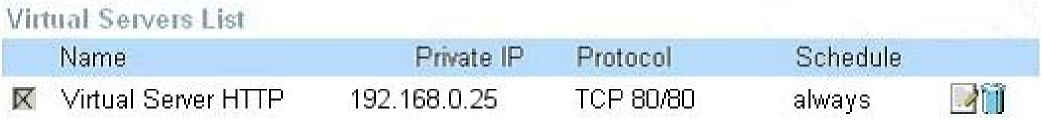
Using the Configuration Menu (continued)

Advanced > Virtual Server *continued*



Virtual Servers List

	Name	Private IP	Protocol	Schedule	
☒	Virtual Server HTTP	192.168.0.25	TCP 80/80	always	✎ 🗑

✎ 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.

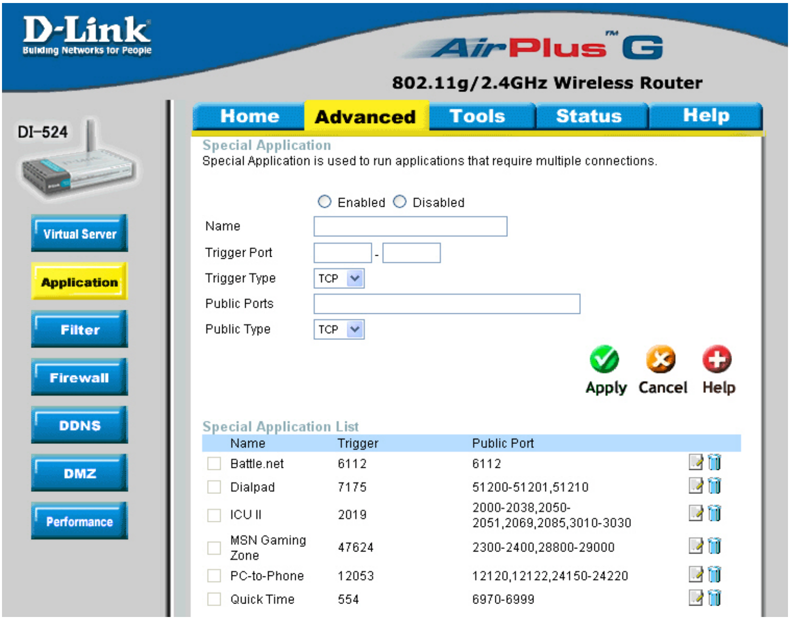
Name: FTP Server
Private IP: 192.168.0.30
Protocol Type: TCP
Private Port: 21
Public Port: 2100

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



Special Application

Special Application is used to run applications that require multiple connections.

○ Enabled ○ Disabled

Name	
Trigger Port	-
Trigger Type	TCP
Public Ports	
Public Type	TCP

Special Application List

	Name	Trigger	Public Port
□	Battle.net	6112	6112
□	Dialpad	7175	51200-51201,51210
□	ICU II	2019	2000-2038,2050-2051,2069,2085,3010-3030
□	MSN Gaming Zone	47624	2300-2400,28800-29000
□	PC-to-Phone	12053	12120,12122,24150-24220
□	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.

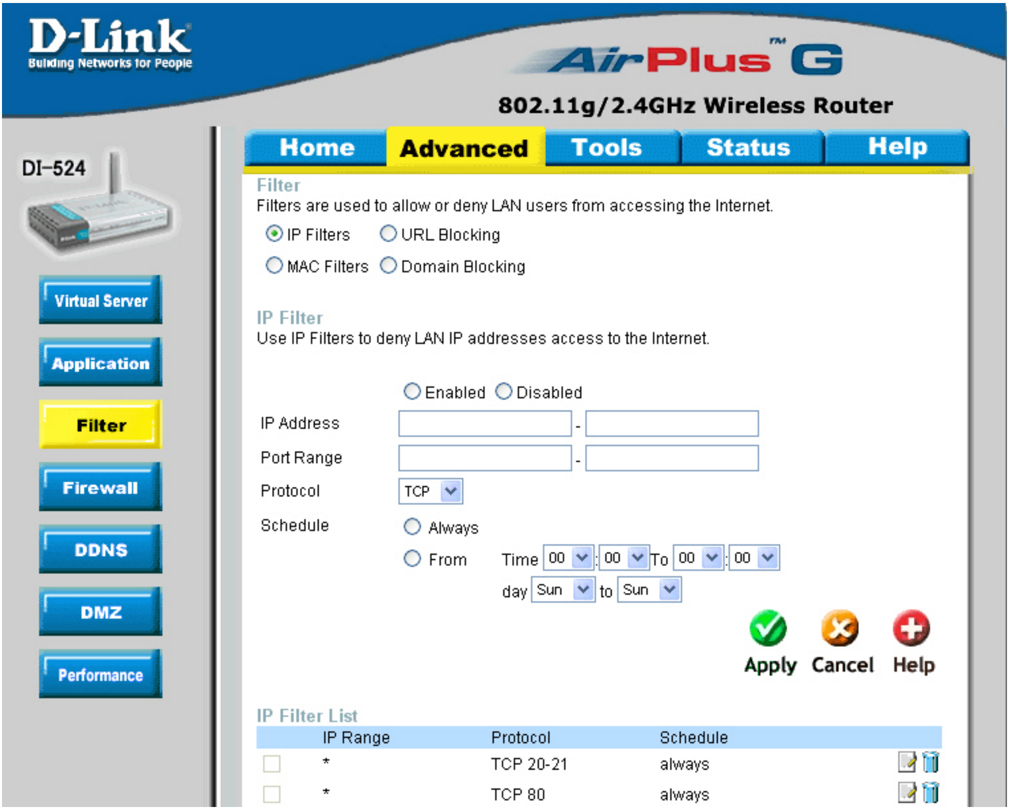
Trigger Type: This is the protocol used to trigger the special application.

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



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

IP Filter List

	IP Range	Protocol	Schedule
□	*	TCP 20-21	always
□	*	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.

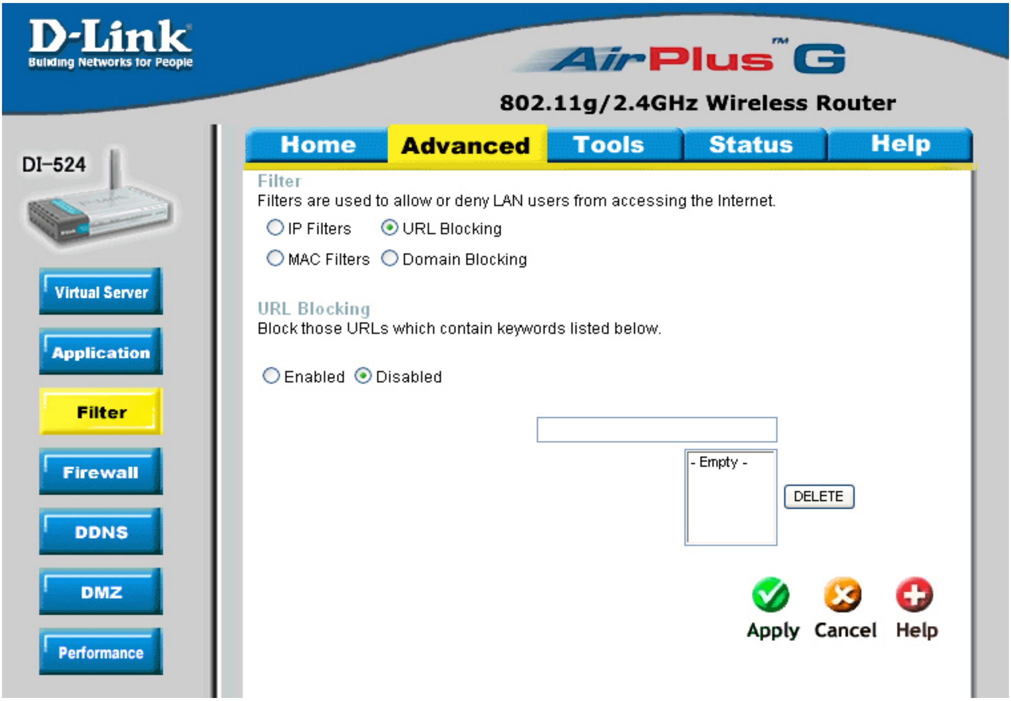
Port Range: The single port or port range that will be denied access to the Internet.

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



Filter

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

○ IP Filters ● URL Blocking

○ MAC Filters ○ Domain Blocking

URL Blocking

Block those URLs which contain keywords listed below.

○ Enabled ● Disabled

- Empty -

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**.

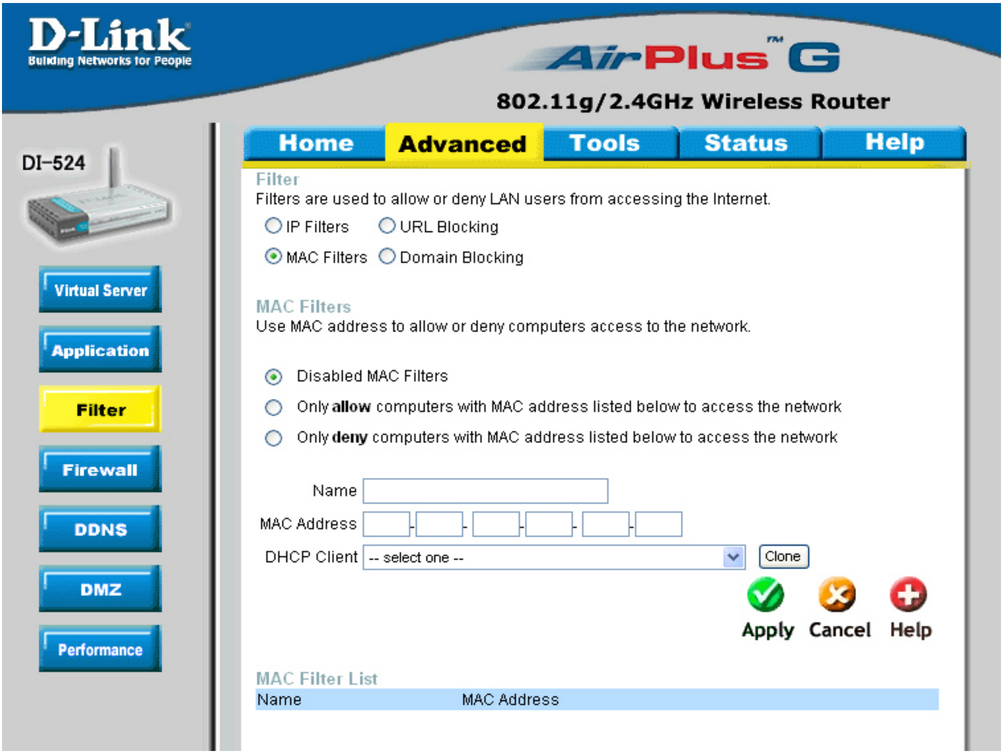
Filters- Select the filter you wish to use; in this case, **URL Blocking** was chosen.

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



Filter

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

○ IP Filters ○ URL Blocking

● MAC Filters ○ Domain Blocking

MAC Filters

Use MAC address to allow or deny computers access to the network.

● Disabled MAC Filters

○ Only **allow** computers with MAC address listed below to access the network

○ Only **deny** computers with MAC address listed below to access the network

Name

MAC Address

DHCP Client -- select one -- Clone

MAC Filter List

Name	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.

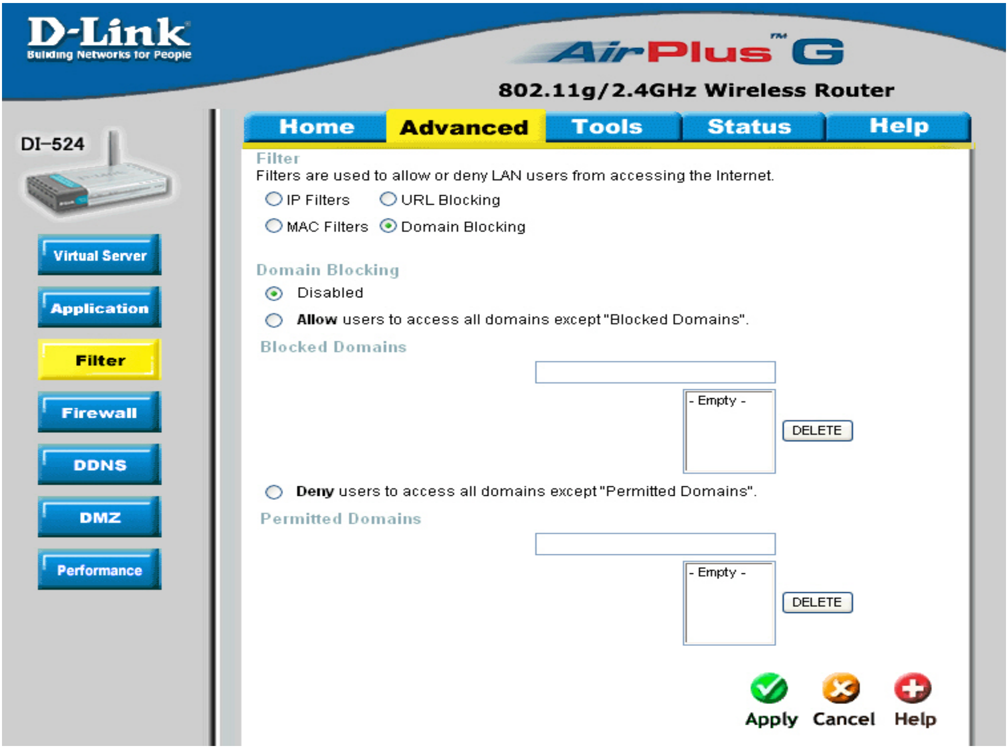
Name- Enter the name here.

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



Filter

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

○ IP Filters ○ URL Blocking

○ MAC Filters ● Domain Blocking

Domain Blocking

● Disabled

○ **Allow** users to access all domains except "Blocked Domains".

Blocked Domains

- Empty -

○ **Deny** users to access all domains except "Permitted Domains".

Permitted Domains

- Empty -

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**

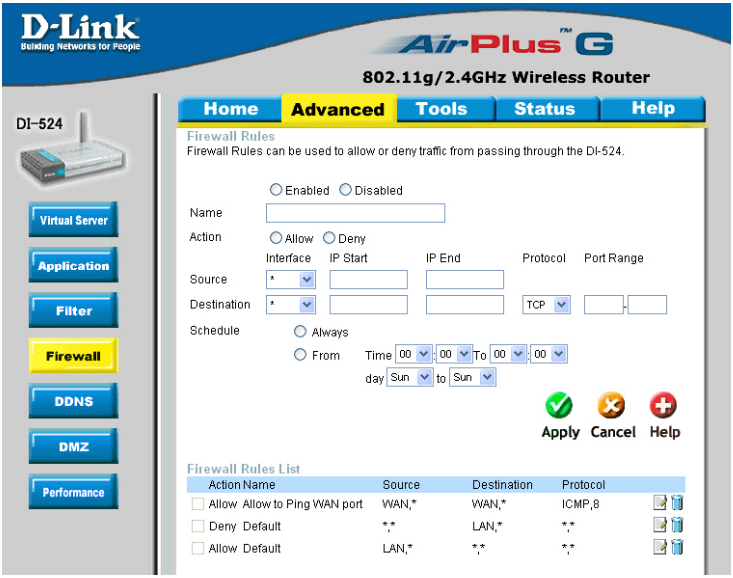
Deny- Denies users access to all domains except **Permitted Domains**

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



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			

Firewall Rules List

	Action	Name	Source	Destination	Protocol
□	Allow	Allow to Ping WAN port	WAN,*	WAN,*	ICMP,8
□	Deny	Default	*,*	LAN,*	*,*
□	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

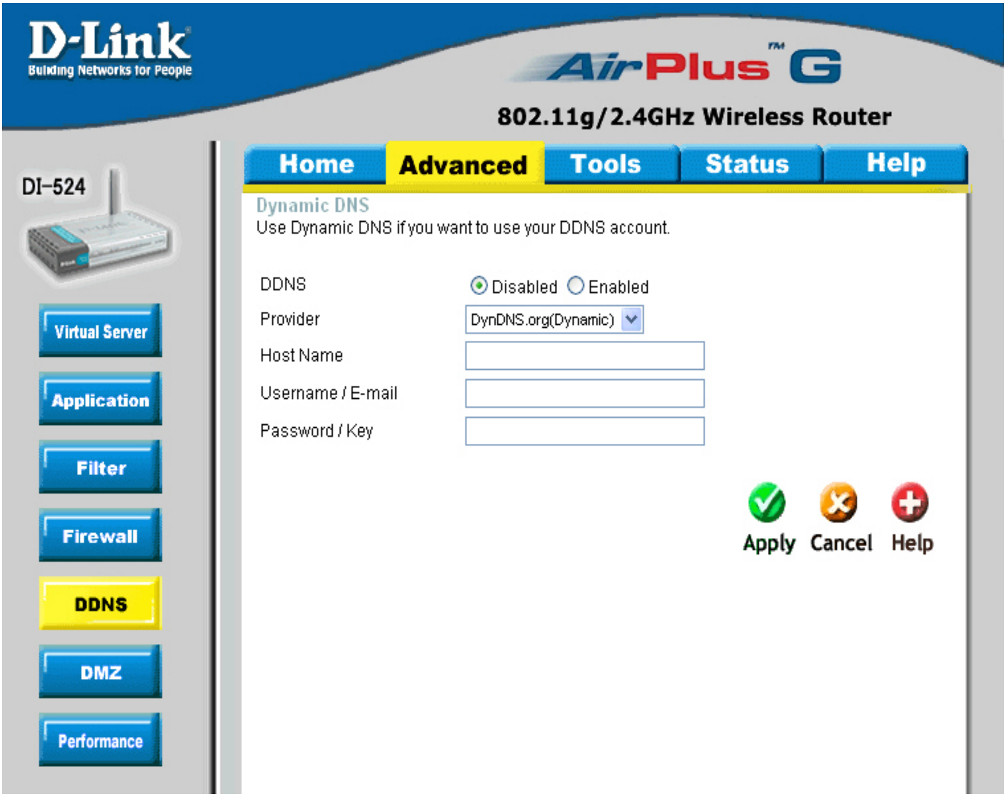
Action- **Allow** or **Deny**

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**.

Advanced > DDNS



Dynamic DNS

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

DDNS ● Disabled ○ Enabled

Provider DynDNS.org(Dynamic)

Host Name

Username / E-mail

Password / Key

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

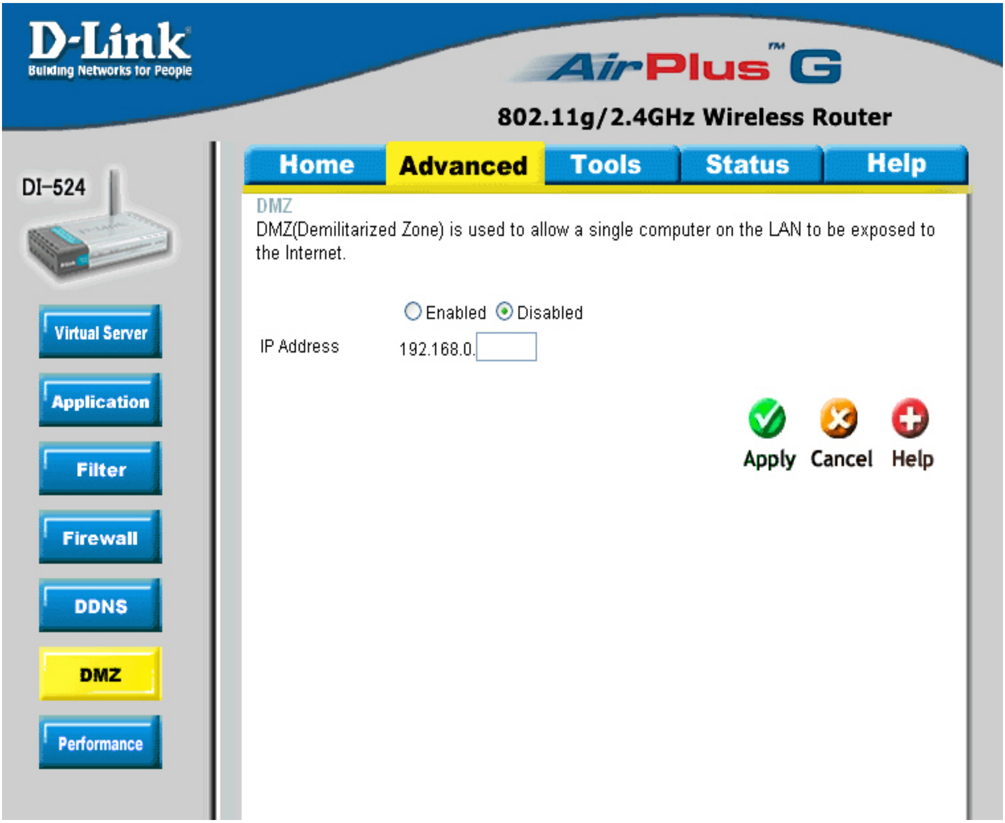
Provider- Select from the list of DDNS servers available.

Host Name- Enter your DDNS account host name.

Username/Email- Enter your DDNS account username.

Password/Key- Enter your DDNS account password.

Advanced > DMZ



DMZ

DMZ(Demilitarized Zone) is used to allow a single computer on the LAN to be exposed to the Internet.

○ Enabled ● Disabled

IP Address 192.168.0.

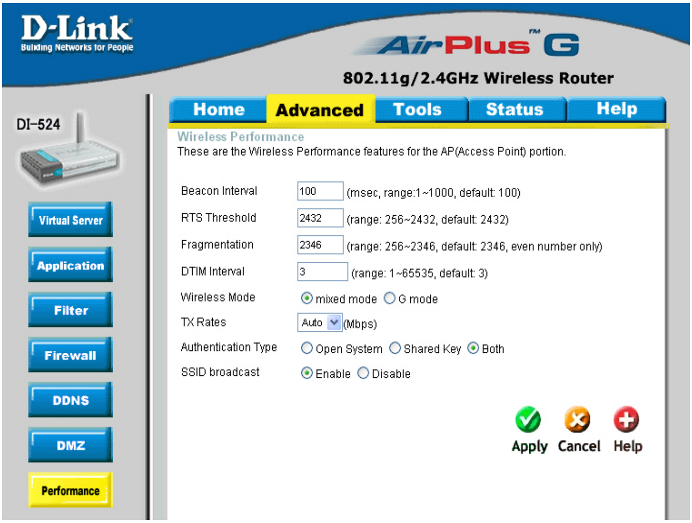
If you have a client PC that cannot run Internet applications properly from behind the DI-524, then you can set the client up for unrestricted Internet access. It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes. Enter the IP address of the internal computer 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



Wireless Performance

These are the Wireless Performance features for the AP(Access Point) portion.

Beacon Interval 100 (msec, range:1~1000, default: 100)

RTS Threshold 2432 (range: 256~2432, default: 2432)

Fragmentation 2346 (range: 256~2346, default: 2346, even number only)

DTIM Interval 3 (range: 1~65535, default: 3)

Wireless Mode ● mixed mode ○ G mode

TX Rates Auto (Mbps)

Authentication Type ○ Open System ○ Shared Key ● Both

SSID broadcast ● Enable ○ Disable

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.

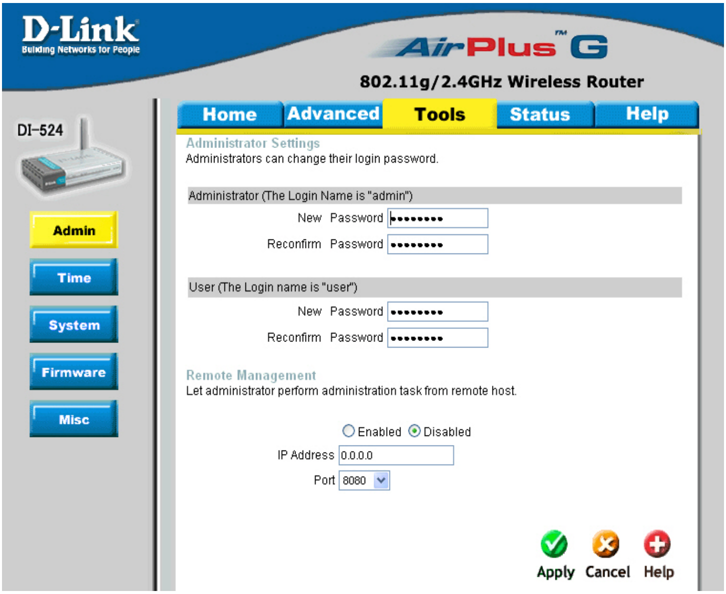
Wireless Mode- Select **Short** or **Long Preamble.** The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the wireless router and the roaming wireless network adapters. *Note: High network traffic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

TX Rates- **Auto** is the default selection. Selct 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.

Using the Configuration Menu (continued)

Tools> Admin



Administrator Settings

Administrators can change their login password.

Administrator (The Login Name is "admin")

New Password ••••••••

Reconfirm Password ••••••••

User (The Login name is "user")

New Password ••••••••

Reconfirm Password ••••••••

Remote Management

Let administrator perform administration task from remote host.

○ Enabled ● Disabled

IP Address 0.0.0.0

Port 8080

At this page, the DI-524 administrator can change the system password. There are two accounts that can access the Broadband Router's Web-Management interface. They 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.

Administrator- **admin** is the **Administrator login name**

Password- Enter the password and enter again to confirm

User- **user** is the **User login name**

Password- Enter the password and enter again to confirm

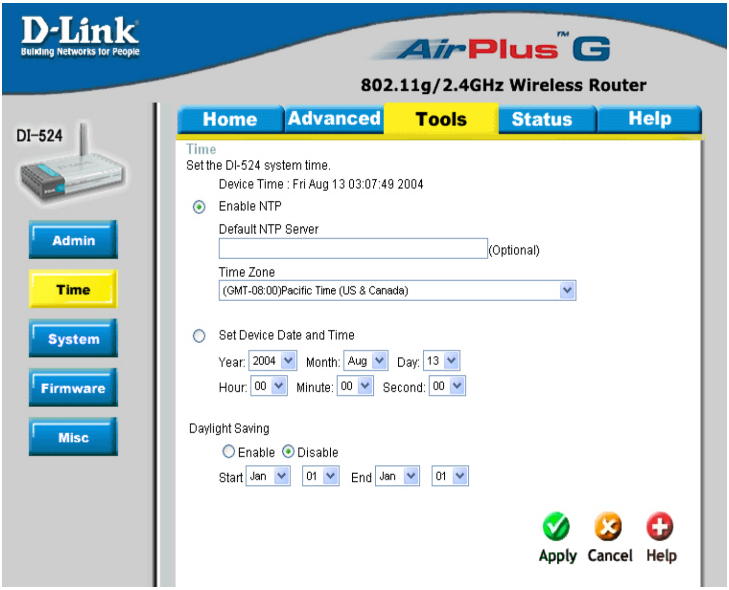
Remote Management- Remote management allows the DI-524 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform **Administrator** tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

IP Address- The Internet IP address of the computer that has access to the Broadband Router. If you input an asterisk (*) into this field, then any computer will be able to access the Router. Putting an asterisk (*) into this field would present a security risk and is not recommended.

Port- The port number used to access the Broadband Router.

Example- http://x.x.x.x:8080 where x.x.x.x is the WAN IP address of the Broadband Router and 8080 is the port used for the Web-Mangement interface.

Tools > Time



Time

Set the DI-524 system time.

Device Time : Fri Aug 13 03:07:49 2004

● Enable NTP

Default NTP Server

(Optional)

Time Zone

(GMT-08:00)Pacific Time (US & Canada)

○ Set Device Date and Time

Year: 2004 Month: Aug Day: 13

Hour: 00 Minute: 00 Second: 00

Daylight Saving

○ Enable ● Disable

Start Jan 01 End Jan 01

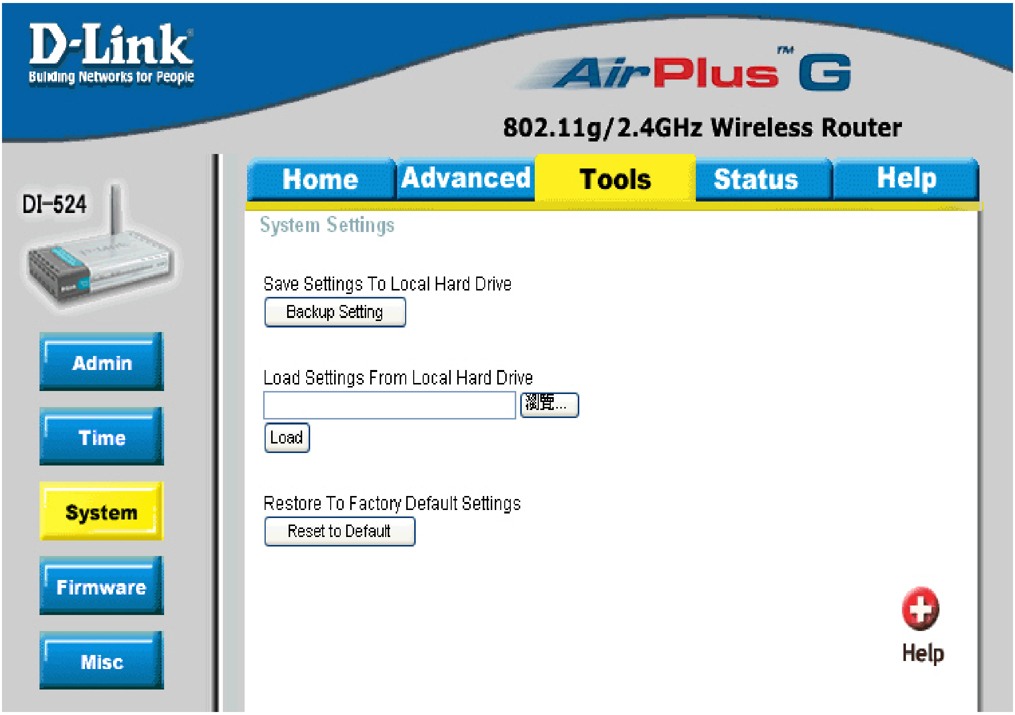
Default NTP Server- NTP is short for *Network Time Protocol.* NTP synchronizes computer clock times in a network of computers.
This field is optional.

Time Zone- Set Device Date and Time: To manually input the time. Enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second.

Set the Time- To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second. Click **Set Time**.

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.

Tools > System



System Settings

Save Settings To Local Hard Drive

Backup Setting

Load Settings From Local Hard Drive

瀏覽...

Load

Restore To Factory Default Settings

Reset to Default

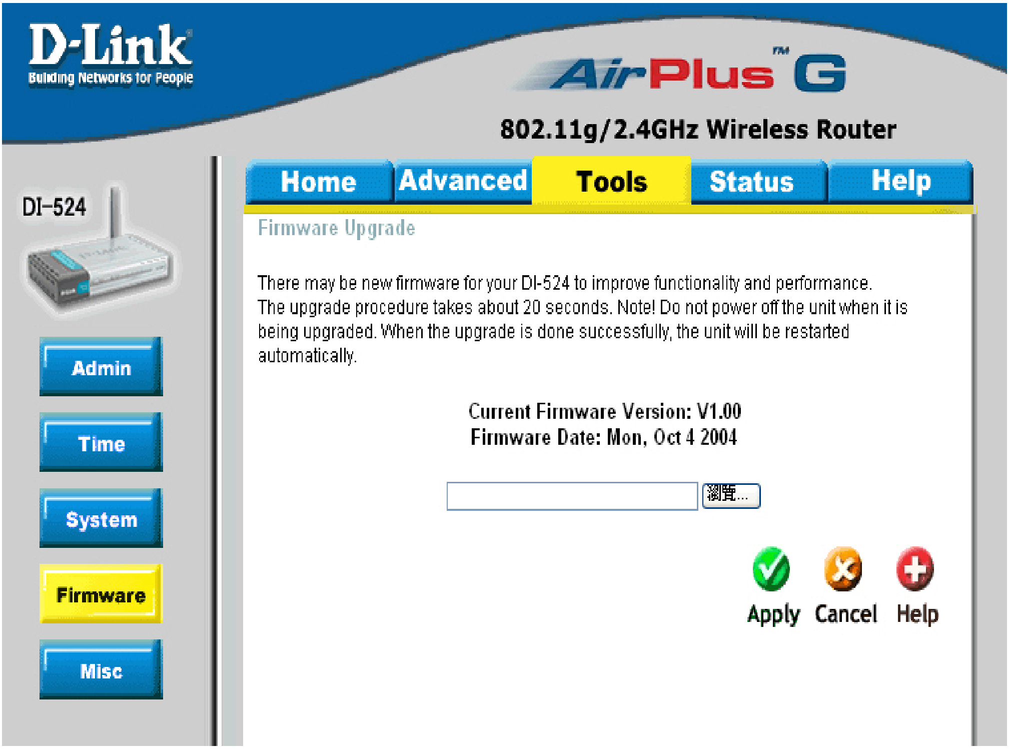
The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file can be loaded back on the Broadband Router. To reload a system settings file, click on **Browse** to browse the local hard drive and locate the system file to be used. You may also reset the Broadband Router back to factory settings by clicking on **Restore.**

Save Settings to Local Hard Drive- Click **Save** to save the current settings to the local Hard Drive

Load Settings from Local Hard Drive- Click **Browse** to find the settings, then click **Load**

Restore to Factory Default Settings- Click **Restore** to restore the factory default settings

Tools > Firmware



Firmware Upgrade

There may be new firmware for your DI-524 to improve functionality and performance. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

Current Firmware Version: V1.00
Firmware Date: Mon, Oct 4 2004

You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to browse the local hard drive and locate the firmware to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Upgrade- Click on the link in this screen to find out if there is an updated firmware; if so, download the new firmware to your hard

Browse- After you have downloaded the new firmware, click **Browse** in this window to locate the firmware update on your hard drive. Click **Apply** to complete the firmware upgrade.