

# Firewall Settings

A firewall protects your network from the outside world. The DIR-825 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

**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.

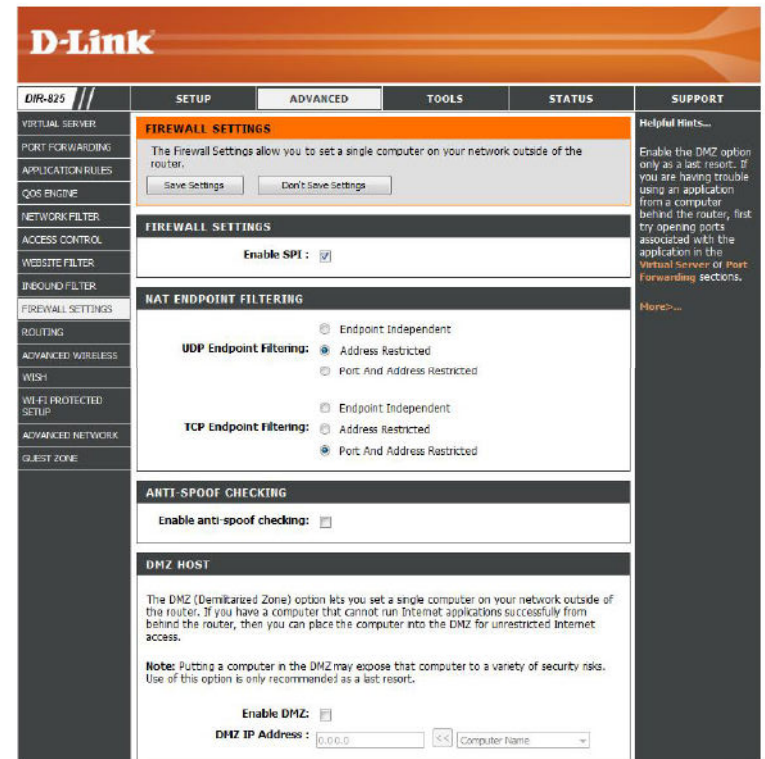
**Address + Port Restriction** - Incoming traffic must match the IP address and port of the outgoing connection.

**Anti-Spoof Check:** Enable this feature to protect your network from certain kinds of “spoofing” attacks.

**Enable DMZ:** 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.

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



# Routing

The Routing option is an advanced method of customizing specific routes of data through your network.

**Destination IP:** Enter the IP address of packets that will take this route.

**Netmask:** Enter the netmask of the route, please note that the octets must match your destination IP address.

**Gateway:** Enter your next hop gateway to be taken if this route is used.

**Metric:** The route metric is a value from 1 to 16 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

**Interface:** Select the interface that the IP packet must use to transit out of the router when this route is used.

**D-Link**

DIR-825 // SETUP ADVANCED TOOLS STATUS SUPPORT

**ROUTING**

This Routing page allows you to specify custom routes that determine how data is moved around your network.

Save Settings Don't Save Settings

**32--ROUTE LIST**

Name	Destination IP	Metric	Interface
<input type="checkbox"/> Name	0.0.0.0	1	WAN
<input type="checkbox"/> Netmask	0.0.0.0		
<input type="checkbox"/> Name	0.0.0.0	1	WAN
<input type="checkbox"/> Netmask	0.0.0.0		
<input type="checkbox"/> Name	0.0.0.0	1	WAN
<input type="checkbox"/> Netmask	0.0.0.0		
<input type="checkbox"/> Name	0.0.0.0	1	WAN
<input type="checkbox"/> Netmask	0.0.0.0		

**Helpful Hints...**

Each route has a check box next to it. Check this box if you want the route to be enabled.

The name field allows you to specify a name for identification of the route, e.g. 'Network 2'

The destination IP address is the address of the host or network you wish to reach.

The netmask field identifies the portion of the destination IP in use.

The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

[More...](#)

## Advanced Wireless Settings

### 802.11n/g (2.4GHz)

**Transmit Power:** Set the transmit power of the antennas.

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

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

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

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

**WLAN Partition:** Enable this option to prevent associated wireless clients from communicating with each other.

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

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

**ADVANCED WIRELESS SETTINGS**

**Wireless Band :** 2.4GHz Band

**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 :**

## Advanced Wireless Settings

### 802.11n/a (5GHz)

**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 2342. If inconsistent data flow is a problem, only a minor modification should be made.

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

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

**WLAN Partition:** Enable this option to prevent associated wireless clients from communicating with each other.

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

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

**ADVANCED WIRELESS SETTINGS**

**Wireless Band :** 5GHz Band

**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 :**

# WISH Settings

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

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

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

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

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

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

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

The screenshot displays the WISH configuration interface for a D-Link DIR-825 router. The 'WISH' section is active, showing the 'Enable WISH' checkbox checked. Under 'PRIORITY CLASSIFIERS', 'HTTP' and 'Windows Media Center' are checked, while 'Automatic' is unchecked. Below, there are two 'WISH RULES' sections, each with fields for Name, Priority (Best Effort Low (BE LO)), Protocol (6), Host 1 IP Range (0.0.0.0 to 255.255.255.255), Host 1 Port Range (0 to 65535), Host 2 IP Range (0.0.0.0 to 255.255.255.255), and Host 2 Port Range (0 to 65535).

**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.

Name	Priority	Protocol
<input type="text"/>	Best Effort Low(BE LO) ▼	6 << TCP ▼
Host 1 IP Range	Host 1 Port Range	
<input type="checkbox"/> 0.0.0.0 to 255.255.255.255	0 to 65535	
Host 2 IP Range	Host 2 Port Range	
0.0.0.0 to 255.255.255.255	0 to 65535	

## Wi-Fi Protected Setup (WPS)

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

**Enable:** Enable the Wi-Fi Protected Setup feature.

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

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

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

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

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

**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. If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN. However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

Save Settings    Don't Save Settings

---

**WI-FI PROTECTED SETUP**

Enable :

Lock Wireless Security Settings :

Reset to Unconfigured

---

**PIN SETTINGS**

Current PIN : 67252190

Reset PIN to Default    Generate New PIN

---

**ADD WIRELESS STATION**

Add Wireless Device with WPS

---

**Helpful Hints...**

Enable if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup.

Only "Admin" account can change security settings.

Lock Wireless Security Settings after all wireless network devices have been configured.

Click Add Wireless Device Wizard to use Wi-Fi Protected Setup to add wireless devices to the wireless network.

More...

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

**Station:**

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

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

**Add Wireless** Start the wizard.

**Device Wizard:**



# Advanced Network Settings

**Enable UPnP:** 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 DIR-825 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 Ping Inbound Filter:** Select from the drop-down menu if you would like to apply the Inbound Filter to the WAN ping. Refer to page 45 for more information regarding Inbound Filter.

**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.

**D-Link**

DIR-825 // SETUP ADVANCED TOOLS STATUS SUPPORT

**ADVANCED NETWORK**

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

Save Settings Don't Save Settings

**UPNP**

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

Enable UPnP :

**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 :

Details :

**WAN PORT SPEED**

WAN Port Speed :

**MULTICAST STREAMS**

Enable Multicast Streams :

**Helpful Hints...**

UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.

For added security, it is recommended that you disable the WAN Ping Respond option. Ping is often used by malicious Internet users to locate active networks or PCs.

The WAN speed is usually detected automatically. If you are having problems connecting to the WAN, try selecting the speed manually.

If you are having trouble receiving multicast streams from the Internet, make sure the Multicast Streams option is enabled.

More...

**WIRELESS**

# Guest Zone

The Guest Zone feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network. You may configure different zones for the 2.4GHz and 5.0GHz wireless bands.

**Enable Guest Zone:** Check to enable the Guest Zone feature.

**Schedule:** The schedule of time when the Guest Zone will be active. 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.

**Wireless Network Name:** Enter a wireless network name (SSID) that is different from your main wireless network.

**Enable Routing Between Zones:** Check to allow network connectivity between the different zones created.

**Security Mode:** Select the type of security or encryption you would like to enable for the guest zone.

The screenshot shows the D-Link DIR-825 router configuration interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections, with GUEST ZONE selected. The main content area is titled 'GUEST ZONE' and contains two sections for configuring guest zones.

**GUEST ZONE**  
Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.  
Save Settings Don't Save Settings

**GUEST ZONE SELECTION**

Enable Guest Zone:  Always

Wireless Band: 2.4GHz Band

Wireless Network Name: dlink\_guest (Also called the SSID)

Enable Routing Between Zones:

Security Mode: None

**GUEST ZONE SELECTION**

Enable Guest Zone:  Always

Wireless Band: 5GHz Band

Wireless Network Name: dlink\_media\_guest (Also called the SSID)

Enable Routing Between Zones:

Security Mode: None

Helpful Hints...  
Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.  
More...

WIRELESS