. You must click Save Settings at the top for your schedules to go into effect.

Schedule Rules List: The list of schedules will be listed here. Click the **Edit** icon to make changes or click the **Delete** icon to remove the schedule.



SCHEDULES

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : 12 : 0 AM (hour:minute, 12 hour time)

End Time : 12 : 0 AM (hour:minute, 12 hour time)

SCHEDULE RULES LIST

Name	Day(s)	Time Frame

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

Device Information

This page displays the current information for the DGL-4500. It will display the LAN, WAN (Internet), and Wireless information.

If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

General: Displays the router's time and firmware version.

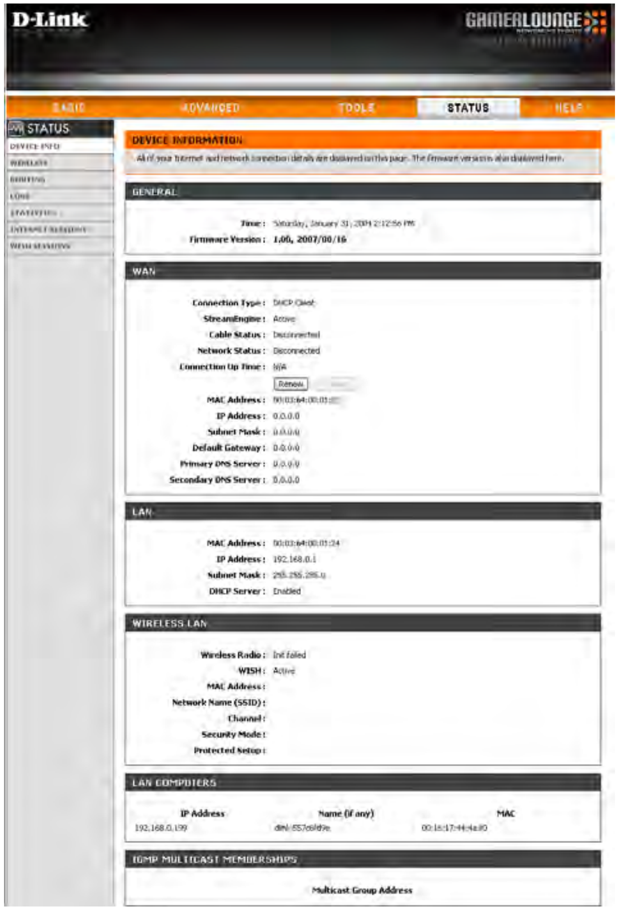
WAN: Displays the MAC address and the public IP settings for the router.

LAN: Displays the MAC address and the private (local) IP settings for the router.

Wireless LAN: Displays the wireless MAC address and your wireless settings such as SSID and Channel.

LAN Computers: Displays computers and devices that are connected to the router via Ethernet and that are receiving an IP address assigned by the router (DHCP).

IGMP Multicast Memberships: Displays the Multicast Group IP Address.



DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

GENERAL

Time : Saturday, January 31, 2004 2:12:56 PM
Firmware Version : 1.00, 2007/00/16

WAN

Connection Type : DHCP Client
StreamEngine : Active
Cable Status : Disconnected
Network Status : Disconnected
Connection Up Time : N/A
MAC Address : 00:03:64:00:01:25
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0

LAN

MAC Address : 00:03:64:00:01:24
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

Wireless Radio : Init failed
WISH : Active
MAC Address :
Network Name (SSID) :
Channel :
Security Mode :
Protected Setup :

LAN COMPUTERS

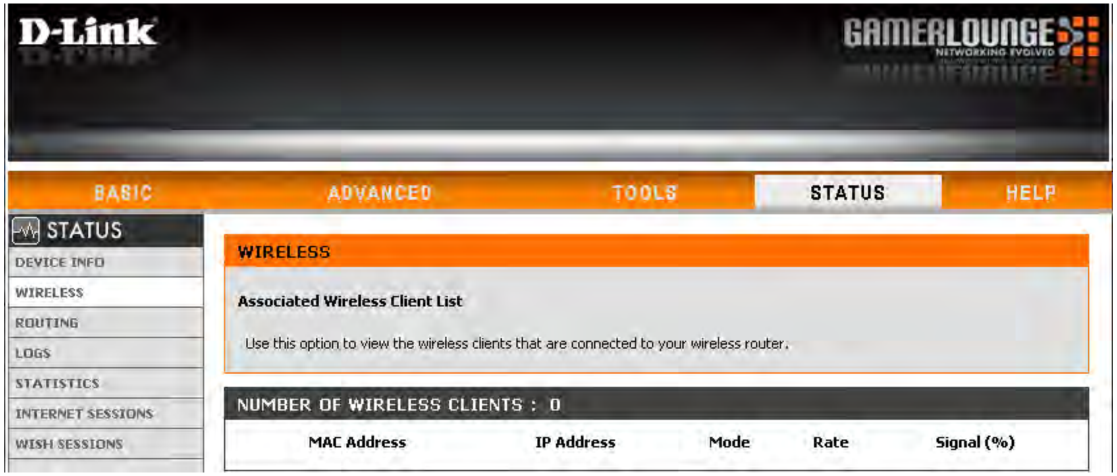
IP Address	Name (if any)	MAC
192.168.0.199	dlink-557e6fd9e	00:16:17:44:4a:80

IGMP MULTICAST MEMBERSHIPS

Multicast Group Address

Wireless

The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.



WIRELESS

Associated Wireless Client List

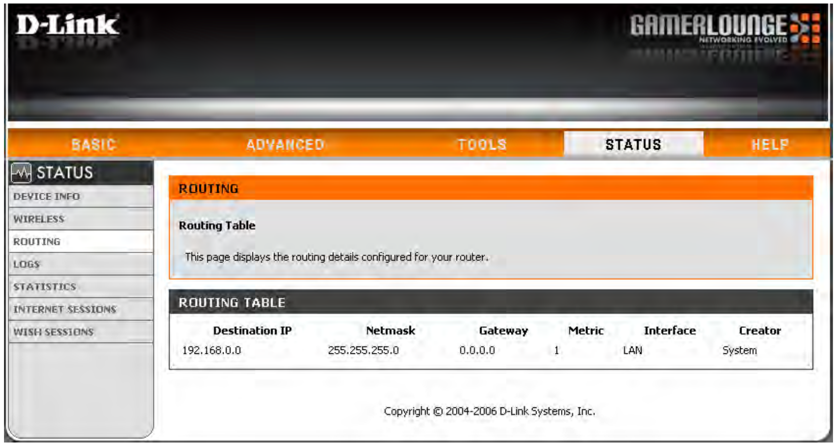
Use this option to view the wireless clients that are connected to your wireless router.

NUMBER OF WIRELESS CLIENTS : 0

MAC Address	IP Address	Mode	Rate	Signal (%)

Routing

The Routing page displays the routing table.



ROUTING

Routing Table

This page displays the routing details configured for your router.

ROUTING TABLE

Destination IP	Netmask	Gateway	Metric	Interface	Creator
192.168.0.0	255.255.255.0	0.0.0.0	1	LAN	System

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

Logs

The router automatically logs (records) events of possible interest in it’s internal memory. If there isn’t enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

What to View: You can select the types of messages that you want to display from the log. Firewall & Security, System, and Router Status messages can be selected.

View Levels: There are three levels of message importance: Informational, Warning, and Critical. Select the levels that you want displayed in the log.

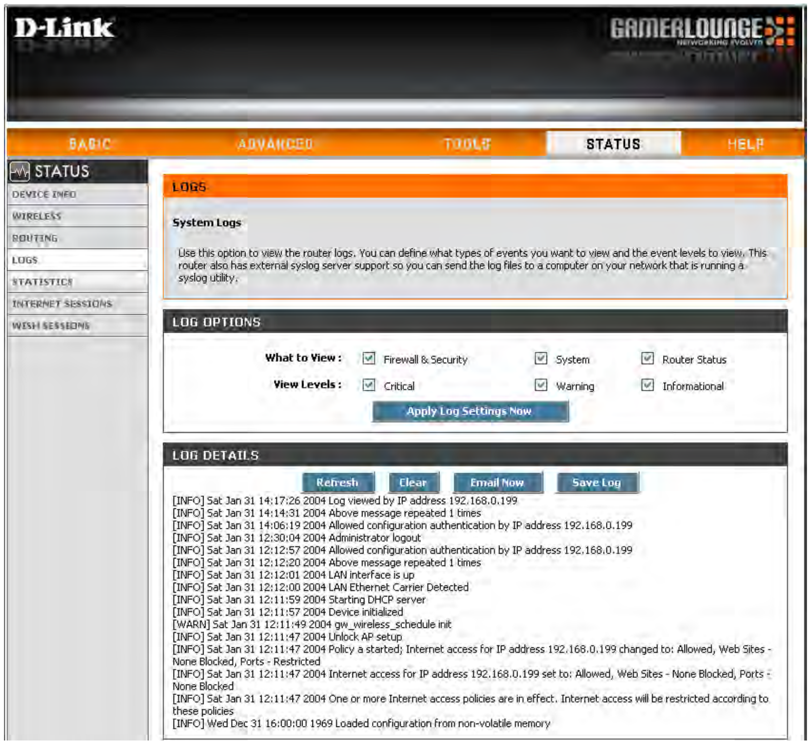
Apply Log Settings: Will filter the log results so that only the selected options appear.

Refresh: Updates the log details on the screen so it displays any recent activity.

Clear: Clears all of the log contents.

Email Now: This option will send a copy of the router log to the email address configured in the **Tools** > **Email** screen.

Save Log: This option will save the router to a log file on your computer.



LOGS

System Logs

Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has external syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

LOG OPTIONS

What to View : ☑ Firewall & Security ☑ System ☑ Router Status

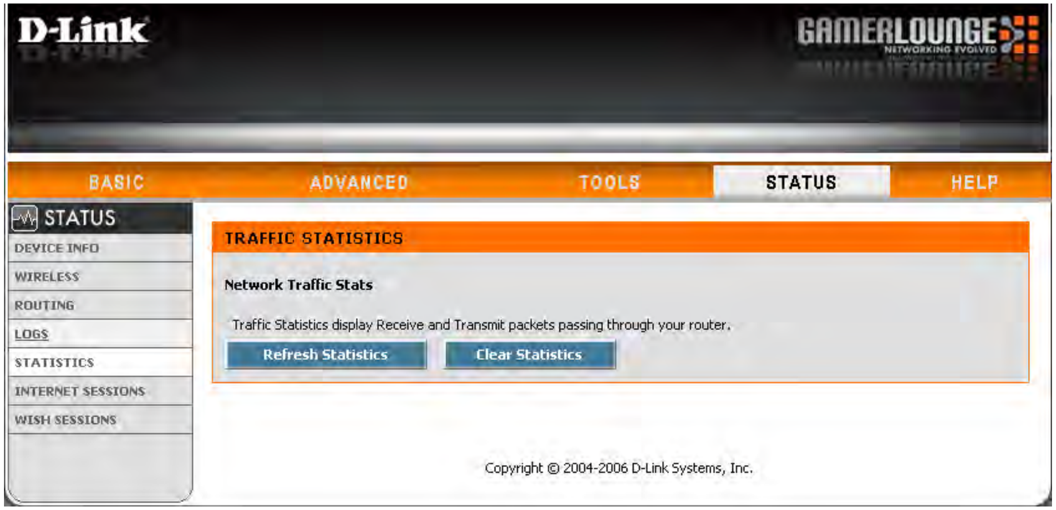
View Levels : ☑ Critical ☑ Warning ☑ Informational

LOG DETAILS

```
[INFO] Sat Jan 31 14:17:26 2004 Log viewed by IP address 192.168.0.199
[INFO] Sat Jan 31 14:14:31 2004 Above message repeated 1 times
[INFO] Sat Jan 31 14:06:19 2004 Allowed configuration authentication by IP address 192.168.0.199
[INFO] Sat Jan 31 12:30:04 2004 Administrator logout
[INFO] Sat Jan 31 12:12:57 2004 Allowed configuration authentication by IP address 192.168.0.199
[INFO] Sat Jan 31 12:12:20 2004 Above message repeated 1 times
[INFO] Sat Jan 31 12:12:01 2004 LAN interface is up
[INFO] Sat Jan 31 12:12:00 2004 LAN Ethernet Carrier Detected
[INFO] Sat Jan 31 12:11:59 2004 Starting DHCP server
[INFO] Sat Jan 31 12:11:57 2004 Device initialized
[WARN] Sat Jan 31 12:11:49 2004 gw_wireless_schedule init
[INFO] Sat Jan 31 12:11:47 2004 Unlock AP setup
[INFO] Sat Jan 31 12:11:47 2004 Policy a started; Internet access for IP address 192.168.0.199 changed to: Allowed, Web Sites -
None Blocked, Ports - Restricted
[INFO] Sat Jan 31 12:11:47 2004 Internet access for IP address 192.168.0.199 set to: Allowed, Web Sites - None Blocked, Ports -
None Blocked
[INFO] Sat Jan 31 12:11:47 2004 One or more Internet access policies are in effect. Internet access will be restricted according to
these policies
[INFO] Wed Dec 31 16:00:00 1969 Loaded configuration from non-volatile memory
```

Statistics

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DGL-4500 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.



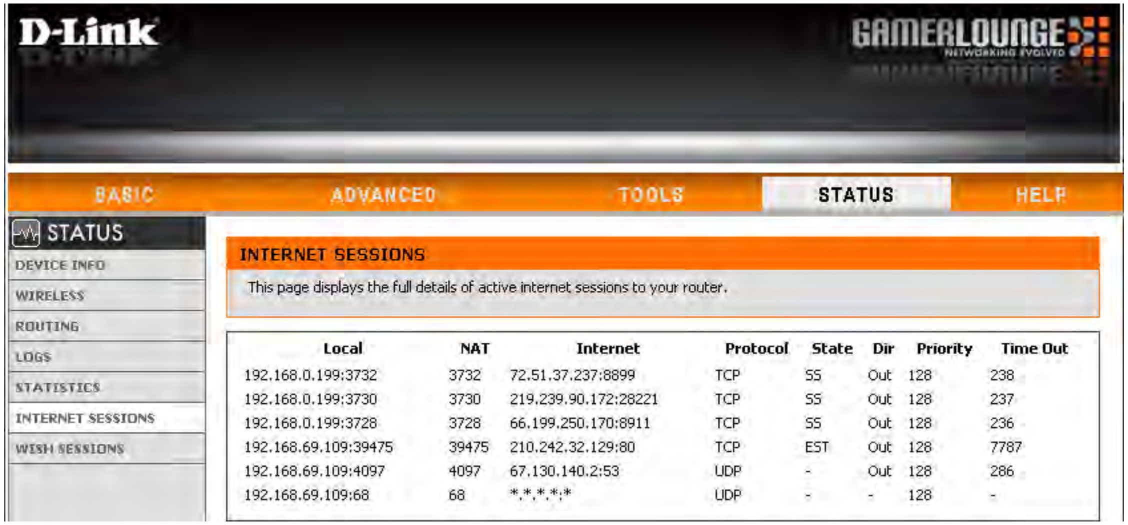
TRAFFIC STATISTICS

Network Traffic Stats

Traffic Statistics display Receive and Transmit packets passing through your router.

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

Internet Sessions

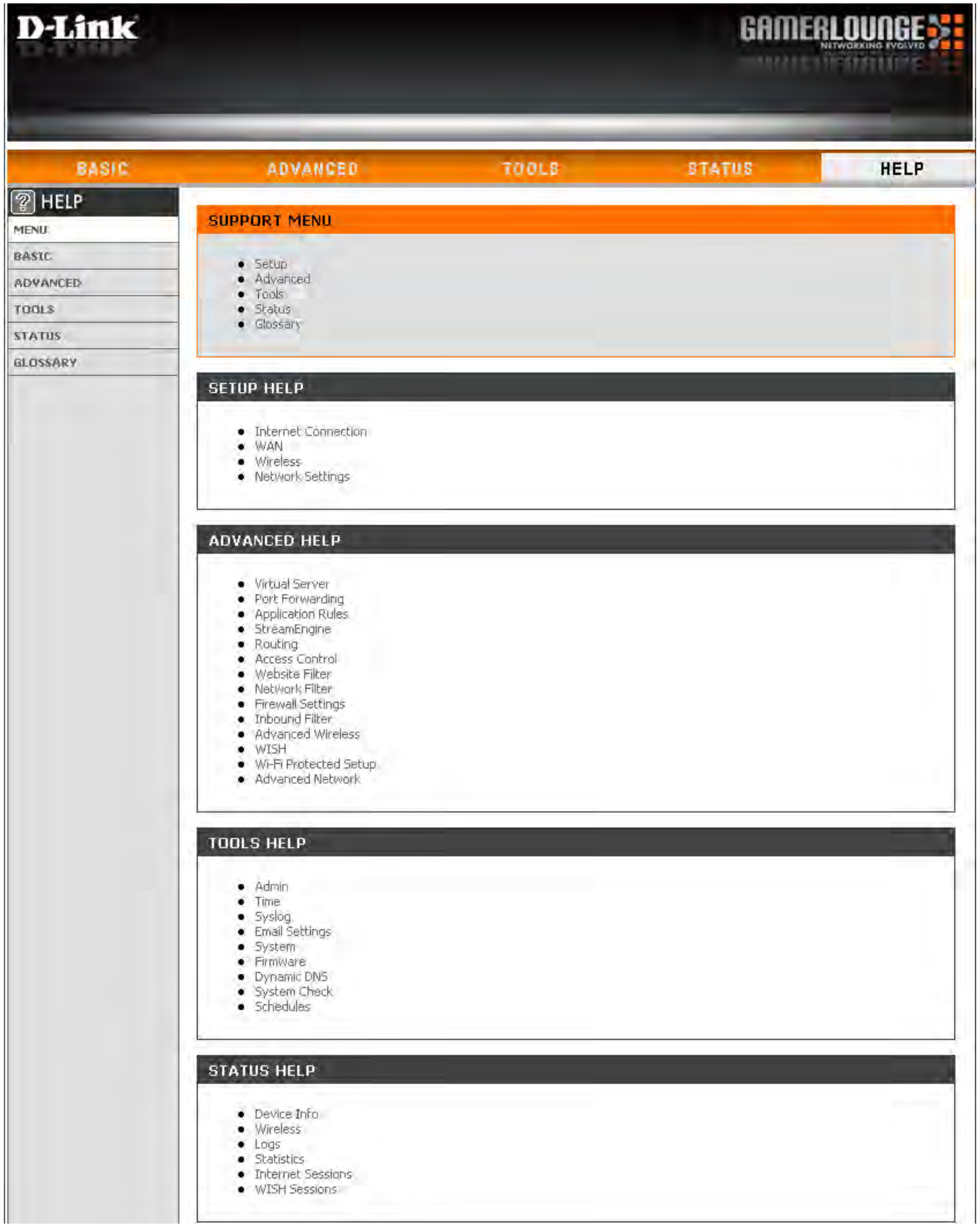


INTERNET SESSIONS

This page displays the full details of active internet sessions to your router.

Local	NAT	Internet	Protocol	State	Dir	Priority	Time Out
192.168.0.199:3732	3732	72.51.37.237:8899	TCP	SS	Out	128	238
192.168.0.199:3730	3730	219.239.90.172:28221	TCP	SS	Out	128	237
192.168.0.199:3728	3728	66.199.250.170:8911	TCP	SS	Out	128	236
192.168.69.109:39475	39475	210.242.32.129:80	TCP	EST	Out	128	7787
192.168.69.109:4097	4097	67.130.140.2:53	UDP	-	Out	128	286
192.168.69.109:68	68	*.*.*.*:*	UDP	-	-	128	-

Help



SUPPORT MENU

- Setup
- Advanced
- Tools
- Status
- Glossary

SETUP HELP

- Internet Connection
- WAN
- Wireless
- Network Settings

ADVANCED HELP

- Virtual Server
- Port Forwarding
- Application Rules
- StreamEngine
- Routing
- Access Control
- Website Filter
- Network Filter
- Firewall Settings
- Inbound Filter
- Advanced Wireless
- WISH
- Wi-Fi Protected Setup
- Advanced Network

TOOLS HELP

- Admin
- Time
- Syslog
- Email Settings
- System
- Firmware
- Dynamic DNS
- System Check
- Schedules

STATUS HELP

- Device Info
- Wireless
- Logs
- Statistics
- Internet Sessions
- WISH Sessions

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DGL-4500 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WPA?

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

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

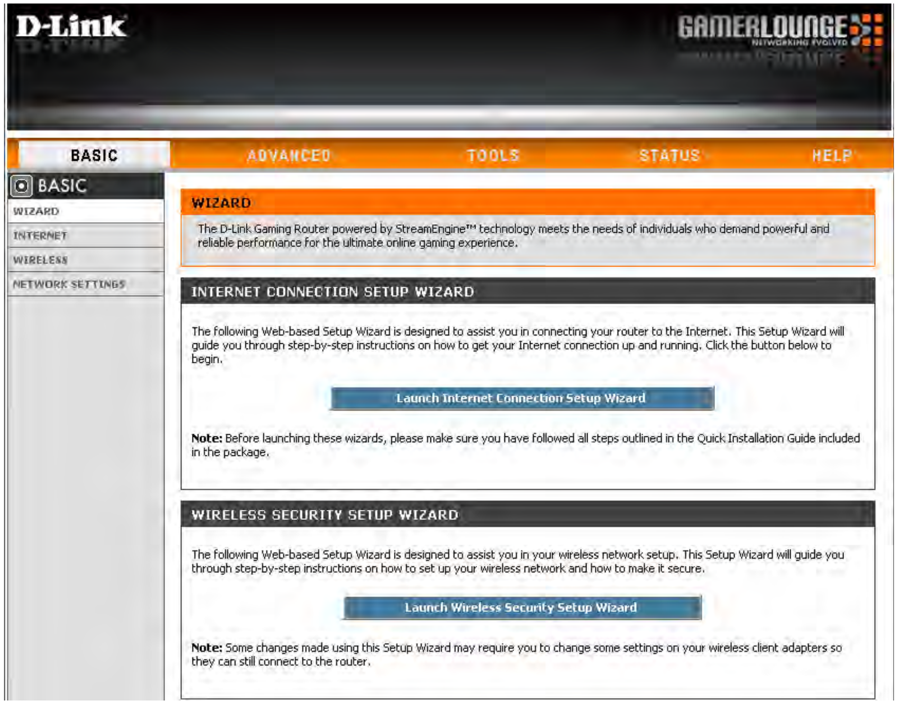
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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

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

Wireless Security Setup Wizard

To run the security wizard, click on Setup at the top and then click **Launch Wireless Security Setup Wizard**.



WIZARD

The D-Link Gaming Router powered by StreamEngine™ technology meets the needs of individuals who demand powerful and reliable performance for the ultimate online gaming experience.

INTERNET CONNECTION SETUP WIZARD

The following Web-based Setup Wizard is designed to assist you in connecting your router to the Internet. This Setup Wizard will guide you through step-by-step instructions on how to get your Internet connection up and running. Click the button below to begin.

Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

WIRELESS SECURITY SETUP WIZARD

The following Web-based Setup Wizard is designed to assist you in your wireless network setup. This Setup Wizard will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

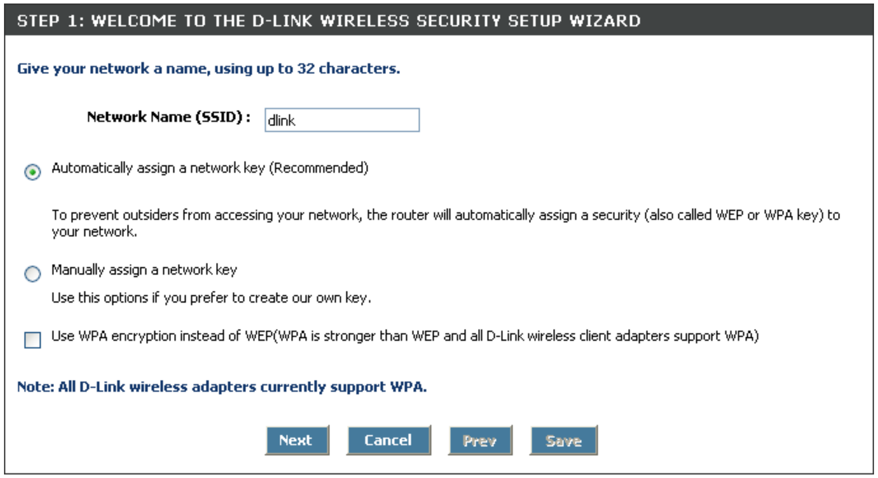
Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the router.

Type your desired wireless network name (SSID).

Automatically: Select this option to automatically generate the router's network key and click **Next**.

Manually: Select this option to manually enter your network key and click **Next**.

Check the "**Use WPA encryption...**" box to use WPA instead of WEP (strongly recommended).



STEP 1: WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Give your network a name, using up to 32 characters.

Network Name (SSID) : dlink

● Automatically assign a network key (Recommended)

To prevent outsiders from accessing your network, the router will automatically assign a security (also called WEP or WPA key) to your network.

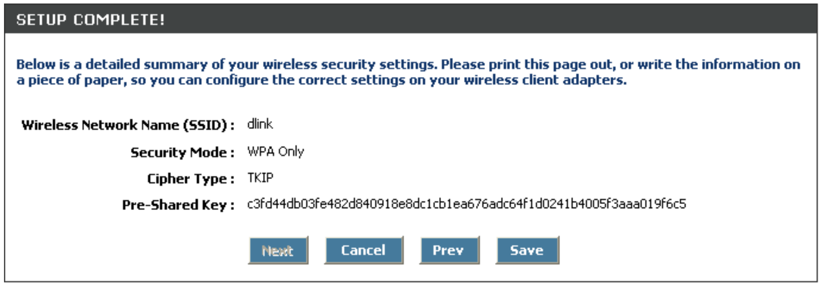
○ Manually assign a network key

Use this options if you prefer to create our own key.

□ Use WPA encryption instead of WEP(WPA is stronger than WEP and all D-Link wireless client adapters support WPA)

Note: All D-Link wireless adapters currently support WPA.

If you selected **Automatically**, the summary window will display your settings. Write down the security key and enter this on your wireless clients. Click **Save** to save your settings.



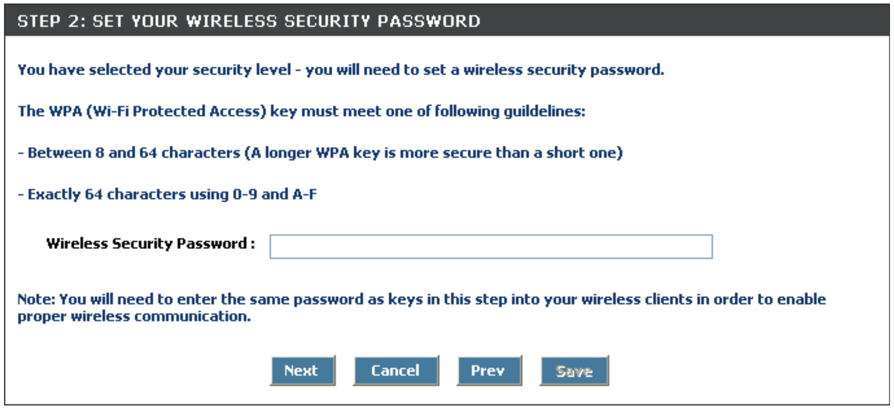
SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) :	dlink
Security Mode :	WPA Only
Cipher Type :	TKIP
Pre-Shared Key :	c3fd44db03fe482d840918e8dc1cb1ea676adc64f1d0241b4005f3aaa019f6c5

If you selected **Manually**, the following screen will appear.

Enter your security key. If you checked the WPA box on the previous page, make sure your key is between 8-64 characters. If you are using WEP (WPA box is unchecked), you must enter exactly 64 characters (only 0-9 and A-F are valid). Click **Save** to save your settings.



STEP 2: SET YOUR WIRELESS SECURITY PASSWORD

You have selected your security level - you will need to set a wireless security password.

The WPA (Wi-Fi Protected Access) key must meet one of following guildelines:

- Between 8 and 64 characters (A longer WPA key is more secure than a short one)

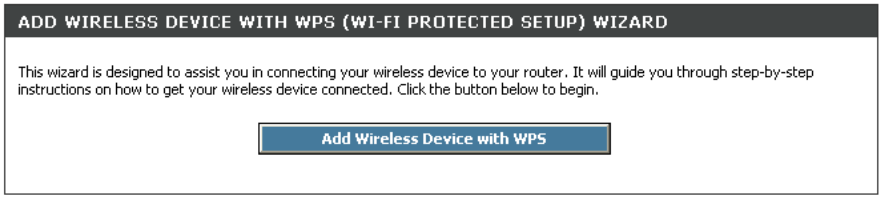
- Exactly 64 characters using 0-9 and A-F

Wireless Security Password :

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

Add Wireless Device with WPS Wizard

From the **Basic** > **Wizard** screen, click **Add Wireless Device with WPS**.

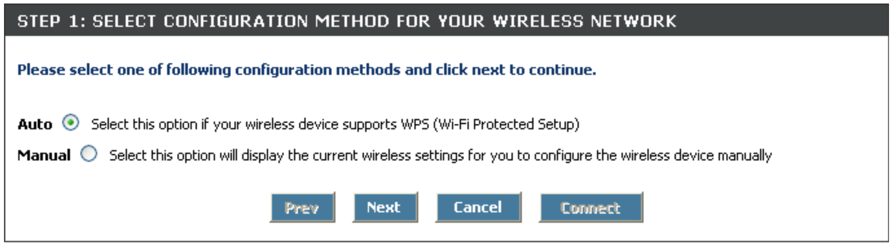


ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

Select **Auto** to add a wireless client using WPS (Wi-Fi Protected Setup). Once you select **Auto** and click **Connect**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

If you select **Manual**, a settings summary screen will appear. Write down the security key and enter this on your wireless clients.



STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

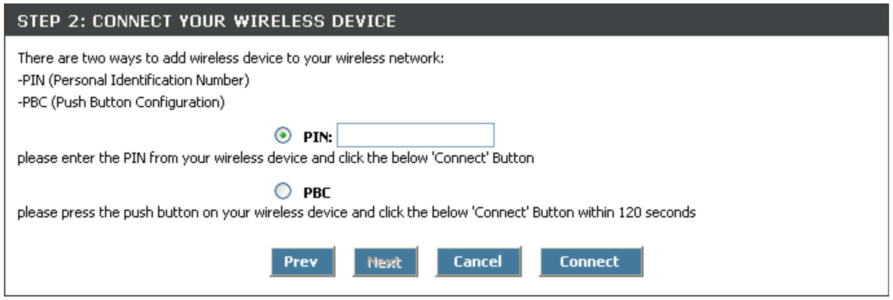
Please select one of following configuration methods and click next to continue.

Auto ● Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

Manual ○ Select this option will display the current wireless settings for you to configure the wireless device manually

PIN: Select this option to use PIN method. In order to use this method you must know the wireless client's 8 digit PIN and click **Connect**.

PBC: Select this option to use PBC (Push Button) method to add a wireless client. Click **Connect**.



STEP 2: CONNECT YOUR WIRELESS DEVICE

There are two ways to add wireless device to your wireless network:
-PIN (Personal Identification Number)
-PBC (Push Button Configuration)

● PIN:

please enter the PIN from your wireless device and click the below 'Connect' Button

○ PBC

please press the push button on your wireless device and click the below 'Connect' Button within 120 seconds

Configure WEP

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.

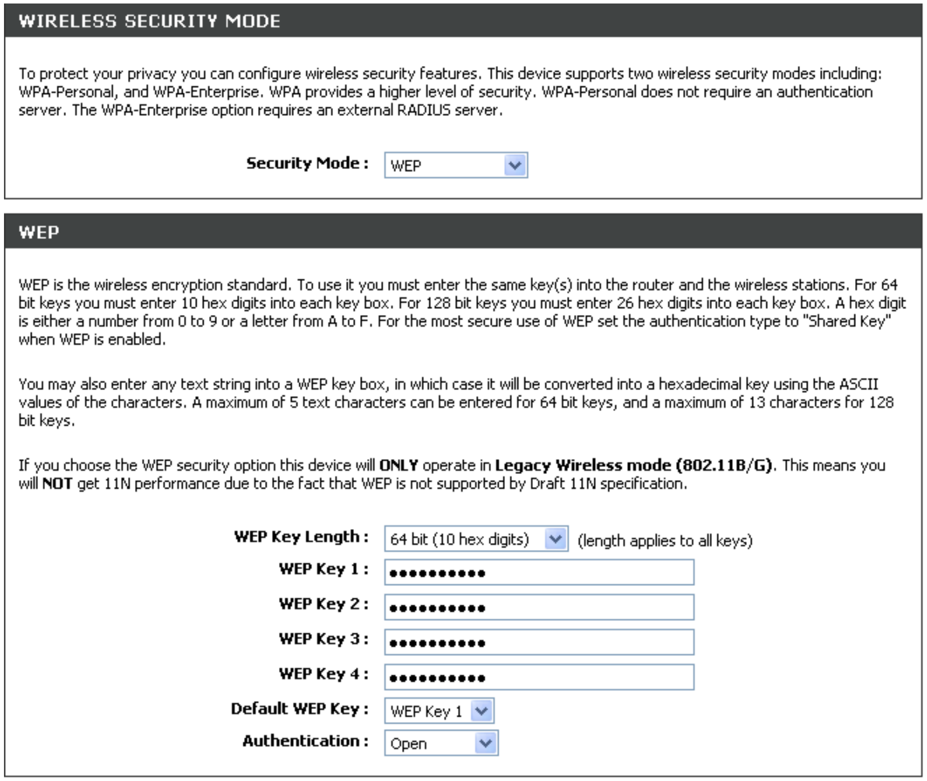
2. Next to *Security Mode*, select **WEP**.

3. Next to *WEP Key Length*, select the level of encryption (64 or 128-bit).

   Hex - (recommended) Letters A-F and numbers 0-9 are valid.

4. Next to *WEP Key 1*, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.

5. Next to *Authentication*, select **Shared Key**.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WPA-Personal, and WPA-Enterprise. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WEP

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by Draft 11N specification.

WEP Key Length : 64 bit (10 hex digits) (length applies to all keys)
WEP Key 1 : ●●●●●●●●●●
WEP Key 2 : ●●●●●●●●●●
WEP Key 3 : ●●●●●●●●●●
WEP Key 4 : ●●●●●●●●●●
Default WEP Key : WEP Key 1
Authentication : Open

6. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the router.

Configure WPA-Personal (PSK)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

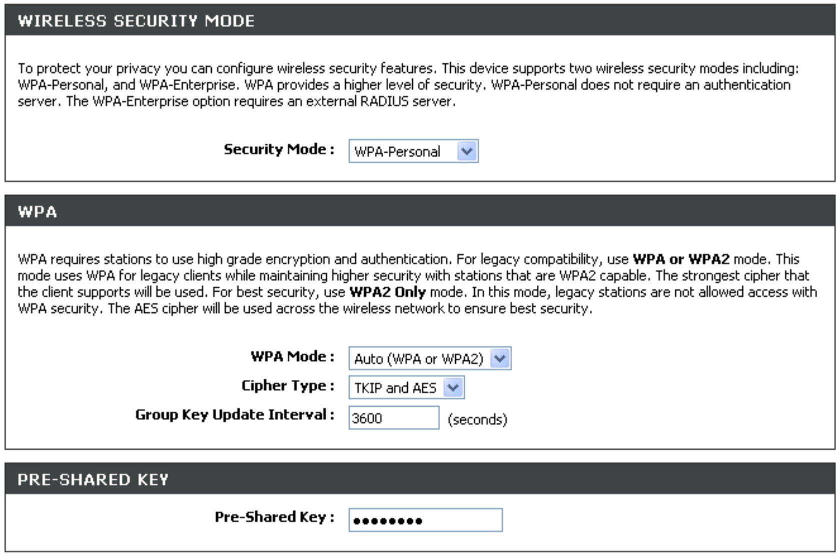
1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.

2. Next to *Security Mode*, select **WPA-Personal**.

3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

4. Next to *Cypher Type*, select **TKIP and AES**, **TKIP**, or **AES**.

5. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WPA-Personal, and WPA-Enterprise. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Personal

WPA

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

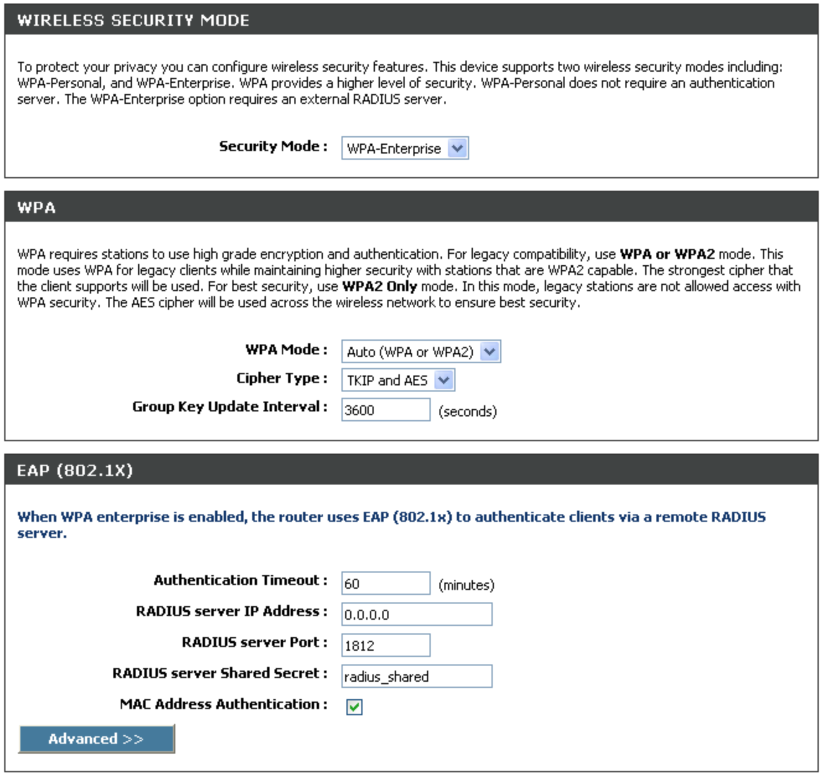
Pre-Shared Key : ••••••••

6. Next to *Pre-Shared Key*, enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.

7. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.

Configure WPA-Enterprise (RADIUS)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WPA-Personal, and WPA-Enterprise. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Enterprise

WPA

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : 60 (minutes)

RADIUS server IP Address : 0.0.0.0

RADIUS server Port : 1812

RADIUS server Shared Secret : radius_shared

MAC Address Authentication : ☑

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.

2. Next to *Security Mode*, select **WPA-Enterprise**.

3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

4. Next to *Cypher Type*, select **TKIP and AES**, **TKIP**, or **AES**.

5. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

6. Next to *Authentication Timeout*, enter the amount of time before a client is required to re-authenticate (60 minutes is default).

7. Next to *RADIUS Server IP Address* enter the IP Address of your RADIUS server.

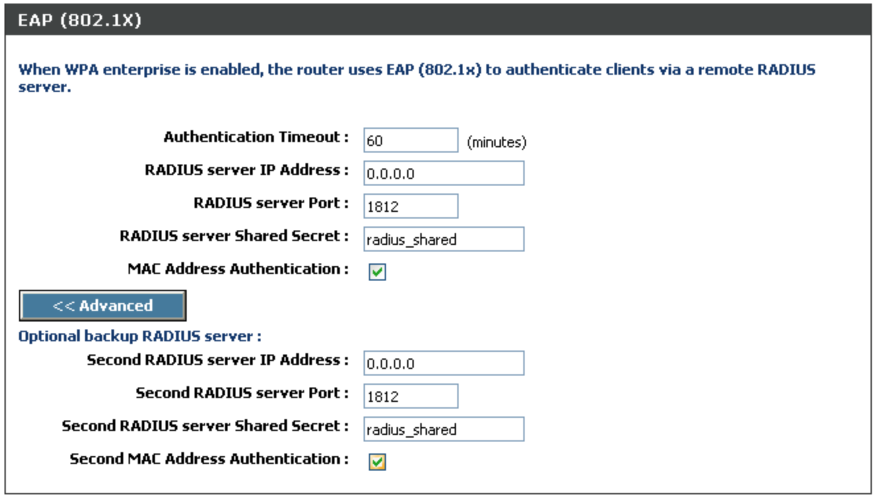
8. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.

9. Next to *RADIUS Server Shared Secret*, enter the security key.

10. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.

11. Click **Advanced** to enter settings for a secondary RADIUS Server.

12. Click **Apply Settings** to save your settings.



EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : 60 (minutes)
RADIUS server IP Address : 0.0.0.0
RADIUS server Port : 1812
RADIUS server Shared Secret : radius_shared
MAC Address Authentication : ☑

Optional backup RADIUS server :
Second RADIUS server IP Address : 0.0.0.0
Second RADIUS server Port : 1812
Second RADIUS server Shared Secret : radius_shared
Second MAC Address Authentication : ☑