

DNS Servers: The DNS server information will be supplied by your ISP (Internet Service Provider.)

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Internet Setup

L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

Address Mode: Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**.

L2TP IP Address: Enter the L2TP IP address supplied by your ISP (Static only).

L2TP Subnet Mask: Enter the Subnet Mask supplied by your ISP (Static only).

L2TP Gateway: Enter the Gateway IP Address provided by your ISP.

L2TP Server IP: Enter the Server IP provided by your ISP (optional).

Username: Enter your L2TP username.

Password: Enter your L2TP password and then retype the password in the next box.

Reconnect Mode: Select either **Always-on**, **On-Demand**, or **Manual**.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

DNS Servers: Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : L2TP (Username / Password) ▼

L2TP INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : Dynamic IP Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : Always on On demand Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1400

MAC Address :

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

Clone MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Internet Setup Static (assigned by ISP)

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

IP Address: Enter the IP address assigned by your ISP.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

DNS Servers: The DNS server information will be supplied by your ISP (Internet Service Provider.)

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

INTERNET CONNECTION TYPE	
Choose the mode to be used by the router to connect to the Internet.	
My Internet Connection is :	Static IP <input type="button" value="v"/>
STATIC IP ADDRESS INTERNET CONNECTION TYPE :	
Enter the static address information provided by your Internet Service Provider (ISP).	
IP Address :	<input type="text" value="0.0.0.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Default Gateway :	<input type="text" value="0.0.0.0"/>
Primary DNS Server :	<input type="text" value="0.0.0.0"/>
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>
MTU :	<input type="text" value="1500"/> (bytes) MTU default = 1500
MAC Address :	<input type="text" value="00:00:00:00:00:00"/>
	<input type="button" value="Clone Your PC's MAC Address"/>

Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click **Wireless Network Setup Wizard** and refer to page 71.

Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 73.

If you want to manually configure the wireless settings on your router click **Manual Wireless Network Setup** and refer to the next page.

D-Link

DIR-825

INTERNET

WIRELESS SETTINGS

NETWORK SETTINGS

SETUP ADVANCED TOOLS STATUS

WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection. Before purchasing these wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

[Wireless Network Setup Wizard](#)

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 D-Link Router.

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

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

[Add Wireless Device with WPS](#)

MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

[Manual Wireless Network Setup](#)

Helpful Hints...

If you already have a wireless network setup with Wi-Fi Protected Setup, click on **Add Wireless Device with WPS Wizard** to add new device to your wireless network.

If you are new to wireless networking and have never configured a wireless router before, click on **Wireless Network Setup Wizard** and the router will guide you through a few simple steps to get your wireless network up and running.

If you consider yourself an advanced user and have configured a wireless router before, click **Manual Wireless Network Setup** to input all the settings manually.

[More...](#)

WIRELESS

Manual Wireless Settings 802.11n/g (2.4GHz)

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

Schedule: Select the time frame that you would like your wireless network enabled. The schedule may be set to **Always**. Any schedule you create will be available in the drop-down menu. Click **Add New** to create a new schedule.

Wireless Network Name: Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

802.11 Mode: Select one of the following:

802.11g Only - Select if all of your wireless clients are 802.11g.

Mixed 802.11n and 802.11g - Select if you are using both 802.11n and 802.11g wireless clients.

802.11n Only - Select only if all of your wireless clients are 802.11n.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DIR-825 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-825. 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.

WIRELESS NETWORK SETTINGS

Wireless Band : 2.4GHz Band

Enable Wireless : Always Add New

Wireless Network Name : dlink (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Enable Auto Channel Scan :

Wireless Channel : 2.437GHz - CH 6

Transmission Rate : Best (automatic) (Mbit/s)

Channel Width : 20 MHz

Visibility Status : Visible Invisible

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. 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

Channel Width: Select the Channel Width:

Auto 20/40 - This is the default setting. 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.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-825. If Invisible is selected, the SSID of the DIR-825 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-825 in order to connect to it.

Wireless Security: Refer to page 71 for more information regarding wireless security.

802.11n/a (5GHz)

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

Schedule: Select the time frame that you would like your wireless network enabled. The schedule may be set to **Always**. Any schedule you create will be available in the drop-down menu. Click **Add New** to create a new schedule.

Wireless Network Name: Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

802.11 Mode: Select one of the following:

802.11a Only - Select if all of your wireless clients are 802.11a.

Mixed 802.11n and 802.11a - Select if you are using both 802.11n and 802.11a wireless clients.

802.11n Only - Select only if all of your wireless clients are 802.11n.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DIR-825 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-825. 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.

WIRELESS NETWORK SETTINGS

Wireless Band : **5GHz Band**

Enable Wireless : Always Add New

Wireless Network Name : (Also called the SSID)

802.11 Mode : Mixed 802.11n and 802.11a

Enable Auto Channel Scan :

Wireless Channel : 5, 200 GHz - CH 40

Transmission Rate : Best (automatic) (Mbit/s)

Channel Width : 20 MHz

Visibility Status : Visible Invisible

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. 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 : None

Channel Width: Select the Channel Width:

Auto 20/40 - This is the default setting. 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.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-825. If Invisible is selected, the SSID of the DIR-825 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-825 in order to connect to it.

Wireless Security: Refer to page 71 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.

Router Settings

Router 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.

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
Device Name: dlinkrouter
Local Domain Name: (optional)
Enable DNS Relay:

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-825 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 DIR-825. 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.
Server: 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: 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

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:

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address
NUMBER OF DYNAMIC DHCP CLIENTS: 1			
Hardware Address	Assigned IP	Hostname	Expires
00:16:36:a6:58:11	192.168.0.172	Ferrari-5000	22 Hours 3 Minutes
			Revoke Reserve

Virtual Server

The DIR-825 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 DIR-825 firewall filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-825 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 DIR-825 redirects the external service request to the appropriate server within the LAN network.

The DIR-825 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 the next page.

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 <<.

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.

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

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.

DIR-825

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

24--VIRTUAL SERVERS LIST

Name	IP Address	Application Name	Computer Name	Port	Traffic Type	Schedule
	0.0.0.0			Public	TCP	Always
	0.0.0.0			Private	6	Inbound Filter
	0.0.0.0			Public	Protocol	Schedule
	0.0.0.0			Private	TCP	Always
	0.0.0.0			Public	6	Inbound Filter
	0.0.0.0			Private	Protocol	Schedule
	0.0.0.0			Public	TCP	Always
	0.0.0.0			Private	6	Inbound Filter
	0.0.0.0			Public	Protocol	Schedule
	0.0.0.0			Private	TCP	Always
	0.0.0.0			Public	6	Inbound Filter
	0.0.0.0			Private	Protocol	Schedule
	0.0.0.0			Public	TCP	Always
	0.0.0.0			Private	6	Inbound Filter
	0.0.0.0			Public	Protocol	Schedule
	0.0.0.0			Private	TCP	Always
	0.0.0.0			Public	6	Inbound Filter
	0.0.0.0			Private	Protocol	Schedule
	0.0.0.0			Public	TCP	Always

Helpful Hints--

Check the Application Name drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the Computer Name drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.

Select a schedule for which the virtual server will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools > Schedules** screen and create a new schedule.

Select a filter that restricts the Internet hosts that can access this virtual server. If you do not see the filter you need in the list of filters, go to the **Advanced Filter** screen and create a new filter.

Home--

Port Forwarding

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

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.

PORT FORWARDING

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, 85, 888), or Mixed (1020-5000, 599). This option is only applicable to the INTERNET session.

Save Settings Port Forward Settings

24 -- PORT FORWARDING RULES

Name	Application Name	Computer Name	Ports to Open	Schedule
<input type="checkbox"/> IP Address 0.0.0.0	<<	<<	TCP	Always
<input type="checkbox"/> Name	<<	<<	LDP	Inbound Filter Allow All
<input type="checkbox"/> IP Address 0.0.0.0	<<	<<	LDP	Schedule Always
<input type="checkbox"/> Name	<<	<<	LDP	Inbound Filter Allow All
<input type="checkbox"/> IP Address 0.0.0.0	<<	<<	TCP	Schedule Always
<input type="checkbox"/> Name	<<	<<	LDP	Inbound Filter Allow All
<input type="checkbox"/> IP Address 0.0.0.0	<<	<<	TCP	Schedule Always
<input type="checkbox"/> Name	<<	<<	LDP	Inbound Filter Allow All
<input type="checkbox"/> IP Address 0.0.0.0	<<	<<	TCP	Schedule Always
<input type="checkbox"/> Name	<<	<<	LDP	Inbound Filter Allow All

Helpful Hints:

Check the Application Name drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding fields.

You can select a computer from the list of DHCP clients in the Computer Name drop down menu, or you can manually enter the IP address of the LAN computer to which you would like to open the specified port.

Select a schedule for when the rule will be enabled. If you do not see the schedule you need in the list of schedules, go to the Tools > Schedules screen and create a new schedule.

You can enter ports in various formats:

Range (50-100)
Individual (80, 66, 688)
Mixed (1020-5000, 888)

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 DIR-825. 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 DIR-825 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

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.

DIR-825

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

24 -- APPLICATION RULES

Name	Application	Trigger	Port	Traffic Type	Schedule
<input type="checkbox"/>	<< Application Name >>	Trigger	Trigger	TCP	Always
<input type="checkbox"/>	<< Application Name >>	Firewall	Firewall	TCP	Always
<input type="checkbox"/>	<< Application Name >>	Trigger	Trigger	TCP	Always
<input type="checkbox"/>	<< Application Name >>	Firewall	Firewall	TCP	Always
<input type="checkbox"/>	<< Application Name >>	Trigger	Trigger	TCP	Always
<input type="checkbox"/>	<< Application Name >>	Firewall	Firewall	TCP	Always
<input type="checkbox"/>	<< Application Name >>	Trigger	Trigger	TCP	Always
<input type="checkbox"/>	<< Application Name >>	Firewall	Firewall	TCP	Always

Helpful Hint...

Use this feature if you are trying to execute one of the listed network applications and it is not communicating as expected.

Check the Application Name drop-down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop-down menu to fill out the corresponding field.

Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools > Schedules** screen and create a new schedule.

[More...](#)

QoS Engine

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

Enable Traffic Shaping: 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 Uplink Speed: This option is enabled by default when the QoS Engine 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.

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.

QoS ENGINE
Use this section to configure D-Link's QoS engine. The QoS engine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as web browsing, file transfers, etc. The Automatic Classification option is auto-enabled; set the priority for your applications.

Save Settings Don't Save Settings

WAN TRAFFIC SHAPING

Enable Traffic Shaping:
 Automatic Uplink Speed:
 Measured Uplink Speed: Not Estimated
 Manual Uplink Speed: 178 kbps << Speed Transient Rate >>
 Connection Type: Auto-detect
 Detected xDSL or Other Frame Relay Network:

QoS ENGINE SETUP

Enable QoS Engine:
 Automatic Classification:
 Dynamic Fragmentation:

1.0 QoS ENGINE RULES

Name	Priority	Protocol
Local IP Range	1 (1..255)	TCP
Remote IP Range	0	0
Local Port Range	0	65535
Remote Port Range	0	65535

SUPPORT
Helpful links...
If the Measured Uplink Speed is shown to be incorrect, this is due to network congestion or performance. Check Automatic Uplink Speed and click the Manual Uplink Speed. Some experimentation and patience may be required to converge on the optimal value. [Here...](#)

Enable QoS Engine: 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.

Network 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 Filtering**, or **Deny MAC Filtering**.
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.

Clear: Click to remove the MAC address.

24 -- MAC FILTERING RULES
 Configure MAC Filtering below:
 Turn MAC Filtering OFF

MAC Address	DHCP Client List	Clear
<input type="text"/>	Computer Name	Clear
<input type="text"/>	Computer Name	Clear
<input type="text"/>	Computer Name	Clear
<input type="text"/>	Computer Name	Clear
<input type="text"/>	Computer Name	Clear
<input type="text"/>	Computer Name	Clear

Helpful Hints...
 Create a list of MAC addresses that you would either like to allow or deny access to your network.
 Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a client from the drop-down menu, then click the arrow to add that device's MAC address to the list.
 Click the **Clear** button to remove the MAC address from the MAC Filtering list.
[More...](#)

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.