LAN Setup

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router. See the next section for information on DHCP setup.

To access the **LAN Setup** menu, click the **LAN Setup** button in the **Setup** directory.

To change the LAN **IP Address** or **Subnet Mask**, type in the desired values and click the **Add/Apply** button. Your web browser should automatically be redirected to the new IP address. You will asked to login again to the Router's web manager.

The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the Router though the Ethernet port. When the Router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router the range of IP addresses in the pool used for DHCP on the LAN will also be changed. The IP address pool can be up to 253 IP addresses.

There are two options for DHCP service:

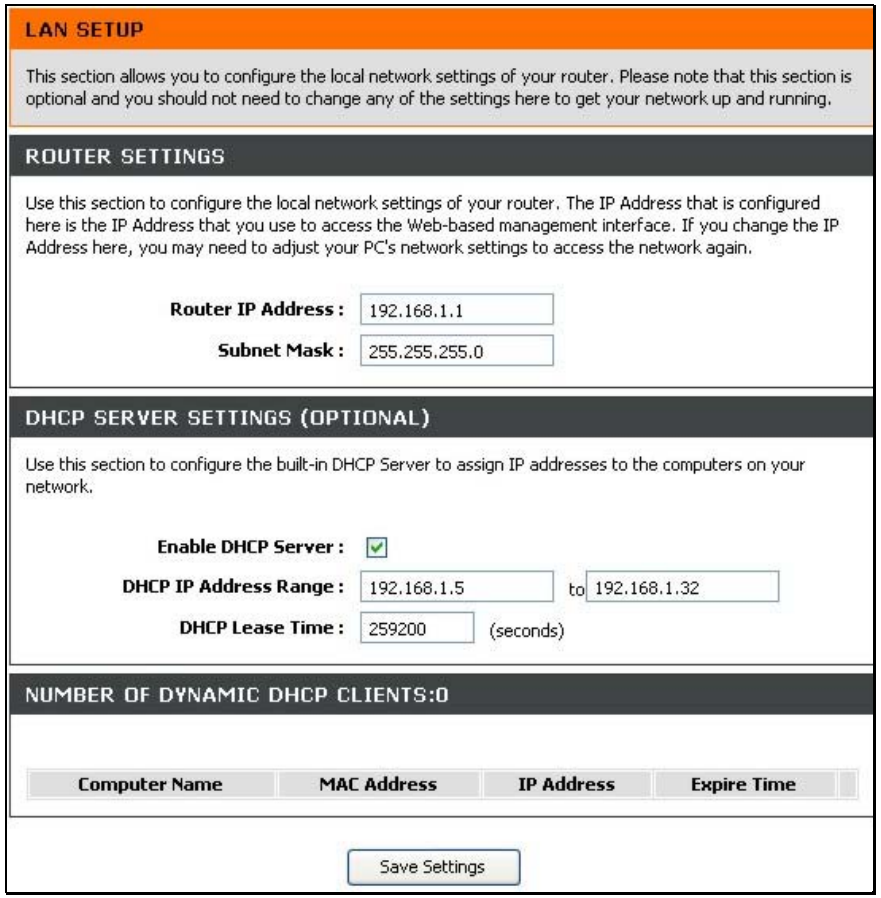
- You can use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for workstations.

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured the DHCP Settings as you want them, click the **Add/Apply** button to commit the new settings.

Use the Router for DHCP

To use the built-in DHCP server, click to select the **Enable DHCP Server** option if it is not already selected. The IP address pool settings can be adjusted beginning with the first address in the **DHCP IP Address Range**. The second IP address entered is the highest IP address number in the pool. Type in the **DHCP Lease Time** in the entry field provided. This is the amount of time in seconds that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

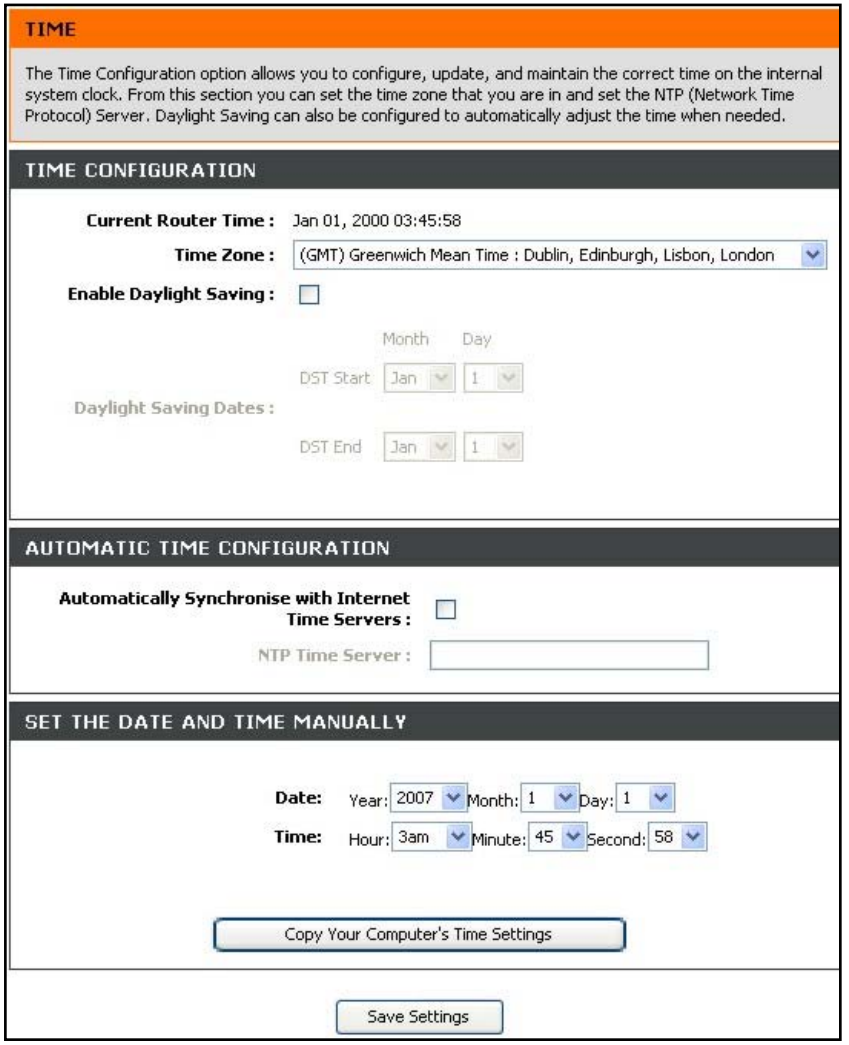
If you opt to disable DHCP service, all IP devices connected to the Router will require manual IP settings configuration or another DHCP server.



Time Setup

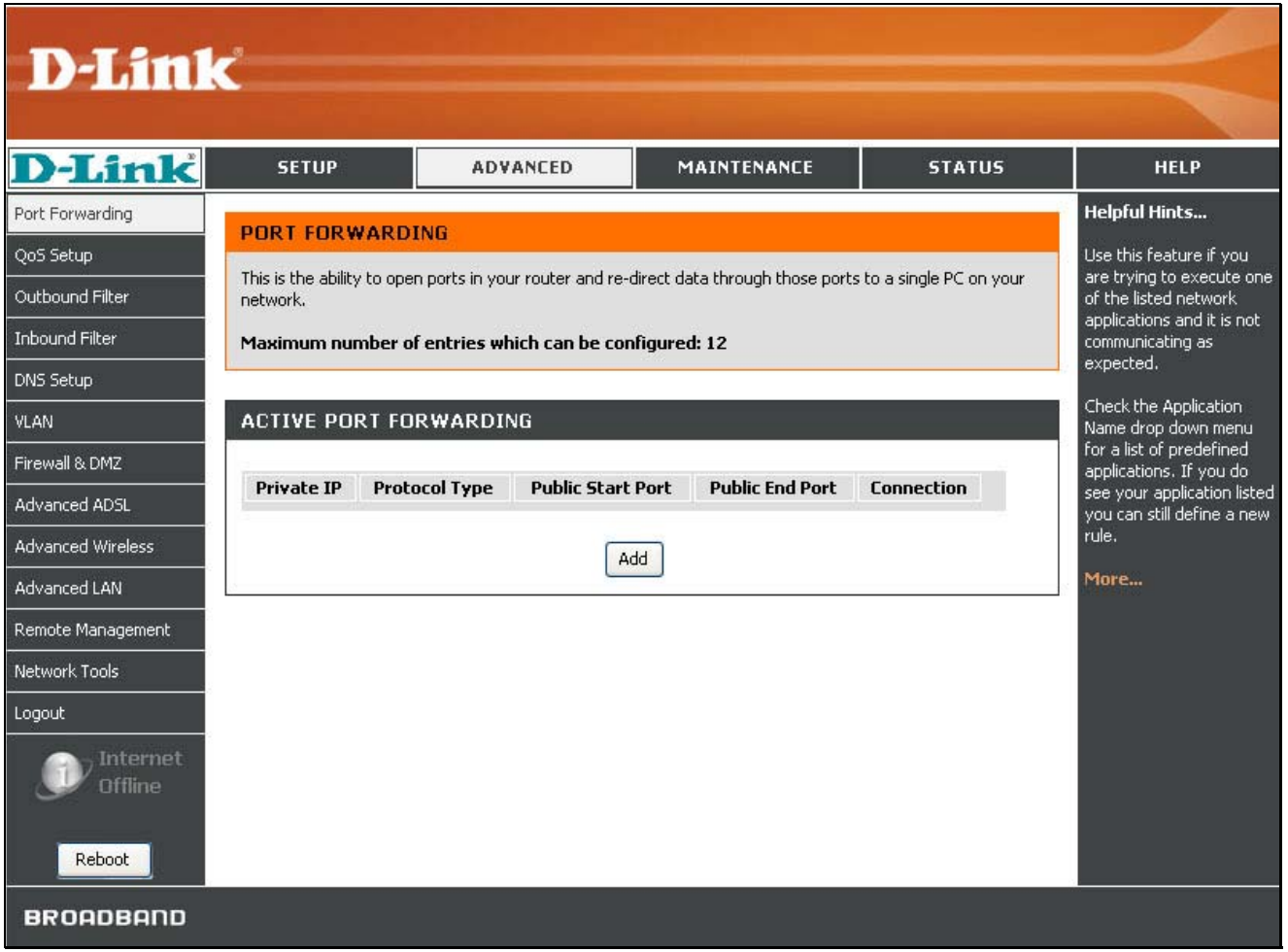
The Router provides a number of options to maintain current date and time including NTP.

To configure system time on the Router, select the method used to maintain time. The options available include Simple Network Time Protocol (SNTP), using your computer's system clock (**Your computer's clock** option), or set the time and date manually. If you opt to use SNTP, you must enter the SNTP server URL or IP address. Click the **Save Settings** button to set the system time.



Advanced Setup

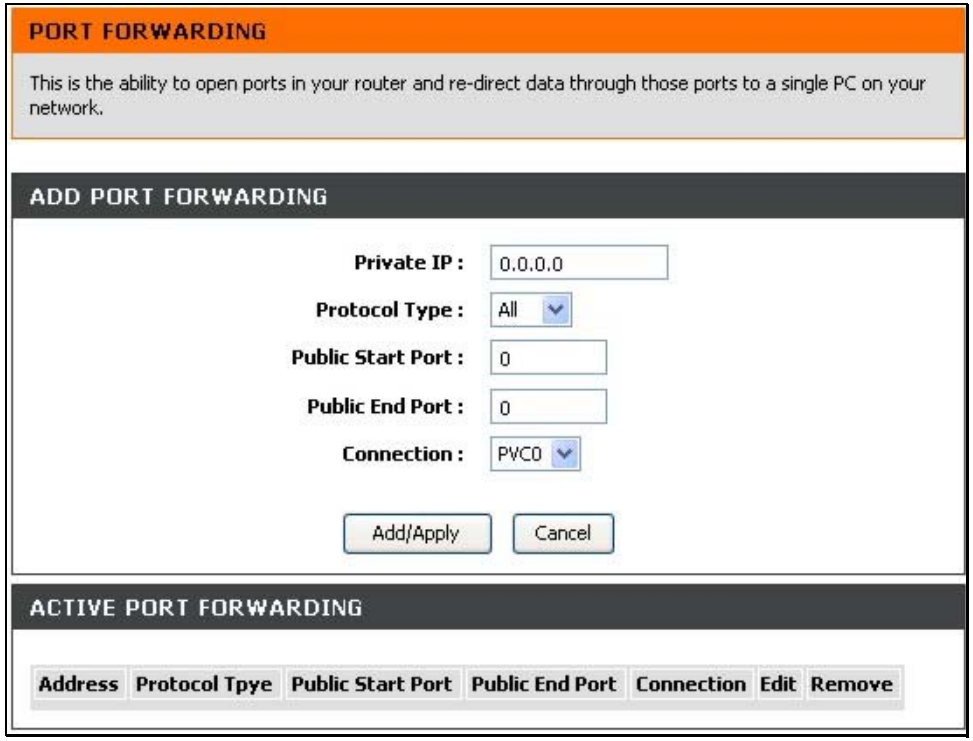
The **Advanced** directory tab offers the following configuration menus: **Port Forwarding**, **QoS Setup**, **Outbound Filter**, **Inbound Filter**, **DNS Setup**, **VLAN**, **Firewall & DMZ**, **Advanced ADSL**, **Advanced Wireless**, **Advanced LAN**, and **Remote Management**. Click the corresponding link in the left panel of the window. **Port Forwarding** is the first menu listed and the first to appear when accessing the **Advanced** directory.



Port Forwarding

The Port Forwarding menu allows configuration for remote users access to various services outside of their LAN through a public IP address, such as FTP (File Transfer Protocol) or HTTPS (Secure Web). After configuring the Router for these features, the Router will redirect these external services to an appropriate server on the users LAN.

Enter an IP address in the Private IP field, select a Protocol Type from the drop-down menu, enter a range of ports in the Public Start Port and Public End Port fields, and then click the **Add/Apply Settings** button. Finally, click the **Reboot** button on the left panel to let your changes take effect.

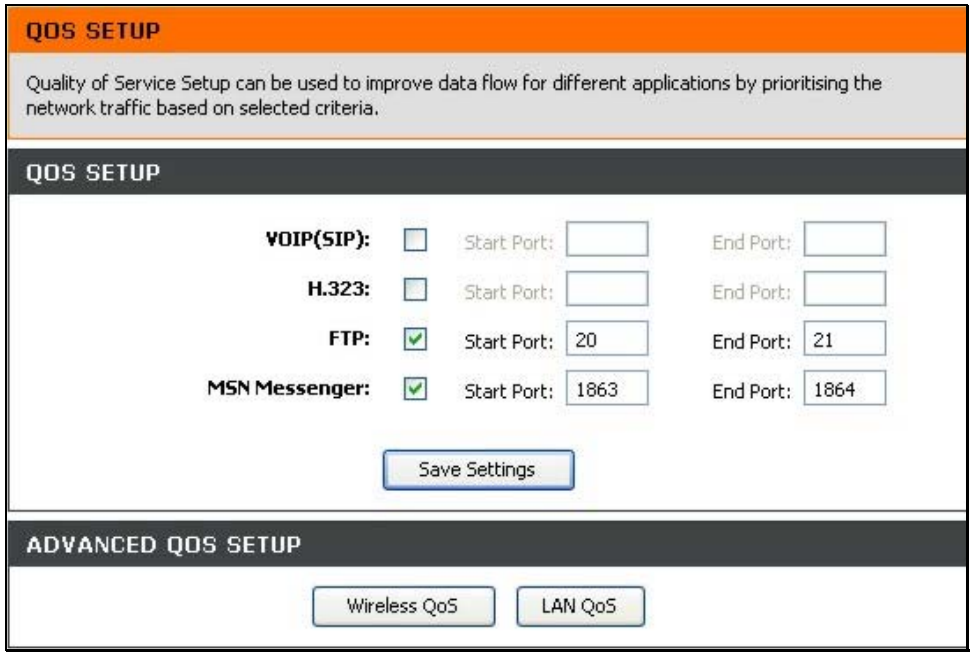


QoS Setup

QoS or Quality of Service allows your Router to help prioritize the data packet flow in your Router and network. This is very important for time sensitive applications such as VoIP where it may help prevent dropped calls. Large amounts of non-critical data can be scaled so as not to affect these prioritized sensitive real-time programs. The basic QoS Setup menu includes some commonly used network services for which QoS can be enabled.

QoS settings can be customized for wireless or Ethernet applications and services that are not included in those listed in the basic QoS menu. To view the QoS settings menu for Wireless LAN, click the Wireless QoS button under Advanced QoS, see the description below. Likewise to configure QoS settings for the Ethernet LAN, click the LAN QoS button to view the settings menu.

Basic QoS settings can be configured by checking any of the listed network applications and entering the ports (Start Port/End Port) used for the application. Click **Save Settings** to apply the QoS settings.



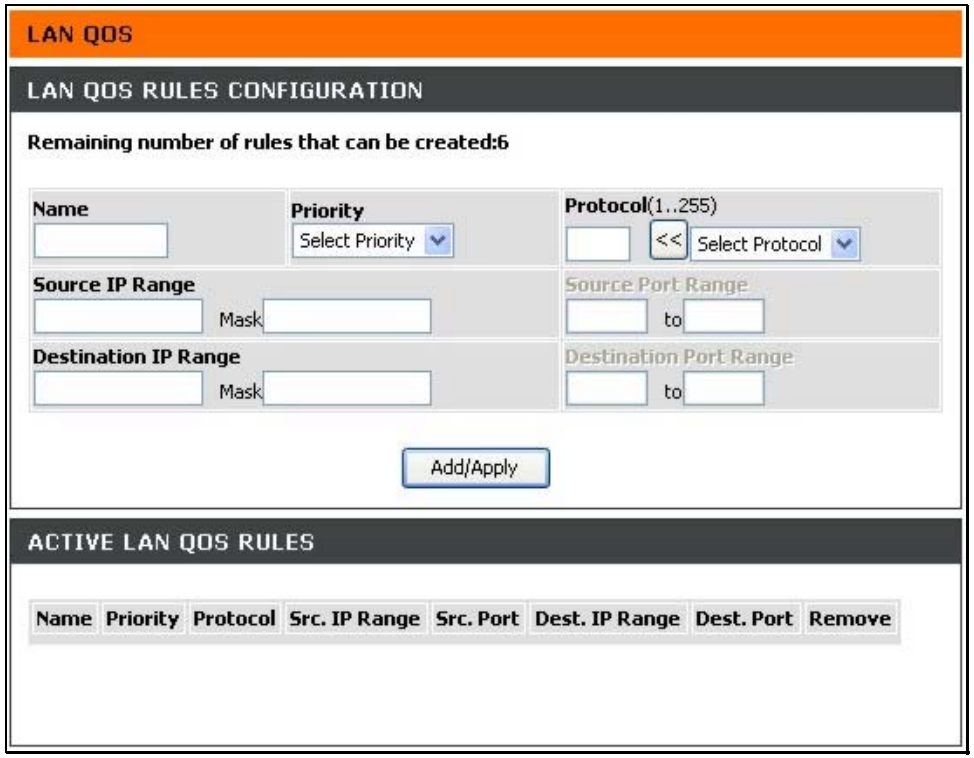
Advanced LAN QoS Setup

Use the LAN QoS Rules Configuration menu to create up to 6 rules to set priority level (low, medium or high) to specified UDP/TCP port or port range; or set priority on specified IP addresses or subnets for ICMP packets.

To create custom QoS rules for the Ethernet LAN, type a **Name** for the rule, choose the **Priority** level from the drop down menu, choose the **Protocol** from the drop-down menu and click the << key to place a corresponding index number in the box; or type an index number in the box.

Type the source port or range and the destination port or range in the spaces provided. Where appropriate (for example ICMP), type a source and destination IP address or subnet. Click **Add/Apply** to create the rule.

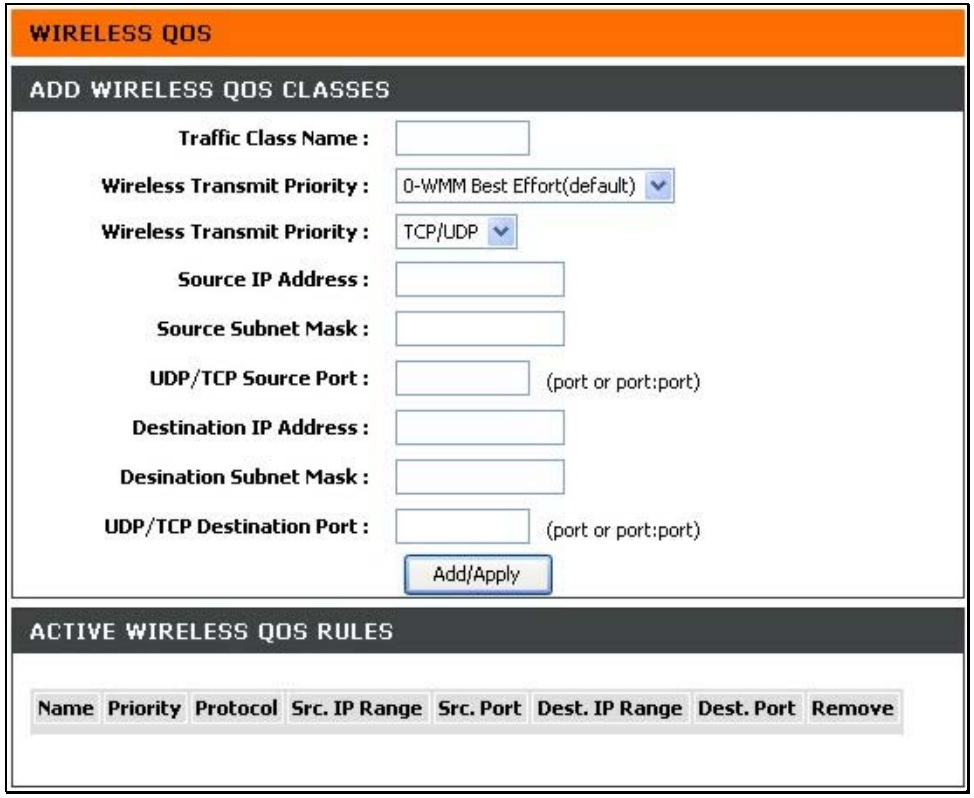
.



Advanced Wireless QoS Setup

Use the Wireless QoS Classes menu to create rules to set wireless transmission priority level (low, medium or high) to specified UDP/TCP port or port range; or set priority on specified IP addresses or subnets for ICMP packets.

To create custom QoS rules for the Ethernet LAN, type a **Traffic Class Name** for the rule, choose the **Wireless Transmit Priority** level from the drop down menu, choose the **Protocol** from the drop-down menu. Type the source port or range and the destination port or range in the spaces provided. Where appropriate (for example ICMP), type a source and destination IP address or subnet. Click **Add/Apply** to create the rule.

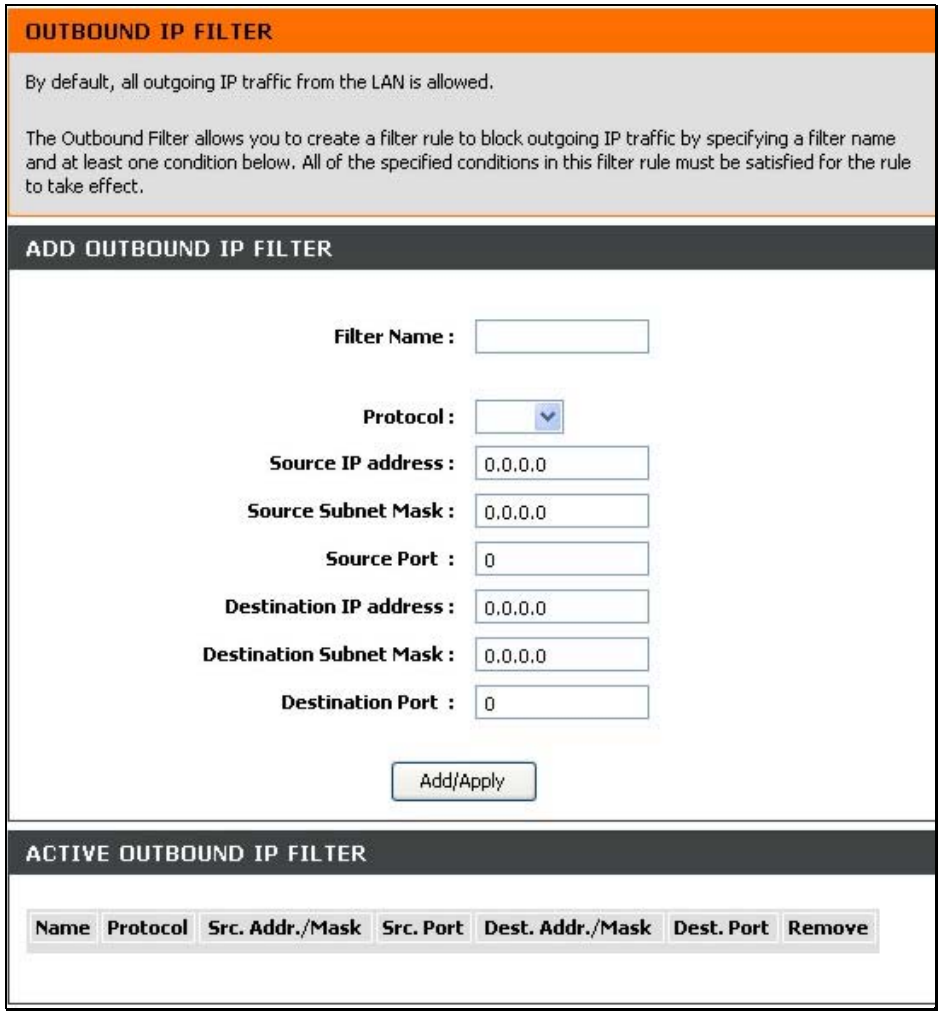


Outbound Filter

Use the **Outbound IP Filter** menu to create **LAN to WAN** outgoing traffic filtering rules that will block traffic as specified.

Type a **Filter Name** used for the rule, select the **Protocol** and type the **Source IP Address** and **Subnet Mask**, and **Source Port** if necessary. The **Destination IP Address**, **Subnet Mask** and **Port** can also be specified if required. Click the **Add/Apply** button to create and activate the new filtering rule.

The new rule appears listed in the **Active Outbound IP Filter** list. A rule can be deleted by selecting the **Remove** option for the rule and clicking the **Remove Selected** button.

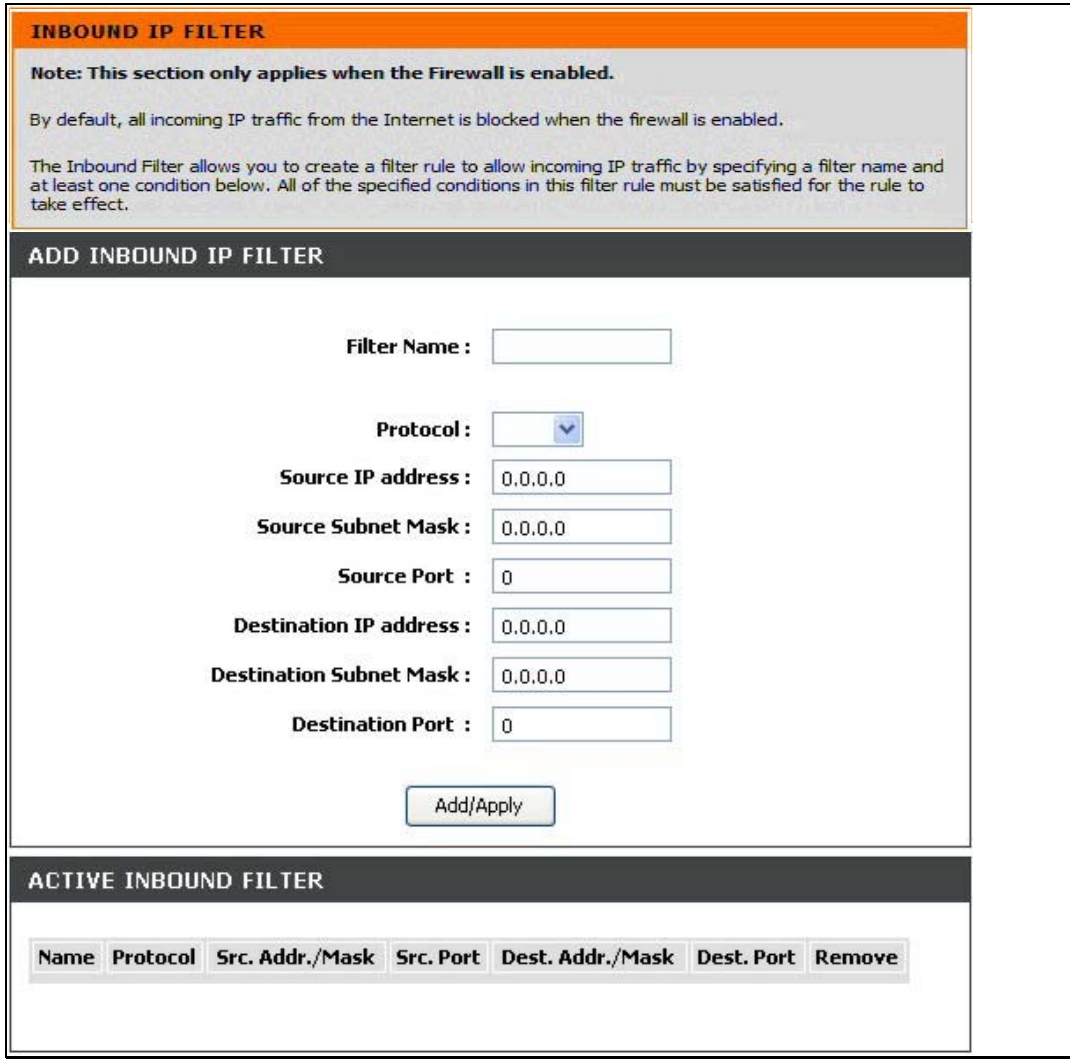


Inbound Filter

Use the **Inbound IP Filter** menu to create **WAN to LAN** incoming traffic filtering rules that will block traffic as specified. **Note that the default IP Filter setting blocks all incoming IP traffic when the firewall is enabled.** Use the Inbound Filter menu to specify the traffic that will be allowed.

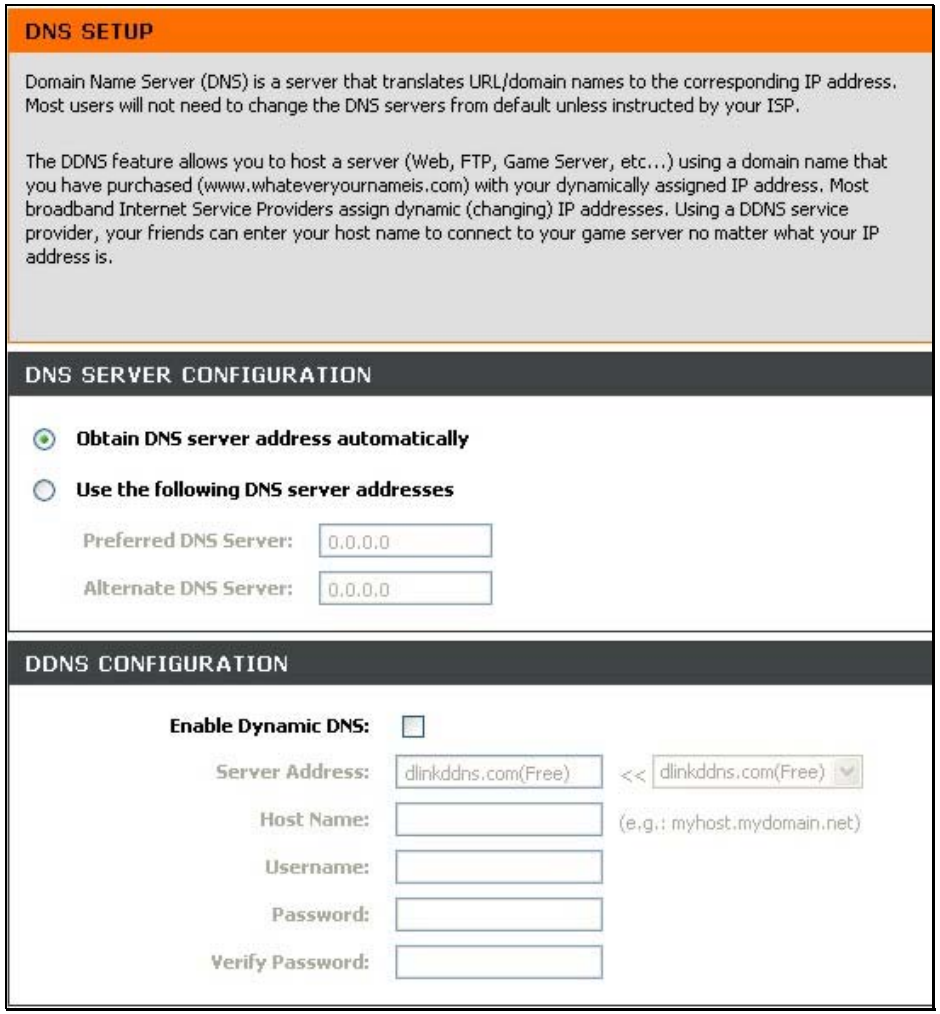
Type a **Filter Name** used for the rule, select the **Protocol** and type the **Source IP Address** and **Subnet Mask**, and **Source Port** if necessary. The **Destination IP Address**, **Subnet Mask** and **Port** can also be specified if required. Click the **Add/Apply** button to create and activate the new filtering rule.

The new rule appears listed in the **Active Inbound IP Filter** list. A rule can be deleted by selecting the **Remove** option for the rule and clicking the **Remove Selected** button.



DNS Setup

Use the DNS Setup menu to configure standard DNS server IP settings or to configure and enable DDNS for the Router.



DNS Server

Choose to “Obtain DNS server address automatically” from the ISP or enter DNS IP address information manually. The **Preffered DNS Server** address is required, the **Alternate DNS Server** address is used for a back up DNS server.

DDNS

Dynamic DNS allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specific host from various locations on the Internet. With this function enabled, remote access to a host will be allowed by clicking a URL hyperlink in the following form: *dlinkddns.com* Because many ISPs assign public IP addresses using DHCP, it can be difficult to locate a specific host on the LAN using the standard DNS. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS servers.

To implement Dynamic DNS, first select the **Enable Dynamic DNS** option and choose the **Server Address** from the list in the pull-down menu. Enter the **Host Name** of the LAN to be accessed, and the **Username** and **Password** for the DDNS account. Click the **Apply Settings** button to save changes made.

VLAN Setup

Use the VLAN Setup menu to create VLAN groups for the Wireless and Ethernet LANs. For ADSL accounts using multiple ATM VCs, VLANs can be created and customized for each separate VC.

VLAN Group Setting

Use the VLAN Index menu to choose a number for the VLAN group. To make sure additional VLAN groups use unique index numbers, the menu will automatically select a new index number for configuration after apllying the VLAN group settings.

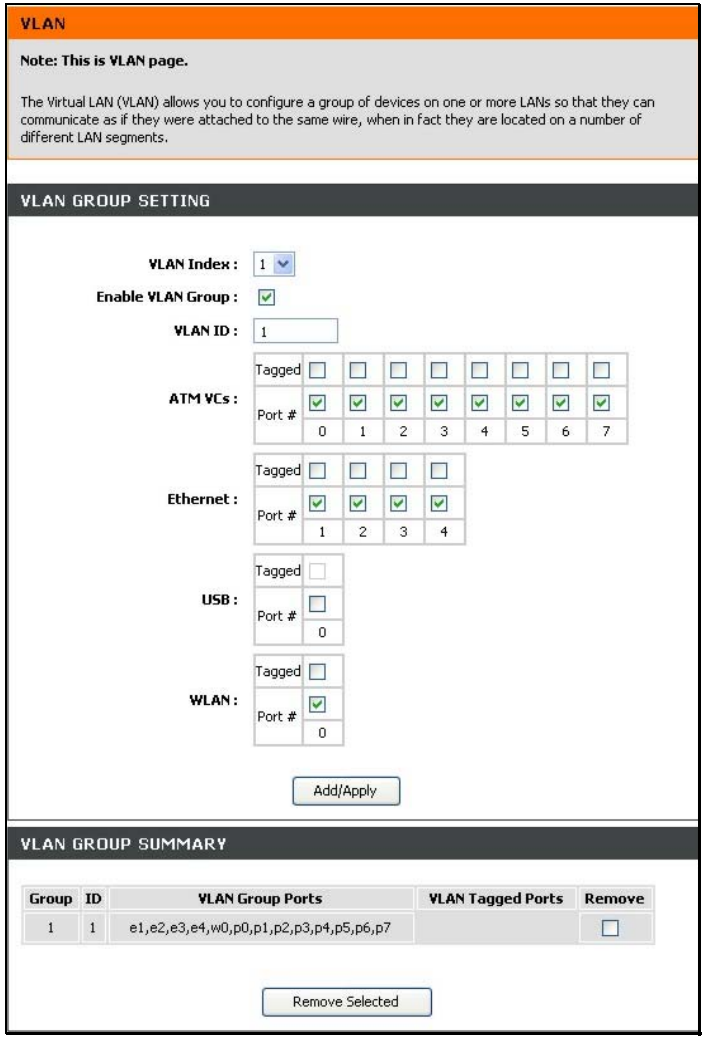
Click to select the member ports of each VLAN group for **Ethernet** ports and **WLAN** interface and the **ATM VCs** ports for each VLAN. Any port may be specified as **Tagged**.

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Select the **Tagged** option to enable tagging for the port. Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

VLAN Group is enabled by default. VLAN Groups can be disabled without changing the previously configured VLAN arrangement. To disabled VLAN Groups click the **Enable VLAN Group** box to remove the check mark.

Click the **ADD/Apply** to apply the settings.



DMZ and Firewall Setup

Use the Firewall and DMZ menu to enable or disable basic firewall protection from Denial of Service and other attacks from the WAN.

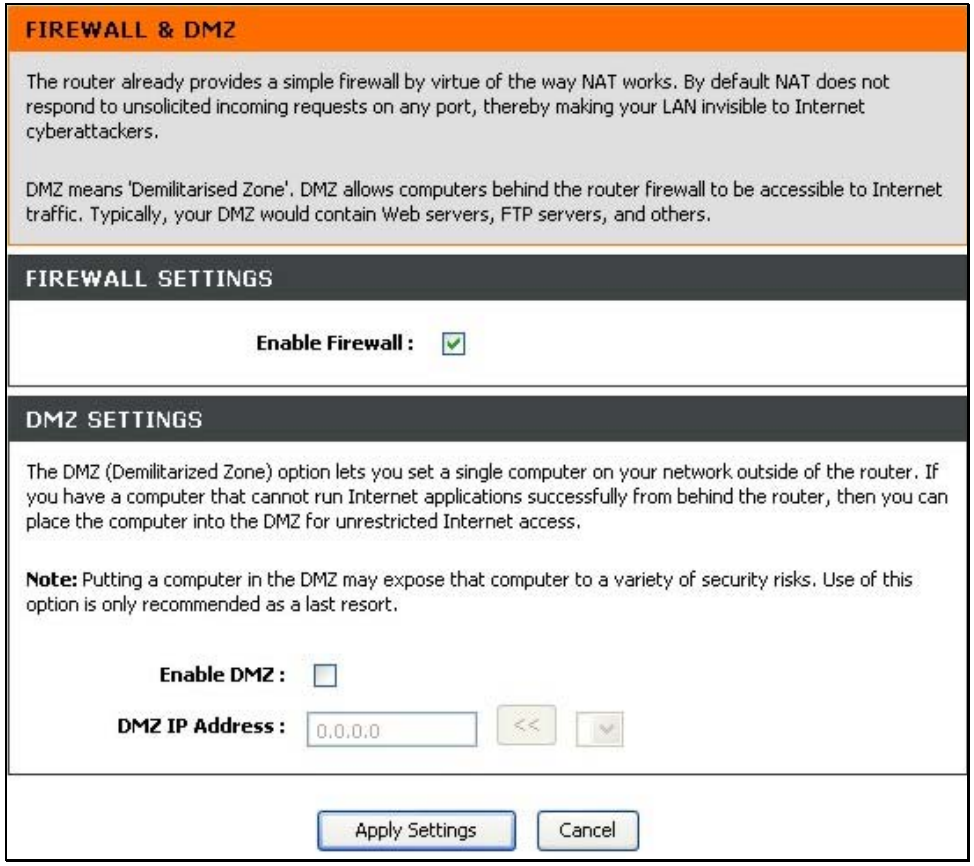
Firewall Settings

Enable the Firewall to block Denial of Service attacks, flood pings, port scans and other common exploitative attacks that might come from the Internet. This is enabled by default. To disable it, click the Enable Firewall box to remove the check mark and click the **Apply Settings** button.

DMZ Settings

Firewalls may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a firewall bypass can be set up using a DMZ IP address. The DMZ IP address is a “visible” address and does not benefit from the full protection of the firewall function. Therefore it is advisable that other security precautions be enabled to protect the other computers and devices on the LAN. It may be wise to use isolate the device with the DMZ IP address from the rest of the LAN.

For example, if you want to use video conferencing and still use a firewall, you can place the server in the DMZ. The IP address of this server will then be the DMZ IP address. You can designate the server’s IP address as the DMZ by typing in the IP address in the **DMZ IP Address** space provided and then enabling its status by selecting the **Enable DMZ** option. Click the **Apply Settings** button at the top of the window when you are finished.

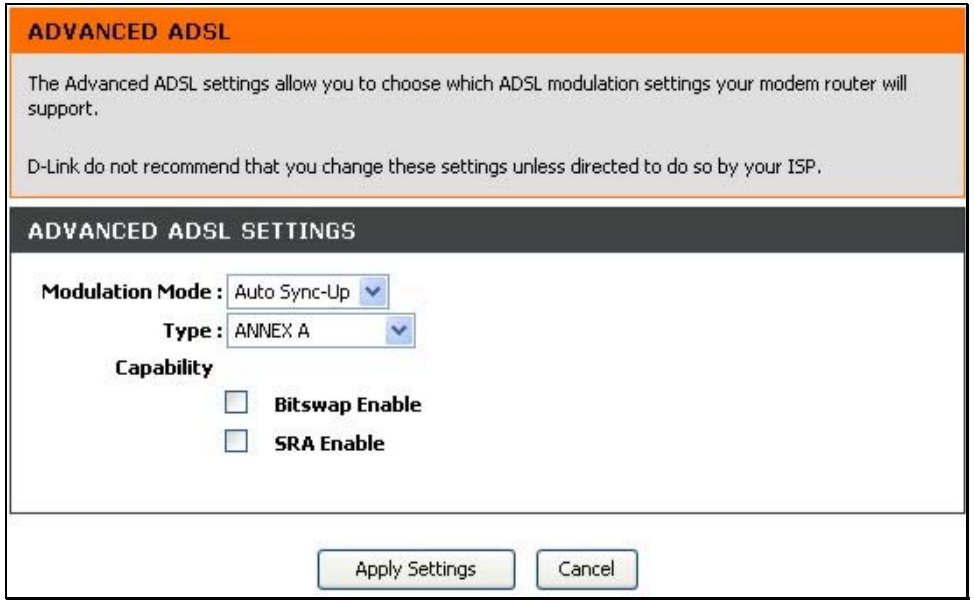


Advanced ADSL

ADSL modulation is configured in the Advanced ADSL menu. The default setting automatically detects the appropriate modulation for the connection, therefore it should not be necessary to change this setting for the Router to function.

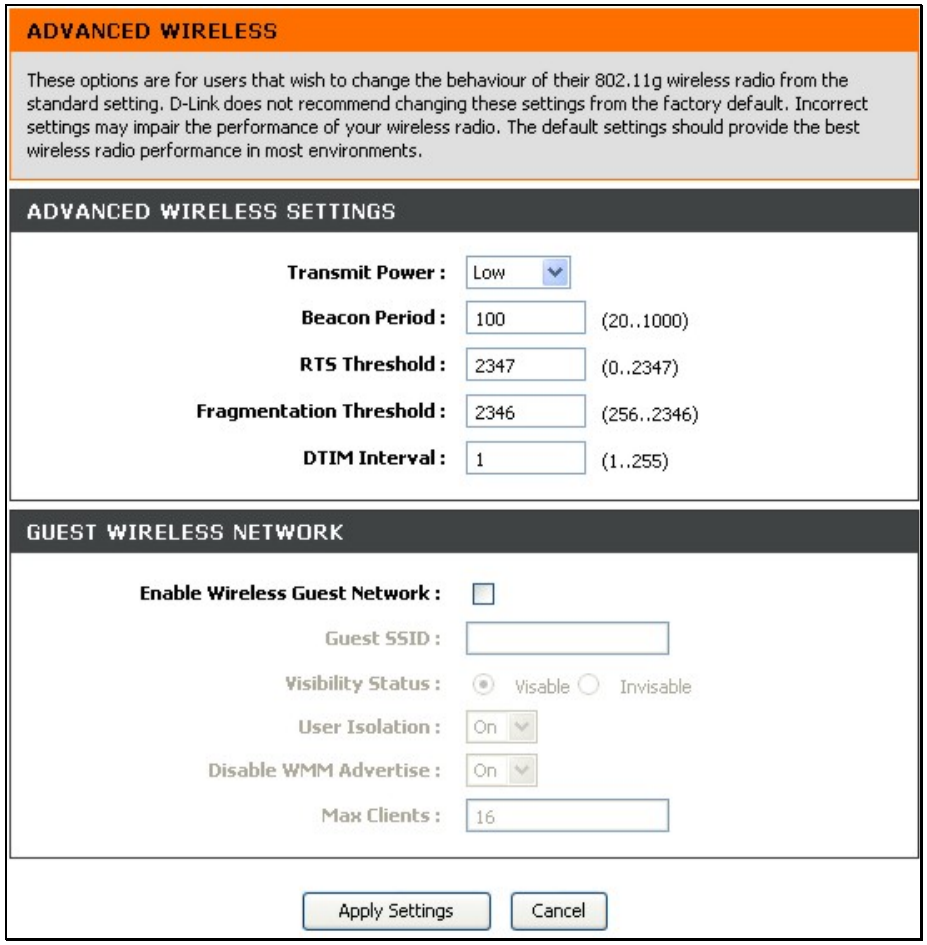
Modulation types supported by the Router include: ADSL2, ADSL2+, G.dmt, T1.143 and G.lite. If the **Modulation Mode** is changed from the default Auto Synch-Up, the mode used must be supported by the ISP in order for the ADSL signal to function. Likewise for changing the ANNEX type, if the **Type** used is not supported by the ISP in your region, the ADSL signal will not function.

The **Bitswap** and **SRA** (Seamless Rate Adaptation) features can be enabled here. If your ADSL modulation is ADSL2 or ADSL2+, these features will only be useful if supported by the ISP. If you opt to use either of these, some experimentation might be advisable to test ADSL synchronization and signal performance for improvement or degradation.



Advanced Wireless

Advanced Wireless settings are used to tweak various wireless transmission parameters and to enable an additional SSID or Guest SSID.



Transmit Powers

Allows the user to adjust the transmit power of the router. A high transmit power allows a greater area range of accessibility to the router. When multiple overlapping access points are present, it may be desirable to reduce transmission power.

Beacon Interval

Beacons are emitted from the router in order to synchronize the wireless network. You may set the Beacon Interval range between 20-100 microseconds per beacon sent. The default is 100.

RTS Threshold

The RTS (Request to Send) Threshold controls the size of data packets issued to a RTS packet. A lower level will send packets more frequently which may consume a great amount of the available bandwidth. A high threshold will allow the router to recover from interference or collisions which is more prevalent in a network with high traffic or high electromagnetic interference. The default setting is 2347.

Fragmentation Threshold

The fragmentation threshold will determine if packets are to be fragmented. Packets over the 2346 byte limit will be fragmented before transmission. 2346 is the default setting.

DTIM Interval

DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next menu for listening to broadcast and multicast messages. The default setting is 1.

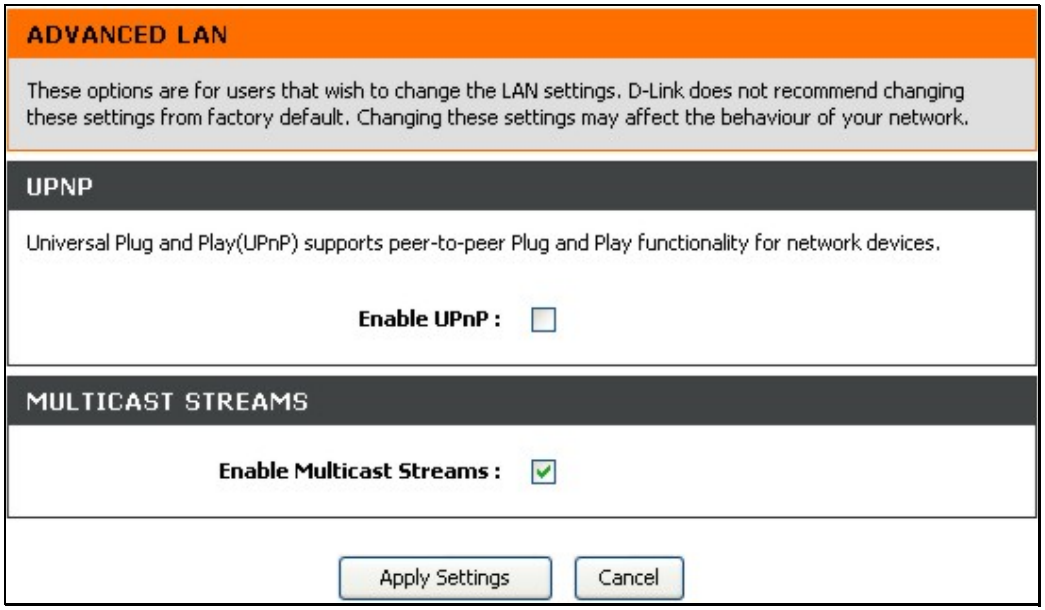
Guest Wireless Network

A second SSID can be enabled and used for the wireless LAN. The additional **Guest SSID** can be **Visible** or **Invisible** to roaming wireless nodes. By default, **User Isolation** is *On* (enabled), **Disable WMM Advertise** is *On* (i.e. SSID advertising is disabled) and a maximum number of clients allowed (**Max Clients**) is *16*. When User Isolation is On, Guest SSID member clients will be unable to transmit to other wireless clients, however they will have access to network resources through the Ethernet or Internet.

Click on the **Apply Settings** button to save and apply the advanced wireless configuration.

Advanced LAN

Use the Advanced LAN menu to enable or disable UPnP and multicast streaming.



UPnP or Universal Plug and Play is disabled by default. This network protocol is used to simplify networking and is supported on many types of networking devices. Devices that support UPnP advertise their services and capabilities to other UPnP enabled devices to facilitate network applications such as streaming audio or video. To use UPnP click the **Enable UPnP** option to check the box.

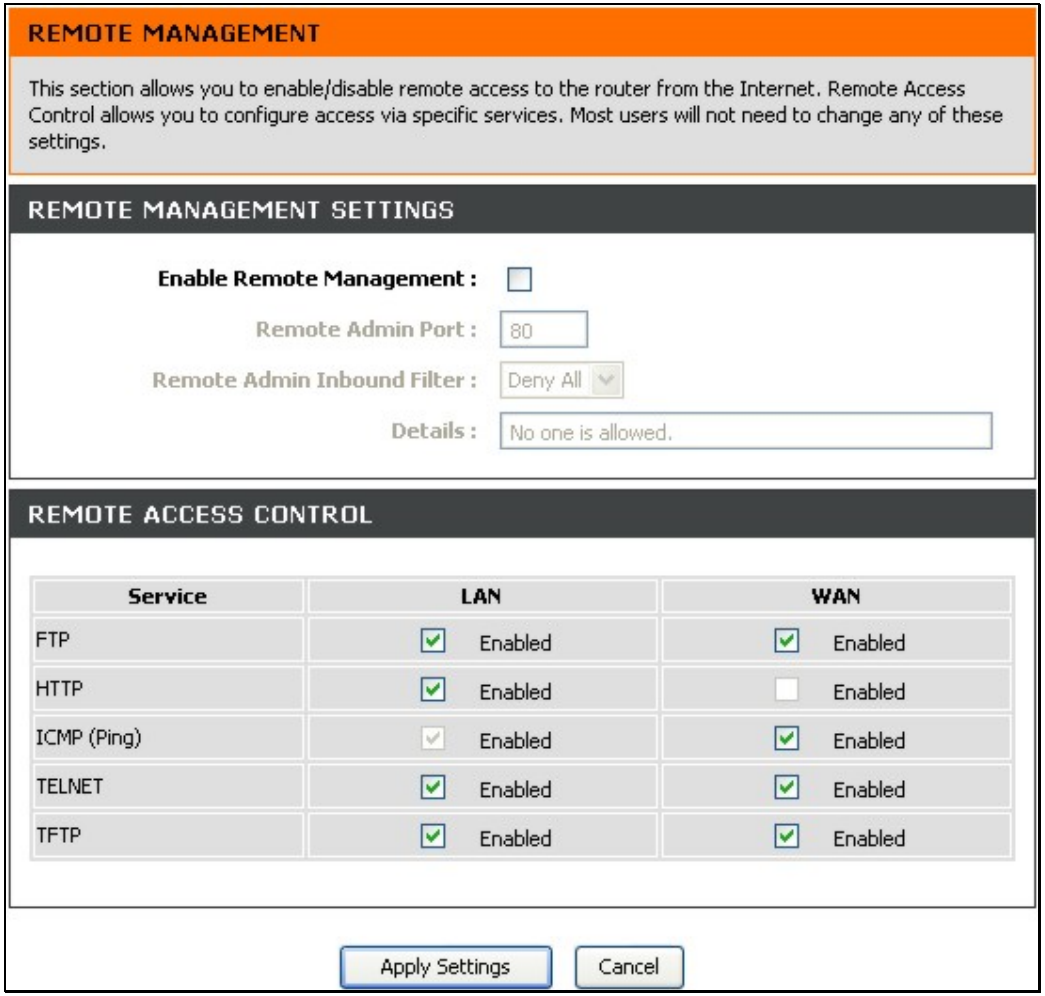
Multicast streaming support is enabled by default to allow streaming of audio and video and other multicast applications to pass through the Router. To disable multicast streams click the **Enable Multicast Streams** box to remove the check mark. Keep in mind that Internet radio and similar multicast services will not function if the Enable Multicast Streams option is not checked.

Click on the **Apply Settings** button to save and apply the advanced LAN configuration.

Remote Management

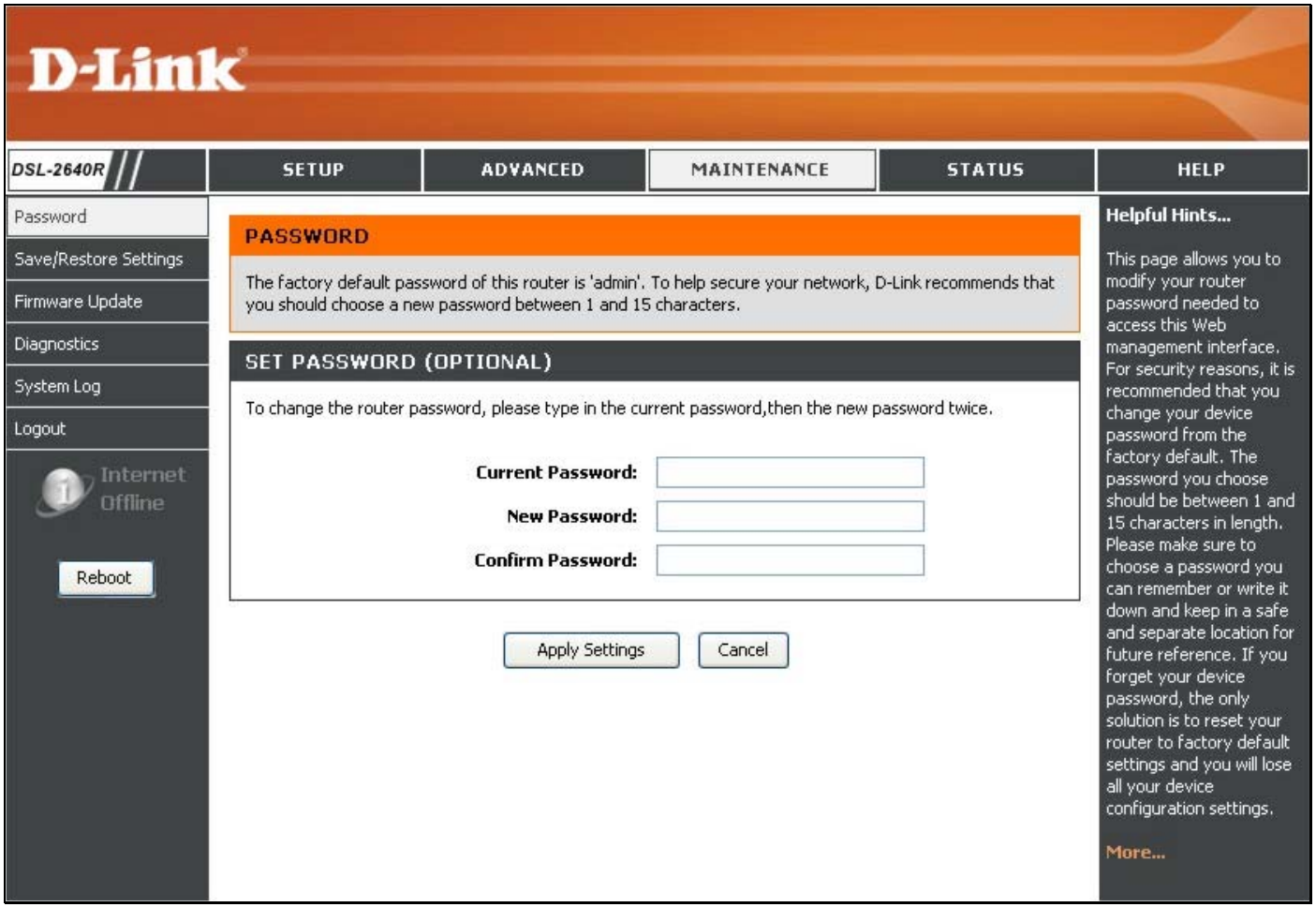
Use the Remote Management menu to enable and configure remote management of the Router through the WAN interface. In addition, management access from either the LAN or WAN side can be restricted to the Router by specifying services allowed for management.

When remote management is enabled, the options available are to either *Allow All* or *Deny All* with the **Remote Admin Inbound Filter** pull-down menu. Choose the services allowed from the LAN or WAN by checking the **Enabled** box for the service in the **Remote Access Control** list. Click the **Apply Settings** button to make the change.



Maintenance

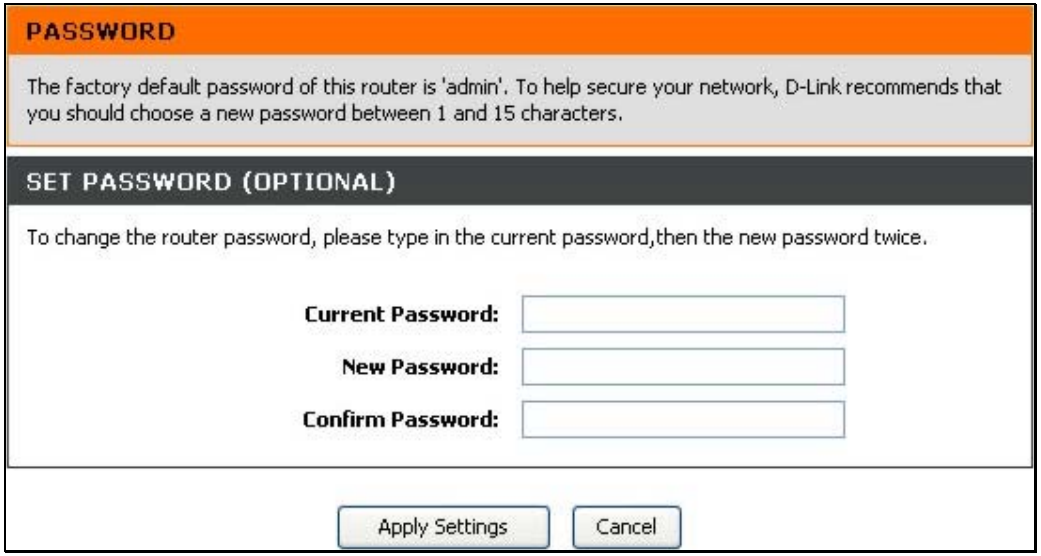
Use the menus in the Maintenance directory to perform routine maintenance functions such as save configuration settings to hard disk and upgrading device firmware, view system log and perform device diagnostic tests.



Password

Typically on first things the administrator is likely to change is the device password used to access the management software. The administrator's user name of the Router, admin, cannot be changed. The default password can be changed with the Password menu.

Change the password and click the **Apply Settings** button to establish the new password.



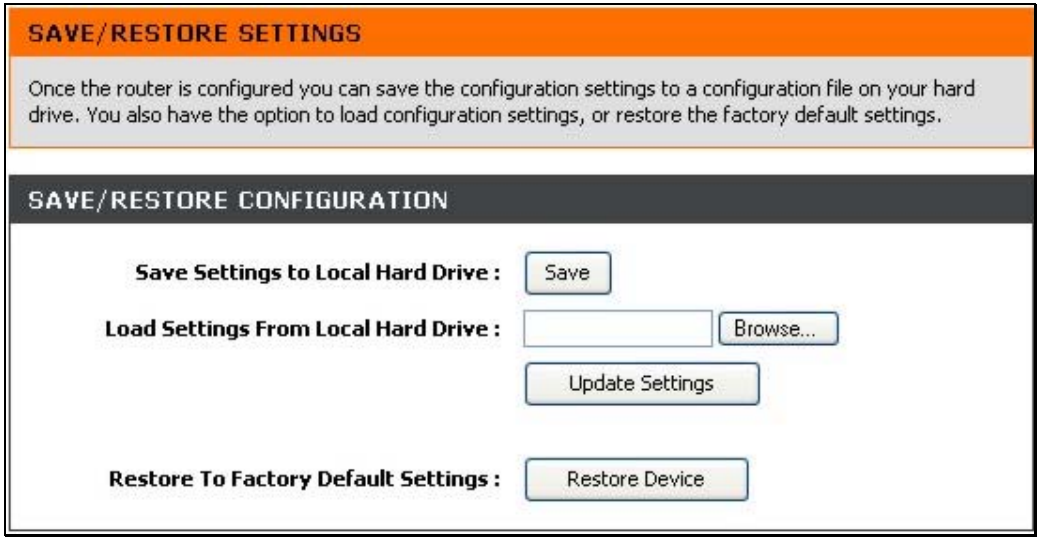
Save/Restore Settings

It is a good idea to store a back up copy of the configuration settings file on the hard drive of the system used to administer the Router. Use this menu to save a settings file, load a settings file or restore the device to factory default settings.

To save the current configuration settings to your computer, click the **Save/Restore Settings** button in the **Maintenance** directory to display the **System Settings** menu. Click the **Save** button to Save Settings to Local Hard Drive. You will be prompted to select a location on your computer to put the file.

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Upload Settings** button to **Load Settings From Local Hard Drive**. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.

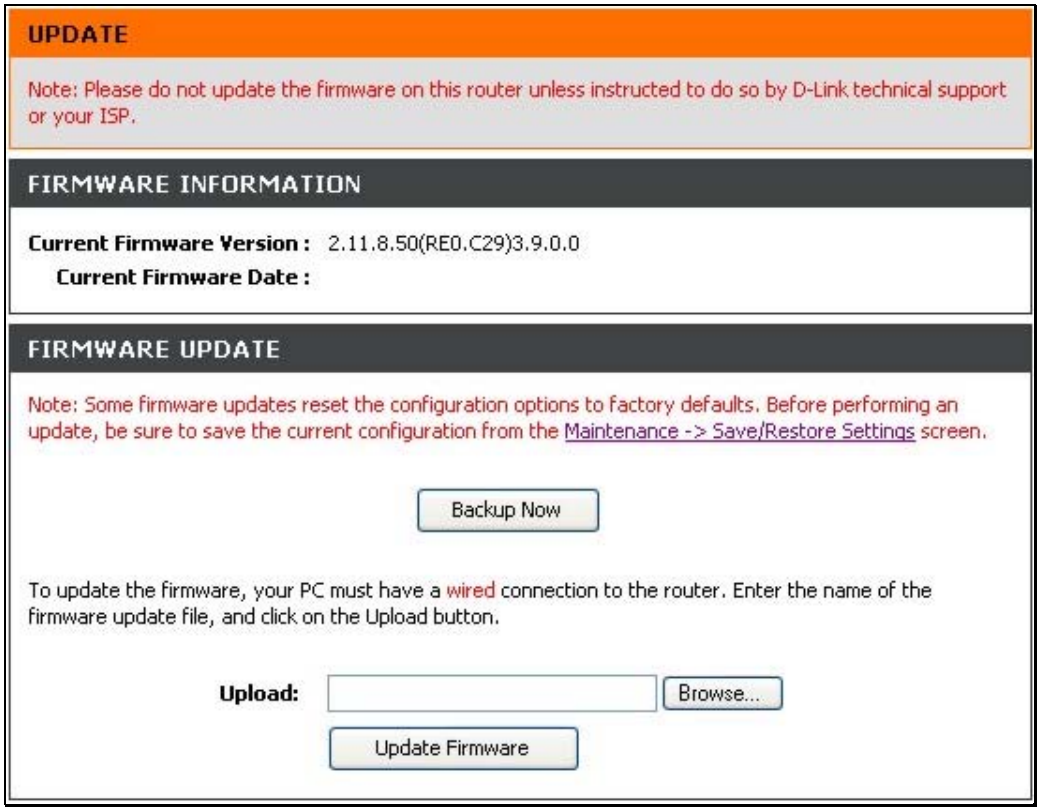
To reset the Router to its factory default settings, click the **Restore Device** button. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP address (192.168.1.1) with DHCP enabled and default administrator password (admin).



Firmware Upgrade

Use this menu to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the **Save/Restore Settings** menu described above or click the Backup Now button to go through the same procedure.

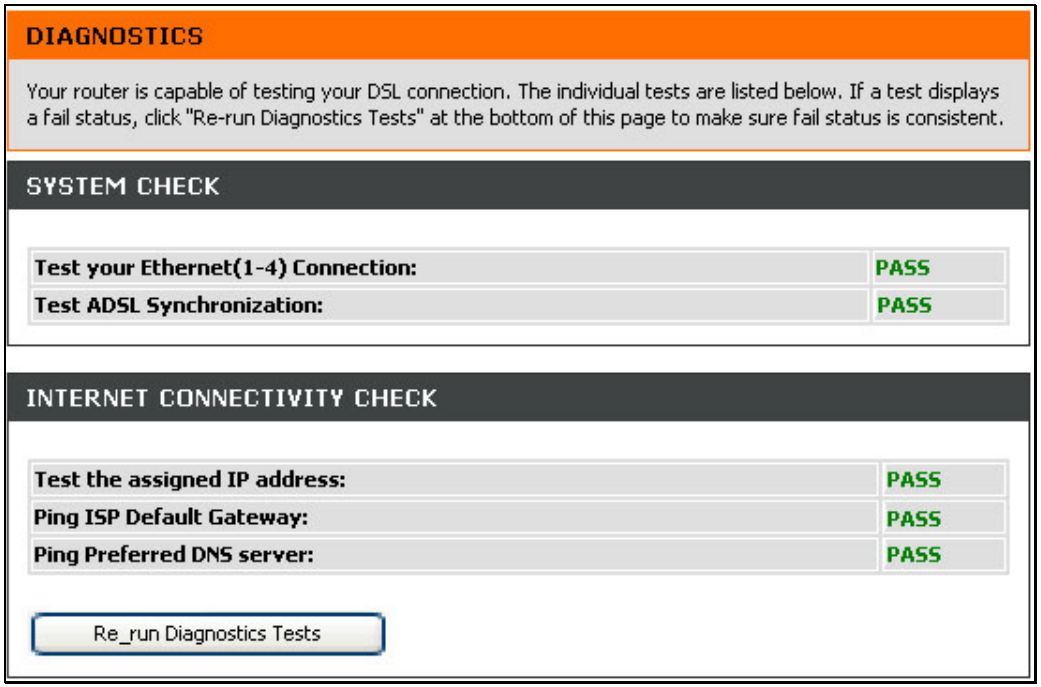
To upgrade firmware, type in the name and path of the file or click on the **Browse** button to search for the file. Click the **Upgrade Firmware** button to begin copying the file. The file will load and restart the Router automatically.



Diagnostics

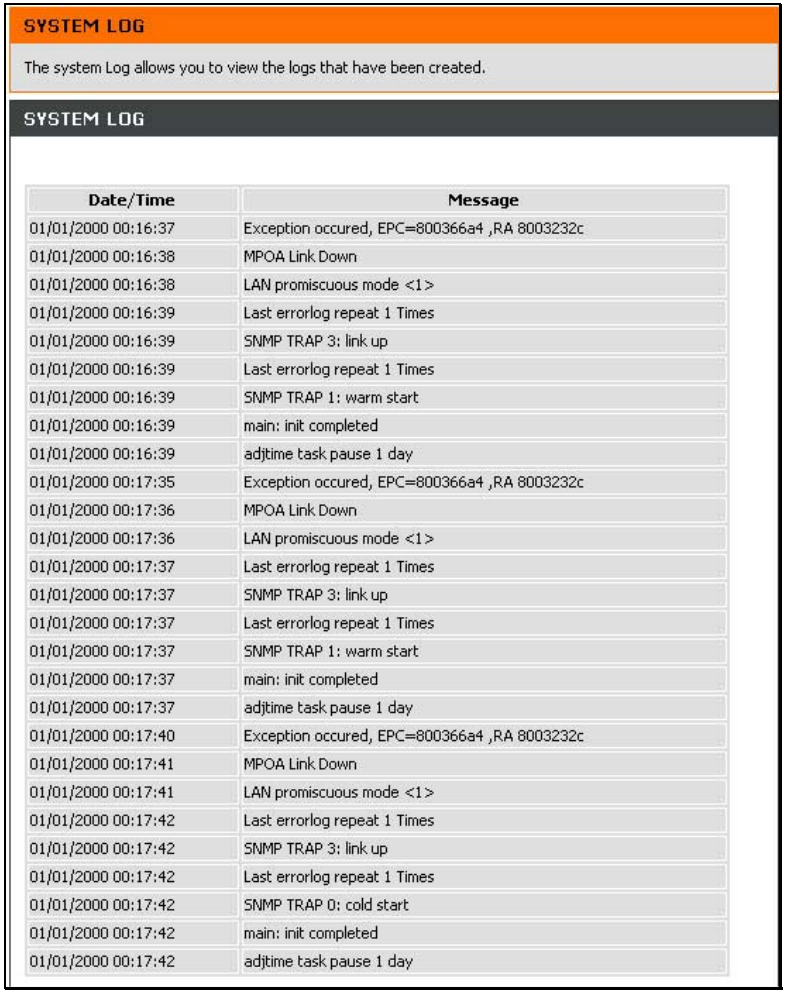
This menu is used to test connectivity of the Router. A Ping test may be done through the local or external interface to test connectivity to known IP addresses. The diagnostics feature executes a series of tests of your system software and hardware connections. Use this menu when working with your ISP to troubleshoot problems.

Click the **Re_run Diagnostics Tests** button to view the connectivity status of the WAN connection.



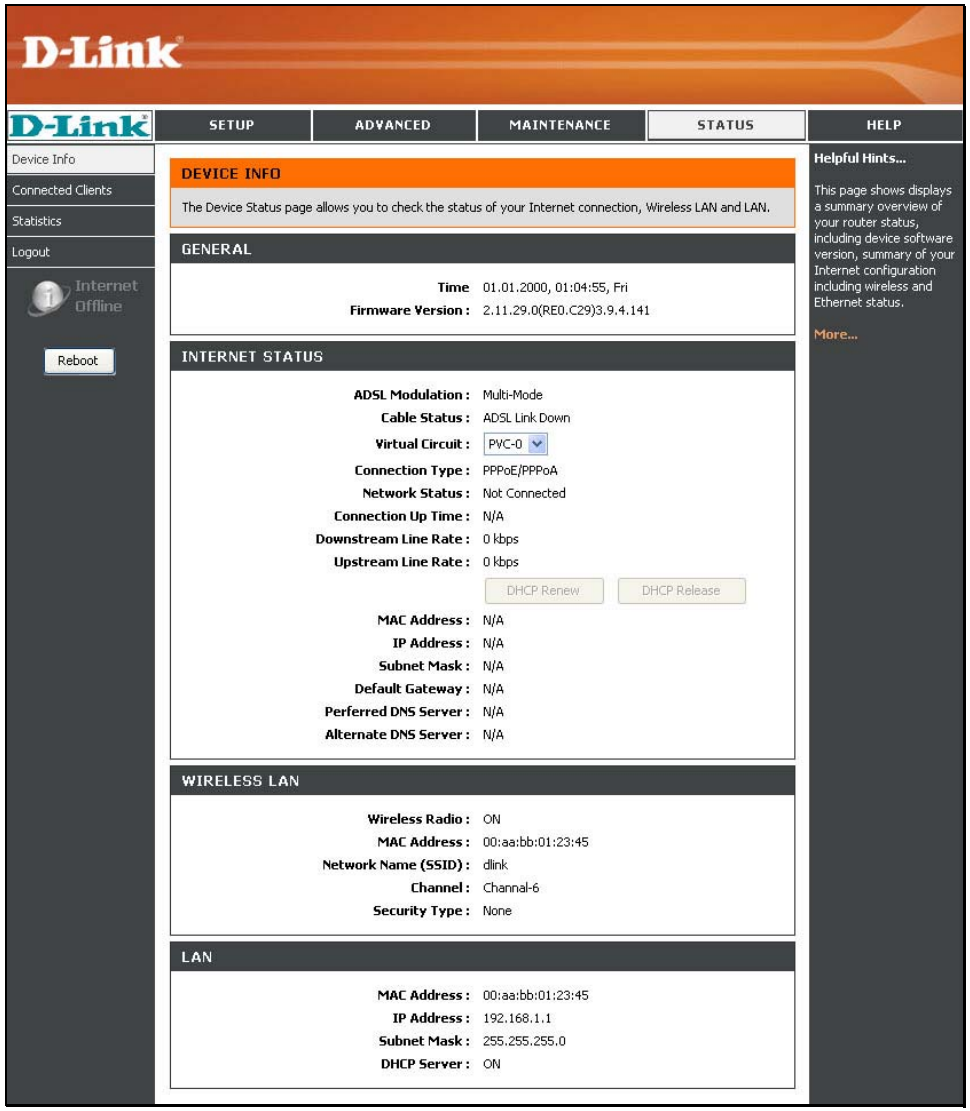
System Log

Use the System Log to view a log of events that occur on the Router.



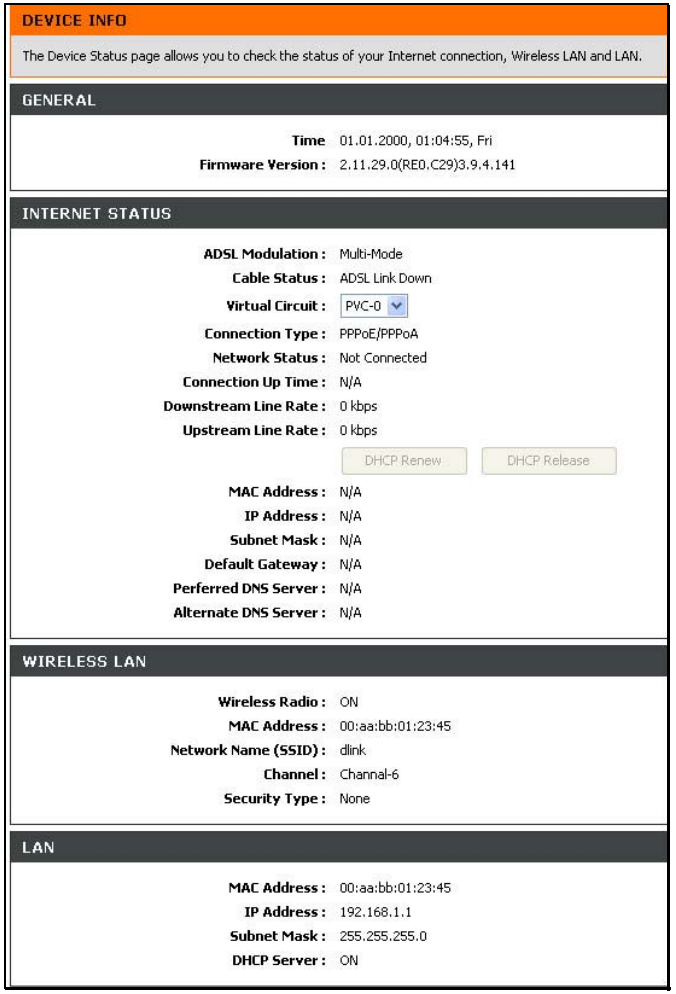
Status

Use these read-only menus to view system information and monitor performance.



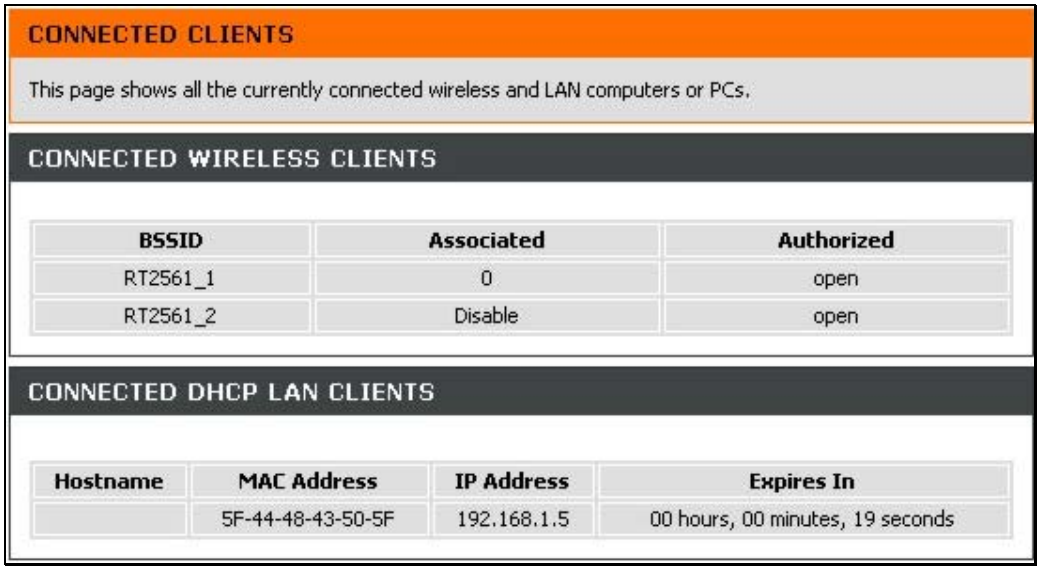
Device Info

Use this menu to quickly view basic current information about the LAN and WAN interfaces and device information including Firmware Version and MAC address.



Connected Clients

The Connected LAN Clients list displays active DHCP clients when the router is acting as a DHCP server and wireless clients.



CONNECTED CLIENTS

This page shows all the currently connected wireless and LAN computers or PCs.

CONNECTED WIRELESS CLIENTS

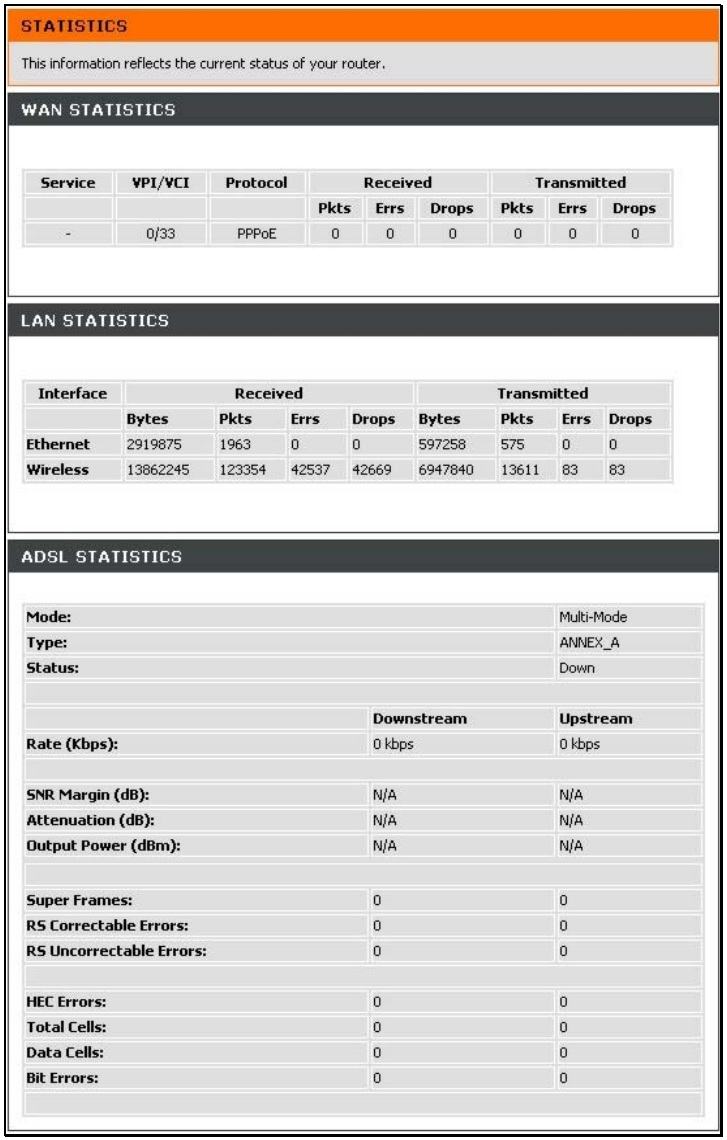
BSSID	Associated	Authorized
RT2561_1	0	open
RT2561_2	Disable	open

CONNECTED DHCP LAN CLIENTS

Hostname	MAC Address	IP Address	Expires In
	5F-44-48-43-50-5F	192.168.1.5	00 hours, 00 minutes, 19 seconds

Statistics

Use this menu to monitor traffic on the Ethernet LAN, Wireless LAN or ADSL interface. This menu also displays information on the ADSL signal status.



STATISTICS

This information reflects the current status of your router.

WAN STATISTICS

Service	VPI/VCI	Protocol	Received			Transmitted		
			Pkts	Errs	Drops	Pkts	Errs	Drops
-	0/33	PPPoE	0	0	0	0	0	0

LAN STATISTICS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	2919875	1963	0	0	597258	575	0	0
Wireless	13862245	123354	42537	42669	6947840	13611	83	83

ADSL STATISTICS

Mode:		Multi-Mode
Type:		ANNEX_A
Status:		Down
	Downstream	Upstream
Rate (Kbps):	0 kbps	0 kbps
SNR Margin (dB):	N/A	N/A
Attenuation (dB):	N/A	N/A
Output Power (dBm):	N/A	N/A
Super Frames:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	0	0
Total Cells:	0	0
Data Cells:	0	0
Bit Errors:	0	0

Technical Specifications

ADSL Standards

- Full-rate ANSI T1.413 Issue 2
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)

ADSL2 Standards

- ITU G.992.3 (G.dmt.bis)

ADSL2+ Standards

- ITU G.992.5 (G.dmt.bisplus)

Protocols

- IEEE 802.1d Spanning Tree
- TCP/UDP
- ARP
- RARP
- ICMP
- RFC1058 RIP v1
- RFC1213 SNMP v1 & v2c
- RFC1334 PAP
- RFC1389 RIP v2
- RFC1577 Classical IP over ATM
- RFC1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)
- RFC1661 Point to Point Protocol
- RFC1994 CHAP
- RFC2131 DHCP Client / DHCP Server
- RFC2364 PPP over ATM
- RFC2516 PPP over Ethernet

DC Power

- Input: 100-120V 0.4A, 50-60 Hz
- Output: 12V 1.2A

Data Transfer Rate

- G.dmt full rate downstream: up to 8 Mbps / upstream: up to 1 Mbps
- G.lite: ADSL downstream up to 1.5 Mbps / upstream up to 512 Kbps
- G.dmt.bis full rate downstream: up to 12 Mbps / upstream: up to 1 Mbps
- ADSL2+ full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps

Wireless Transfer Rates

- IEEE 802.11b: 11, 5.5, 2, and 1Mbps
- IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

Media Interface

- ADSL interface: RJ-11 connector for connection to 24/26 AWG twisted pair telephone line
- LAN interface: four RJ-45 ports for 10/100BASE-T Ethernet connection

Default Settings

IP Settings: IP Address 192.168.1.1 Netmask 255.255.255.0
User Name: admin **Password:** admin
DHCP Server: Enabled