

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.

INBOUND FILTER

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

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

ADD INBOUND FILTER RULE

Name :

Action : 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
<input type="checkbox"/>	0.0.0.0	255.255.255.255
<input type="checkbox"/>	0.0.0.0	255.255.255.255

Add Clear

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range

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 store 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.

More...

Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-628 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 **Basic > DHCP** page so that the IP address of the DMZ machine does not change.

The screenshot shows the D-Link DIR-628 web interface for Firewall Settings. The left sidebar contains a navigation menu with options like VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS (selected), ROUTING, ADVANCED WIRELESS, WI-FI PROTECTED SETUP, and ADVANCED NETWORK. The main content area is titled 'FIREWALL SETTINGS' and includes a 'Helpful Hints...' section on the right. The settings are organized into several sections:

- FIREWALL SETTINGS:** Includes a description: 'The Firewall Settings allow you to set a single computer on your network outside of the router.' and buttons for 'Save Settings' and 'Don't Save Settings'.
- FIREWALL SETTINGS:** A sub-section with 'Enable SPI' checked.
- NAT ENDPOINT FILTERING:** Contains two sections:
 - UDP Endpoint Filtering:** Radio buttons for 'Endpoint Independent', 'Address Restricted' (selected), and 'Port And Address Restricted'.
 - TCP Endpoint Filtering:** Radio buttons for 'Endpoint Independent', 'Address Restricted', and 'Port And Address Restricted' (selected).
- ANTI-SPOOF CHECKING:** 'Enable anti-spoof checking' is unchecked.
- DMZ HOST:** Includes a description of DMZ, a 'Note' about security risks, and an 'Enable DMZ' checkbox (unchecked). Below it, 'DMZ IP Address' is set to '0.0.0.0' and 'Computer Name' is selected from a dropdown.
- APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION:** Checkboxes for 'PPTP', 'IPSec (VPN)', 'RTSP', and 'SIP', all of which are checked.

The bottom of the page shows the 'WIRELESS' section of the interface.

Application Level Gateway Configuration

Here you can enable or disable ALG's. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

PPTP: Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

IPSEC (VPN): Allows multiple VPN clients to connect to their corporate network using IPsec. Some VPN clients support traversal of IPsec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

RTSP: Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.

SIP: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

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-628 // 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"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	WAN
	Netmask	Gateway		
	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>		
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	WAN
	Netmask	Gateway		
	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>		
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	WAN
	Netmask	Gateway		
	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>		
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	WAN
	Netmask	Gateway		
	<input type="text" value="0.0.0.0"/>	<input type="text" value="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 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 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

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.

The screenshot shows the D-Link DIR-628 Advanced Wireless Settings page. The navigation menu on the left includes: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS (selected), WI-FI PROTECTED SETUP, and ADVANCED NETWORK. The main content area is titled 'ADVANCED WIRELESS' and contains a warning message: 'If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.' Below this are 'Save Settings' and 'Don't Save Settings' buttons. The 'ADVANCED WIRELESS SETTINGS' section includes: Transmit Power (High), Beacon Period (100, range 20..1000), RTS Threshold (2346, range 0..2347), Fragmentation Threshold (2346, range 256..2346), DTIM Interval (1, range 1..255), WLAN Partition (unchecked), WMM Enable (checked), and Short GI (checked). A 'Helpful Hints...' sidebar on the right states: '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. More...'

Wi-Fi Protected Setup

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 displays the D-Link DIR-628 router's configuration interface. The main content area is titled "WI-FI PROTECTED SETUP" and contains the following elements:

- Enable:**
- Lock Wireless Security Settings:**
- Buttons:** "Save Settings", "Don't Save Settings", "Reset to Unconfigured", "Reset PIN to Default", "Generate New PIN", "Add Wireless Device with WPS".
- Current PIN:** 24681353

The right sidebar contains "Helpful Hints..." with the following text:

- 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

UPnP: To use the Universal Plug and Play (UPnP™) feature check the **Enabled UPnP** box. UPnP provides compatibility with networking equipment, software and peripherals.

WAN Ping: Unchecking the box will not allow the DIR-628 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the WAN port to be “pinged”.

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.

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-628 // 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 : 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.

[More...](#)

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 DIR-628 router.

Remote Management: Remote management allows the DIR-628 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-628.
Example: `http://x.x.x.x:8080` where x.x.x.x is the Internet IP address of the DIR-628 and 8080 is the port used for the Web Management interface.

Inbound Filter: This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.

The screenshot shows the D-Link DIR-628 web management interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The main content area is titled "ADMINISTRATOR SETTINGS" and contains the following sections:

- ADMINISTRATOR SETTINGS:** A text box with instructions: "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." Below this are "Save Settings" and "Don't Save Settings" buttons.
- ADMIN PASSWORD:** A section with the instruction "Please enter the same password into both boxes, for confirmation." It contains two input fields: "Password:" and "Verify Password:".
- USER PASSWORD:** A section with the instruction "Please enter the same password into both boxes, for confirmation." It contains two input fields: "Password:" and "Verify Password:".
- SYSTEM NAME:** A section with the label "Gateway Name:" and a text input field containing "D-Link Systems DIR-628".
- ADMINISTRATION:** A section with the following options:
 - Enable Remote Management:** A checkbox that is currently unchecked.
 - Remote Admin Port:** A text input field containing "8080".
 - Remote Admin Inbound Filter:** A dropdown menu currently set to "Allow All".
 - Details:** A text input field containing "Allow All".

On the right side of the interface, there is a "Helpful Hints..." section with the following text: "For security reasons, it is recommended that you change the password for the Admin and User accounts. Be sure to write down the new passwords to avoid having to reset the router in case they are forgotten." Below this, it says: "Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet." and "Choose a port to open for remote management." At the bottom of the hints section, it says: "Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the Advanced --> Inbound Filter screen and create a new filter." A "More..." link is also visible at the bottom right.

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**.

D-Link

DIR-628 // SETUP ADVANCED TOOLS STATUS SUPPORT

TIME

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.

Save Settings Don't Save Settings

TIME CONFIGURATION

Current Router Time : Saturday, January 31, 2004 11:58:11 AM
 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 : florida.ath.cx << Select NTP Server

SET THE DATE AND TIME MANUALLY

Date And Time : Year 2004 Month Jan Day 31
 Hour 11 Minute 57 Second 27 AM

Copy Your Computer's Time Settings

WIRELESS

Helpful Hints...
 Good timekeeping is important for accurate logs and scheduled firewall rules.
 More...

SysLog

The Broadband Router keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server on your network.

Enable Logging to SysLog Server: Check this box to send the router logs to a SysLog Server.

SysLog Server IP Address: The address of the SysLog server that will be used to send the logs. You may also select your computer from the drop-down menu (only if receiving an IP address from the router via DHCP).

The screenshot shows the D-Link web interface for the DIR-628 router. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'SYSLOG' page is active, displaying the following configuration options:

- Enable Logging To Syslog:**
- Syslog Server IP Address:** 0.0.0.0
- Server:** Computer Name (dropdown menu)

Buttons for 'Save Settings' and 'Don't Save Settings' are visible. A sidebar on the right provides helpful hints: 'A System Logger (syslog) is a server that collects in one place the logs from different sources. If the LAN includes a syslog server, you can use this option to send the router's logs to that server.' A 'More...' link is also present.