

Access Control Wizard (continued)

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

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

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

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

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

Access Control Wizard (continued)

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 Filter Rules.
Specify rules to permit access to specific IP addresses and ports.

| Enable | Name | Dest IP Start | Dest IP End | Protocol | Dest Port Start | Dest Port End |
|--------------------------|------|---------------|-----------------|----------|-----------------|---------------|
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |
| <input type="checkbox"/> | | 3.3.0.0 | 192.168.192.255 | Any | 1 | 65535 |

Apply Cancel Save Cancel

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

Save Cancel Save Cancel

Your newly created policy will now show up under **Policy Table**.

D-Link

MANAGE // SETUP // ADVANCED // TOOLS // STATUS // SUPPORT

ACCESS CONTROL
This Access Control policy allows you to control access to any LAN or wireless network. You can specify the type of access, and the source IP address, and the destination IP address and port.

Access Control Table

| NAME | ENABLE | PROTOCOL | DEST IP START | DEST IP END | DEST PORT START | DEST PORT END | SCHEDULE | LOGGING |
|-------------------------|--------|----------|---------------|-------------|-----------------|---------------|----------|---------|
| Multiple Access Control | On | Any | | | | | | On |

POLICY TABLE

| Name | Policy | Protocol | Priority | Logging Schedule |
|-------------------------|--------|----------|----------|---------------------|
| Multiple Access Control | Any | Any | 100 | 10:00:00 - 20:00:00 |

Apply Cancel Save Cancel

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 **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section (page 41).

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

Website URL/ Domain: Enter the keywords or URLs that you want to allow or block. Click **Save Settings**.

The screenshot shows the D-Link DIR-825 web interface. The top navigation bar includes 'D-Link', 'DIR-825', and a list of menu items: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QoS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER (highlighted), INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WDS, WPA-PSK PROTECTED SETUP, ADVANCED NETWORK, and GUEST ZONE. The main content area is titled 'WEBSITE FILTER' and is divided into 'SETUP' and 'ADVANCED' tabs. The 'SETUP' tab is active and contains the following text: 'The Website Filter option allows you to set up a list of Web sites you would like to allow or deny through your network. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. To the right of the main content is a 'SUPPORT' section with 'Helpful Hints...' and a paragraph: 'Create a list of Web sites to which you would like to deny or allow through the network. Use with Advanced Access Control. More...'. Below the main content is a section titled '64 WEBSITE FILTERING RULES' with the instruction: 'Configure Website Filter below: DENY computers access to ONLY these sites'. There is a 'Clear the list below...' button and a table with the header 'Website URL / Domain' and several empty rows for input.

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.

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

Remote 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.

The screenshot shows the D-Link DIR-825 Web Management Interface. The top navigation bar includes 'VIRTUAL SERVER', 'PORT FORWARDING', 'APPLICATION RULES', 'QoS ENGINE', 'NETWORK FILTER', and 'ACCESS CONTROL'. The 'ACCESS CONTROL' section is active, showing 'WEBSITE FILTER' and 'INBOUND FILTER'. The 'INBOUND FILTER' page has tabs for 'SETUP', 'ADVANCED', 'TOOLS', and 'STATUS'. The 'SETUP' tab is selected, displaying the 'ADD INBOUND FILTER RULE' form. The form includes fields for 'Name', 'Action' (set to 'Deny'), 'Remote IP Range', 'Remote IP Start', and 'Remote IP End'. Below the form is a table titled 'INBOUND FILTER RULES LIST' with columns for 'Name', 'Action', and 'Remote IP Range'. A 'Helpful Hints...' section at the bottom provides additional information about the feature.

Helpful Hints...

Give each rule a **Name** that is meaningful to you.

Each rule can either **Allow** or **Deny** access from the WAN.

Up to eight ranges of WAN IP addresses can be controlled by each rule. The checkbox by each IP range can be used to disable ranges already defined.

The starting and ending IP addresses are WAN side address.

Click the **Add** or **Update** button to add a finished rule in the Rules List below.

Click the **Edit** icon in the Rules List to change a rule.

Click the **Delete** icon in the Rules List to permanently remove a rule.

Help...

ADD INBOUND FILTER RULE

Name: _____

Action: Deny

Remote IP Range: Enable **Remote IP Start** **Remote IP End**

| | | |
|--------------------------|---------|-----------------|
| <input type="checkbox"/> | 0.0.0.0 | 255.255.255.255 |
| <input type="checkbox"/> | 0.0.0.0 | 255.255.255.255 |
| <input type="checkbox"/> | 0.0.0.0 | 255.255.255.255 |
| <input type="checkbox"/> | 0.0.0.0 | 255.255.255.255 |
| <input type="checkbox"/> | 0.0.0.0 | 255.255.255.255 |
| <input type="checkbox"/> | 0.0.0.0 | 255.255.255.255 |
| <input type="checkbox"/> | 0.0.0.0 | 255.255.255.255 |

INBOUND FILTER RULES LIST

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

WIRELESS

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 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.

D-Link

DIR-825

DIR-825

POST-CONFIGURING

ACTIVATION GUIDE

QSS GUIDE

NETWORK TIPS

ALL-NEW USER MANUAL

DOWNLOADS

FIREWALL SETTINGS

TOOLS

STATUS

SUPPORT

FIREWALL SETTINGS

The "FIREWALL SETTINGS" allow you to set a single computer on your network outside of the router.

Save Settings

FIREWALL SETTINGS

Enable SPI:

NAT ENDPOINT FILTERING

Endpoint Independent: Address Restricted: Nat. Jan. Address Restriction:

Endpoint Independent: Address Restricted: Port/Jan. Address Restricted:

ANTI-SPOOF CHECKING

enable anti-spoof checking:

DMZ HOST

enable DMZ:

DMZ IP Address:

Helpful links:
Enable the DMZ option only on a LAN that you are having trouble with. If you are having trouble with a computer behind the router, first try connecting the computer to the Virtual Server or Port Forwarding tool first.

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you are having trouble with a computer behind the router, first try connecting the computer to the Virtual Server or Port Forwarding tool first.

Never put any computer in the DMZ unless you are sure that it is completely trustworthy. Use of the DMZ is not recommended as a last resort.

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.

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 this 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 to use.
The gateway IP address is the IP address of the router, if any, used to reach the specified destination.
[More...](#)

3.2 - ROUTE LIST

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

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 : | <input type="checkbox"/> |
| WMM Enable : | <input checked="" type="checkbox"/> |
| Short GI : | <input checked="" type="checkbox"/> |

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 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 : | 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 : | <input type="checkbox"/> | | |
| WMM Enable : | <input checked="" type="checkbox"/> | | |
| Short GI : | <input checked="" type="checkbox"/> | | |

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 shows the D-Link router's configuration interface. The 'WISH' section is active, with the following settings:

- WISH:** Description: WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications. Save Settings Don't Save Settings
- Enable WISH:**
- HTTP:**
- Windows Media Center:**
- Automatic:** (default if not matched by anything else)

The 'WISH RULES' section shows two rules:

| Name | Priority | Best Effort/Low(BE/LO) | Protocol |
|---|----------|------------------------|----------|
| Host 1 IP Range 0.0.0.0 to 255.255.255.255 | 6 | <<< | TCP |
| Host 2 IP Range 0.0.0.0 to 255.255.255.255 | 6 | <<< | TCP |

Helpful Hints...
 -Enable this option if you want to allow WISH to prioritize wireless traffic.
 For most applications, the priority classifiers ensure the right priorities, and specific WISH Rules are not required.
 Home...

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 |
|---|-----------------------|---------------------------------|
| Host 1 IP Range 0.0.0.0 to 255.255.255.255 | Best Effort Low(BELO) | 6. << TCP |
| Host 2 IP Range 0.0.0.0 to 255.255.255.255 | | Host 1 Port Range 0 to 65535 |
| | | Host 2 Port Range 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.

The screenshot shows the D-Link router's configuration page for Wi-Fi Protected Setup. The top navigation bar includes links for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The main content area is titled 'Wi-Fi Protected Setup' and contains the following sections:

- WPS Protected Setup:** A text box explaining that WPS Protected Setup is used to easily add devices to a network using a PIN or button press. It includes a 'Save Settings' button and a 'Don't Save Settings' button.
- WPS Protected Setup:** A section with 'Enable' checked and 'Lock Wireless Security Settings' unchecked. It includes a 'Reset to Unconfigured' button.
- PIN Settings:** A section showing the 'Current PIN' as 07252130 and a 'Generate New PIN' button.
- ADD WIRELESS STATION:** A section with an 'Add Wireless Device with WPS' button.

The left sidebar contains a list of configuration categories: DIR-825, VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QoS/ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WDS, WPS, WPS PROTECTED SETUP, ADVANCED NETWORK, and GUEST ZONE. The right sidebar contains a 'Helpful Hint...' section with additional information about WPS and a 'More...' link.

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

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.

DIR-825 // **ADVANCED NETWORK** **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 : Allow All
Details : Allow All

WAN PORT SPEED
WAN Port Speed : Auto (10/100Mbps

MULTICAST STREAMS
Enable Multicast Streams :

WIRELESS

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.

Virtual Server
Port Forwarding
Application Rules
QoS Engine
Network Filter
Access Control
Website Filter
Inbound Filter
IPsec VPN Settings
Routing
Advanced Wireless
WDS
WIFI Protected Setup
Advanced Network
Setup
Wireless

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.

System Name: Enter a name for the DIR-825 router.

Enable HTTPS Server: Check to enable HTTPS to connect to the router securely.

Enable Remote Management: Remote management allows the DIR-825 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 DIR-825. Example: http://x.x.x.x:8080 whereas x.x.x.x is the Internet IP address of the DIR-825 and 8080 is the port used for the Web Management interface. If you have enabled **HTTPS Server** and checked **Use HTTPS**, you must enter **https://** as part of the URL to access the router remotely.

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.

The screenshot shows the D-Link DIR-825 web interface. At the top, there are tabs for SETUP, ADVANCED, TOOLS, and STATUS. The main content area is titled 'ADMINISTRATOR SETTINGS' and contains the following sections:

- ADMINISTRATOR SETTINGS:** A warning message states that '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, which is highly recommended to be changed. There are 'Save Settings' and 'Don't Save Settings' buttons.
- ADMIN PASSWORD:** A prompt asks the user to enter the same password into two boxes for confirmation. There are 'Password' and 'Verify Password' input fields.
- USER PASSWORD:** A prompt asks the user to enter the same password into two boxes for confirmation. There are 'Password' and 'Verify Password' input fields.
- SYSTEM NAME:** A field for 'Gateway Name' with the value 'D-Link Spalpa CR-825'.
- ADMINISTRATION:** A section with several checkboxes: 'Enable HTTPS Server' (checked), 'Enable Remote Management' (unchecked), 'Remote Admin Port' (set to 8080), and 'Use HTTPS' (unchecked). Below these are 'Inbound Filter' and 'User' dropdown menus, and a 'Details' link.

On the right side of the page, there is a 'SUPPORT' section with the heading 'Helpful hints...' and several paragraphs of text providing troubleshooting tips for connectivity issues, password resets, and remote management.