

Using the Configuration Menu (continued)

Advanced > Virtual Server *continued*

Name	Private IP	Protocol	Schedule	
<input checked="" type="checkbox"/> Virtual Server HTTP	192.168.0.25	TCP-8081	Weekends	



Click on this icon to edit the virtual service



Click on this icon to delete the virtual service

Example #2:

If you have an FTP server that you wanted Internet users to access by WAN port 2100 and only during the weekends, you would need to enable it as such. FTP server is on LAN computer 192.168.0.30. FTP uses port 21, TCP.

Name: FTP Server
Private IP: 192.168.0.30
Protocol Type: TCP
Private Port: 21
Public Port: 2100

Schedule: From: 01:00AM to 01:00AM, Sat to Sun

All Internet users who want to access this FTP Server must connect to it from port 2100. This is an example of port redirection and can be useful in cases where there are many of the same servers on the LAN network.

Using the Configuration Menu (continued)

Advanced > Applications

The screenshot shows the D-Link DI-524 router configuration interface. The top navigation bar includes 'Home', 'Advanced' (selected), 'Tools', 'Status', and 'Help'. The main content area is titled 'Special Application' and contains a form for configuring a special application. The form includes fields for Name, Trigger Port, Trigger Type (set to TCP), Public Ports, and Public Type (set to TCP). There are radio buttons for 'Enabled' and 'Disabled'. Below the form is a 'Special Application List' table with columns for Name, Trigger, and Public Port. The table lists several predefined applications with checkboxes for selection and icons for edit/delete.

Name	Trigger	Public Port		
<input type="checkbox"/> Battle.net	6112	6112		
<input type="checkbox"/> Dialpad	7175	51200-51201,51210		
<input type="checkbox"/> ICU II	2019	2000-2038,2050-2051,2069,2085,3010-3030		
<input type="checkbox"/> MSN Gaming Zone	47624	2300-2400,28800-29000		
<input type="checkbox"/> PC-to-Phone	12053	12120,12122,24150-24220		
<input type="checkbox"/> Quick Time	554	6970-6999		

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 DI-524. 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 public ports associated with the trigger port to open them for inbound traffic.

The DI-524 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

Note! Only one PC can use each Special Application tunnel.

Name: This is the name referencing the special application.

Trigger Port: This is the port used to trigger the application. It can be either a single port or a range of ports.

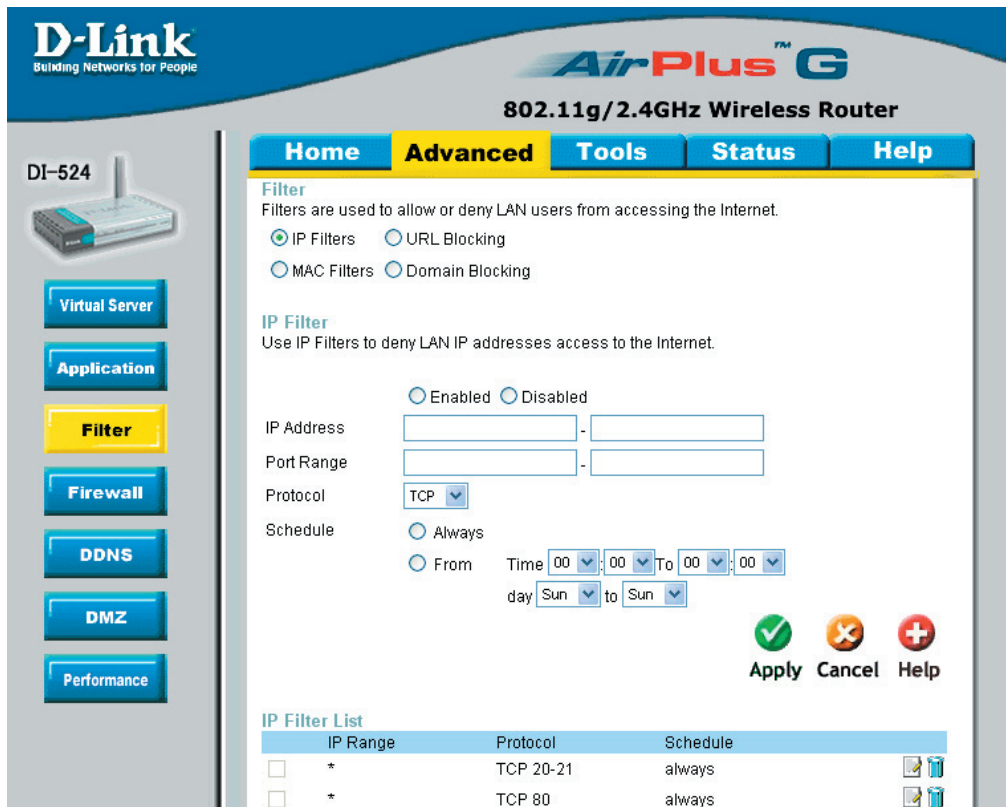
Trigger Type: This is the protocol used to trigger the special application.

Public Port: This is the port number on the WAN 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.

Public Type: This is the protocol used for the special application.

Using the Configuration Menu (continued)

Advanced > Filters > IP Filters



DI-524

Virtual Server
Application
Filter
Firewall
DDNS
DMZ
Performance

802.11g/2.4GHz Wireless Router

Home **Advanced** Tools Status Help

Filter
Filters are used to allow or deny LAN users from accessing the Internet.

IP Filters URL Blocking
 MAC Filters Domain Blocking




IP Filter
Use IP Filters to deny LAN IP addresses access to the Internet.

Enabled Disabled

IP Address: [] - []
Port Range: [] - []
Protocol: TCP
Schedule: Always
 From Time [00]:[00] To [00]:[00] day [Sun] to [Sun]

Apply Cancel Help

IP Filter List

	IP Range	Protocol	Schedule	
<input type="checkbox"/>	*	TCP 20-21	always	 
<input type="checkbox"/>	*	TCP 80	always	 

Filters are used to deny or allow LAN (Local Area Network) computers from accessing the Internet. The DI-524 can be setup to deny internal computers by their IP or MAC addresses. The DI-524 can also block users from accessing restricted web sites.

IP Filters:

IP Filter is used to deny LAN IP addresses from accessing the Internet. You can deny specific port numbers or all ports for the specific IP address.

IP Address:

The IP address of the LAN computer that will be denied access to the Internet.

Port Range:

The single port or port range that will be denied access to the Internet.

Protocol Type:

Select the protocol type

Schedule:

This is the schedule of time when the IP Filter will be enabled.

Using the Configuration Menu (continued)

Advanced > Filters > URL Blocking

The screenshot shows the configuration interface for a D-Link DI-524 802.11g/2.4GHz Wireless Router. The page is titled "AirPlus G" and "802.11g/2.4GHz Wireless Router". The navigation menu includes "Home", "Advanced" (selected), "Tools", "Status", and "Help". On the left sidebar, there are buttons for "Virtual Server", "Application", "Filter" (highlighted in yellow), "Firewall", "DDNS", "DMZ", and "Performance". The main content area is titled "Filter" and explains that filters are used to allow or deny LAN users from accessing the Internet. It offers four filter types: IP Filters, URL Blocking (selected), MAC Filters, and Domain Blocking. Below this, the "URL Blocking" section is shown, which is currently "Disabled". A text input field is present, and a dropdown menu is open showing "- Empty -" with a "DELETE" button next to it. At the bottom right, there are three buttons: "Apply" (with a green checkmark), "Cancel" (with a red X), and "Help" (with a red plus sign).

URL Blocking is used to deny LAN computers from accessing specific web sites by the URL. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display. To use this feature, enter the text string to be blocked and click **Apply**. The text to be blocked will appear in the list. To delete the text, just highlight it and click **Delete**.

Filters-

Select the filter you wish to use; in this case, **URL Blocking** was chosen.

URL Blocking-

Select **Enabled** or **Disabled**.

Keywords-

Enter the keywords in this field. Block URLs which contain keywords listed below.

Using the Configuration Menu (continued)

Advanced > Filters > MAC Filters

The screenshot shows the configuration interface for a D-Link DI-524 AirPlus G 802.11g/2.4GHz Wireless Router. The page is titled "802.11g/2.4GHz Wireless Router" and has a navigation menu with "Home", "Advanced", "Tools", "Status", and "Help". The "Advanced" tab is selected. On the left sidebar, there is a list of configuration options: "Virtual Server", "Application", "Filter" (highlighted in yellow), "Firewall", "DDNS", "DMZ", and "Performance". The main content area is titled "Filter" and contains the following sections:

- Filter**: "Filters are used to allow or deny LAN users from accessing the Internet." There are four radio buttons: "IP Filters", "URL Blocking", "MAC Filters" (selected), and "Domain Blocking".
- MAC Filters**: "Use MAC address to allow or deny computers access to the network." There are three radio buttons: "Disabled MAC Filters" (selected), "Only **allow** computers with MAC address listed below to access the network", and "Only **deny** computers with MAC address listed below to access the network".
- Form fields**: "Name" (text input), "MAC Address" (six text inputs), "DHCP Client" (pull-down menu with "-- select one --" and a "Clone" button), and three buttons: "Apply" (green checkmark), "Cancel" (orange X), and "Help" (red plus).
- MAC Filter List**: A table with two columns: "Name" and "MAC Address".

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.

Filters-

Select the filter you wish to use; in this case, **MAC filters** was chosen.

MAC Filters-

Choose **Disable** MAC filters; **allow** MAC addresses listed below; or **deny** MAC addresses listed below.

Name-

Enter the name here.

MAC Address-

Enter the MAC Address.

DHCP Client-

Select a DHCP client from the pull-down list; click **Clone** to copy that MAC Address.

Using the Configuration Menu (continued)

Advanced > Filters > Domain Blocking

The screenshot shows the configuration interface for a D-Link DI-524 router. The left sidebar contains navigation buttons: Virtual Server, Application, Filter (highlighted in yellow), Firewall, DDNS, DMZ, and Performance. The main content area is titled "802.11g/2.4GHz Wireless Router" and has tabs for Home, Advanced (selected), Tools, Status, and Help. Under the "Filter" section, there are radio buttons for IP Filters, URL Blocking, MAC Filters, and Domain Blocking (selected). The "Domain Blocking" section has radio buttons for Disabled (selected) and Allow users to access all domains except "Blocked Domains". Below this is a "Blocked Domains" list with an empty input field and a "DELETE" button. The "Deny users to access all domains except 'Permitted Domains'" option is also present, with a "Permitted Domains" list below it, also featuring an empty input field and a "DELETE" button. At the bottom right are "Apply", "Cancel", and "Help" buttons.

Domain Blocking is used to allow or deny LAN (Local Area Network) computers from accessing specific domains on the Internet. Domain blocking will deny all requests to a specific domain such as http and ftp. It can also allow computers to access specific sites and deny all other sites.

Filters-

Select the filter you wish to use; in this case, **Domain Blocking** was chosen.

Domain Blocking-

Disabled-

Select **Disabled** to disable **Domain Blocking**

Allow-

Allows users to access all domains except **Blocked Domains**

Deny-

Denies users access to all domains except **Permitted Domains**

Blocked Domains-

Enter the **Blocked Domains** in this field

Permitted Domains-

Enter the **Permitted Domains** in this field

Using the Configuration Menu (continued)

Advanced > Firewall

DI-524

D-Link
BUILDING NETWORKS FOR PEOPLE

AirPlus G
802.11g/2.4GHz Wireless Router

Home **Advanced** Tools Status Help

Firewall Rules
Firewall Rules can be used to allow or deny traffic from passing through the DI-524.

Enabled Disabled

Name:

Action: Allow Deny

Interface: IP Start: IP End: Protocol: Port Range: -

Source: *

Destination: * TCP -

Schedule: Always From Time 00:00 To 00:00 day Sun to Sun

Apply Cancel Help

Firewall Rules List

Action Name	Source	Destination	Protocol	
<input type="checkbox"/> Allow Allow to Ping WAN port	WAN,*	WAN,*	ICMP,8	
<input type="checkbox"/> Deny Default	**	LAN,*	**	
<input type="checkbox"/> Allow Default	LAN,*	**	**	

Firewall Rules is an advanced feature used to deny or allow traffic from passing through the DI-524. It works in the same way as IP Filters with additional settings. You can create more detailed access rules for the DI-524. When virtual services are created and enabled, it will also display in Firewall Rules. Firewall Rules contain all network firewall rules pertaining to IP (Internet Protocol).

In the Firewall Rules List at the bottom of the screen, the priorities of the rules are from top (highest priority) to bottom (lowest priority.)

Note:

The DI-524 MAC Address filtering rules have precedence over the Firewall Rules.

Firewall Rules-

Enable or disable the Firewall

Name-

Enter the name

Action-

Allow or Deny

Source-

Enter the IP Address range

Destination-

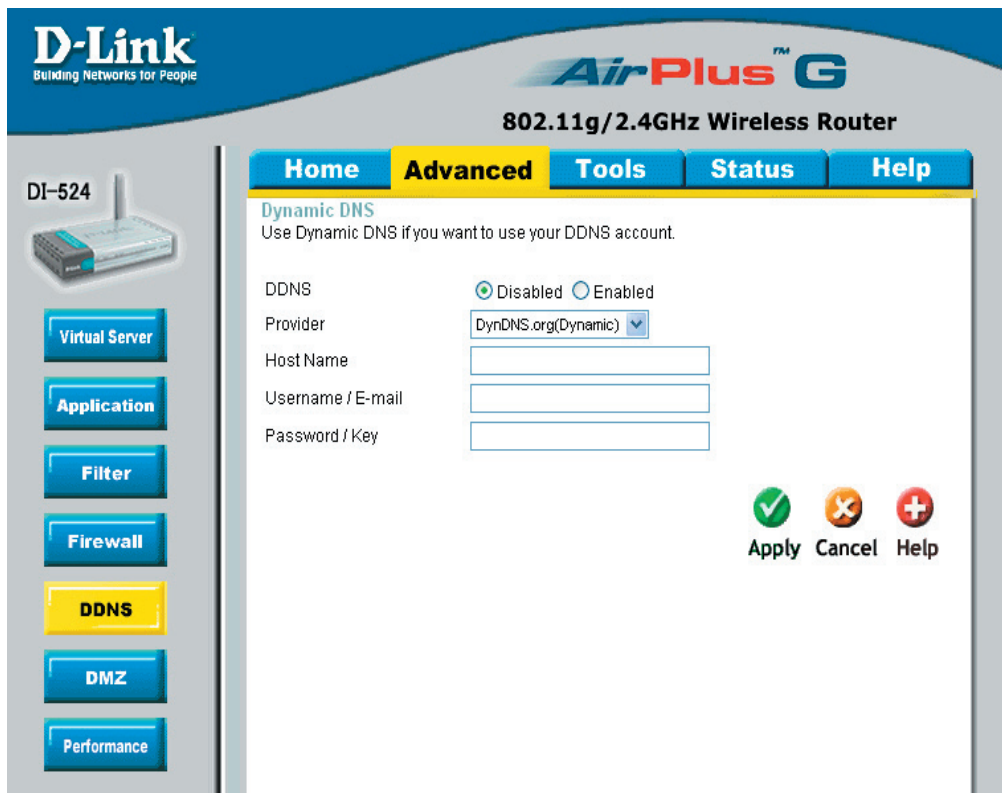
Enter the IP Address range; the Protocol; and the Port Range

Schedule-

Select Always or enter the Time Range.

Using the Configuration Menu (continued)

Advanced > DDNS



D-Link
Building Networks for People

AirPlus™ G
802.11g/2.4GHz Wireless Router

DI-524

Virtual Server
Application
Filter
Firewall
DDNS
DMZ
Performance

Home **Advanced** Tools Status Help

Dynamic DNS
Use Dynamic DNS if you want to use your DDNS account.

DDNS Disabled Enabled

Provider

Host Name

Username / E-mail

Password / Key

Apply Cancel Help

Users who have a Dynamic DDNS account may use this feature on the DI-524.

Provider- Select from the list of DDNS servers available.

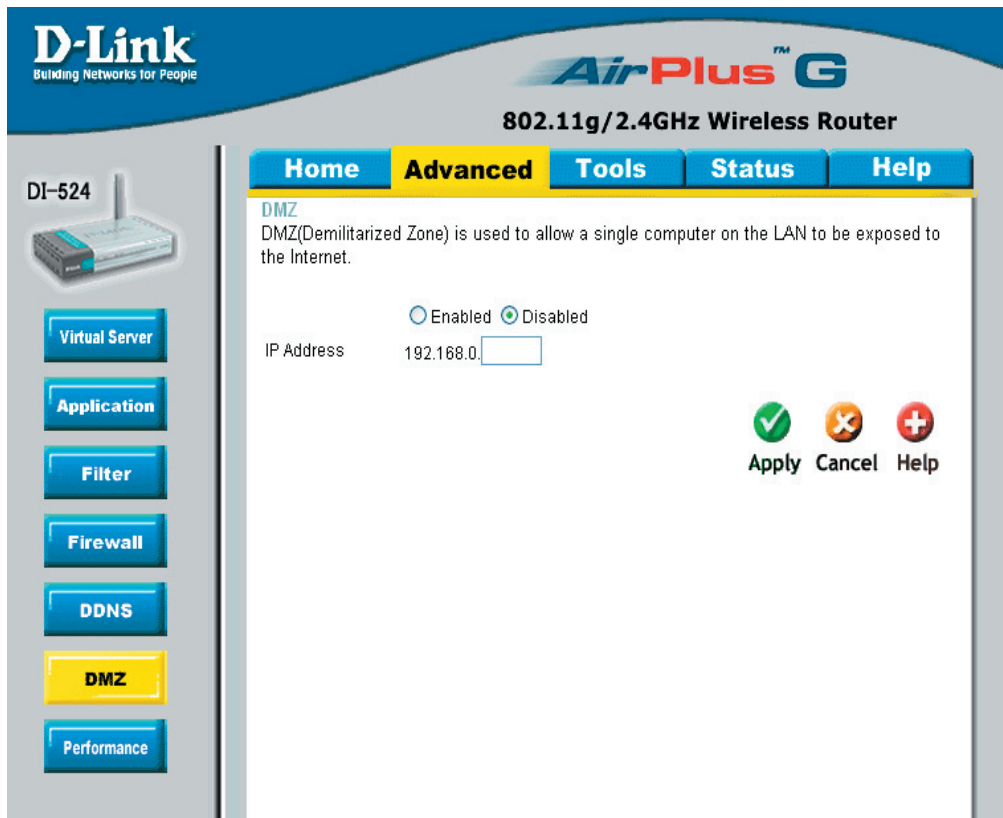
Host Name- Enter your DDNS account host name.

Username/Email- Enter your DDNS account username.

Password/Key- Enter your DDNS account password.

Using the Configuration Menu (continued)

Advanced > DMZ



If you have a client PC that cannot run Internet applications properly from behind the DI-524, then you can set the client up for unrestricted Internet access. It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes. Enter the IP address of the internal computer that will be the DMZ host. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

DMZ-

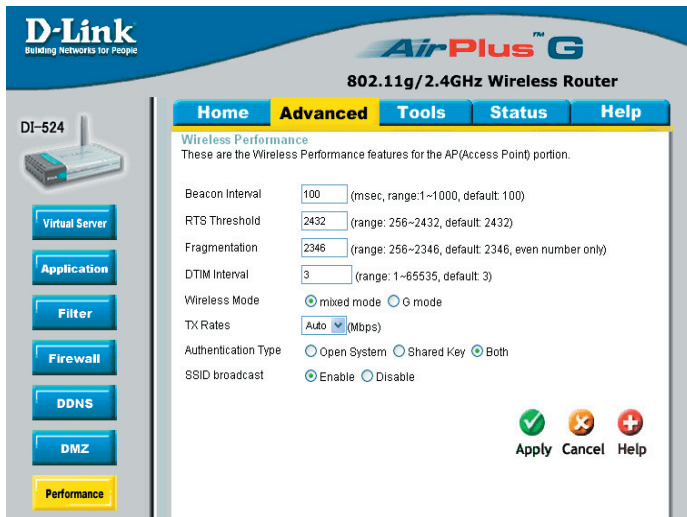
Enable or **Disable** the DMZ. The DMZ (Demilitarized Zone) allows a single computer to be exposed to the internet. By **default** the DMZ is **disabled**.

IP Address-

Enter the **IP Address** of the computer to be in the **DMZ**

Using the Configuration Menu (continued)

Advanced > Performance



Beacon Interval-

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 2432. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation-

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.

Wireless Mode-

Select **Short** or **Long Preamble**. The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the wireless router and the roaming wireless network adapters. *Note: High network traffic areas should use the shorter preamble type.*

TX Rates-

Auto is the default selection. Select from the drop down menu.

SSID Broadcast-

Choose **Enabled** to broadcast the SSID across the network. All devices on a network must share the same SSID (Service Set Identifier) to establish communication. Choose **Disabled** if you do not wish to broadcast the SSID over the network.