D-Link DSL-2640B

Wireless ADSL2/2+ 4-port Ethernet Router (for ToT)

User Manual

D-Link®
Building Networks for People

RECYCLABLE
2007/06/25

Table of Contents

General Information

The D-Link DSL-2640B is an ADSL2+ router that provides a convenient wireless routing function. This user manual offers you with a simple and easy-to-understand format to install and configure your router.

Package Contents

Included in the package is one of each of the following—

- DSL-2640B Wireless ADSL2/2+ 4-port Ethernet Router
- Power adapter
- RJ-11 telephone cable
- RJ-45 Ethernet cable
- CD-ROM *(containing User Manual & Quick Guide)*
- Quick Guide *(booklet)*

Important Safety Instructions

- Place your router on a flat surface close to the cables in a location with sufficient ventilation. Do not mount this device on a wall.

- To prevent overheating, do not obstruct the ventilation openings of this equipment.

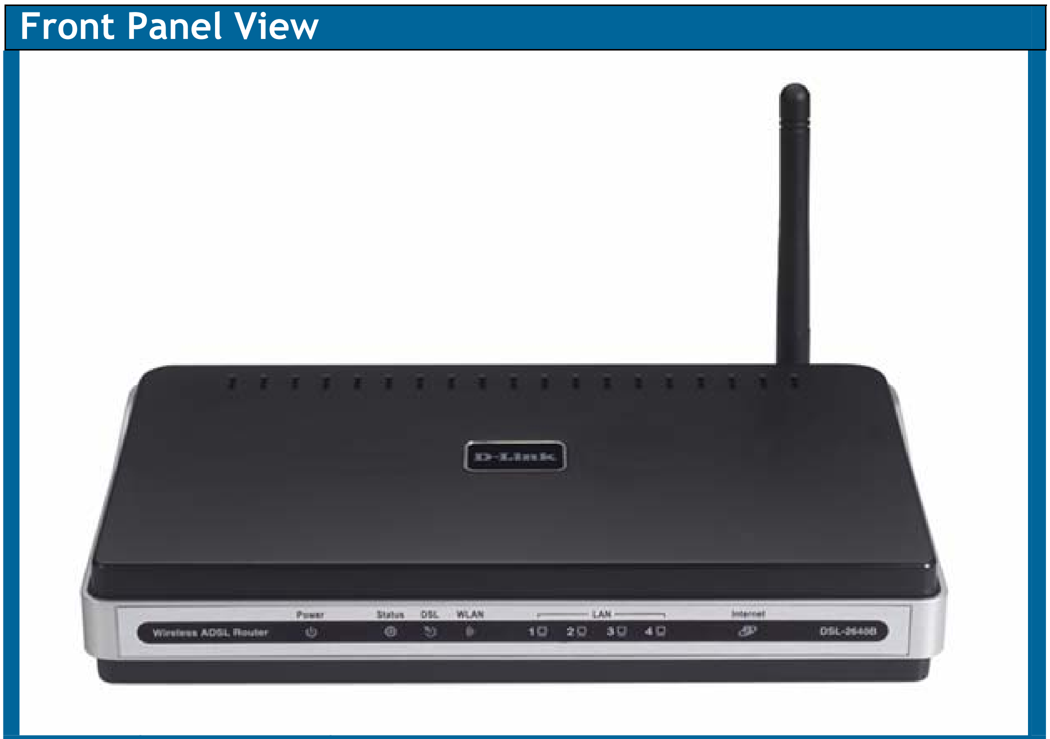
- Plug this equipment into a surge protector to reduce the risk of damage from power surges and lightning strikes.

- Operate this equipment only from an electrical outlet with the correct power source as indicated on the adapter.

- Do not open the cover of this equipment. Opening the cover will void any warranties on the equipment.

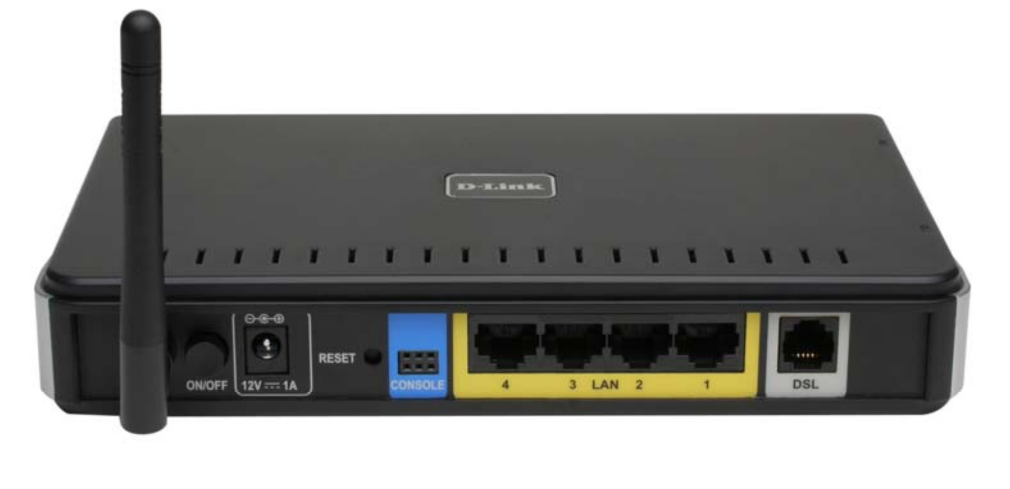
- Unplug equipment first before cleaning. A damp cloth can be used to clean the equipment. Do not use liquid / aerosol cleaners or magnetic / static cleaning devices.

Front Panel View



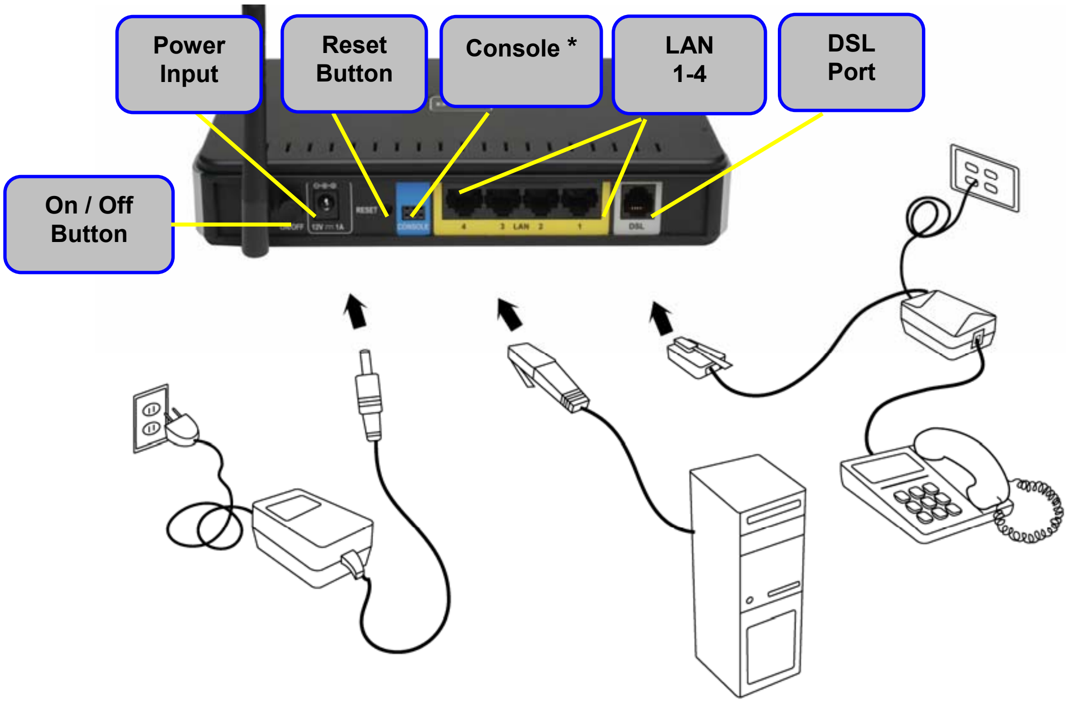
LED	Mode	Indication
Power	Solid Green	The router is powered on. **(READY)**
	No light	The power is off.
	Red	Failure or device malfunction. **(NOT READY)**
Status	Flashing Green	Traffic is passing through the device. **(INTERNET TRAFFIC)**
DSL	Solid Green	DSL is synchronized.
	No Light	No carrier signal.
	Slow Flashing	DSL attempting synch. Trying to detect carrier signal.
	Fast Flashing	Carrier has been detected and modem is trying to train.
WLAN	Solid Green	Wireless is up.
	Flashing	Wireless traffic is passing through.
	No Light	Wireless is down.
LAN 1-4	Solid Green	Powered device connected to associated port
	Flashing Green	LAN activity present (traffic in either direction).
	No Light	No activity, modem power off, no cable or no powered device is connected to the LAN port.
Internet	Solid Green	IP connected (device has a WAN IP address from IPCP or DHCP and DSL is up or a static IP address is configured, PPP negotiation has completed successfully (if used), and DSL is up. **(WAN IP AVAILABLE)**
	No Light	Modem power off, modem in bridge mode or ADSL connection not present.
	Red	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.). **(WAN IP NOT AVAILABLE)**

Back Panel View



Port	Description
On/ Off	Press to turn the router on and off.
Power	Connects to the power adapter.
Reset	Press for less than 3 seconds to reset the router. Press for 3 seconds or more to revert to factory settings.
Console	For use by D-Link service personnel for maintenance purposes only.
LAN 4-1	RJ-45 connects the unit to Ethernet devices such as a PC or a switch.
DSL	RJ-11 telephone port connects telephone cable to telephone or fax machine.

Connecting the Router to Your Computer



** Console—for use by D-Link repair service personnel only.*

Connect the Telephone Cable

- Connect one end of the telephone cable to the **DSL port** on the router and the other end of the cable into the wall socket.

Connect the Ethernet Cable

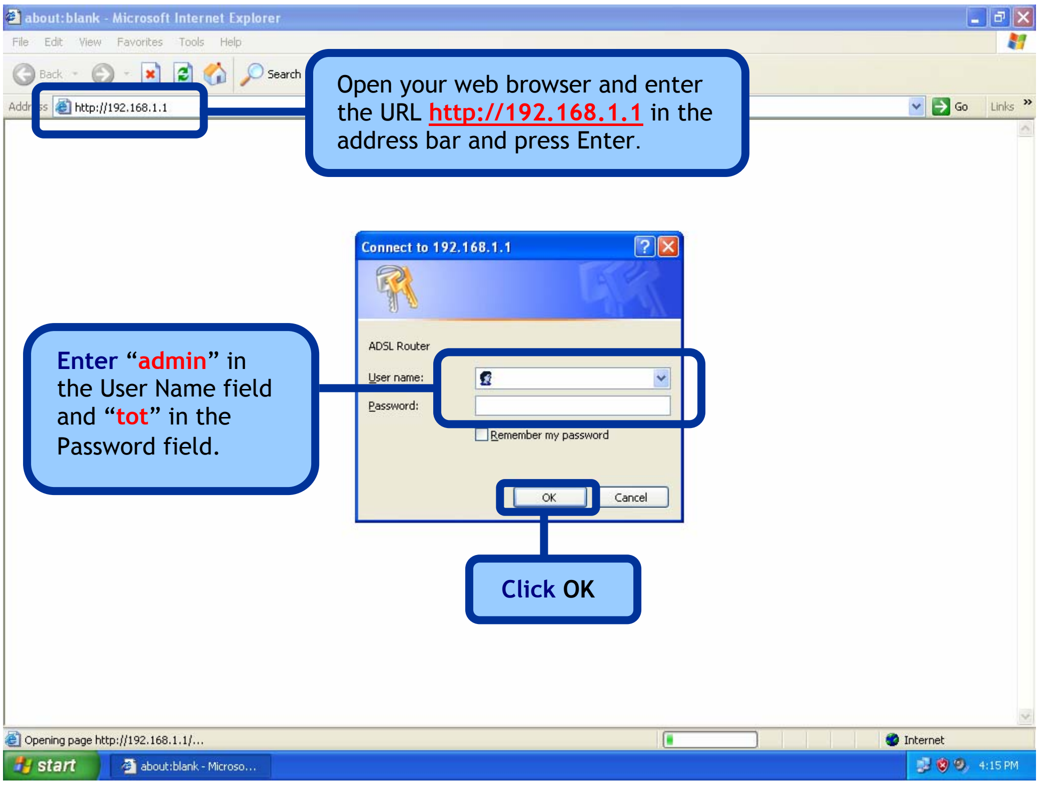
- Connect one end of the Ethernet cable to one of the 4 **LAN ports** on the back of the router and attach the other end to an Ethernet Adapter or available Ethernet port on your computer. Or, you can attach it to a switch / hub first and connect your computer to the switch / hub.

Connect the Power Adapter

- Complete the process by connecting the power adapter to the **Power input** on the back of the router and then plug the other end of power adapter into a wall outlet or power strip. Then turn on the router and boot up your PC and any LAN devices, such as hubs or switches, and any computers connected to them.

Configuring the Router

To use your web browser to access the web pages used to set up the router, your computer must be configured to **"Obtain an IP address automatically"**, that is, you must change the IP network settings of your computer so that it is a **DHCP client**. If you are using Windows XP and do not know how to change your network settings, skip ahead to **Appendix A** and read the instructions provided.

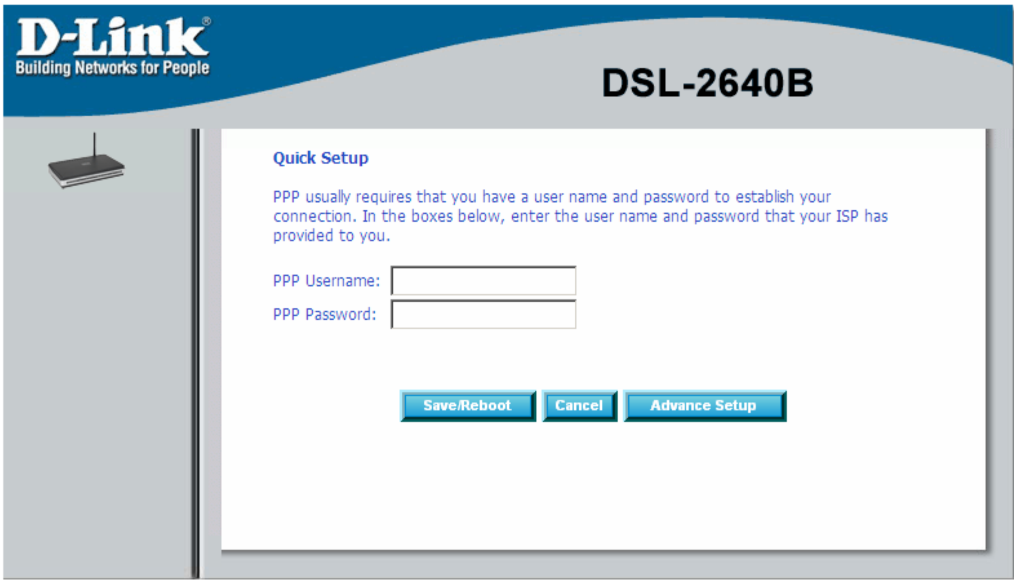


Open your web browser and enter the URL http://192.168.1.1 in the address bar and press Enter.

Enter "admin" in the User Name field and "tot" in the Password field.

Click OK

After you log into the router, the first screen will be the Quick Setup screen which requires you to enter the PPP Username and Password. Click on **Save/Reboot** or click on **Advance Setup** to go directly to the main user interface.



Quick Setup

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Home

The home section provides configurations for general use, including a Quick Setup Wizard with steps to quickly set up your router for Internet connection. Also included in this section are LAN / WAN setup and DNS configuration. The below sections explains the setup for each.

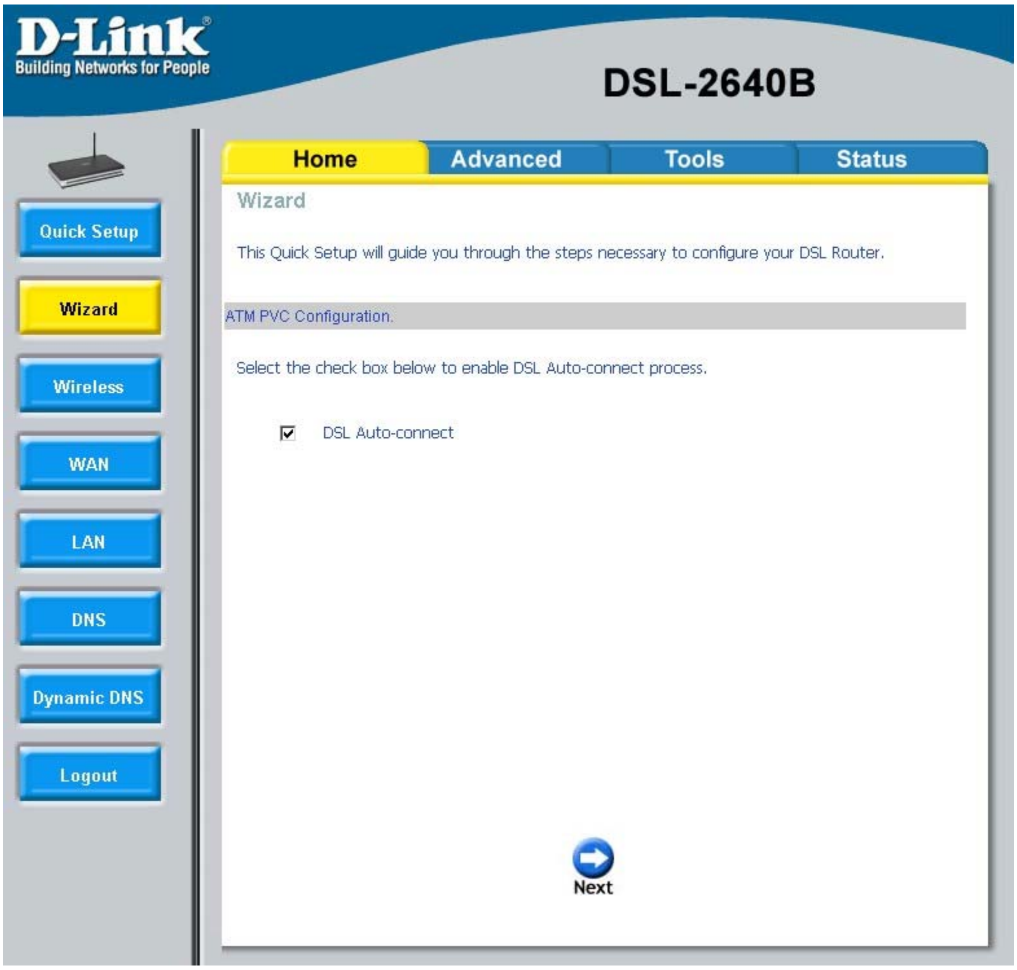
Wizard

This section will explain how to quickly configure the router if your only intention is to access the Internet.

ATM PVC Configuration

To enable the auto-connect process, click on the box labeled DSL Auto-connect, a process that will automatically detect the first usable PVC and automatically detect PPPoE and PPPoA. To continue, click on the **Next** button.

Skip ahead to page 13 if you select *DSL Auto-connect*.



Wizard

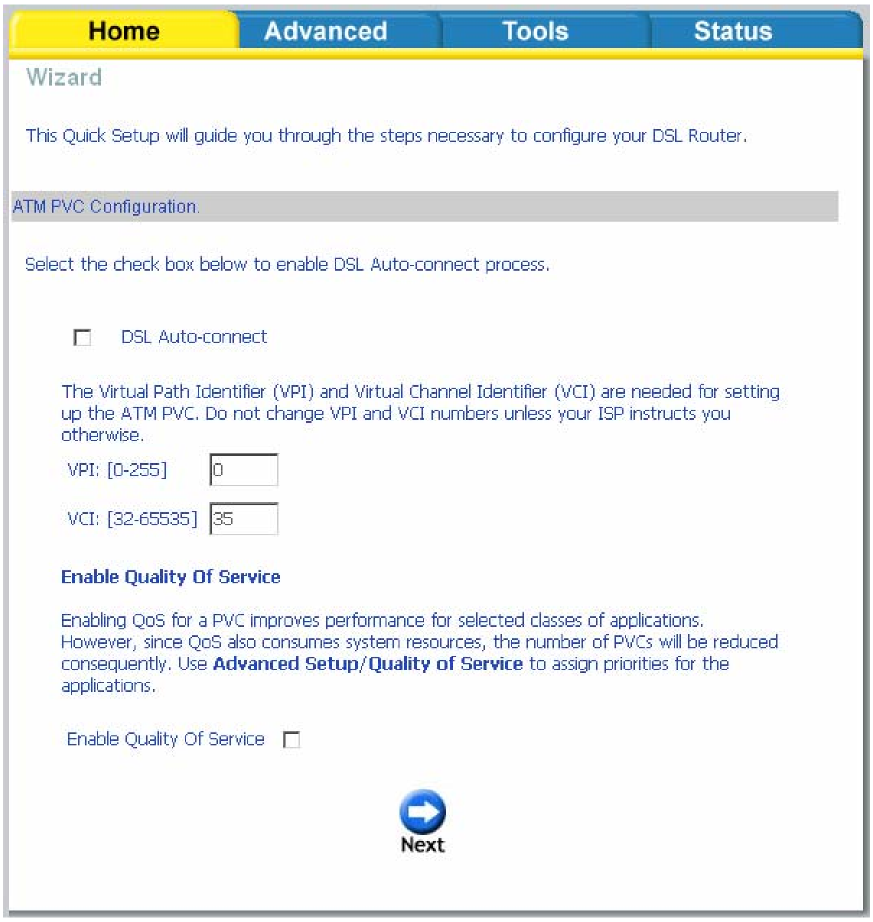
This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration.

Select the check box below to enable DSL Auto-connect process.

☑ DSL Auto-connect

If you uncheck the *DSL Auto-connect* box, the resulting screen is seen below. Enter the VPI / VCI as indicated by your ISP. Also shown will be the Quality of Service.



Wizard

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration.

Select the check box below to enable DSL Auto-connect process.

□ DSL Auto-connect

The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.

VPI: [0-255] 0

VCI: [32-65535] 35

Enable Quality Of Service

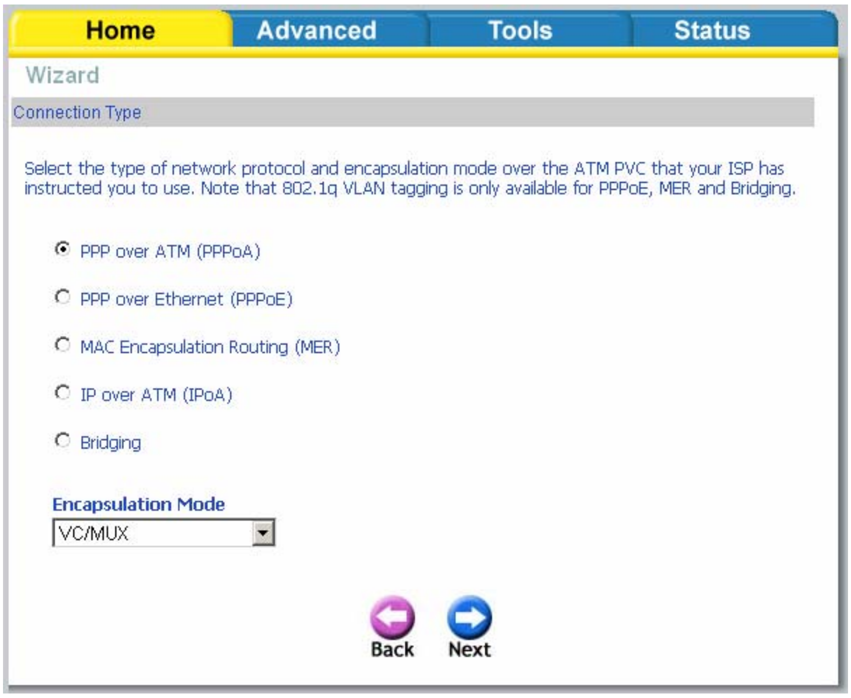
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service □

Connection Type

Following is the Connection Type screen where you select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use.

The following is a PPPoA example. Click on **Next** to continue.



Connection Type

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.

● PPP over ATM (PPPoA)

○ PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

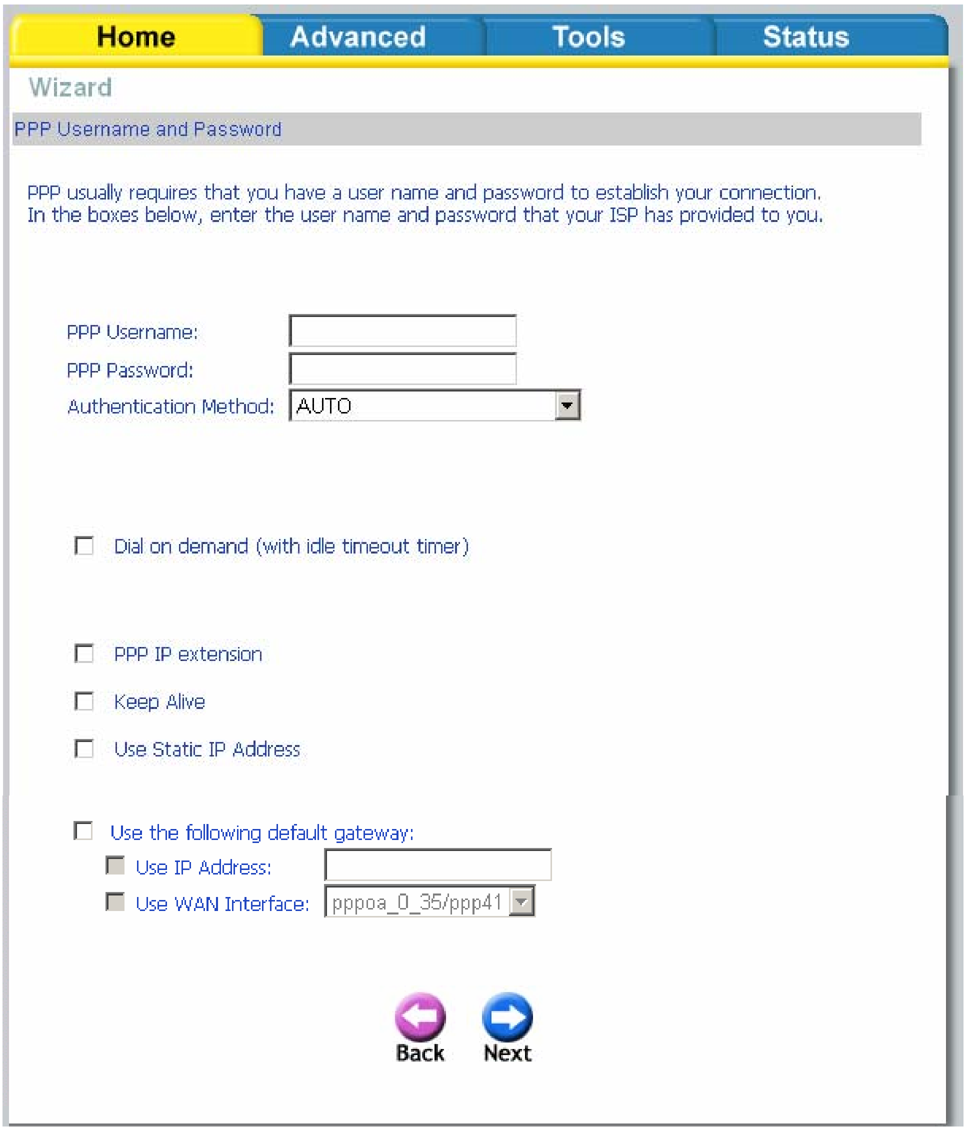
○ IP over ATM (IPoA)

○ Bridging

Encapsulation Mode: VC/MUX

PPP Username and Password

Now, enter the PPP username and password as given by your ISP. Then decide if you will be using any features such as D*ial on demand*, *PPP IP extension*, *Keep Alive* and then click on **Next**.



Wizard

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection.
In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Authentication Method: AUTO

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Keep Alive

□ Use Static IP Address

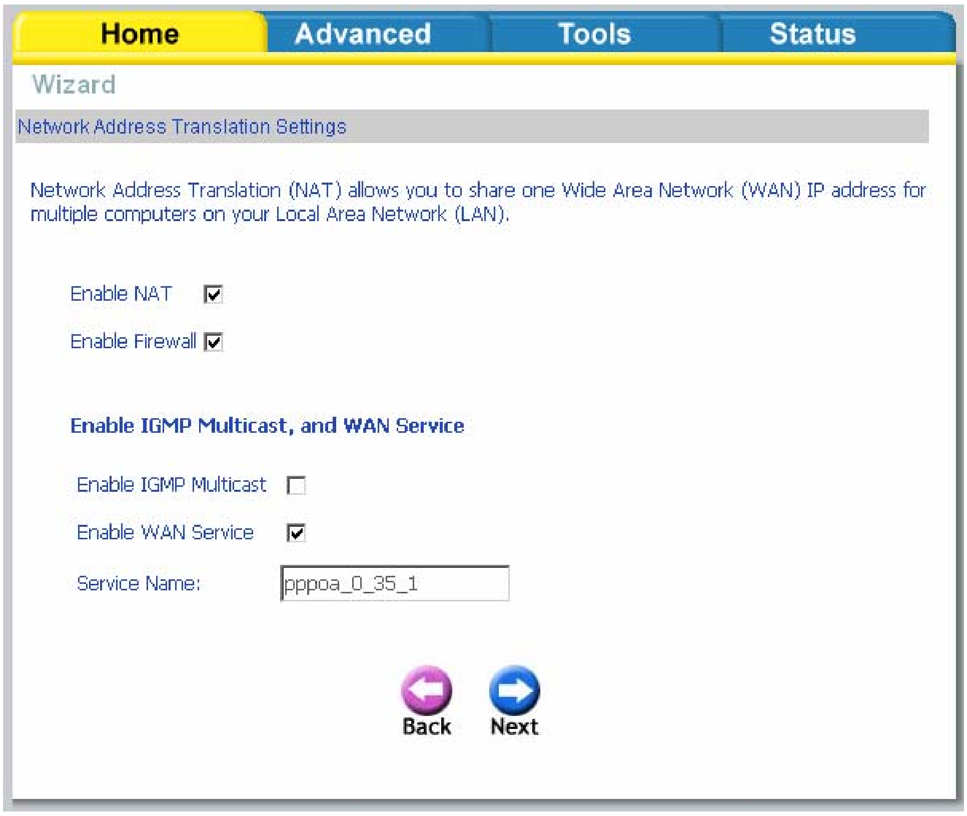
□ Use the following default gateway:

□ Use IP Address:

□ Use WAN Interface: pppoa_0_35/ppp41

Network Address Translation Settings

The next step is to configure the Network Address Translation (NAT) settings. For the example, NAT will be enabled. The remaining fields are left as default and then click on **Next** to continue.



Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT ☑

Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

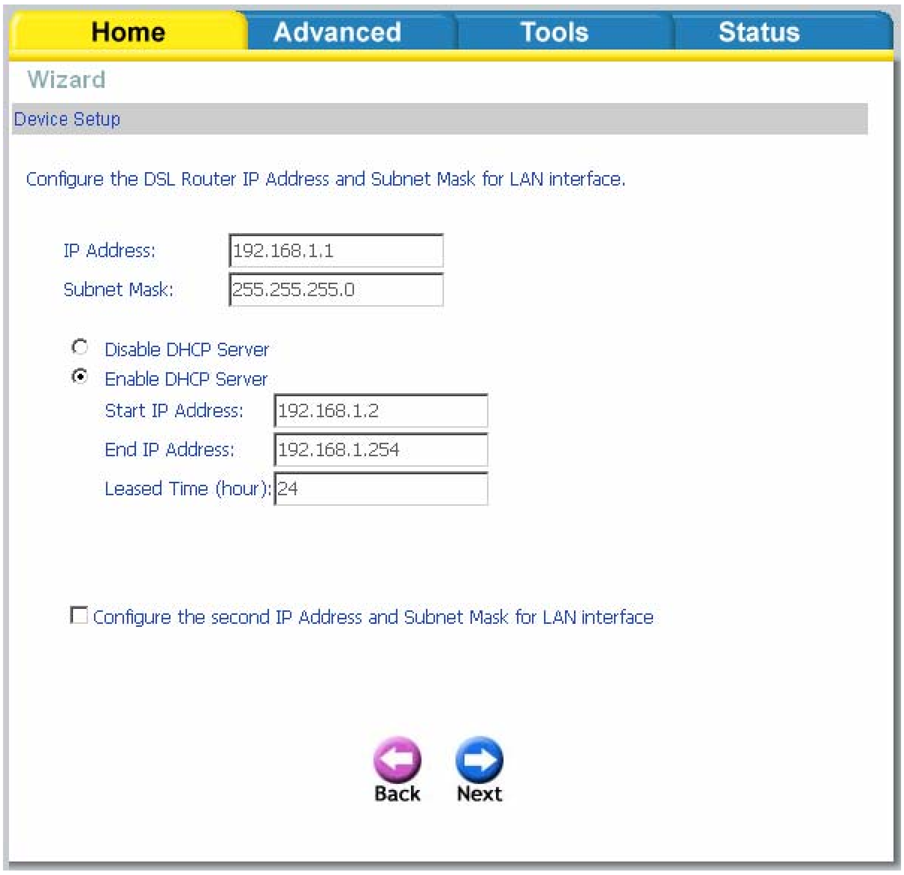
Enable IGMP Multicast □

Enable WAN Service ☑

Service Name: pppoa_0_35_1

Device Setup

You can configure the DSL Router IP address and Subnet Mask for the LAN interface to correspond to your LAN’s IP Subnet. If you want the DHCP server to automatically assign IP addresses, then enable the DHCP server and enter the range of IP addresses that the DHCP server can assign to your computers. Disable the DHCP server if you would like to manually assign IP addresses. Click on **Next** to continue.



Wizard

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

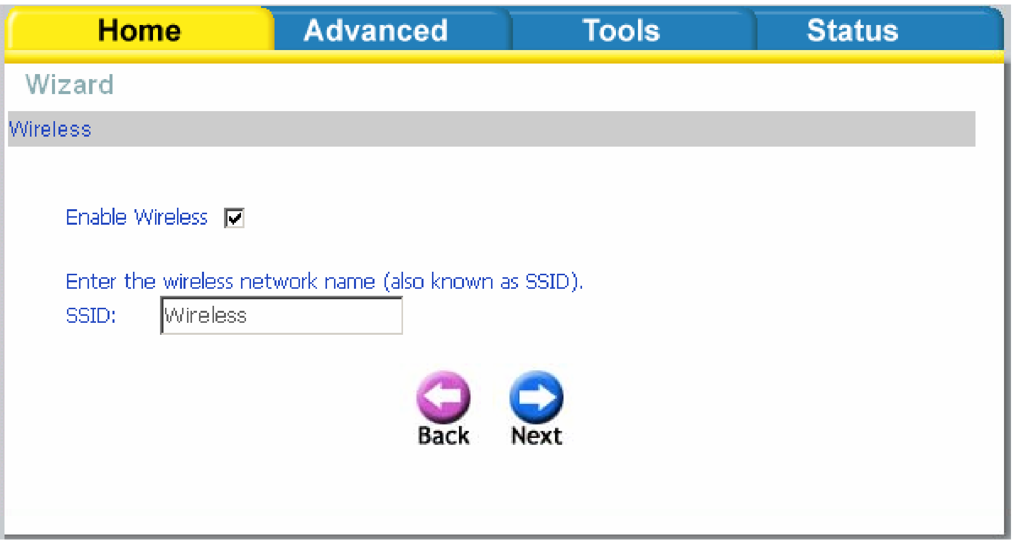
End IP Address: 192.168.1.254

Leased Time (hour): 24

□ Configure the second IP Address and Subnet Mask for LAN interface

Wireless

The router's wireless function can be enabled on the following screen. If the function is enabled, then continue by entering the SSID, the wireless network name. Click on **Next** to continue.



Wizard

Wireless

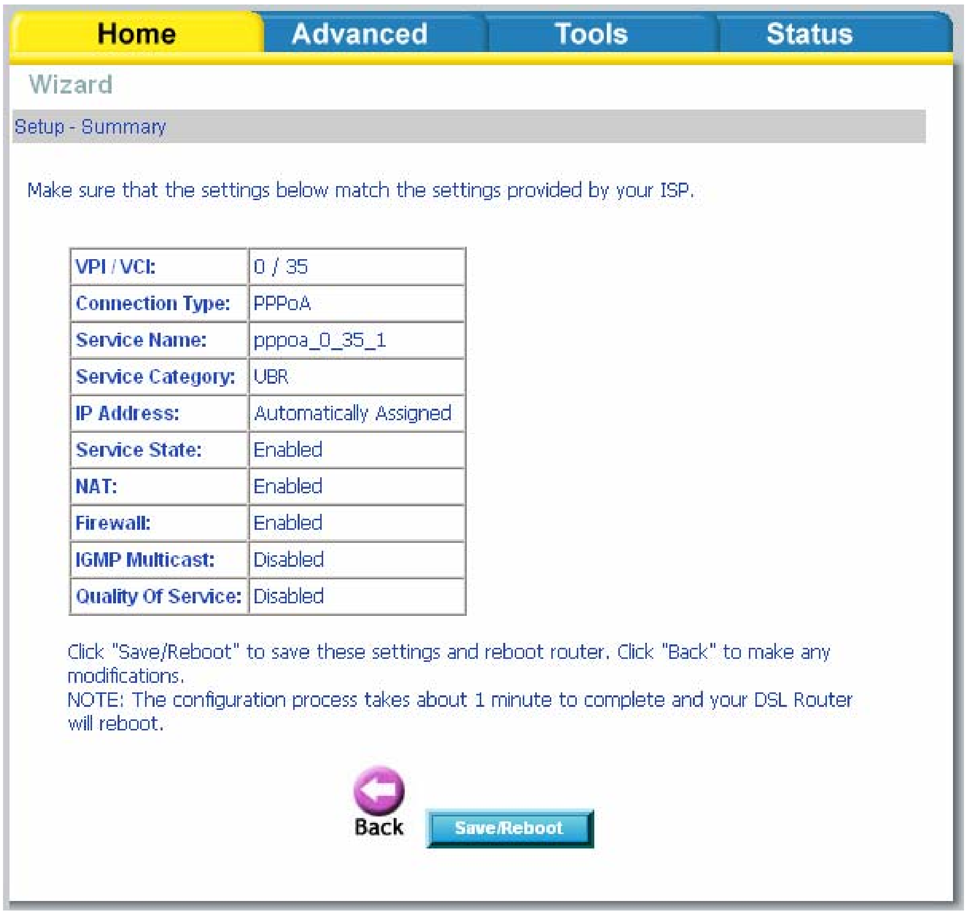
Enable Wireless ☑

Enter the wireless network name (also known as SSID).

SSID: Wireless

Setup - Summary

After all of the configurations are done, the *WAN Setup Summary* screen displays all WAN settings that you have made. Check that the settings are correct before clicking on the **Save / Reboot** button. Clicking on **Save / Reboot** will save your settings and restart your router.



Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

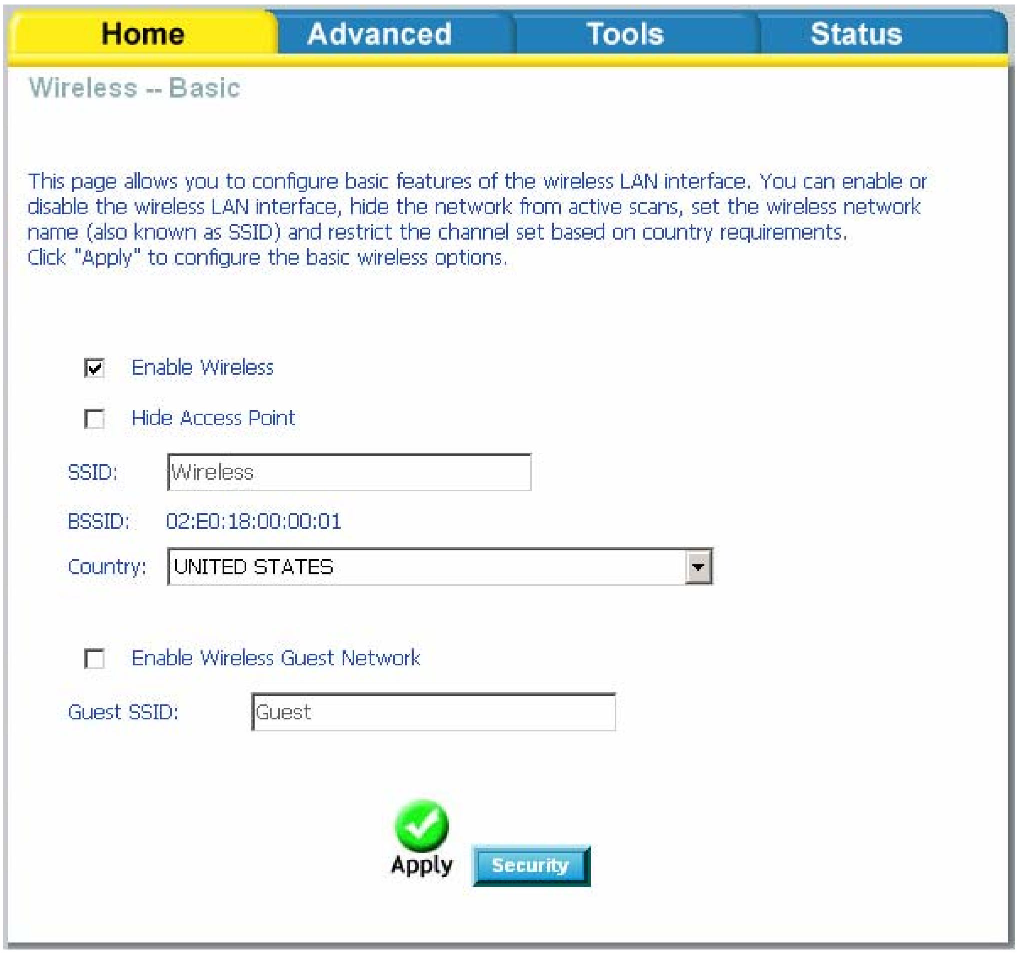
VPI / VCI:	0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

Wireless

Wireless -- Basic

The below **Wireless – Basic** screen lets you enable or disable wireless. The default setting for wireless is enabled. You can also hide the access point so others cannot see your ID on the network. Click on **Apply** to save your configurations before clicking on **Security** to continue to the Security configurations.



Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

SSID: Wireless

BSSID: 02:E0:18:00:00:01

Country: UNITED STATES

□ Enable Wireless Guest Network

Guest SSID: Guest

Wireless - Security

The next screen is the **Wireless - Security** screen which allows you to select the network authentication method and to enable or disable WEP encryption. Note that depending on the network authentication that is selected, the screen will change accordingly so additional fields can be configured for the specific authentication method.

Network authentication methods include the following—

- **Open**—anyone can access the network. The default is a disabled WEP encryption setting.

- **Shared**—WEP encryption is enabled and encryption key strength of 64-bit or 128-bit needs to be selected. Click on **Set Encryption Keys** to manually set the network encryption keys. Up to 4 different keys can be set and you can come back to select which one to use at anytime.

- **802.1X—**requires mutual authentication between a client station and the router by including a RADIUS-based authentication server. Information about the RADIUS server such as its IP address, port and key must be entered. WEP encryption is also enabled and the encryption strength must also be selected.

- **WPA—(Wi-Fi Protected Access)**— usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP uses128-bit dynamic session keys (per user, per session, and per packet keys).

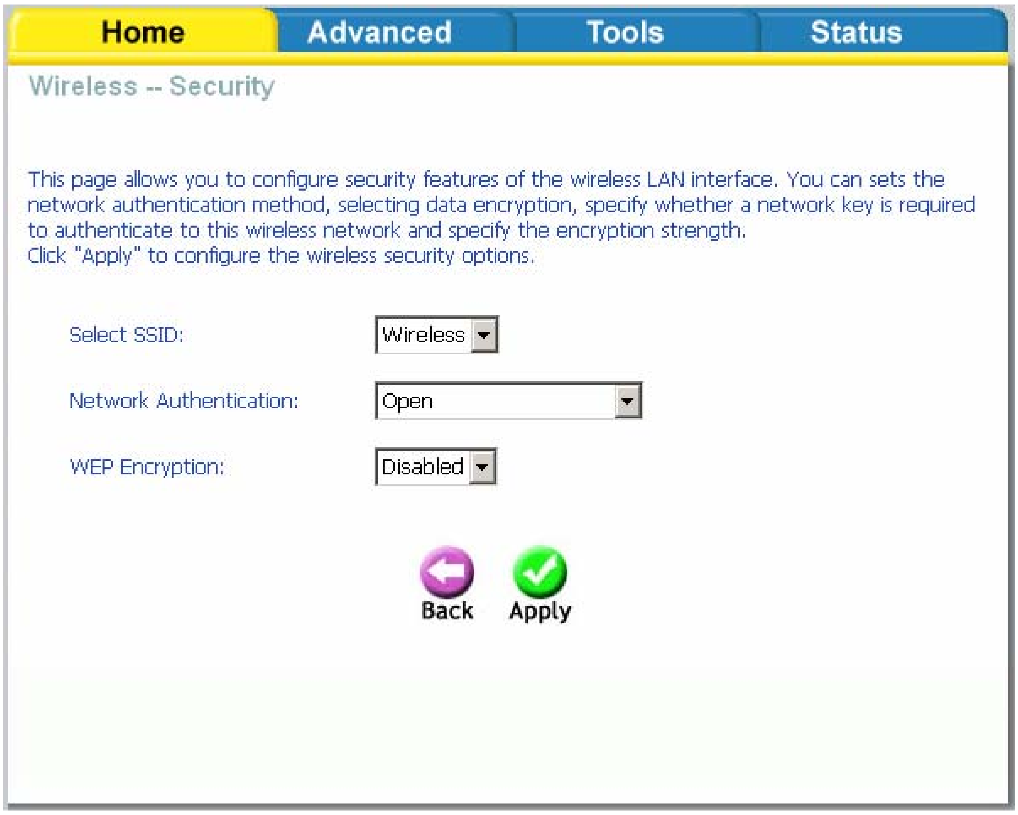
- **WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key)**—WPA for home and SOHO environments also using the same strong TKIP encryption, per-packet key construction, and key management that WPA provides in the enterprise environment. The main difference is that the password is entered manually. A group re-key interval time is also required.

- **WPA2 (Wi-Fi Protected Access 2)**—second generation of WPA which uses AES (Advanced Encryption Standard) instead of TKIP as its encryption method. Network re-auth interval is the time in which another key needs to be dynamically issued.

- **WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key)**—suitable for home and SOHO environments, it also uses AES encryption and requires you to enter a password and an re-key interval time.

- **Mixed WPA2 / WPA**—during transitional times for upgrades in the enterprise environment, this mixed authentication method allows “upgraded” and users not yet “upgraded” to access the network via the router. RADIUS server information must be entered for WPA and a as well as a group re-key interval time. Both TKIP and AES are used.

- **Mixed WPA2 / WPA-PSK**—useful during transitional times for upgrades in the home or SOHO environment, a pre-shared key must be entered along with the group re-key interval time. Both TKIP and AES are also used.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

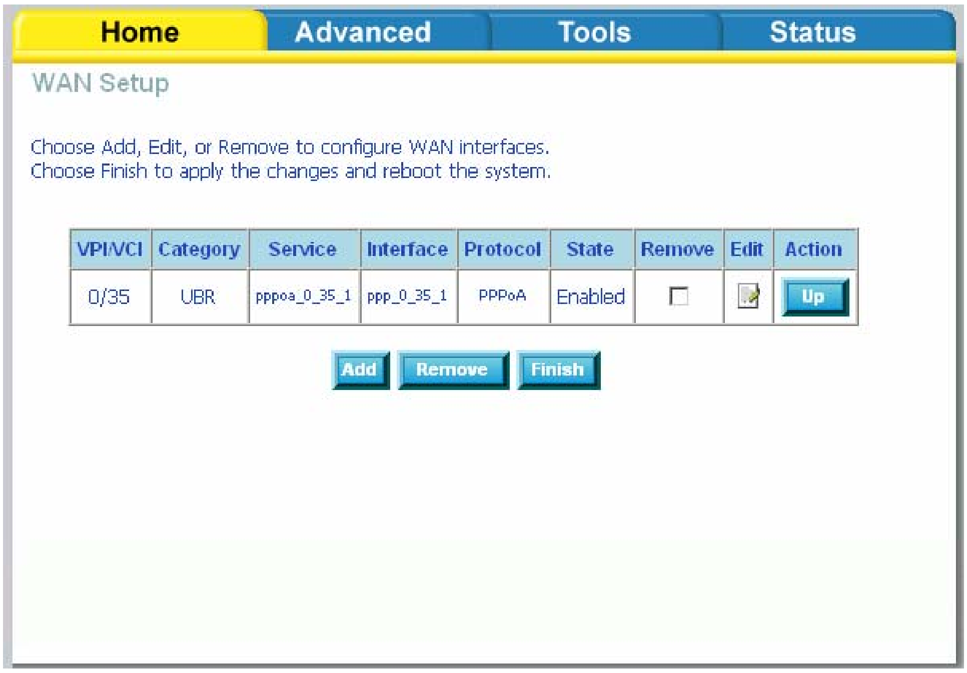
Select SSID: Wireless

Network Authentication: Open

WEP Encryption: Disabled

WAN

Configure the WAN settings as provided by your ISP.



WAN Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Finish to apply the changes and reboot the system.

VPI/VCI	Category	Service	Interface	Protocol	State	Remove	Edit	Action
0/35	UBR	pppoa_0_35_1	ppp_0_35_1	PPPoA	Enabled	□		Up

Click on the **Add** button if you want to add a new connection for the WAN interface and to proceed to the ATM PVC Configuration screen as seen below. The ATM PVC Configuration screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

Find out the following values from your ISP before you change them.

- VPI: Virtual Path Identifier. The valid range is 0 to 255.
- VCI: Virtual Channel Identifier. The valid range is 32 to 65535.
- Service Category: Five classes of traffic are listed—

    - UBR Without PCR *(Unspecified Bit Rate without Peak Cell Rate)*—UBR service is suitable for applications that can tolerate variable delays and some cell losses. Applications suitable for UBR service include text/data/image transfer, messaging, distribution, and retrieval and also for remote terminal applications such as telecommuting.

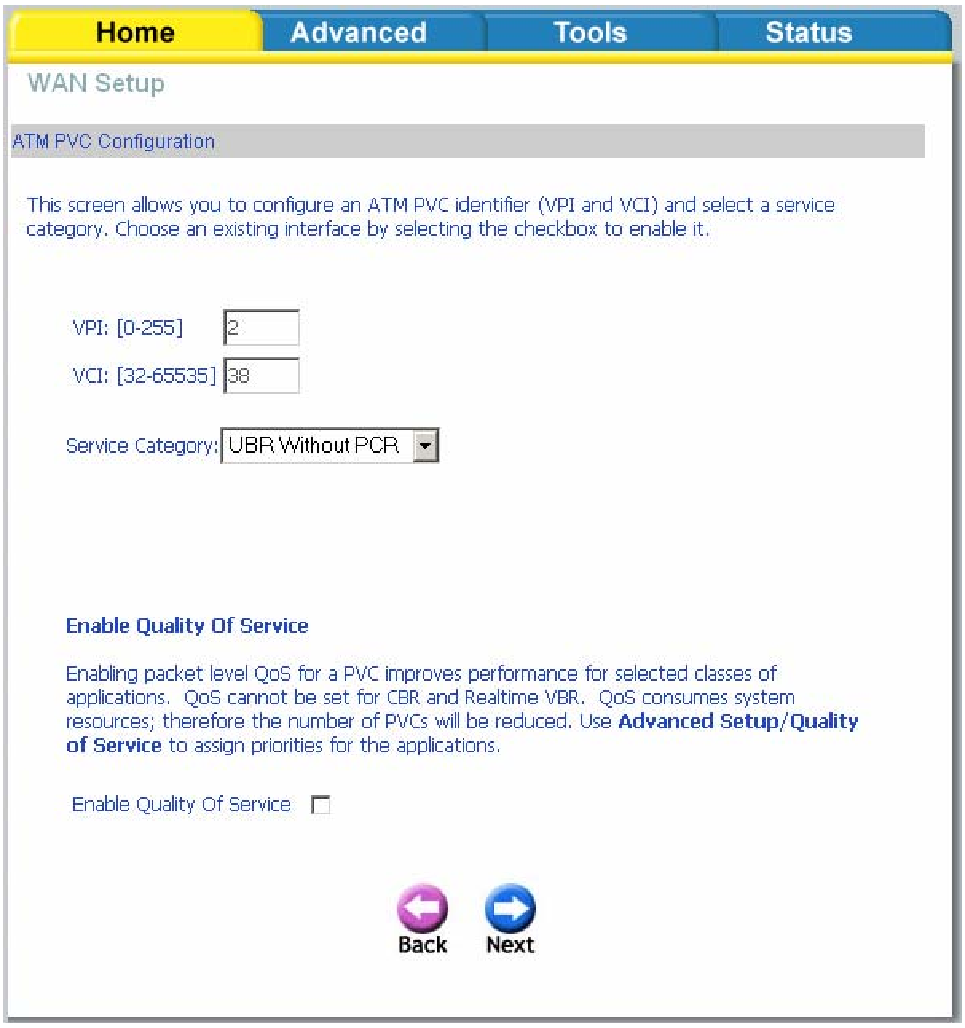
    - UBR With PCR *(Unspecified Bit Rate with Peak Cell Rate)*--

    - CBR *(Constant Bit Rate)*—used by applications that require a fixed data rate that is continuously available during the connection time. It is commonly used for uncompressed audio and video information such as videoconferencing, interactive audio (telephony), audio / video distribution (e.g. television, distance learning, and pay-per-view), and audio / video retrieval (e.g. video-on-demand and audio library).

    - Non Realtime VBR *(Non-Real-time Variable Bit Rate)*—can be used for data transfers that have critical response-time requirements such as airline reservations, banking transactions, and process monitoring.

    - Realtime VBR *(Real-time Variable Bit Rate)*—used by time-sensitive applications such as real-time video. Rt-VBR service allows the network more flexibility than CBR.

- Quality of Service: Can be enabled only for *UBR without PCR*, *UBR with PCR*, and *Non Realtime VPR*.



WAN Setup

ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255] 2

VCI: [32-65535] 38

Service Category: UBR Without PCR

Enable Quality Of Service

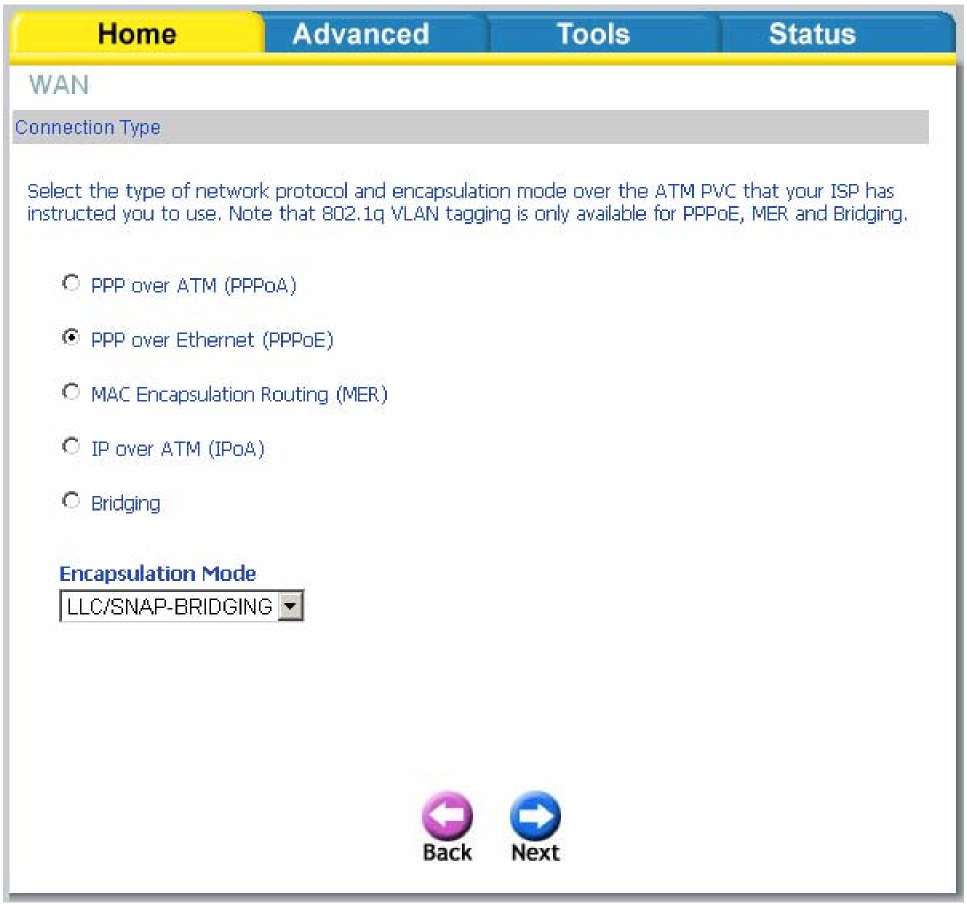
Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service □

The following screen shows the below types of network protocols and encapsulation modes—

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)
- IP over ATM (IpoA)
- Bridging

If you will be using VLAN tagging, then click on the **Enable 802.1q** checkbox and then enter the VLAN ID number. *Note that the 802.1q function is only available if you select PPPoE, MER, or Bridging.* When finished with your selections, click on **Next** to continue.



WAN

Connection Type

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Note that 802.1q VLAN tagging is only available for PPPoE, MER and Bridging.

○ PPP over ATM (PPPoA)

● PPP over Ethernet (PPPoE)

○ MAC Encapsulation Routing (MER)

○ IP over ATM (IPoA)

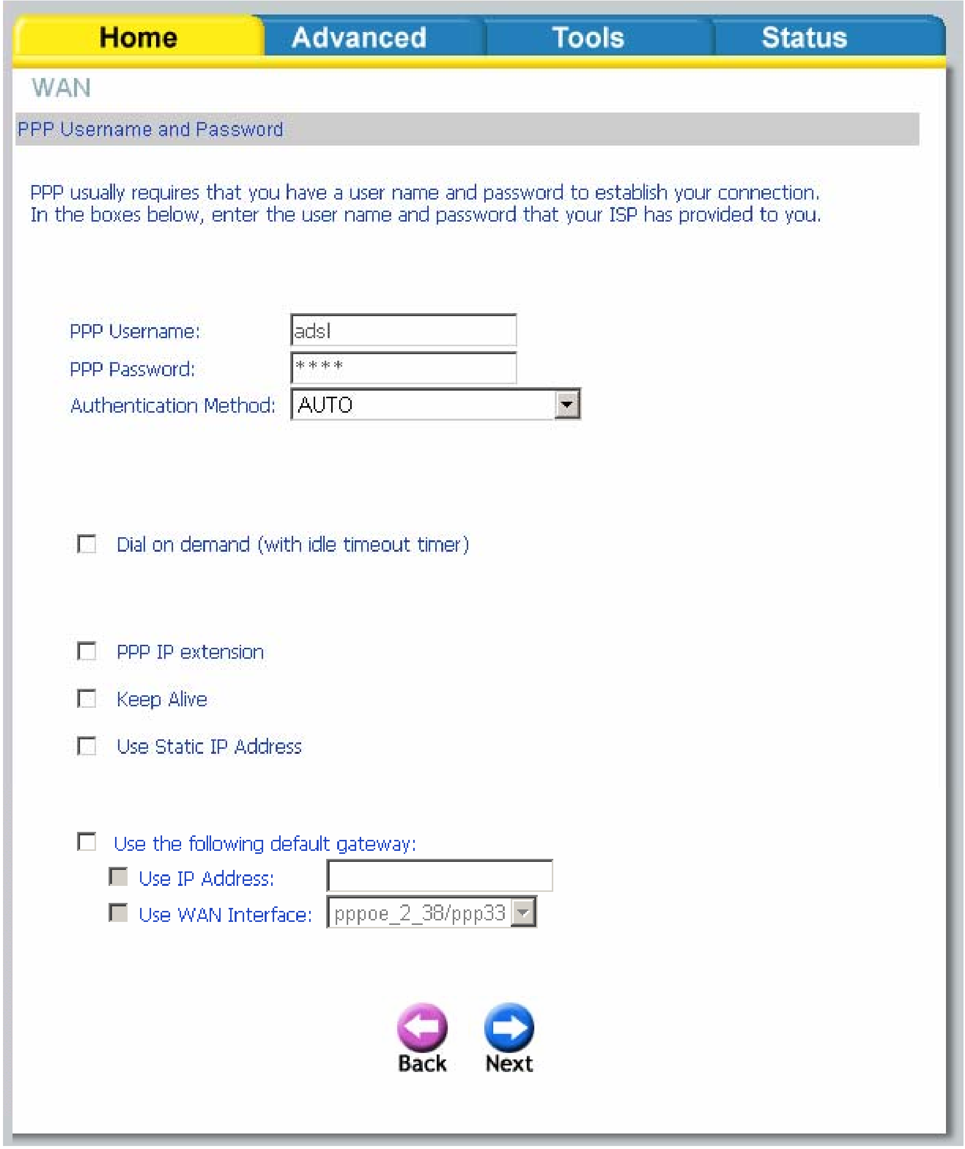
○ Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

The following screen allows you to enter PPP username and password as well as make any selections regarding your connection.

- Dial on demand: Allows you to manually connect to the Internet so you are not permanently connected. Idle timeout timer is included.
- PPP IP extension: Used by some ISP's. Check with your ISP to see if it is required.
- Keep alive: Keeps you connected to your ISP even when no activity is present for a certain period of time.
- Use static IP address: Select if you want to use a non-DHCP issued IP address to connect to the Internet. If selected, you will be asked to enter the static IP address.



WAN

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection.
In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:	adsl
PPP Password:	****
Authentication Method:	AUTO

□ Dial on demand (with idle timeout timer)

□ PPP IP extension

□ Keep Alive

□ Use Static IP Address

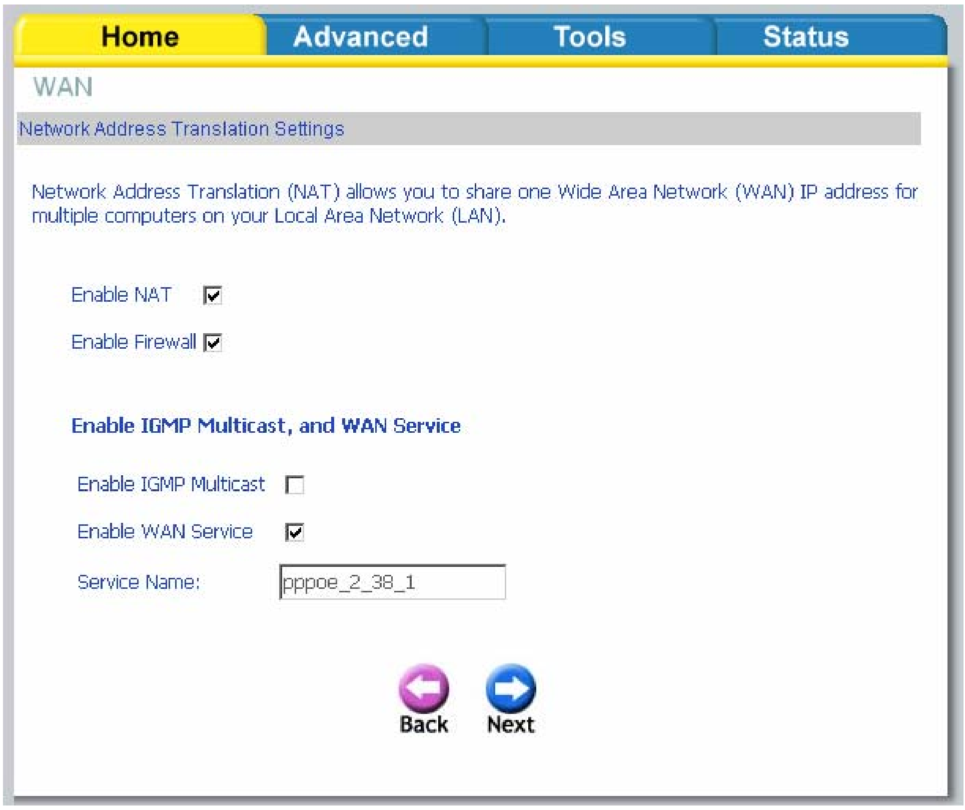
□ Use the following default gateway:

□ Use IP Address:

□ Use WAN Interface: pppoe_2_38/ppp33

When finished, click on **Next** to proceed to the NAT Settings screen.

- Enable NAT: Select enable if you wish to share one WAN IP address for multiple computers on your LAN.
- Enable Firewall: Select if you wish to enable the router's firewall for security.
- Enable IGMP Multicast: Select enable if you wish to be able to provide multicasts, mostly used in video streaming.
- Enable WAN Service: Select if you wish to use WAN service and then set the service name.



WAN

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT ☑

Enable Firewall ☑

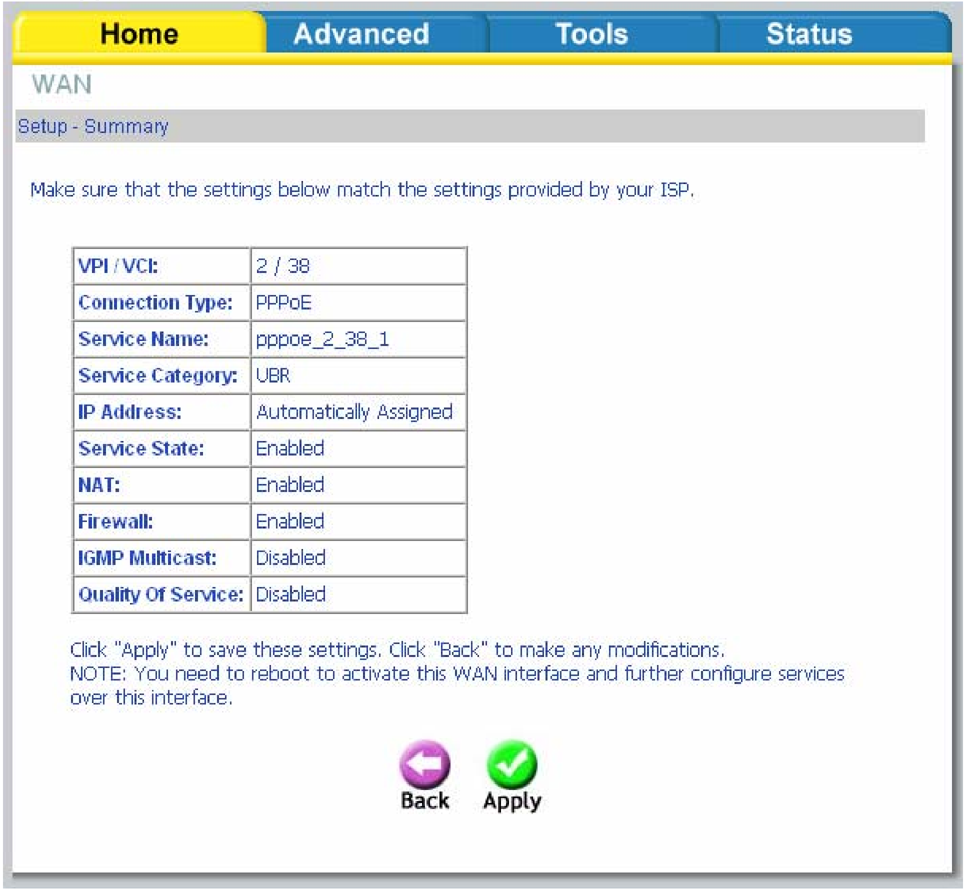
Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast □

Enable WAN Service ☑

Service Name: pppoe_2_38_1

Click **Next** when finished with your configurations and the below screen will follow displaying the WAN settings that you made. When satisfied with the settings click on the **Apply** button.



WAN

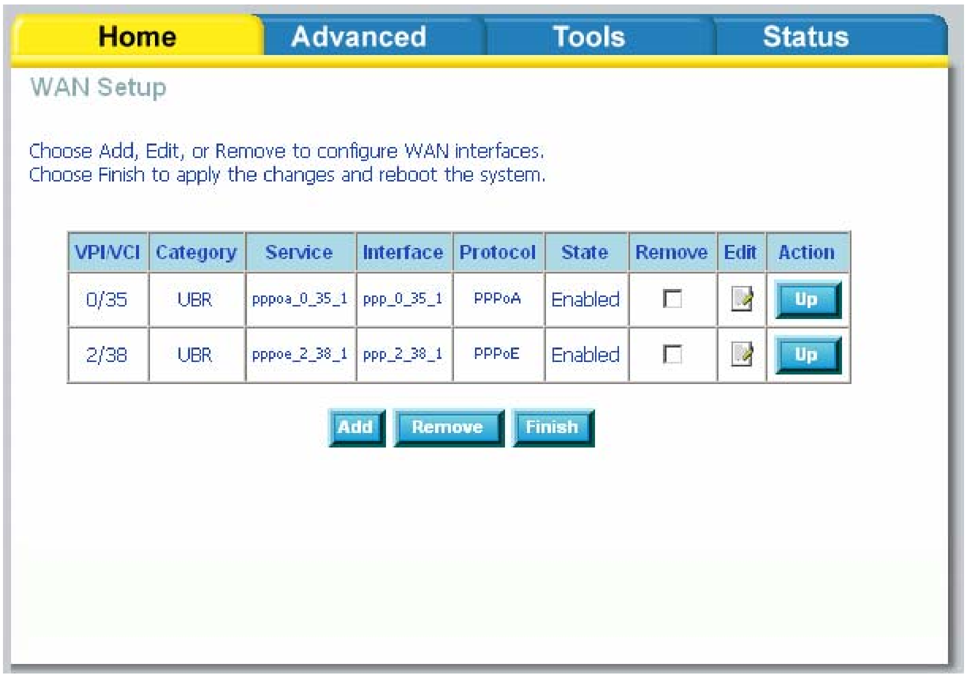
Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	2 / 38
Connection Type:	PPPoE
Service Name:	pppoe_2_38_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

After you apply the configurations, it will return to the WAN Setup screen showing the new configurations. Select the **Finish** button to save the changes and reboot the router.

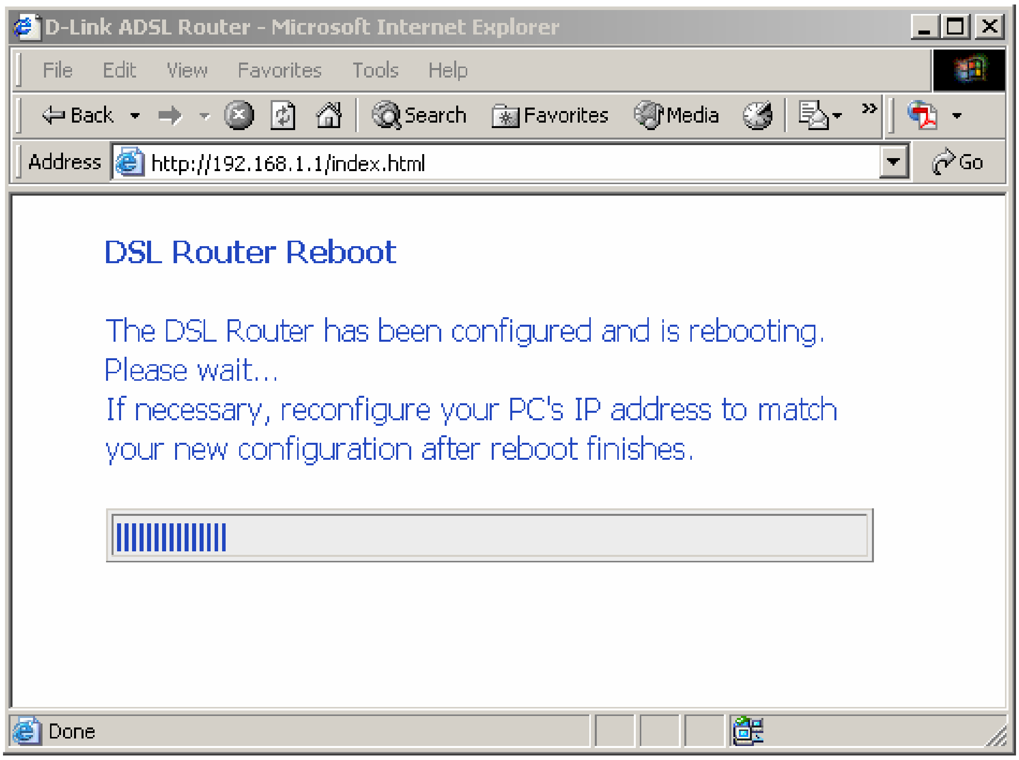


WAN Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Finish to apply the changes and reboot the system.

VPI/VCI	Category	Service	Interface	Protocol	State	Remove	Edit	Action
0/35	UBR	pppoa_0_35_1	ppp_0_35_1	PPPoA	Enabled	□	✎	Up
2/38	UBR	pppoe_2_38_1	ppp_2_38_1	PPPoE	Enabled	□	✎	Up

Below is the DSL Router Reboot screen that will appear during the rebooting process.



Address: http://192.168.1.1/index.html

DSL Router Reboot

The DSL Router has been configured and is rebooting.
Please wait...
If necessary, reconfigure your PC's IP address to match your new configuration after reboot finishes.

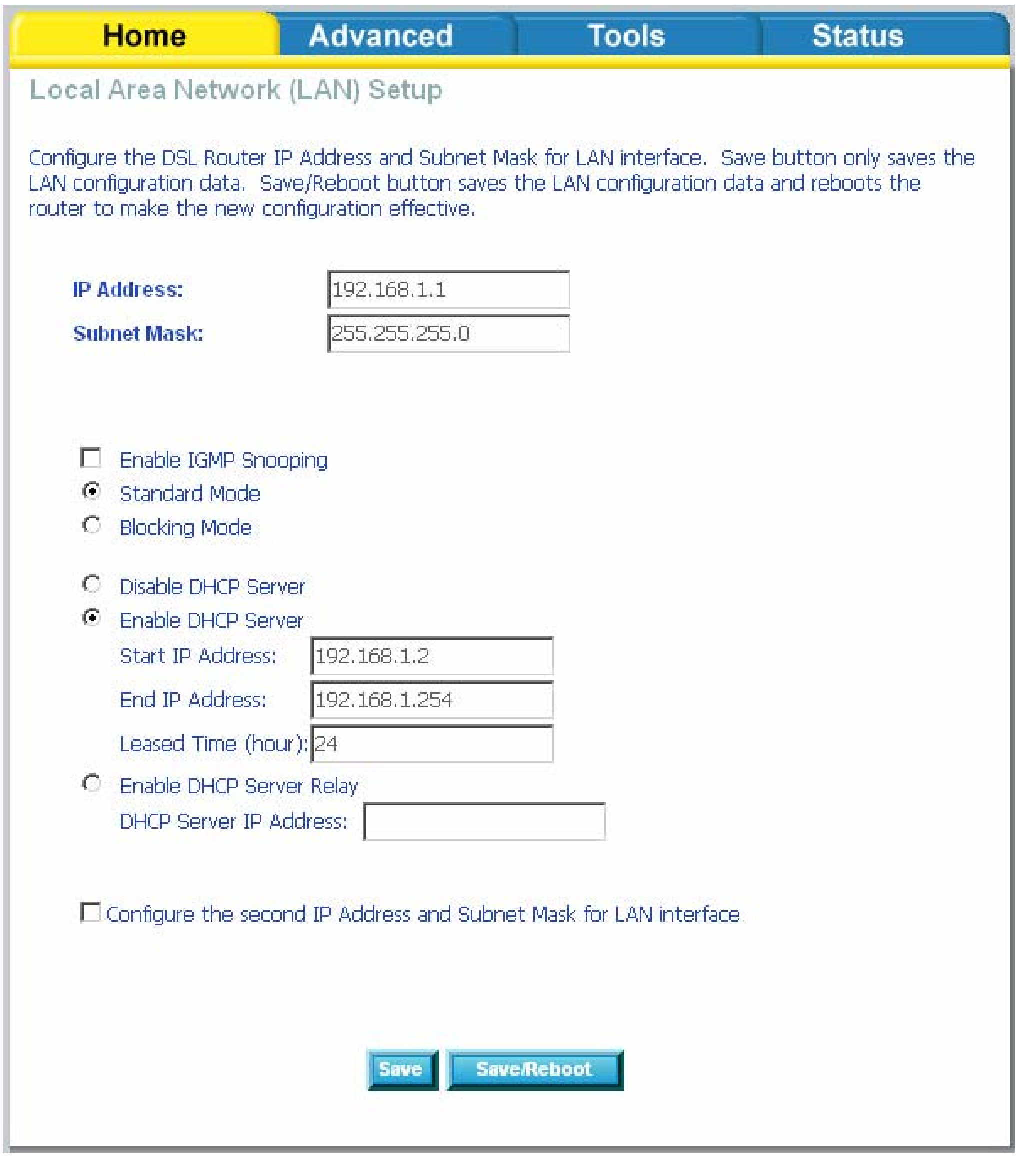
Done

LAN

You can configure the DSL Router IP address and Subnet Mask for the LAN interface.

An available option if you will be multicasting is IGMP snooping, for which you can also select standard or blocking mode.

If you want the DHCP server to automatically assign IP addresses, enable DHCP server and enter the range of IP addresses that DHCP server can assign. Disable DHCP server if you would like to manually assign IP addresses.



Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

☐ Enable IGMP Snooping

● Standard Mode

○ Blocking Mode

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

○ Enable DHCP Server Relay

DHCP Server IP Address:

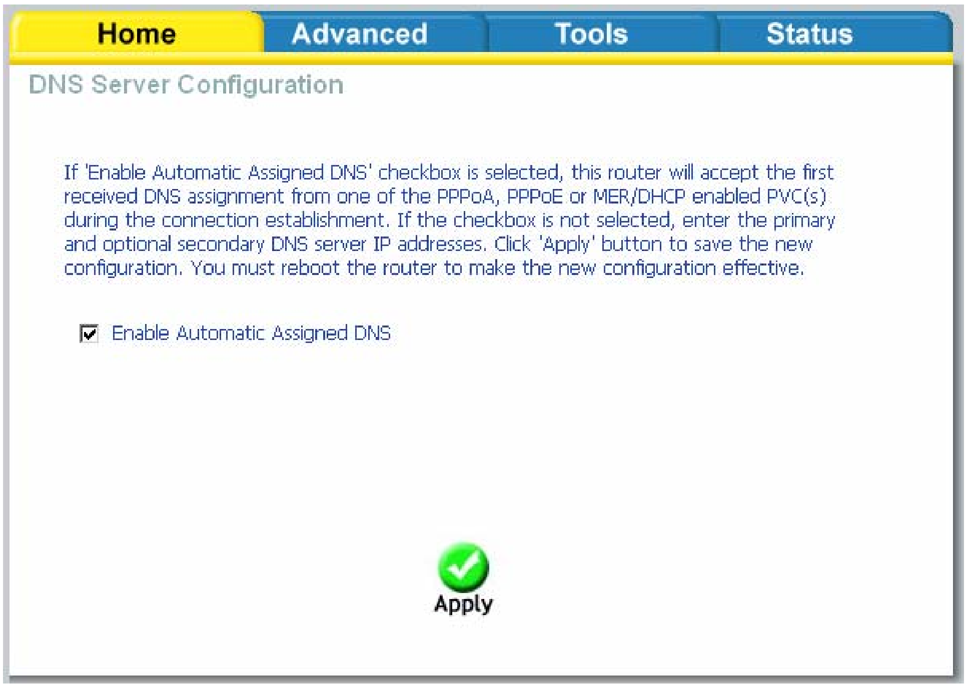
☐ Configure the second IP Address and Subnet Mask for LAN interface

The **Save** button only saves the LAN configuration data, but does not apply the configurations. Select the **Save/Reboot** button to save the LAN configuration data and reboot the router and apply the new configurations.

DNS

DNS Server Configuration

Use the DNS Server screen to request automatic assignment of a DNS or to specify a primary and secondary DNS.

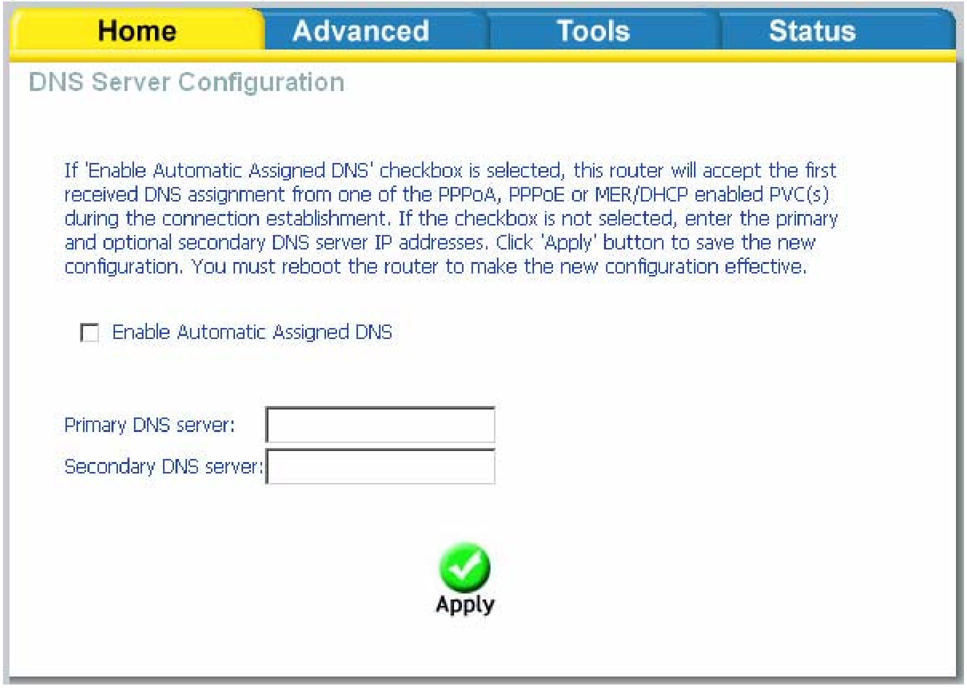


DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Apply' button to save the new configuration. You must reboot the router to make the new configuration effective.

☑ Enable Automatic Assigned DNS

If you uncheck the *Enable Automatic Assigned DNS* checkbox, two additional fields—primary and secondary DNS server—will appear. Enter the information and click on **Apply** to save the configuration.



DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Apply' button to save the new configuration. You must reboot the router to make the new configuration effective.

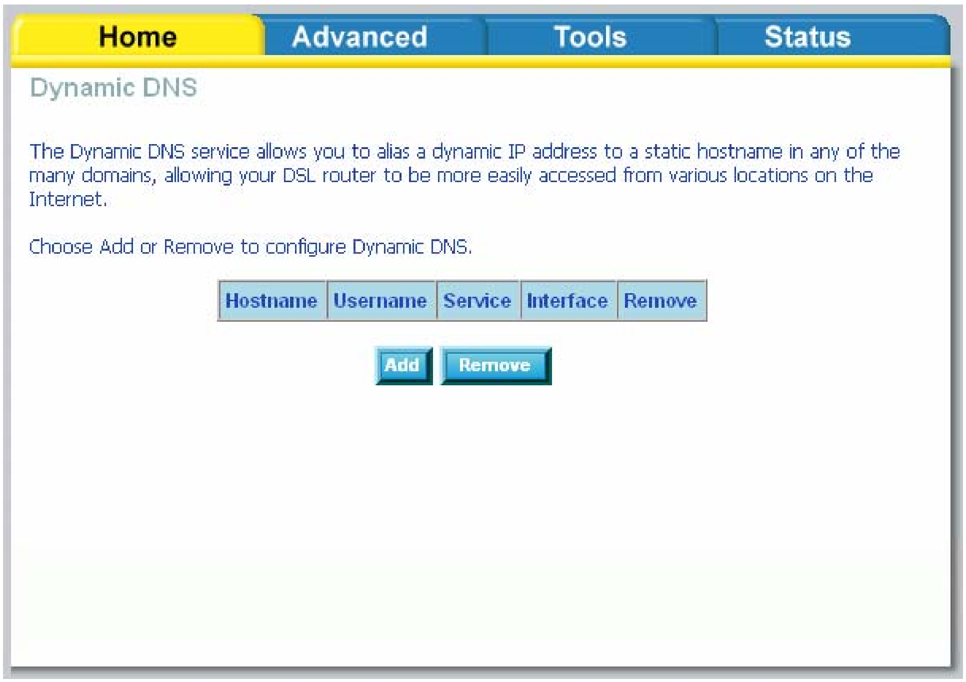
☐ Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

Dynamic DNS

Dynamic DNS is a service for allowing an Internet domain name to be assigned to a varying IP address. This makes it possible for other sites on the Internet to establish connections to you without needing to track the IP address themselves. Click on **Add** to set up a dynamic DNS configuration.



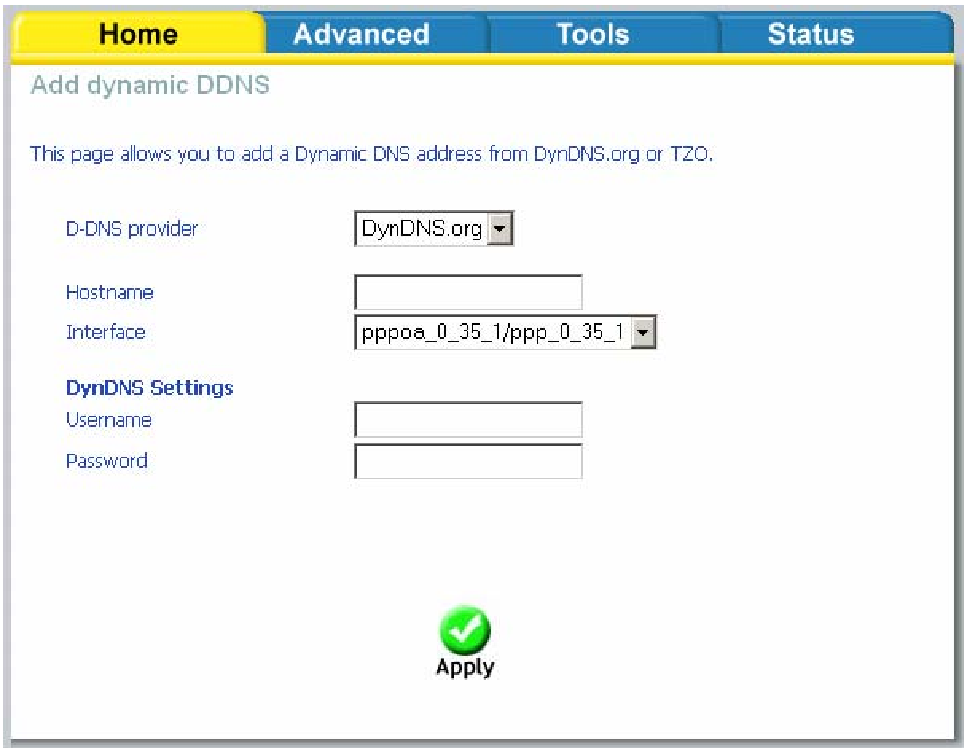
Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

This screen allows you to add a dynamic DNS address from DynDNS.org or TZO. First select the D-DNS provider—*DynDNS.org* or *TZO*—from which you have obtained a dynamic DNS address. Enter the hostname and the interface that you are using. Also enter the username and password assigned by the DNS service. Click on **Apply** to save these configurations.



Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

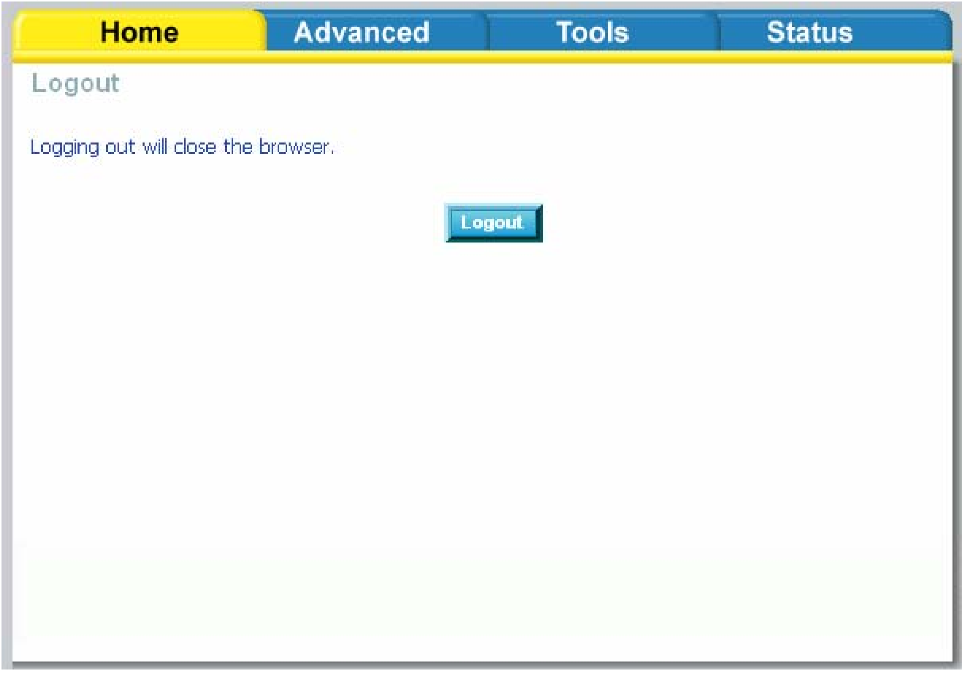
D-DNS provider	DynDNS.org
Hostname	
Interface	pppoa_0_35_1/ppp_0_35_1

DynDNS Settings

Username	
Password	

Logout

To log out of the router’s user interface at any time during the setup, click on the **Logout** button. A confirmation screen will appear confirming that you really want to log out.



Logout

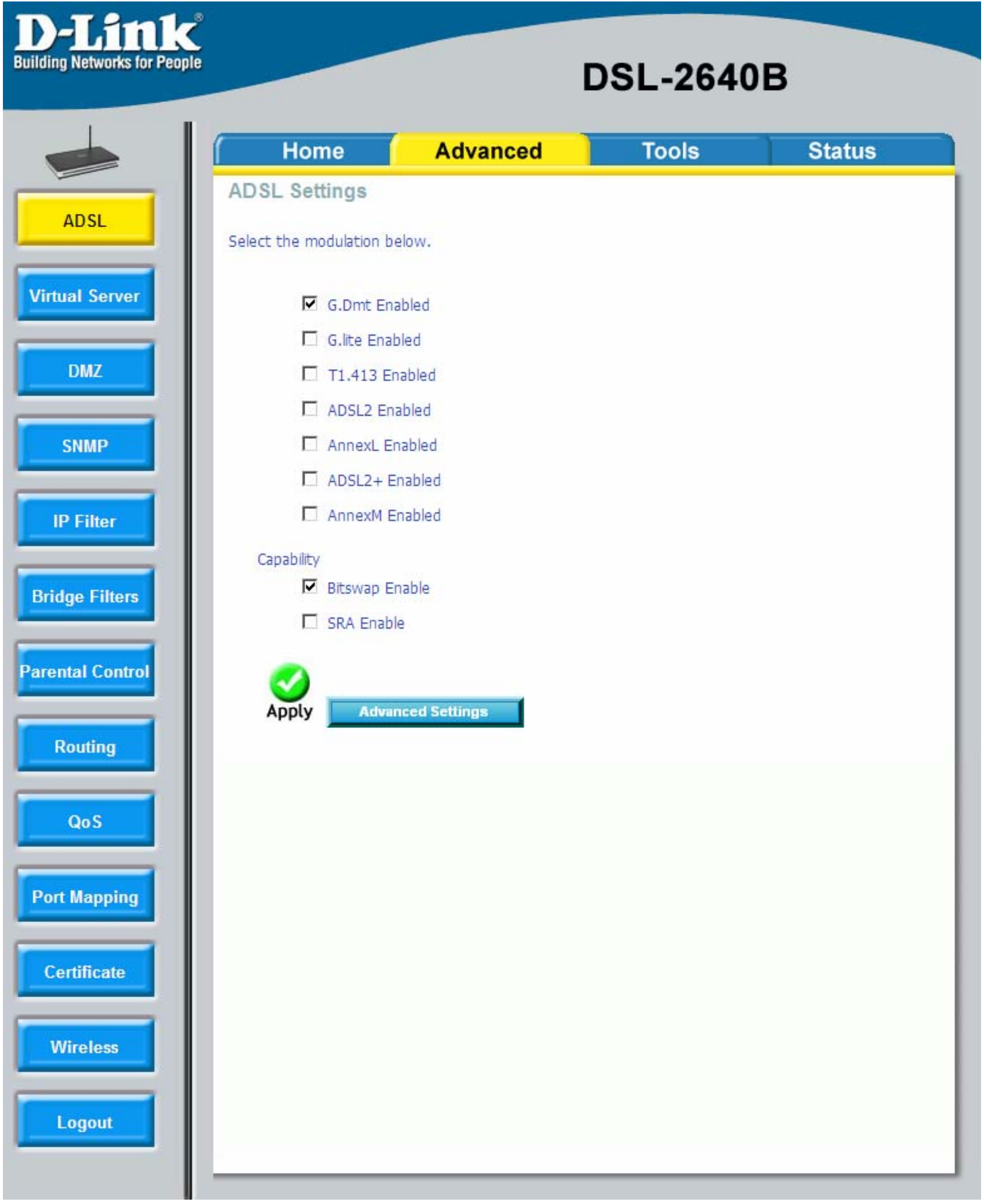
Logging out will close the browser.

Advanced Setup

This section of the setup is an advanced version of the quick setup. If you want to make specific configurations to your router such as creating a virtual server, DMZ, RIP, Quality of Service (QoS), etc., consider going through this advanced setup for a more comprehensive configuration.

ADSL

The ADSL settings page contains a modulation and capability section to be specified by your ISP. Consult your ISP to select the correct settings for each. Then click on **Apply** if you are finished or click on **Advanced Settings** if you want to configure more advanced settings.



ADSL Settings

Select the modulation below.

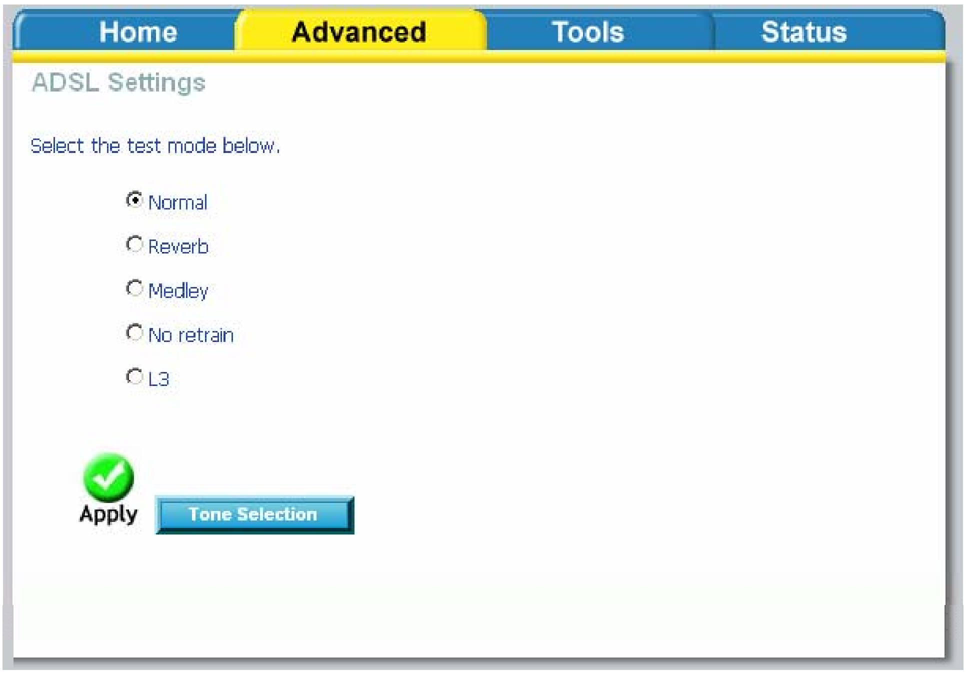
☑ G.Dmt Enabled
☐ G.lite Enabled
☐ T1.413 Enabled
☐ ADSL2 Enabled
☐ AnnexL Enabled
☐ ADSL2+ Enabled
☐ AnnexM Enabled

Capability

☑ Bitswap Enable
☐ SRA Enable

ADSL Settings

The test mode can be selected from the DSL Advanced Settings page. Test modes include—normal, reverb, medley, no retrain, and L3. After you make your selections of the test mode, click on **Apply** to save these settings first before you go to *Tone Selection*.



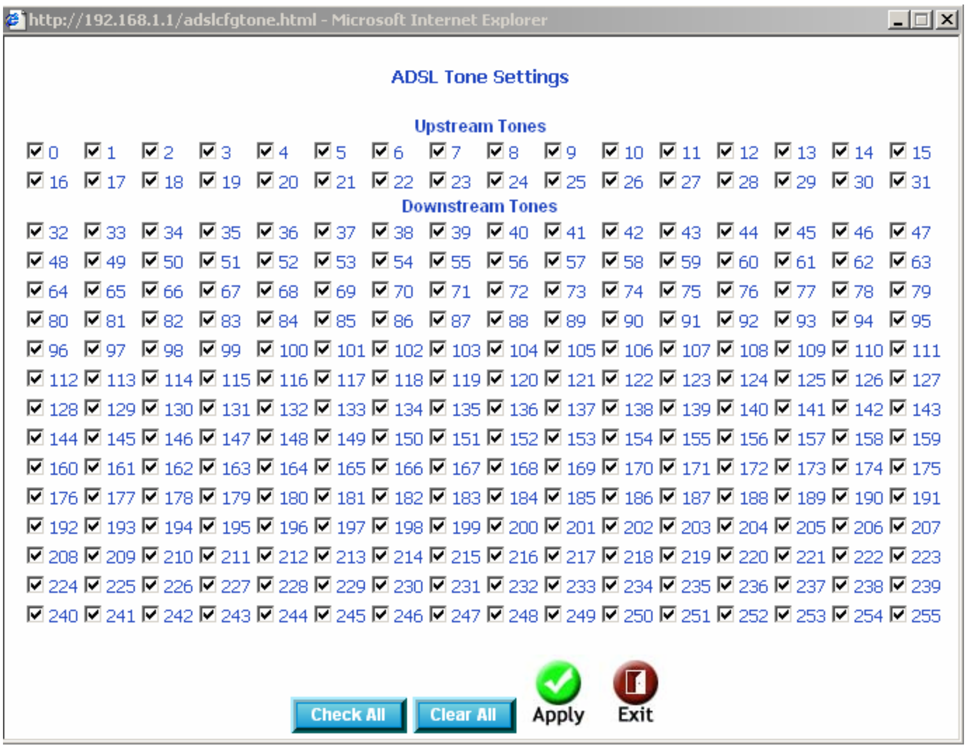
ADSL Settings

Select the test mode below.

● Normal
○ Reverb
○ Medley
○ No retrain
○ L3

ADSL Tone Settings

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart. With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream. Do not change these settings unless directed by your ISP.



http://192.168.1.1/adslcfgtone.html - Microsoft Internet Explorer

ADSL Tone Settings

Upstream Tones

☑ 0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15
☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31

Downstream Tones

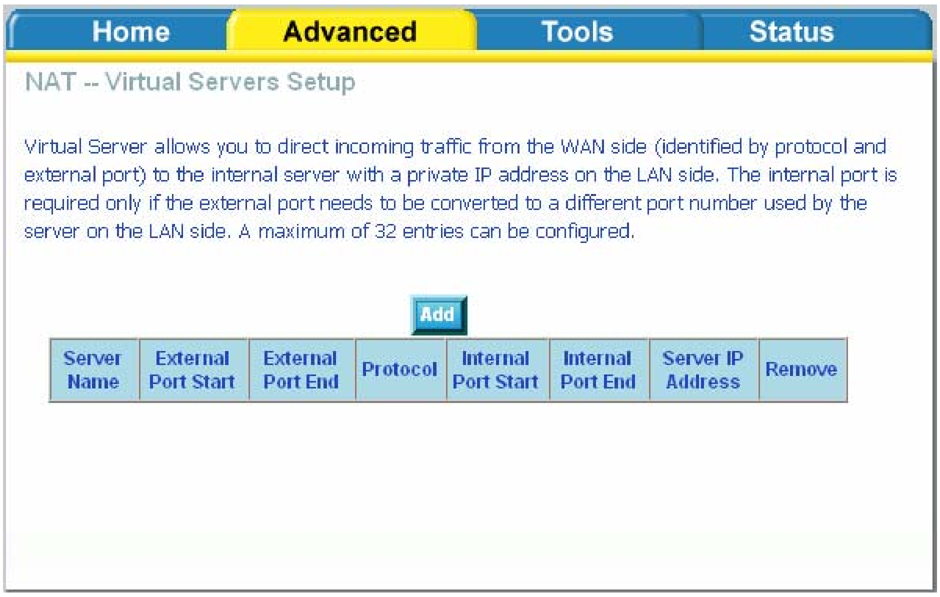
☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42 ☑ 43 ☑ 44 ☑ 45 ☑ 46 ☑ 47
☑ 48 ☑ 49 ☑ 50 ☑ 51 ☑ 52 ☑ 53 ☑ 54 ☑ 55 ☑ 56 ☑ 57 ☑ 58 ☑ 59 ☑ 60 ☑ 61 ☑ 62 ☑ 63
☑ 64 ☑ 65 ☑ 66 ☑ 67 ☑ 68 ☑ 69 ☑ 70 ☑ 71 ☑ 72 ☑ 73 ☑ 74 ☑ 75 ☑ 76 ☑ 77 ☑ 78 ☑ 79
☑ 80 ☑ 81 ☑ 82 ☑ 83 ☑ 84 ☑ 85 ☑ 86 ☑ 87 ☑ 88 ☑ 89 ☑ 90 ☑ 91 ☑ 92 ☑ 93 ☑ 94 ☑ 95
☑ 96 ☑ 97 ☑ 98 ☑ 99 ☑ 100 ☑ 101 ☑ 102 ☑ 103 ☑ 104 ☑ 105 ☑ 106 ☑ 107 ☑ 108 ☑ 109 ☑ 110 ☑ 111
☑ 112 ☑ 113 ☑ 114 ☑ 115 ☑ 116 ☑ 117 ☑ 118 ☑ 119 ☑ 120 ☑ 121 ☑ 122 ☑ 123 ☑ 124 ☑ 125 ☑ 126 ☑ 127
☑ 128 ☑ 129 ☑ 130 ☑ 131 ☑ 132 ☑ 133 ☑ 134 ☑ 135 ☑ 136 ☑ 137 ☑ 138 ☑ 139 ☑ 140 ☑ 141 ☑ 142 ☑ 143
☑ 144 ☑ 145 ☑ 146 ☑ 147 ☑ 148 ☑ 149 ☑ 150 ☑ 151 ☑ 152 ☑ 153 ☑ 154 ☑ 155 ☑ 156 ☑ 157 ☑ 158 ☑ 159
☑ 160 ☑ 161 ☑ 162 ☑ 163 ☑ 164 ☑ 165 ☑ 166 ☑ 167 ☑ 168 ☑ 169 ☑ 170 ☑ 171 ☑ 172 ☑ 173 ☑ 174 ☑ 175
☑ 176 ☑ 177 ☑ 178 ☑ 179 ☑ 180 ☑ 181 ☑ 182 ☑ 183 ☑ 184 ☑ 185 ☑ 186 ☑ 187 ☑ 188 ☑ 189 ☑ 190 ☑ 191
☑ 192 ☑ 193 ☑ 194 ☑ 195 ☑ 196 ☑ 197 ☑ 198 ☑ 199 ☑ 200 ☑ 201 ☑ 202 ☑ 203 ☑ 204 ☑ 205 ☑ 206 ☑ 207
☑ 208 ☑ 209 ☑ 210 ☑ 211 ☑ 212 ☑ 213 ☑ 214 ☑ 215 ☑ 216 ☑ 217 ☑ 218 ☑ 219 ☑ 220 ☑ 221 ☑ 222 ☑ 223
☑ 224 ☑ 225 ☑ 226 ☑ 227 ☑ 228 ☑ 229 ☑ 230 ☑ 231 ☑ 232 ☑ 233 ☑ 234 ☑ 235 ☑ 236 ☑ 237 ☑ 238 ☑ 239
☑ 240 ☑ 241 ☑ 242 ☑ 243 ☑ 244 ☑ 245 ☑ 246 ☑ 247 ☑ 248 ☑ 249 ☑ 250 ☑ 251 ☑ 252 ☑ 253 ☑ 254 ☑ 255

Virtual Server

If you enable NAT (Network Address Translation), you can configure the Virtual Server, Port Triggering, and DMZ Host.

NAT—Virtual Servers Setup

A virtual server allows you to direct incoming traffic from the WAN side to a specific IP address on the LAN side.The following figure shows the screen that allows you to configure your virtual server(s). Click on the **Add** button to configure a virtual server.

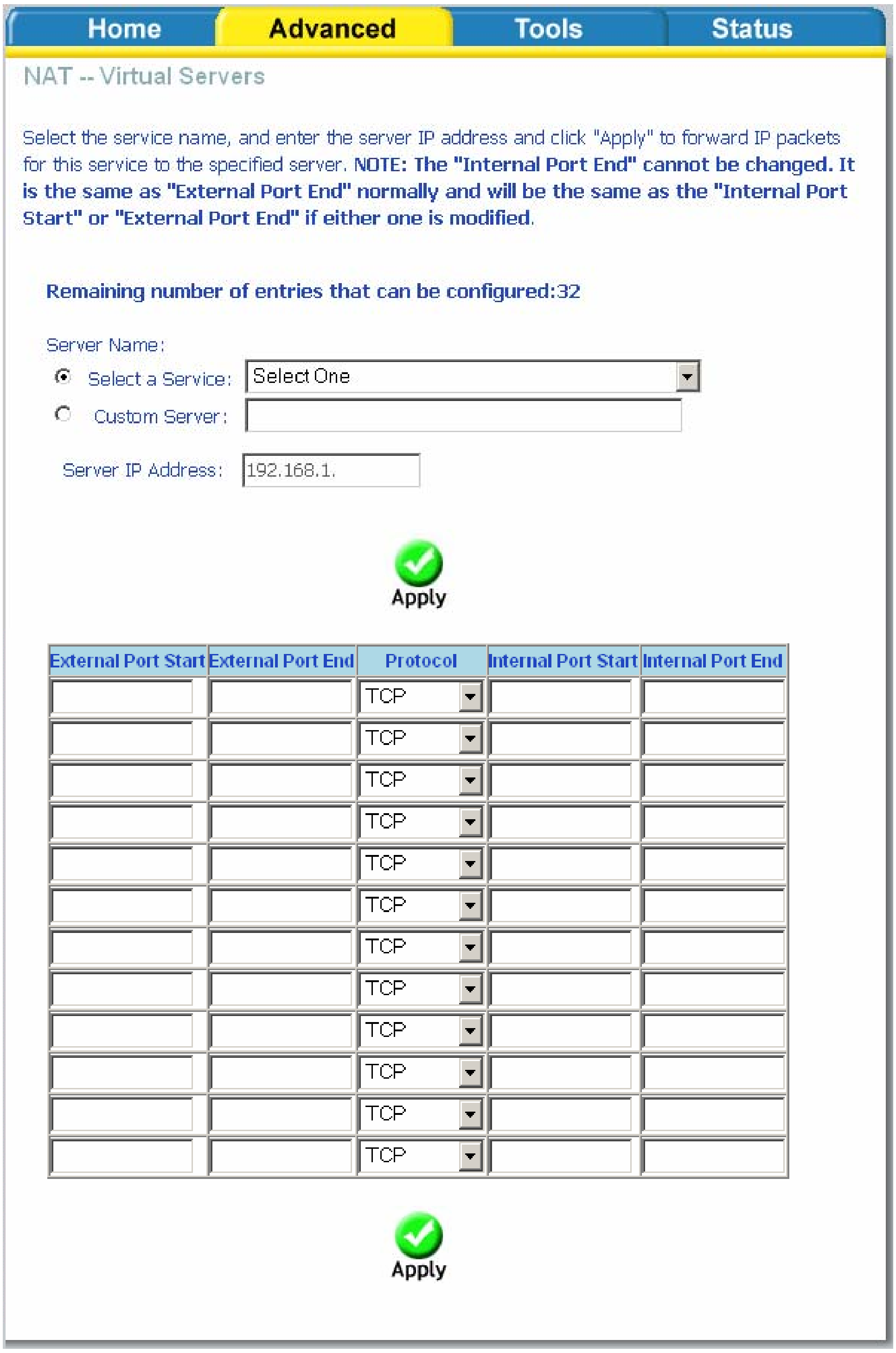


NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove

Select the virtual server from the drop-down list and complete the server IP address, then click on **Apply** once.



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**

Remaining number of entries that can be configured:32

Server Name:

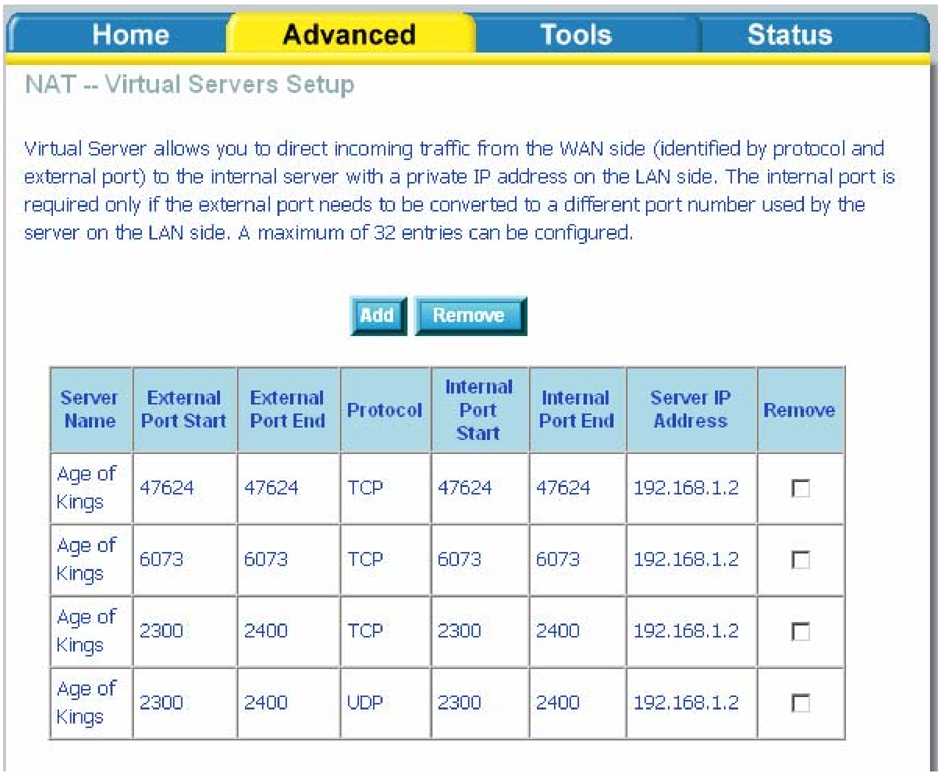
● Select a Service: Select One

○ Custom Server:

Server IP Address: 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

The following screen appears after you save your selection. To add additional virtual servers, click on the **Add** button. If you need to remove any of the server names, select the check box and click on the **Remove** button.



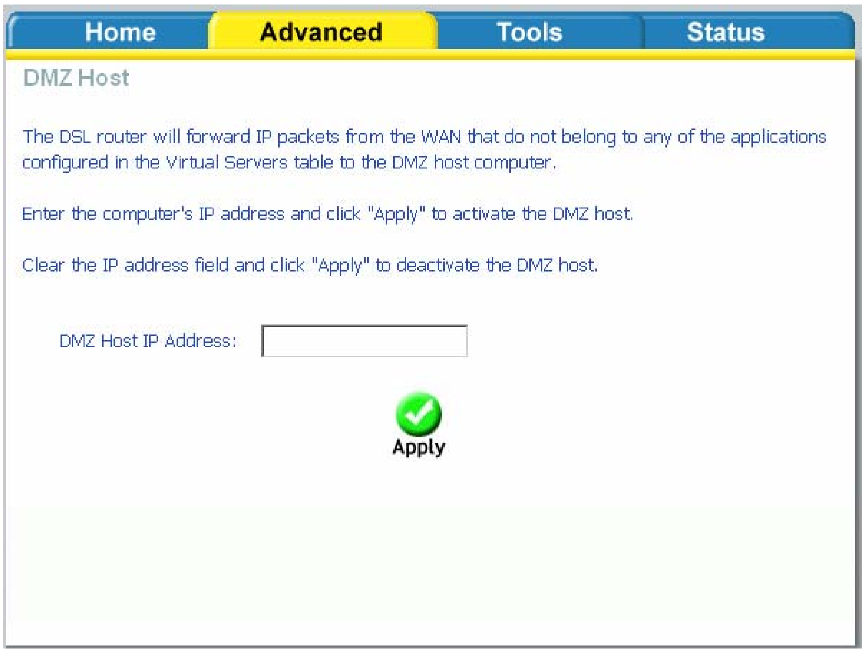
NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
Age of Kings	47624	47624	TCP	47624	47624	192.168.1.2	□
Age of Kings	6073	6073	TCP	6073	6073	192.168.1.2	□
Age of Kings	2300	2400	TCP	2300	2400	192.168.1.2	□
Age of Kings	2300	2400	UDP	2300	2400	192.168.1.2	□

DMZ

You can define the IP address of the DMZ Host on this screen. Enter the IP address and click on **Apply**.



DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

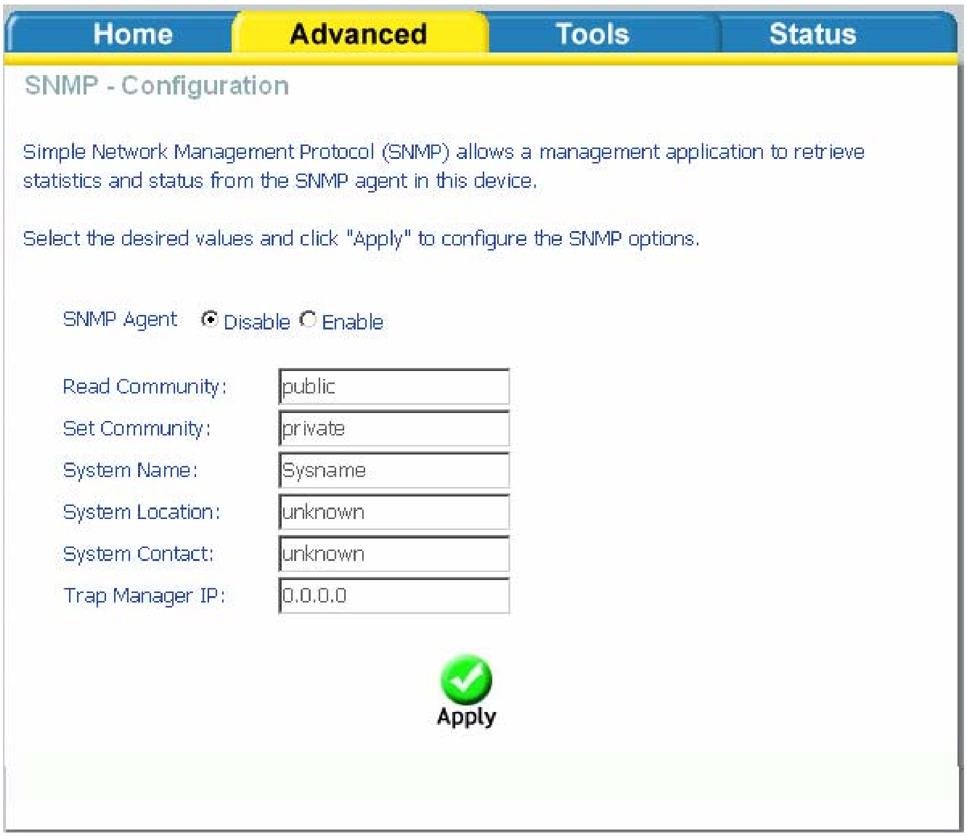
Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

SNMP

SNMP—Configuration

SNMP is Simple Network Management Protocol that provides a means to monitor status and performance as well as set configuration parameters. It enables a management station to configure, monitor and receive trap messages from network devices.



SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

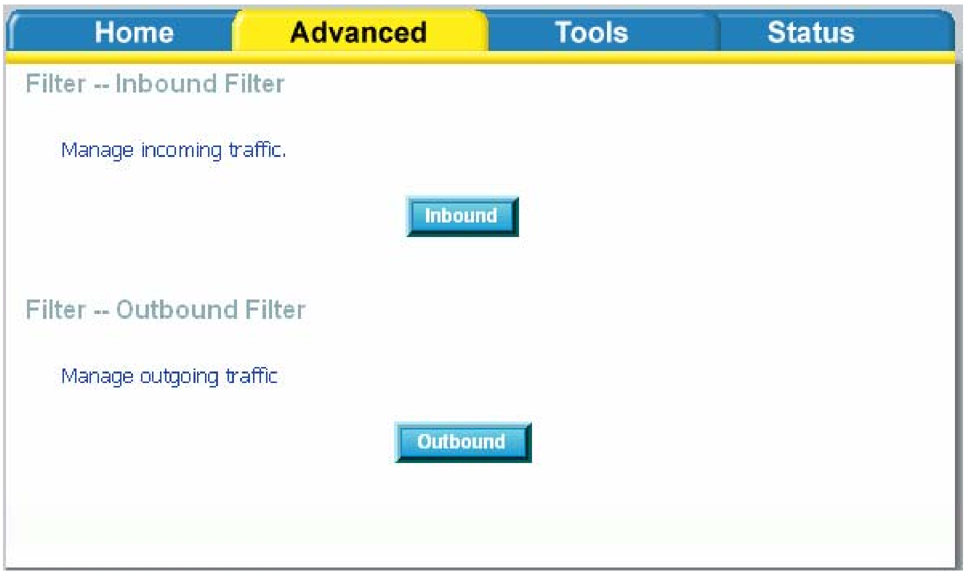
Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ● Disable ○ Enable

Read Community:	public
Set Community:	private
System Name:	Sysname
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

IP Filter

IP filters can be configured to manage your incoming and outgoing traffic. Click on the Inbound and Outbound buttons to advance to the next section for further configuration.



Filter -- Inbound Filter

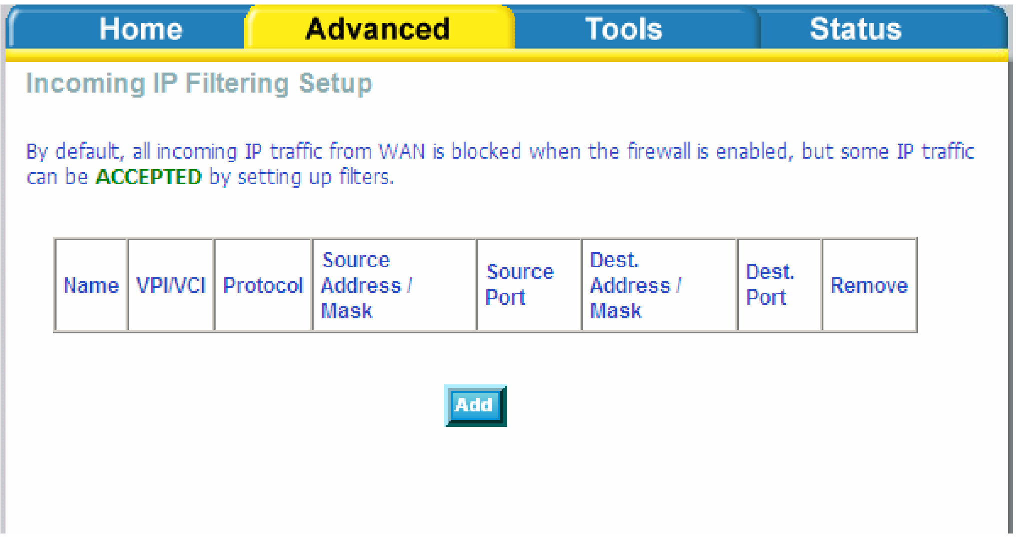
Manage incoming traffic.

Filter -- Outbound Filter

Manage outgoing traffic

Incoming IP Filtering Setup

Incoming IP filter allows specified the WAN traffic to pass through the firewall. Click on the **Add** button to add incoming filter settings.

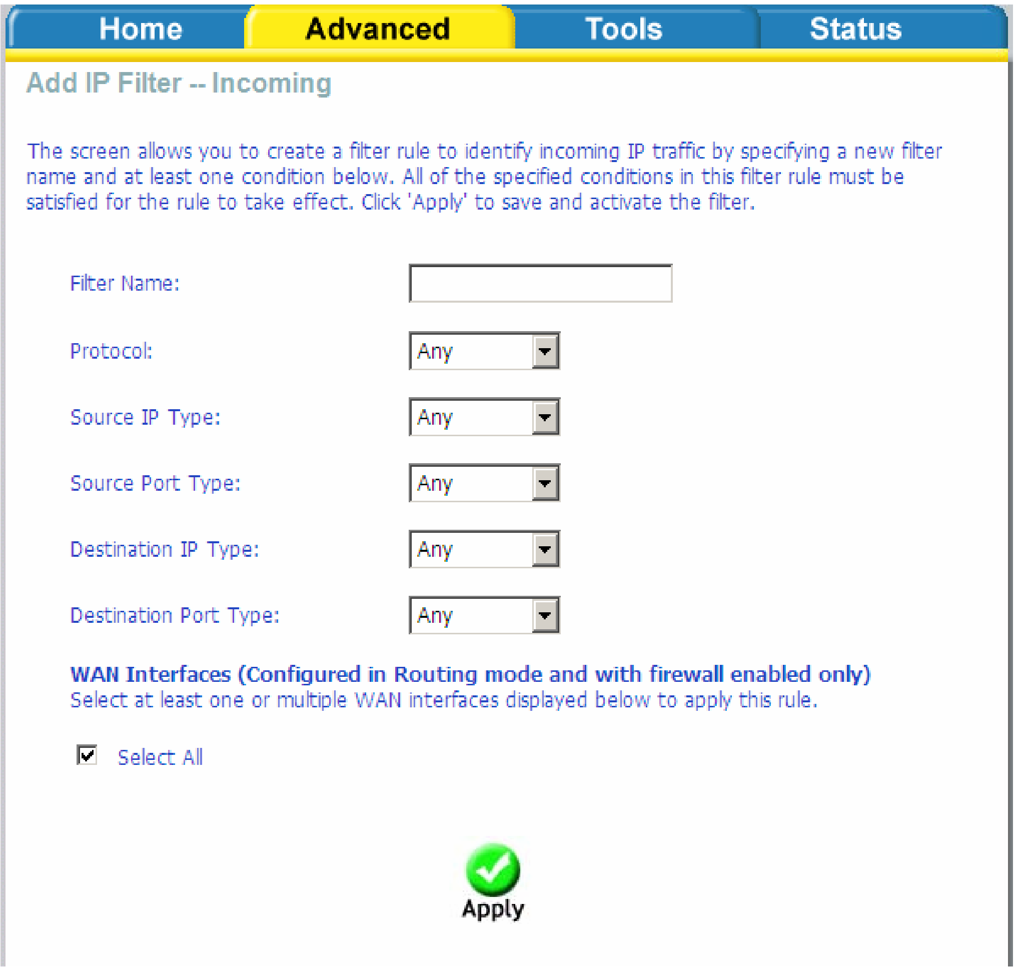


Incoming IP Filtering Setup

By default, all incoming IP traffic from WAN is blocked when the firewall is enabled, but some IP traffic can be ACCEPTED by setting up filters.

Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

Enter a filter name, information about the source address (from the WAN side), and information about the destination address (to the LAN side). Select the protocol and WAN interface, then click on **Apply** to add the setting.



Add IP Filter -- Incoming

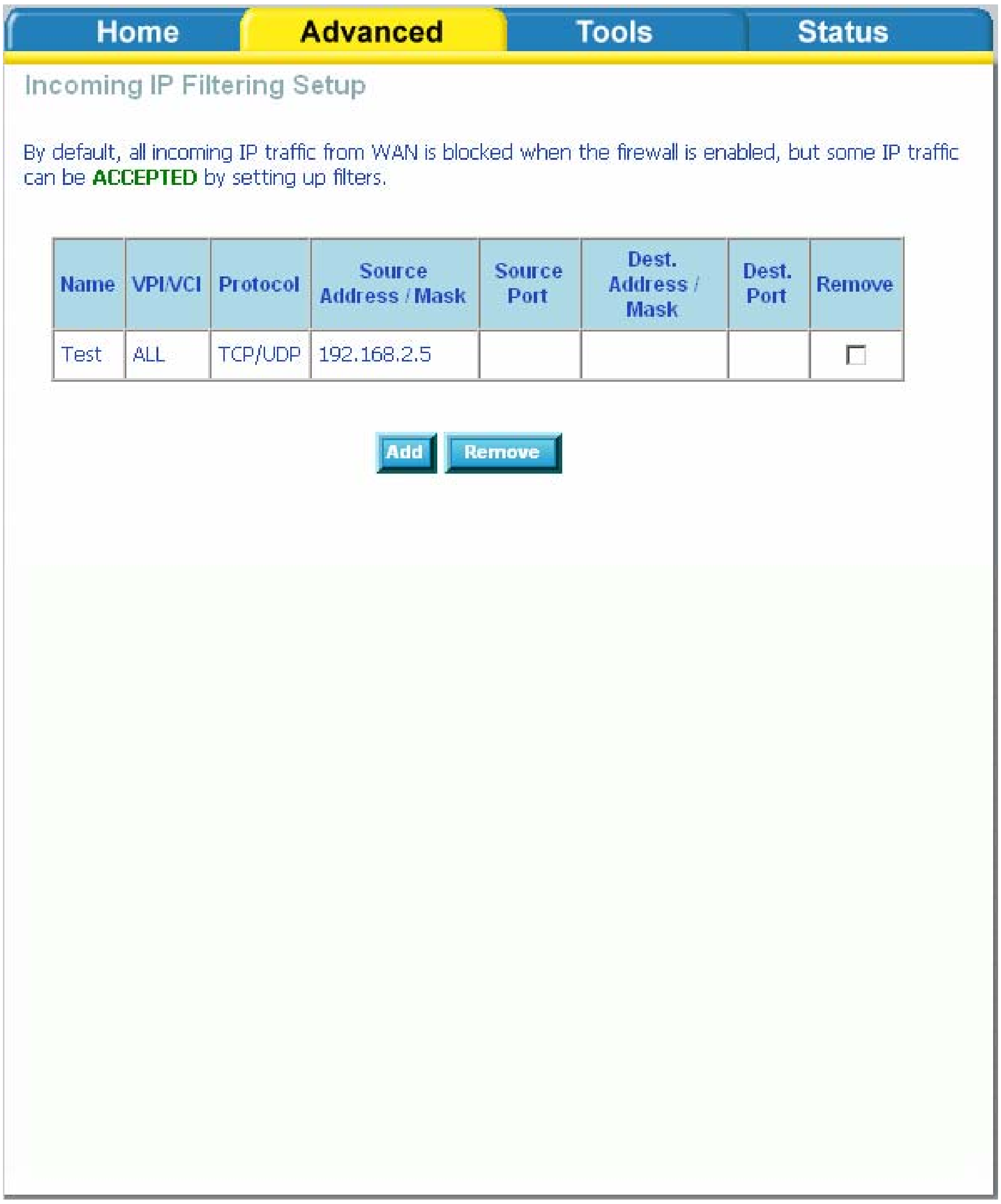
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply' to save and activate the filter.

Filter Name:	
Protocol:	Any
Source IP Type:	Any
Source Port Type:	Any
Destination IP Type:	Any
Destination Port Type:	Any

WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

☑ Select All

The following screen appears when you apply the IP filter. The screen lists the IP filters that were added from the previous screen. To change your settings, click on the **Add** or **Remove** buttons.



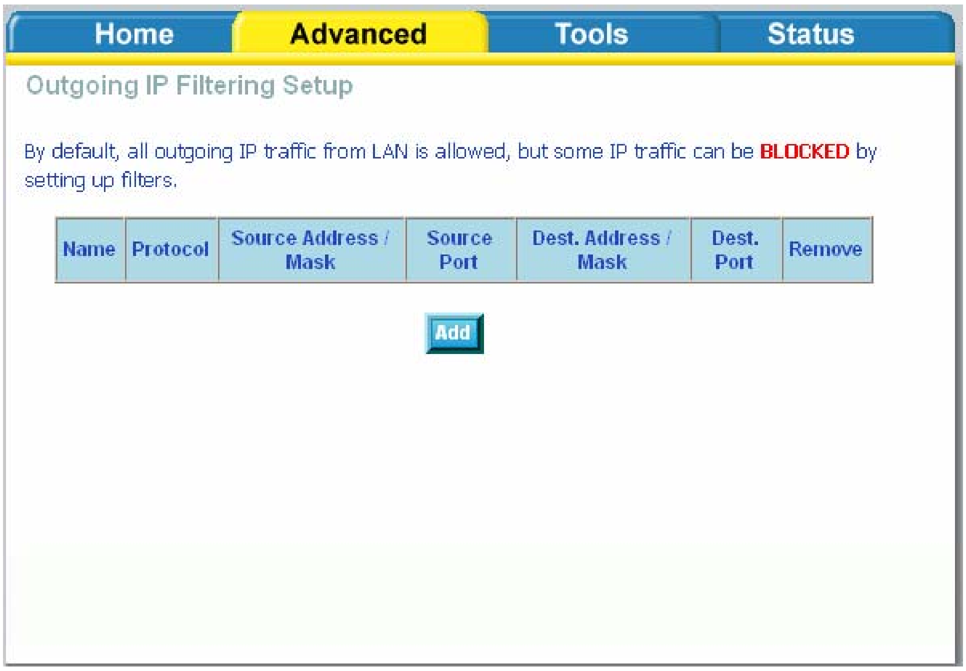
Incoming IP Filtering Setup

By default, all incoming IP traffic from WAN is blocked when the firewall is enabled, but some IP traffic can be **ACCEPTED** by setting up filters.

Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Test	ALL	TCP/UDP	192.168.2.5				□

Outgoing IP Filtering Setup

The outgoing filter will block the LAN traffic from entering the WAN side. Click on the **Add** button to create filters.

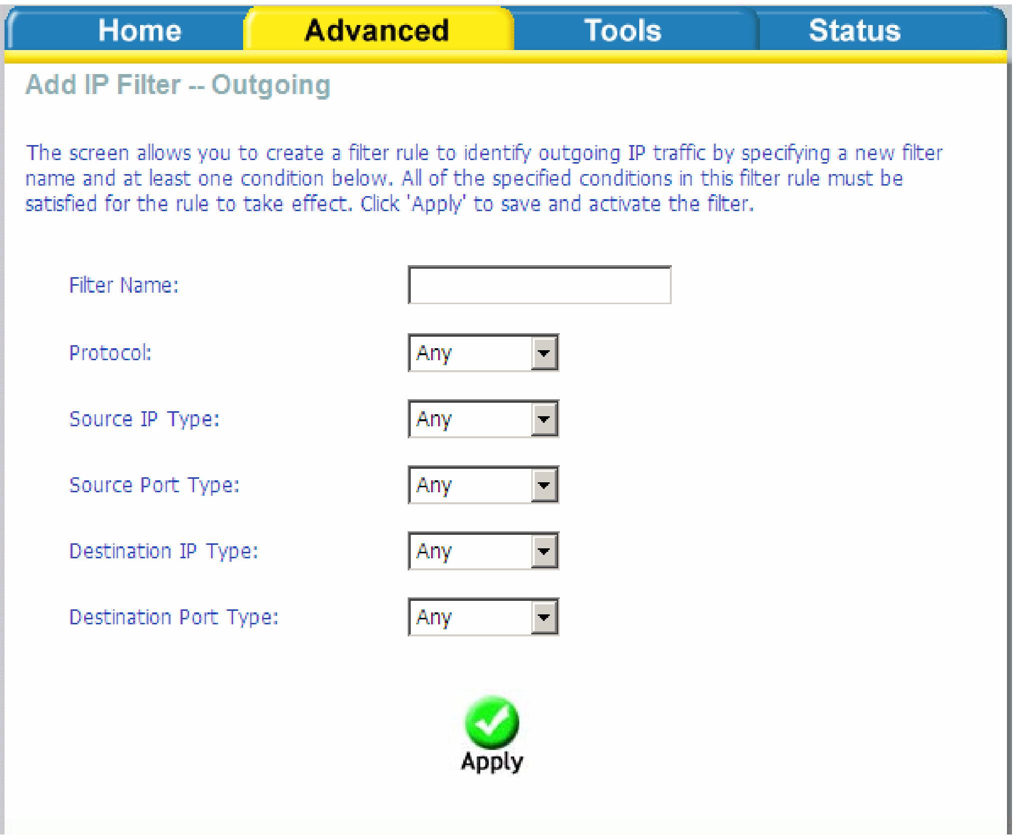


Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

The below screen will appear when you click on **Add**. Input the filter name, source information (from the LAN side), and destination information (from the WAN side). Then click on **Apply** to save.

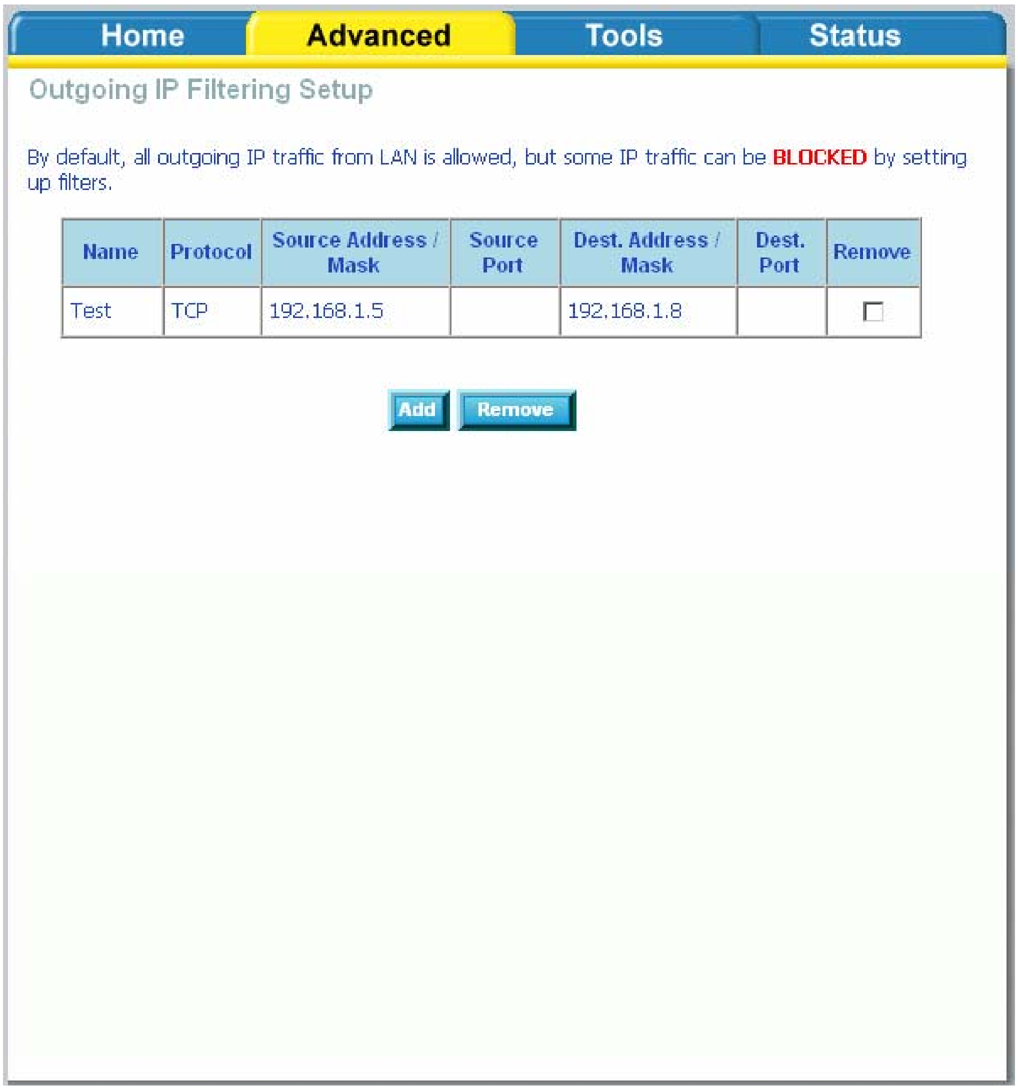


Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply' to save and activate the filter.

Filter Name:	
Protocol:	Any
Source IP Type:	Any
Source Port Type:	Any
Destination IP Type:	Any
Destination Port Type:	Any

The following screen appears when you apply the IP filter. The screen lists the IP filters that were added from the previous screen. To change your settings, click on the **Add** or **Remove** buttons.



Outgoing IP Filtering Setup

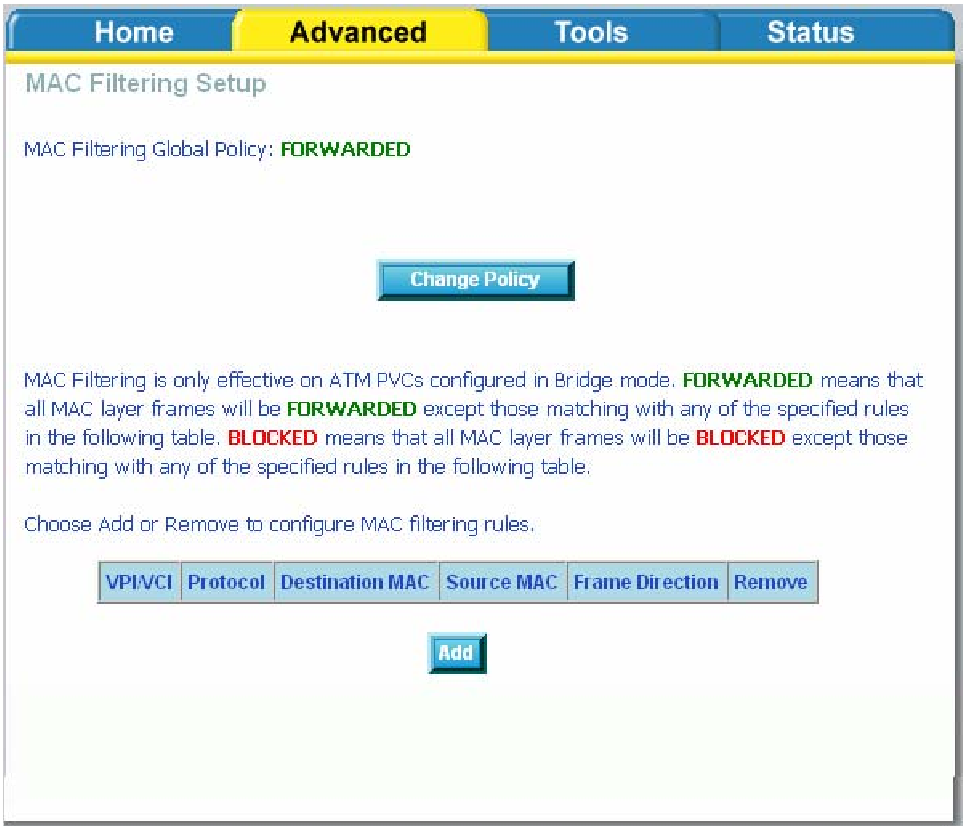
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Test	TCP	192.168.1.5		192.168.1.8		□

Bridge Filters

MAC Filtering Setup

MAC filtering can forward or block traffic by MAC address. You can change the policy or add settings to the MAC filtering table using the MAC Filtering Setup screen.



MAC Filtering Setup

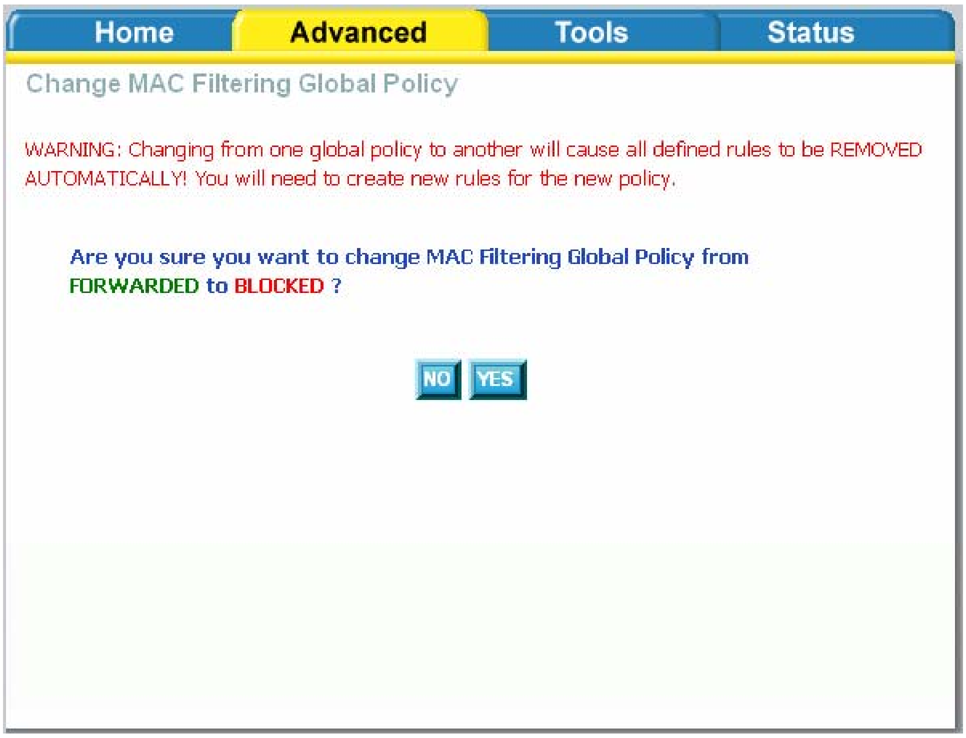
MAC Filtering Global Policy: FORWARDED

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

If you click on **Change Policy**, a confirmation dialog allows you to verify your change.

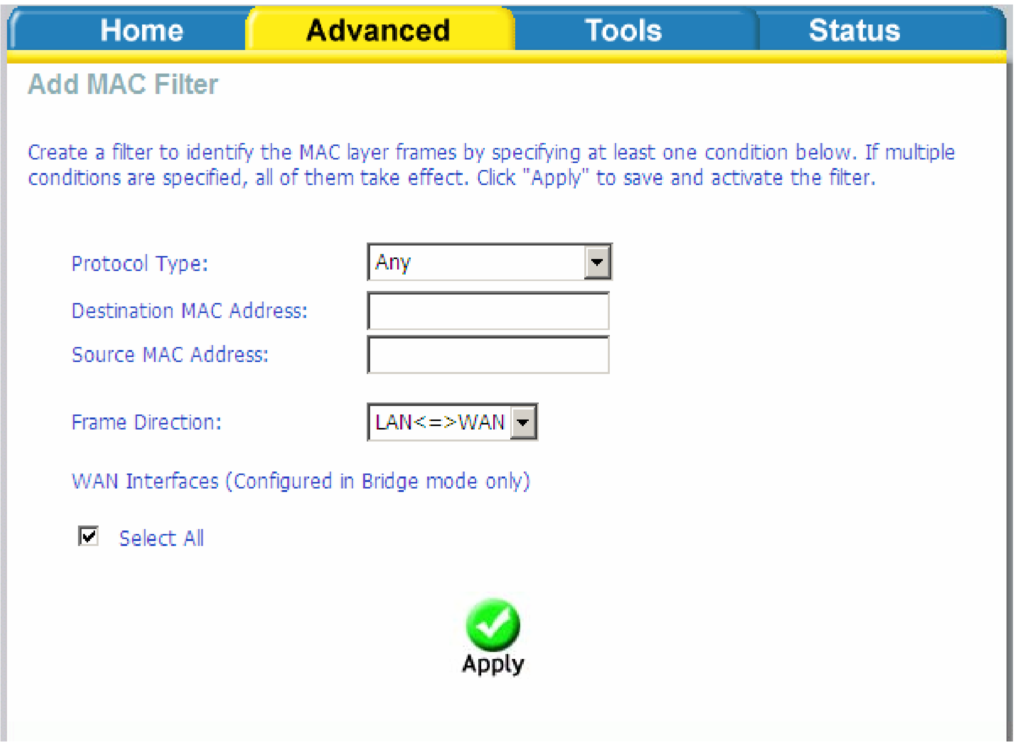


Change MAC Filtering Global Policy

WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Are you sure you want to change MAC Filtering Global Policy from FORWARDED to BLOCKED ?

If you want to add a setting to the MAC filtering table, select protocol type, enter the destination and source MAC address, the necessary frame direction, and WAN interface (bridge mode only). Then click on **Apply** to save.



Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type: Any

Destination MAC Address:

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

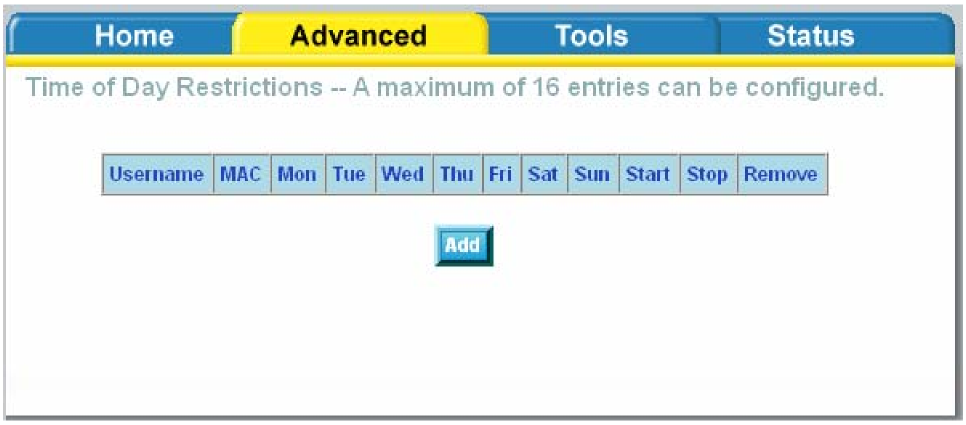
☑ Select All

After you save the settings, a screen showing the settings will appear. On this screen you will be able to view and delete MAC filtering rules.

Parental Control

Time of Day Restrictions

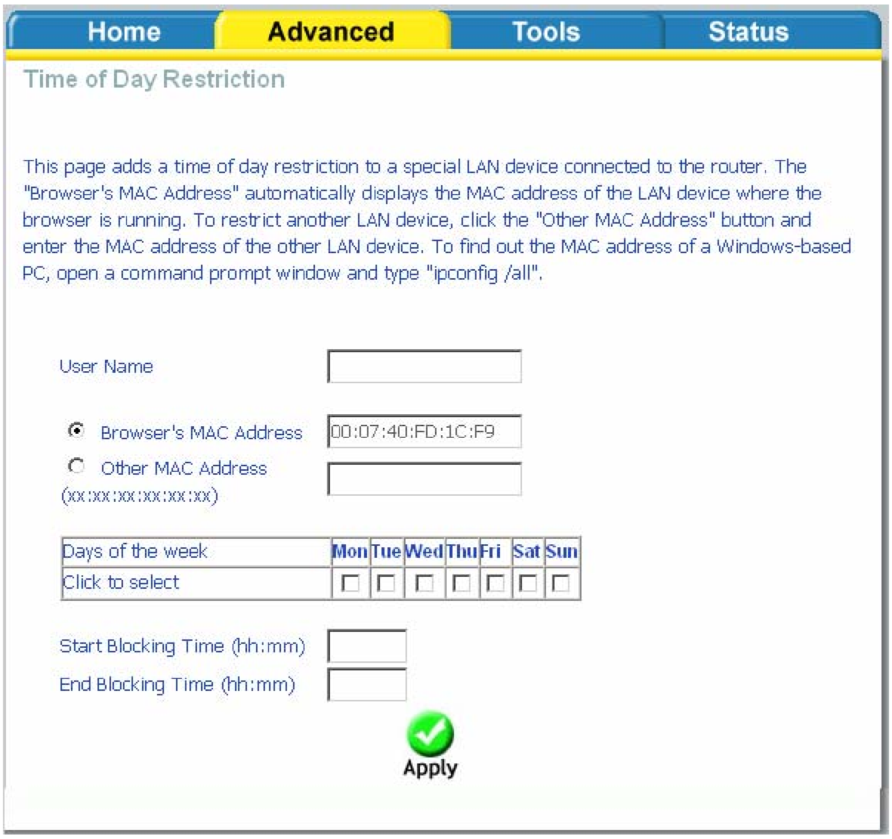
In a home setting, parents can also restrict the day of the week certain computers can access the router. Click on **Add** to set up the restrictions.



Time of Day Restrictions -- A maximum of 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

After you click you on **Add**, you will see the below screen where you will be able to enter the MAC address of the PC that you wish to place on a time of day restriction. Click on **Apply** to save the settings and to continue.



Time of Day Restriction

This page adds a time of day restriction to a special LAN device connected to the router. The "Browser's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".

User Name

● Browser's MAC Address 00:07:40:FD:1C:F9

○ Other MAC Address (xx:xx:xx:xx:xx:xx)

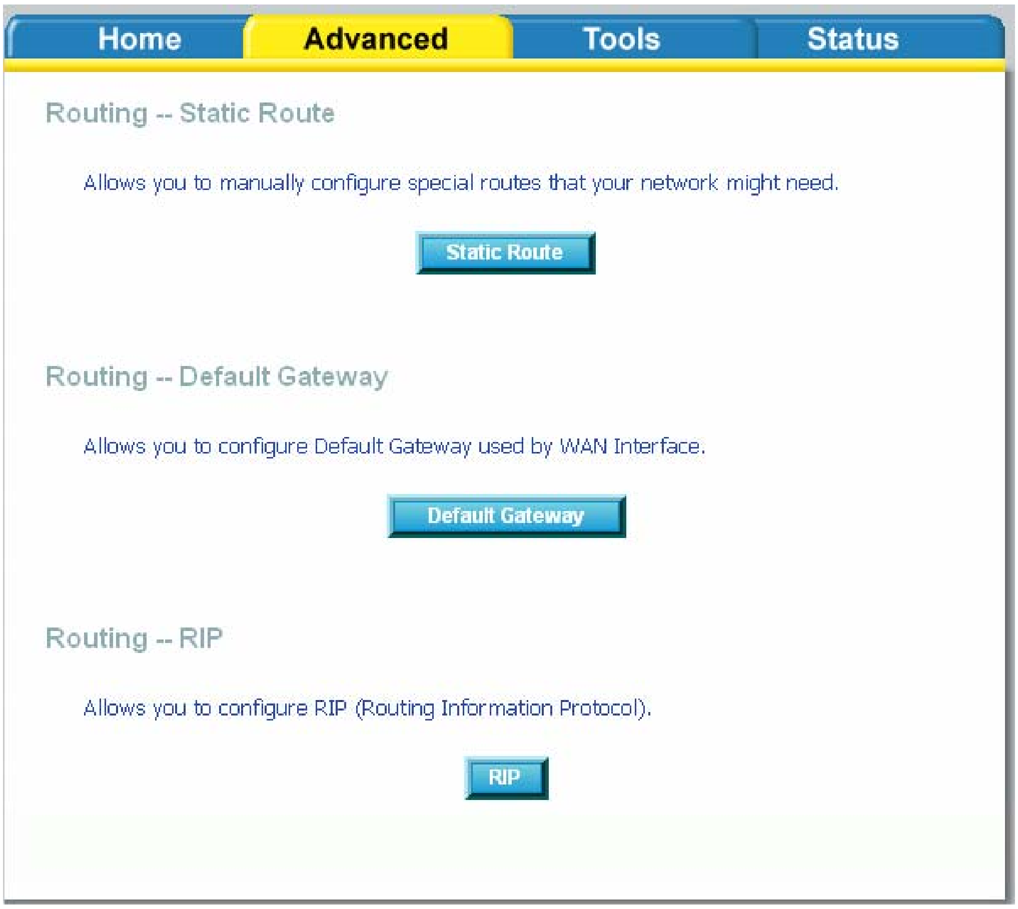
Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Routing

Static route, default gateway, and RIP type routing configurations can be performed here.



Routing -- Static Route

Allows you to manually configure special routes that your network might need.

Routing -- Default Gateway

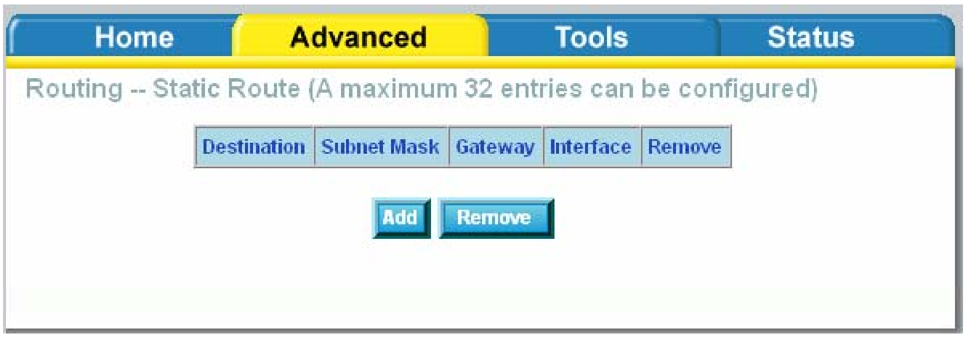
Allows you to configure Default Gateway used by WAN Interface.

Routing -- RIP

Allows you to configure RIP (Routing Information Protocol).

Routing--Static Route

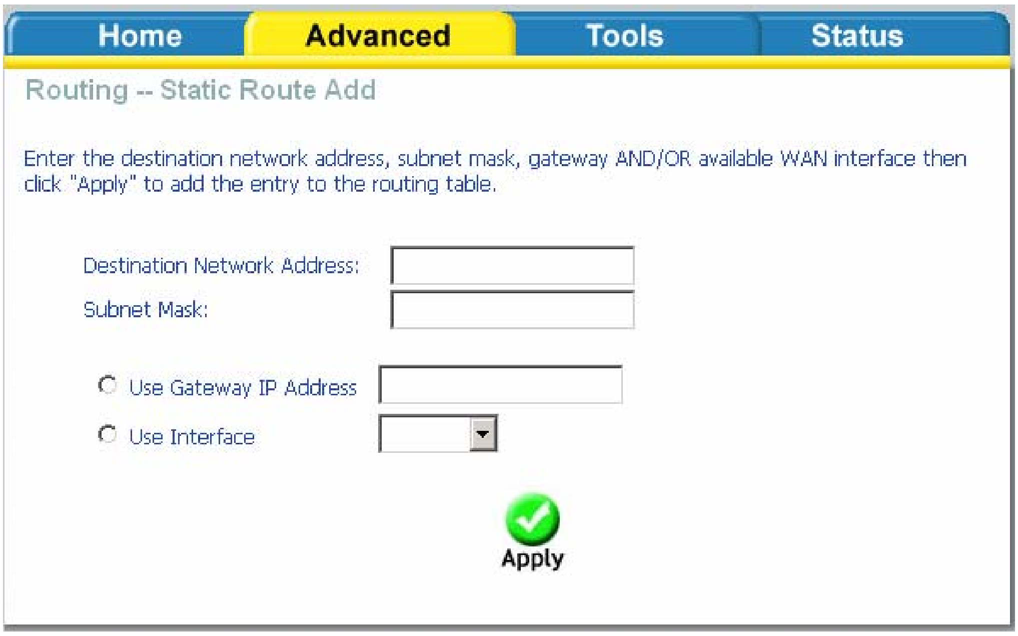
The Static Route page can be used to add a routing table (a maximum of 32 entries can be configured). To proceed, click on **Add**.



Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove

Enter the route information and then apply your configurations.



Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.

Destination Network Address:

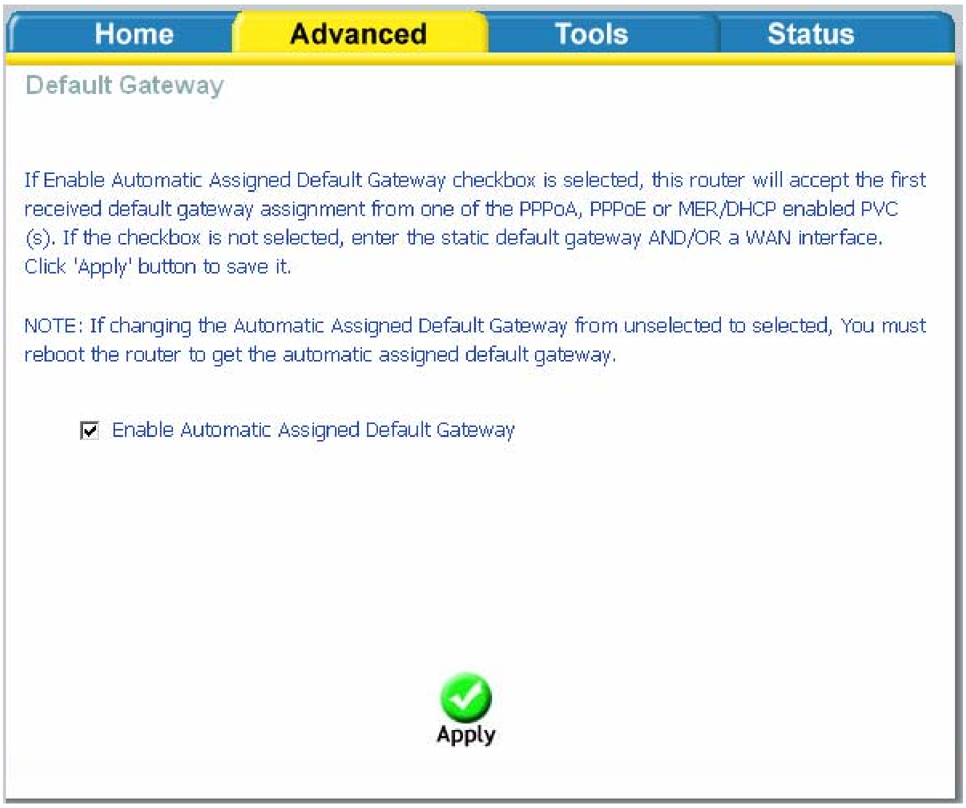
Subnet Mask:

○ Use Gateway IP Address

○ Use Interface

Routing—Default Gateway

The router has the ability to accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC's. This function is enabled by default as seen below.



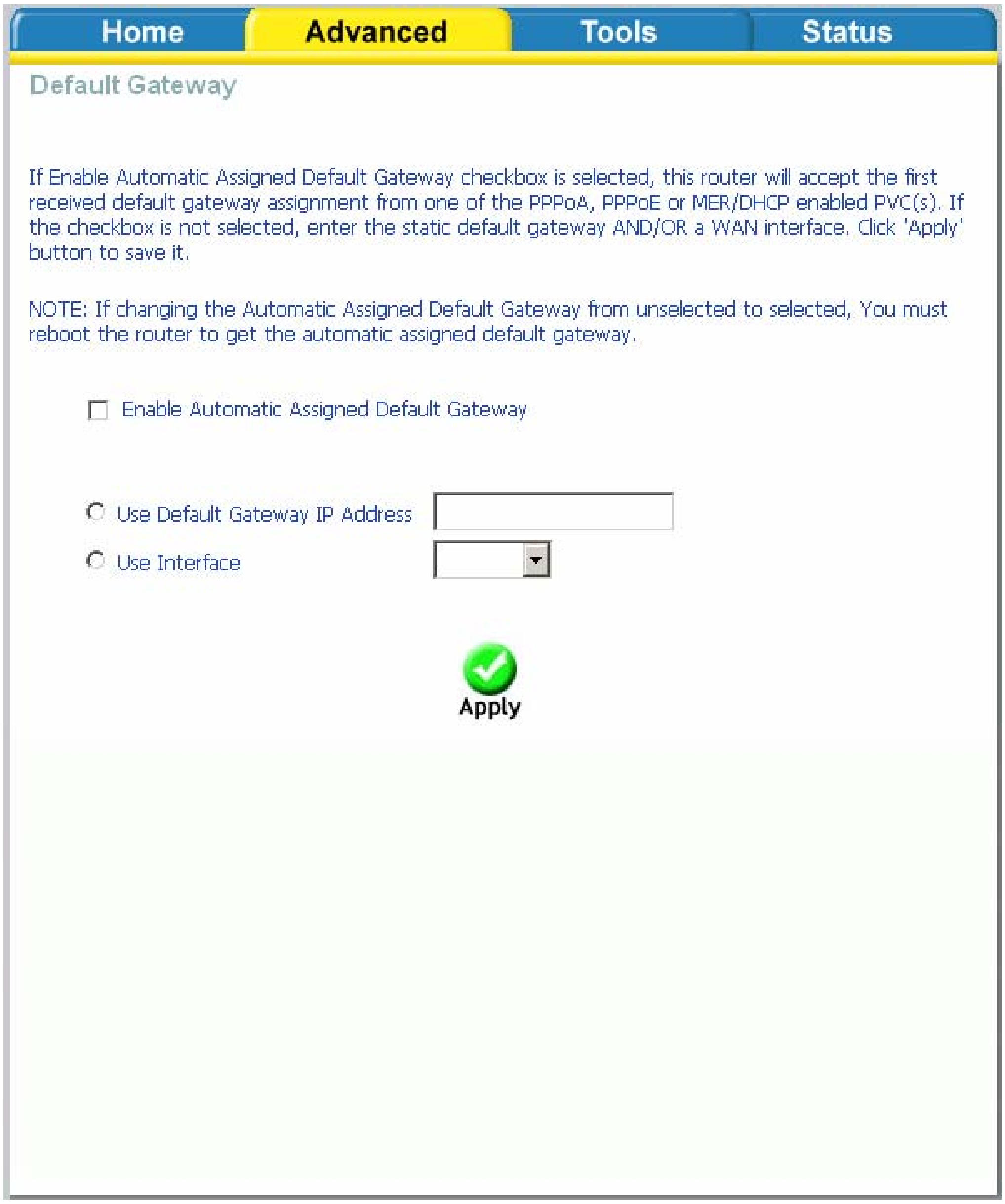
Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC (s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

☑ Enable Automatic Assigned Default Gateway

If you uncheck the **Enable Automatic Assigned Default Gateway** option, the below screen will be shown. Enter the default gateway IP address or select the established gateway to be used.



Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

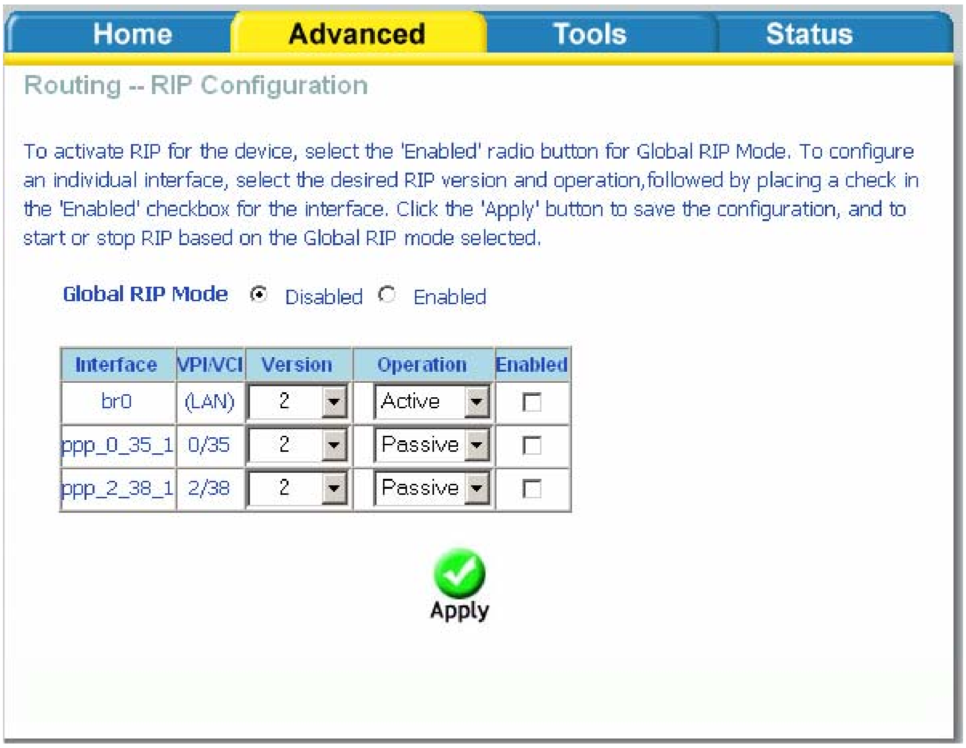
□ Enable Automatic Assigned Default Gateway

○ Use Default Gateway IP Address

○ Use Interface

Routing—RIP Configuration

If RIP is enabled, the router operation can be configured as active or passive.



Routing -- RIP Configuration

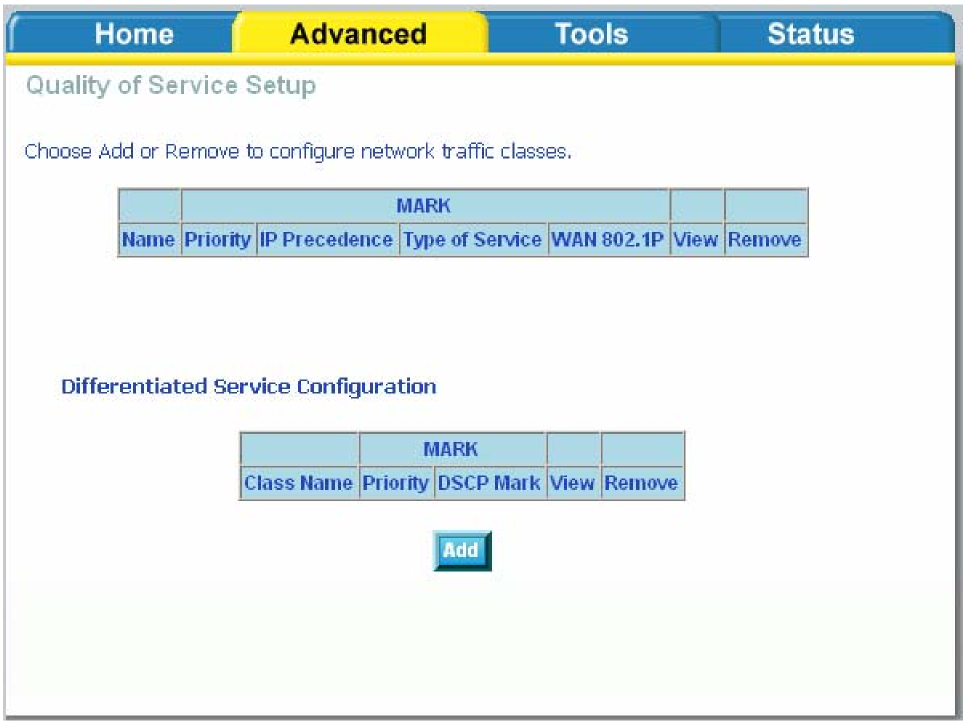
To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation,followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Global RIP Mode ● Disabled ○ Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	□
ppp_0_35_1	0/35	2	Passive	□
ppp_2_38_1	2/38	2	Passive	□

Quality of Service

You can configure the Quality of Service to apply different priorities to traffic on the router. Click on **Add** to view the *Add Network Traffic Class Rule* screen.



Quality of Service Setup

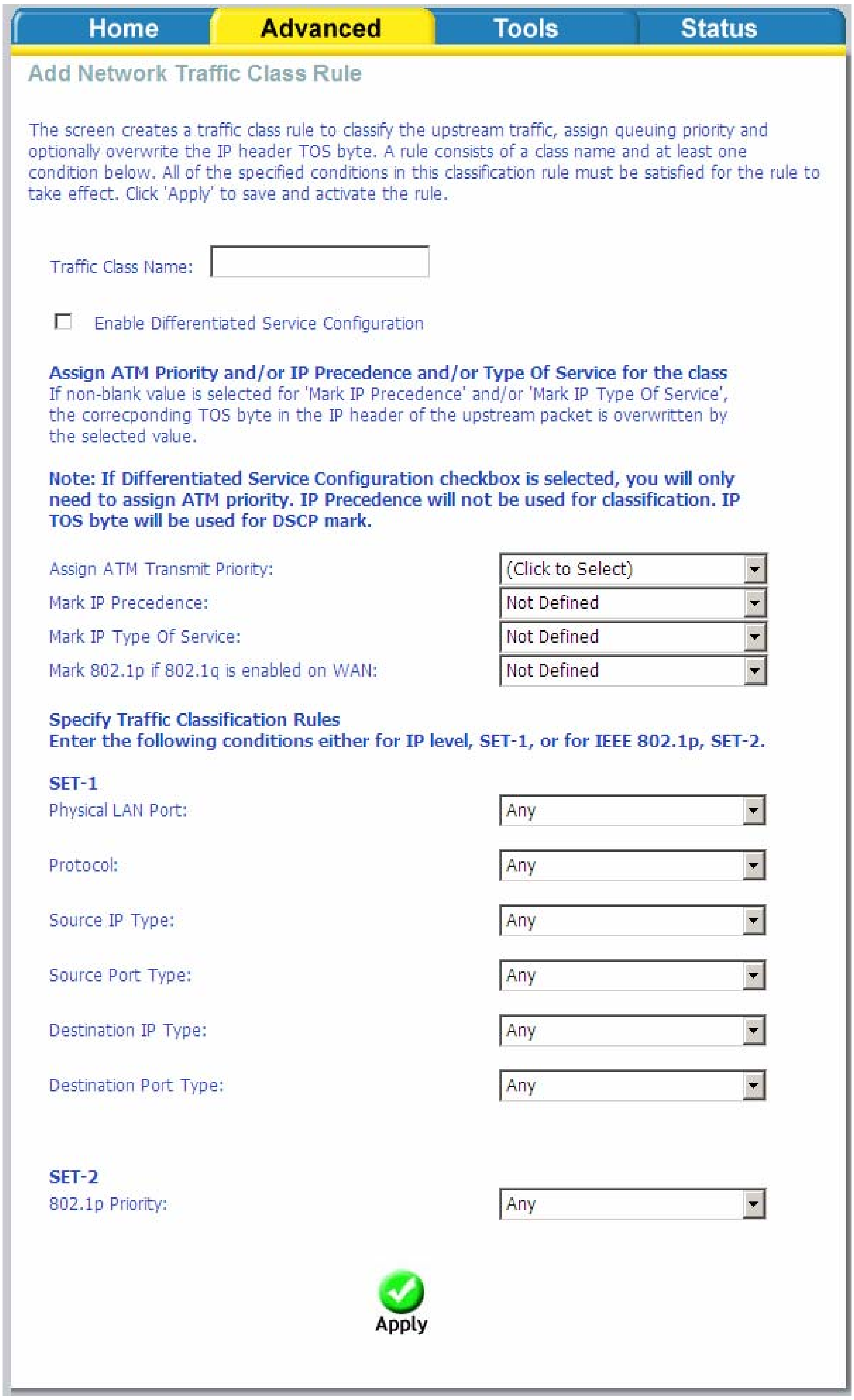
Choose Add or Remove to configure network traffic classes.

	MARK					
Name	Priority	IP Precedence	Type of Service	WAN 802.1P	View	Remove

Differentiated Service Configuration

	MARK			
Class Name	Priority	DSCP Mark	View	Remove

This screen allows you to add a network traffic class rule.



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply' to save and activate the rule.

Traffic Class Name:

□ Enable Differentiated Service Configuration

Assign ATM Priority and/or IP Precedence and/or Type Of Service for the class

If non-blank value is selected for 'Mark IP Precedence' and/or 'Mark IP Type Of Service', the correcponding TOS byte in the IP header of the upstream packet is overwritten by the selected value.

Note: If Differentiated Service Configuration checkbox is selected, you will only need to assign ATM priority. IP Precedence will not be used for classification. IP TOS byte will be used for DSCP mark.

Assign ATM Transmit Priority:	(Click to Select)
Mark IP Precedence:	Not Defined
Mark IP Type Of Service:	Not Defined
Mark 802.1p if 802.1q is enabled on WAN:	Not Defined

Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

SET-1

Physical LAN Port:	Any
Protocol:	Any
Source IP Type:	Any
Source Port Type:	Any
Destination IP Type:	Any
Destination Port Type:	Any

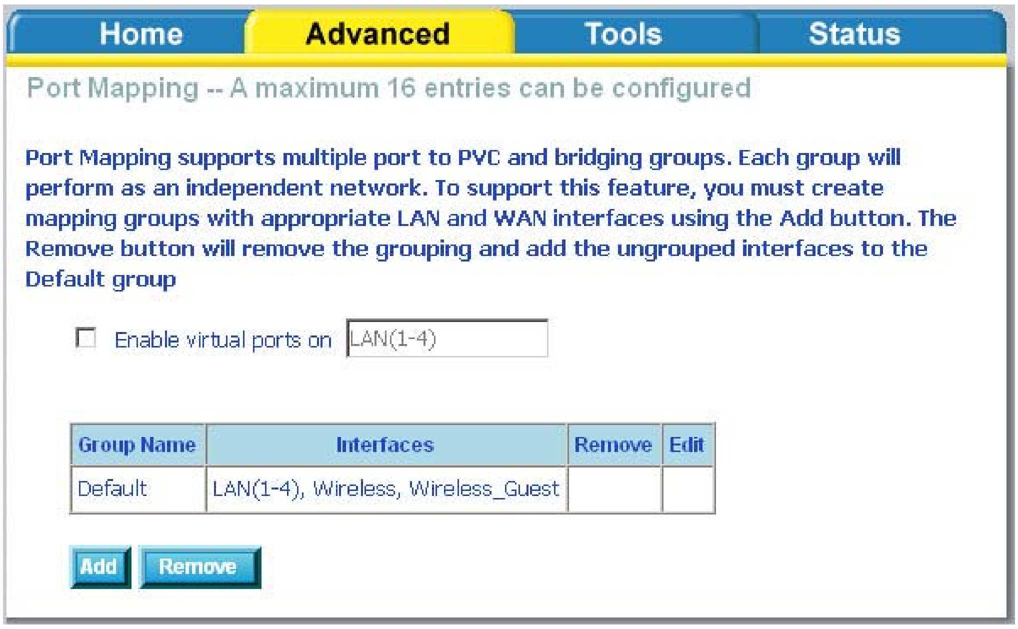
SET-2

802.1p Priority:	Any

Port Mapping

Port mapping is a feature that allows you to open ports to allow certain Internet applications on the WAN side to pass through the firewall and enter your LAN. To use this feature, mapping groups should be created.

Click on the **Add** button as displayed below. If you need to remove an entry, then click on the **Remove** button.



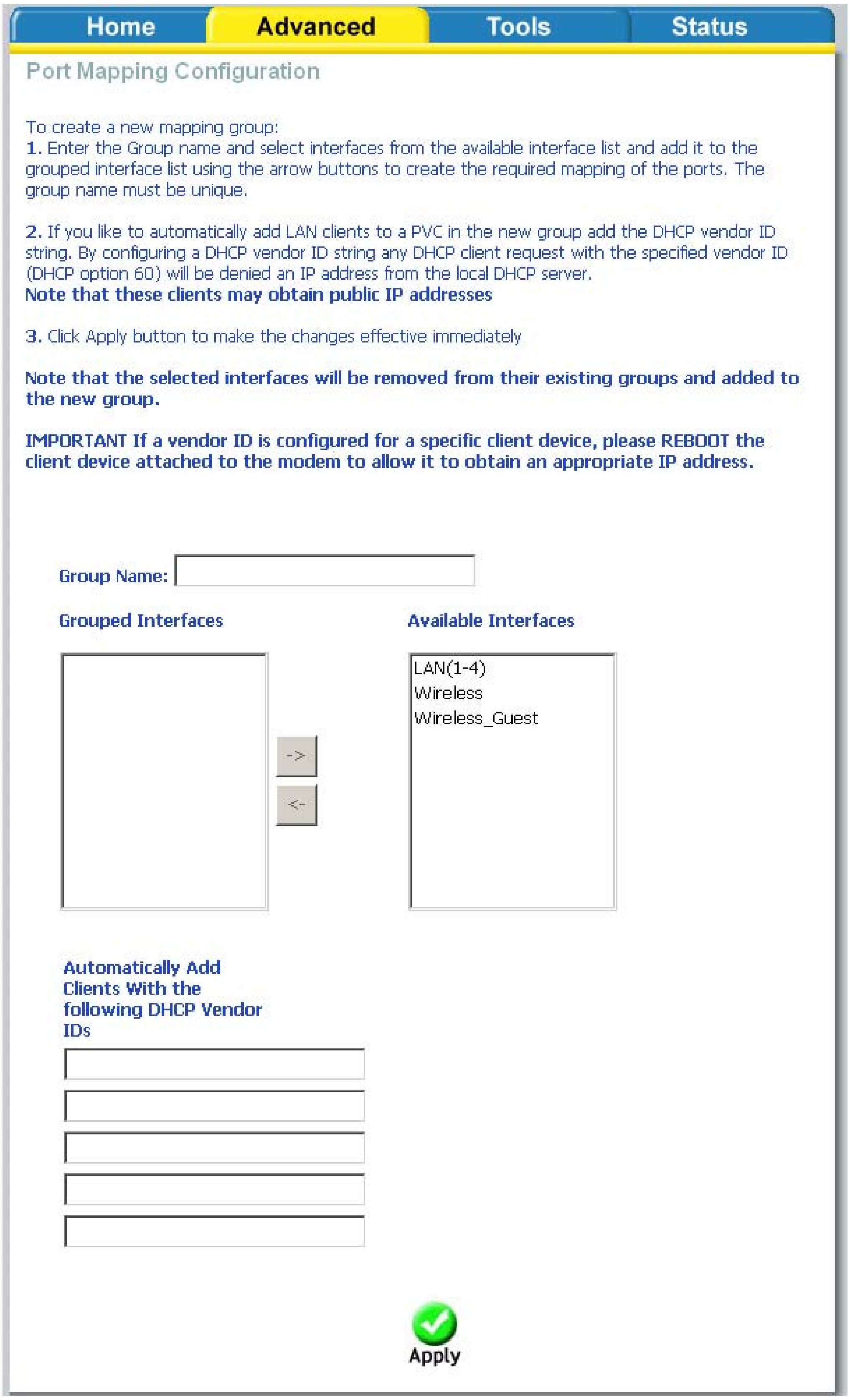
Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group

□ Enable virtual ports on LAN(1-4)

Group Name	Interfaces	Remove	Edit
Default	LAN(1-4), Wireless, Wireless_Guest		

After clicking the **Add** button, the below configuration screen appears, allowing you enter the groups and the interfaces they are associated with.



Port Mapping Configuration

To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses

3. Click Apply button to make the changes effective immediately

Note that the selected interfaces will be removed from their existing groups and added to the new group.

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped Interfaces

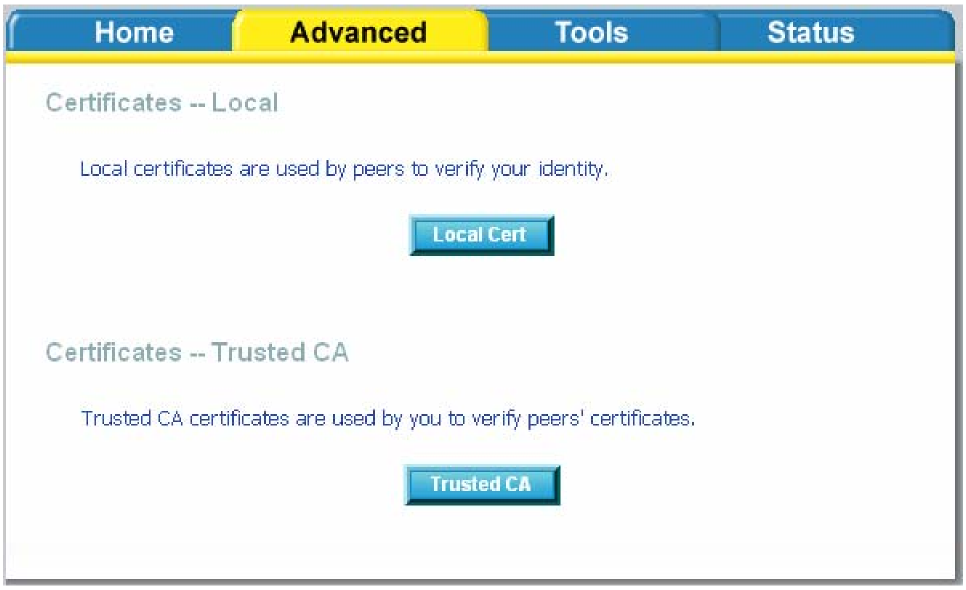
Available Interfaces

LAN(1-4)
Wireless
Wireless_Guest

Automatically Add Clients With the following DHCP Vendor IDs

Certificate

There are two types of certificates—local & trusted CA.



Certificates -- Local

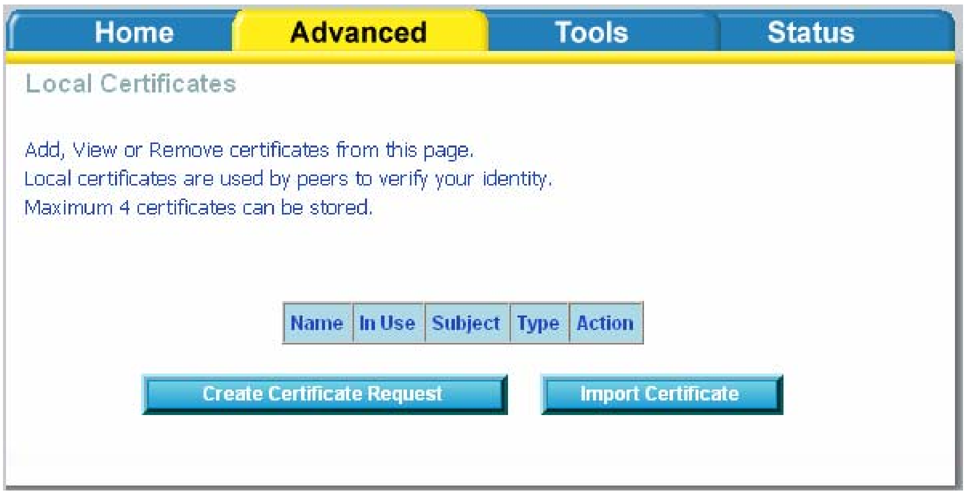
Local certificates are used by peers to verify your identity.

Certificates -- Trusted CA

Trusted CA certificates are used by you to verify peers' certificates.

Local

A local certificate identifies your router over the network. To apply for a certificate, click on **Create Certificate Request** and if you have an existing certificate, click on **Import Certificate** to retrieve it.



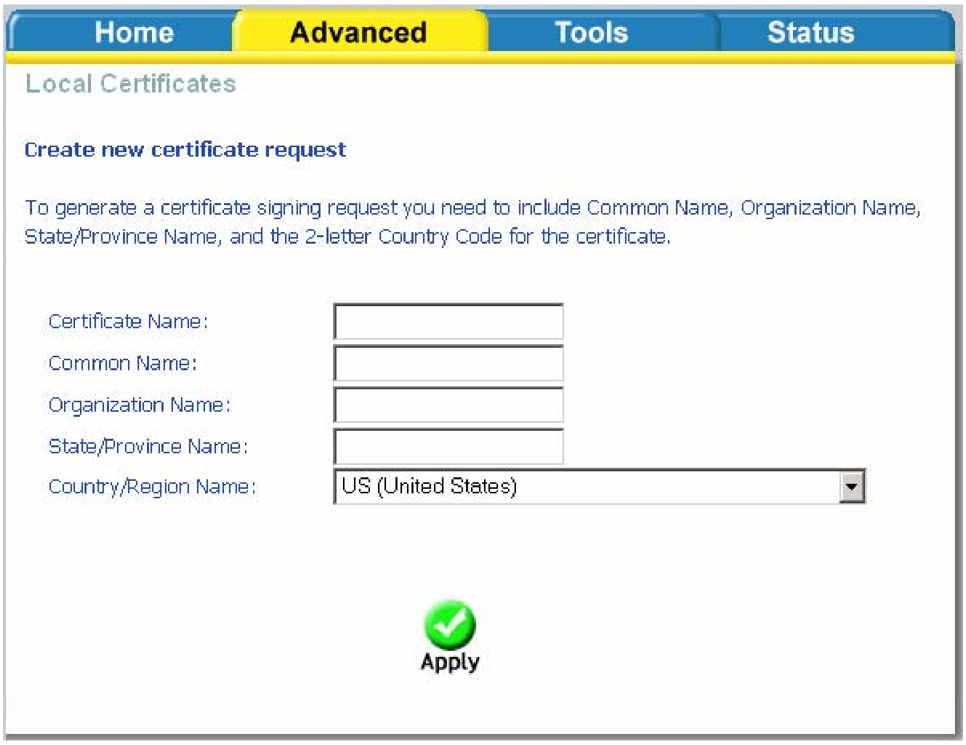
Local Certificates

Add, View or Remove certificates from this page.
Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

If you need to create a certificate request, enter the following information—

- Certificate name
- Common name
- Organization name
- State/province name
- Country/region name.



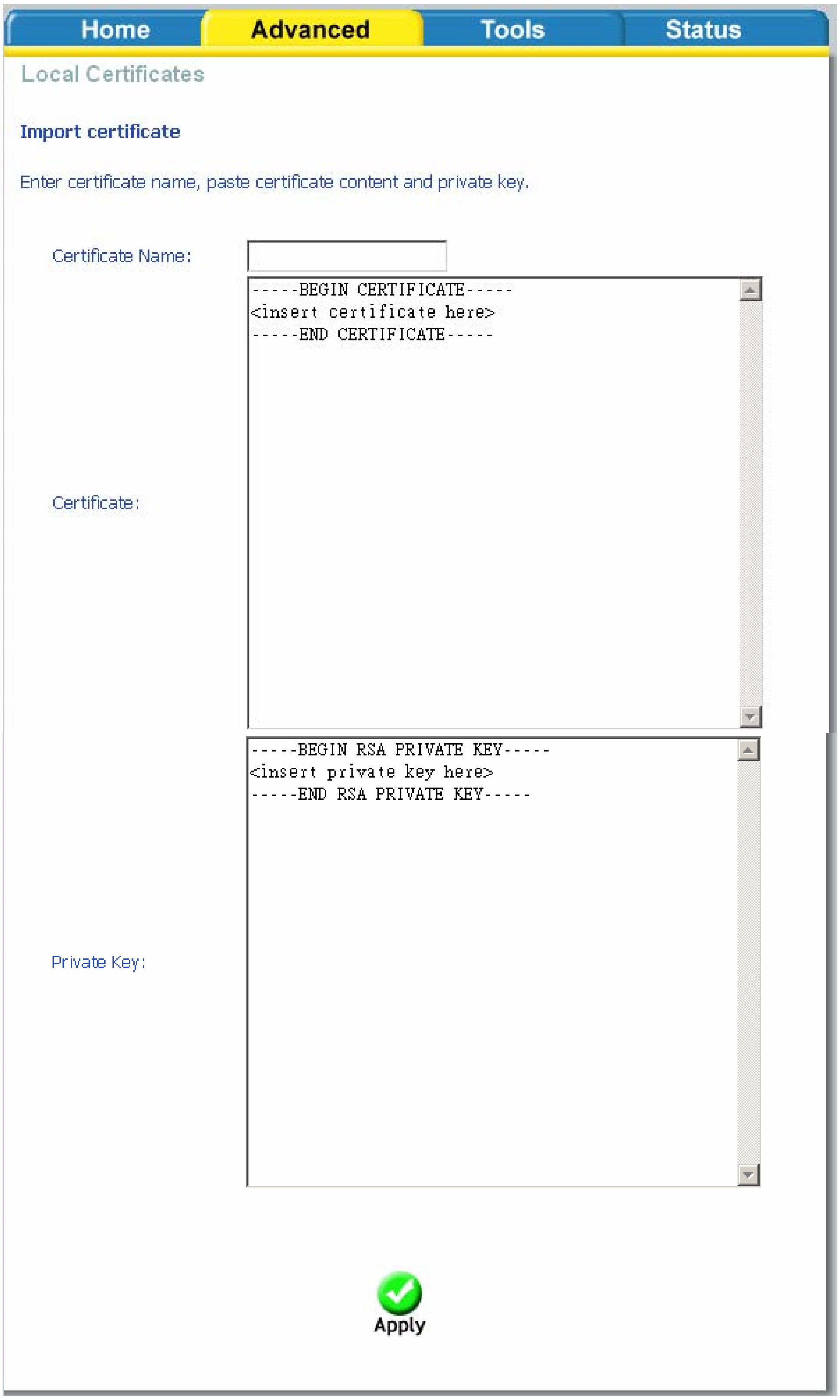
Local Certificates

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:	
Common Name:	
Organization Name:	
State/Province Name:	
Country/Region Name:	US (United States)

If you already have a certificate, then you can simply import the certificate by pasting the certificate content and private key into the space provided. Click **Apply** to submit the request to import the certificate.



Local Certificates

Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

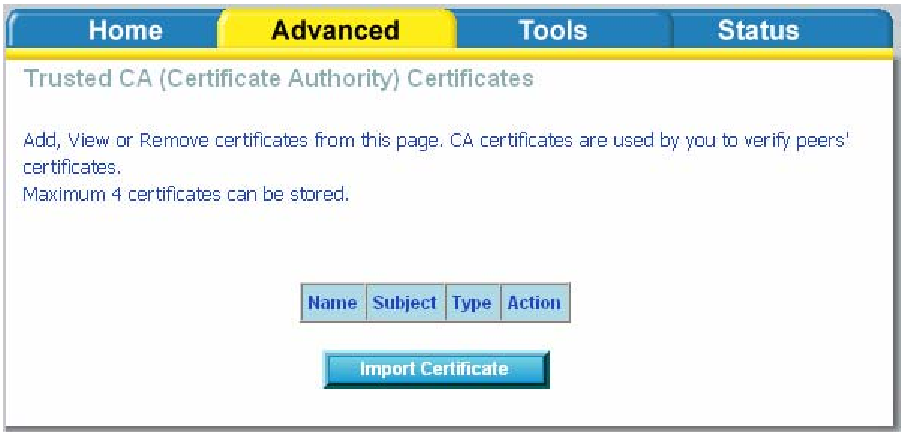
```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

Trusted CA

The trusted certificate authority (CA) allows you to verify the certificates of your peers. Note that you can store up to 4 certificates. The below screen also allows you to view the CA's that you may have already added and can be removed. Click on **Import Certificate** to continue to the next screen.

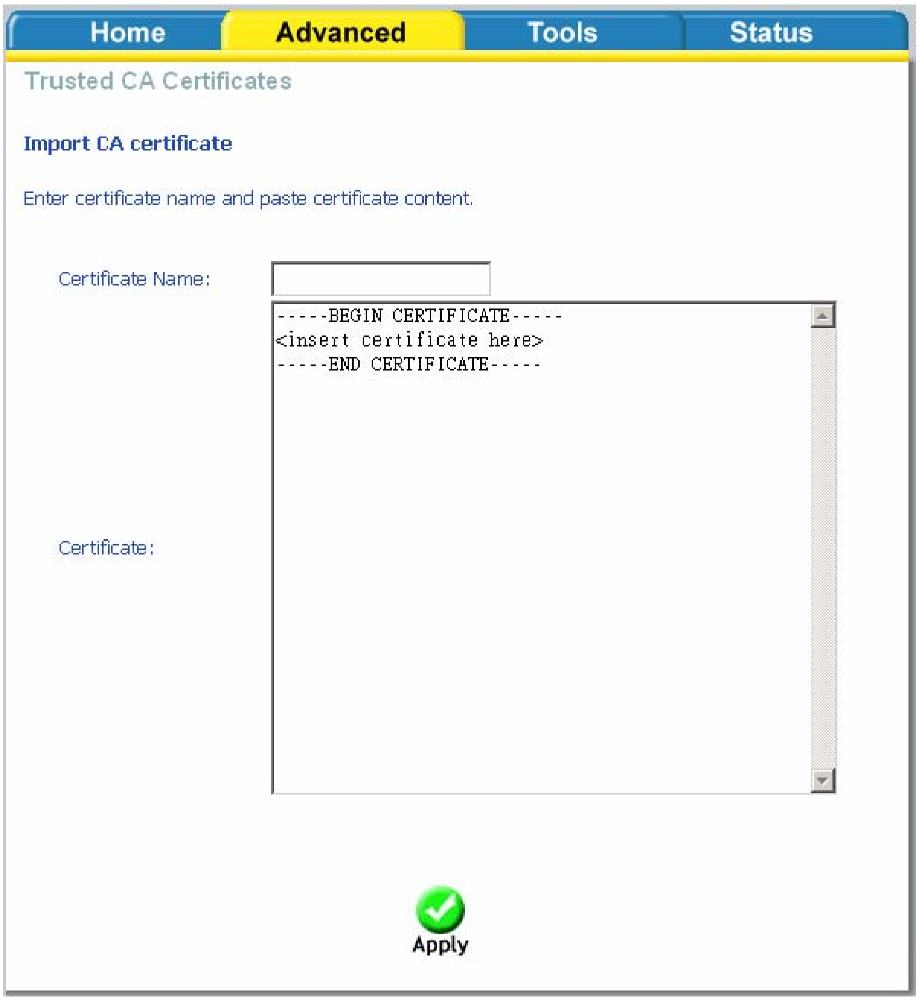


Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.

Name	Subject	Type	Action

Paste the content of the certificate that you wish to add and click **Apply**.



Trusted CA Certificates

Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

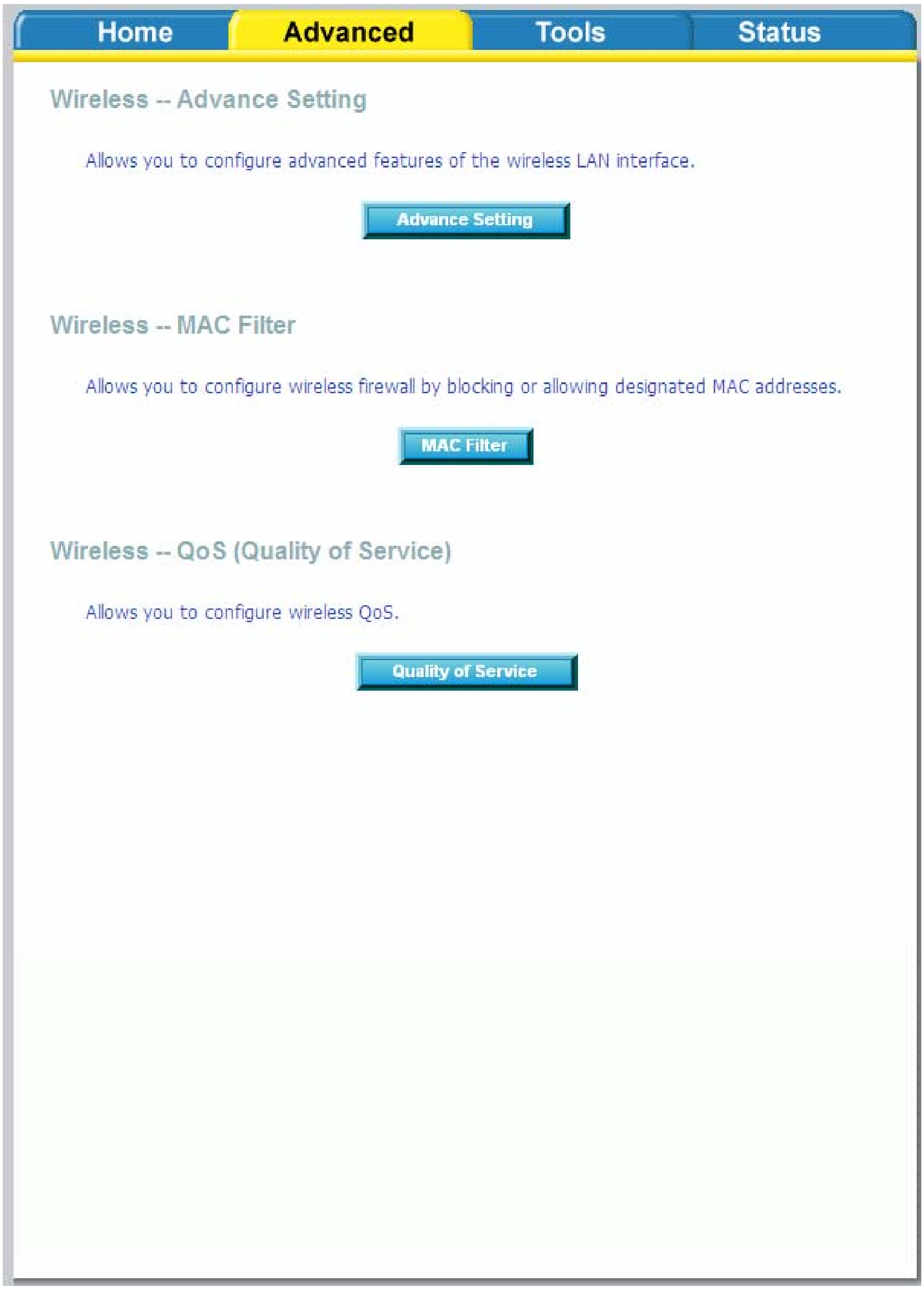
Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Wireless

The Wireless section under Advanced contains three sections for further configurations. Sections include—

- Advanced Settings
- MAC Filter
- Bridge
- QoS (Quality of Service)



Wireless -- Advance Setting

Allows you to configure advanced features of the wireless LAN interface.

Wireless -- MAC Filter

Allows you to configure wireless firewall by blocking or allowing designated MAC addresses.

Wireless -- QoS (Quality of Service)

Allows you to configure wireless QoS.

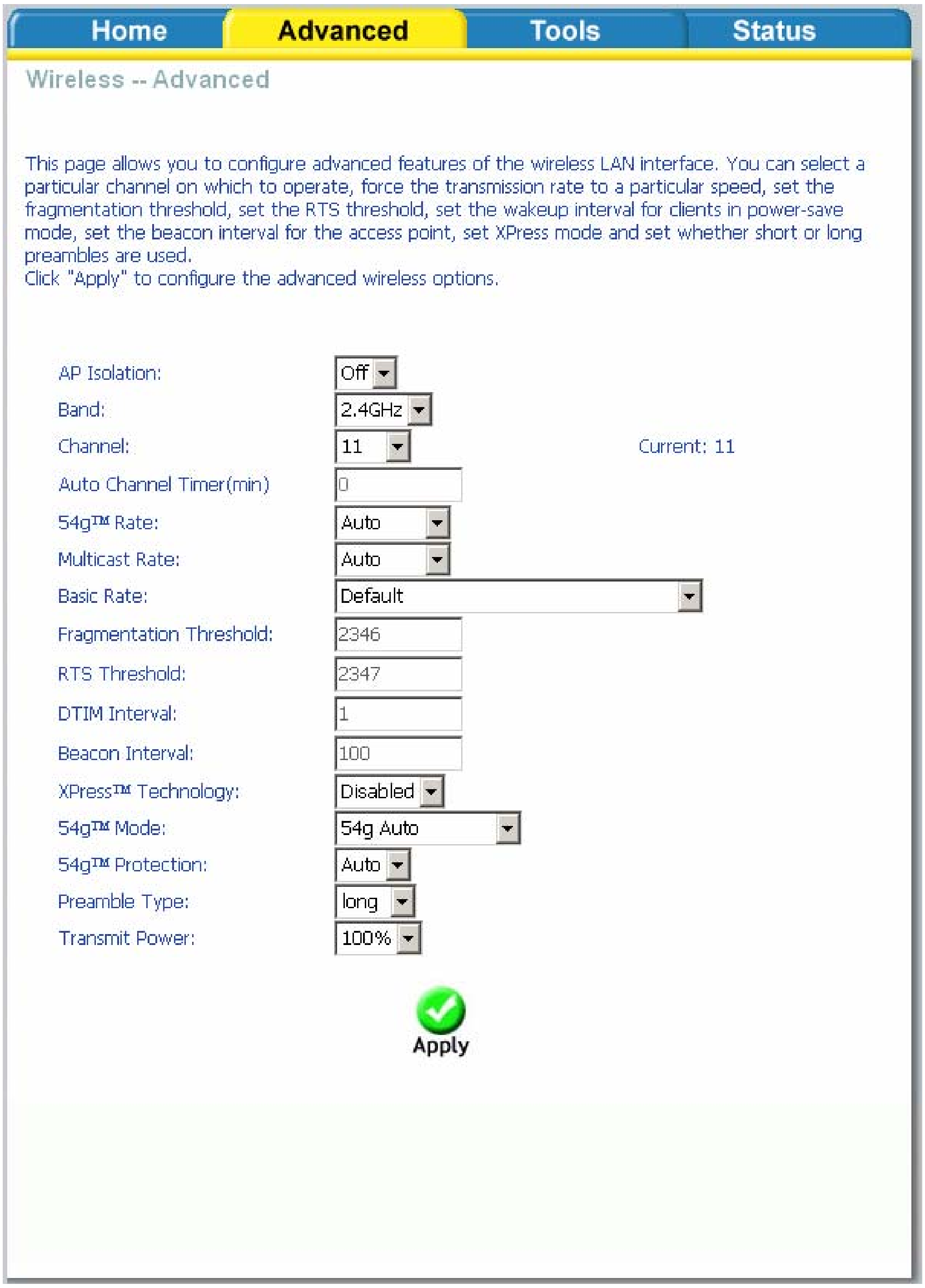
Wireless—Advance Setting

Advanced features of the wireless LAN interface can be configured in this section.

Settings can be configured for the following—

- **AP Isolation**—if you select enable, then each of your wireless clients will not be able to communicate with each other.
- **Band**—a default setting at 2.4GHz - 802.11g
- **Channel**—802.11b and 802.11g use channels to limit interference from other devices. If you are experiencing interference with another 2.4Ghz device such as a baby monitor, security alarm, or cordless phone, then change the channel on your router.
- **54g^{TM} Rate**—the wireless link rate at which information will be received and transmitted on your wireless network.
- **Multicast Rate**—the rate at which a message is sent to a specified group of recipients.
- **Basic Rate**—the set of data transfer rates that all the stations will be capable of using to receive frames from a wireless medium.
- **Fragmentation Threshold**—used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.
- **RTS Threshold (Request to Send Threshold)**—determines the packet size of a transmission through the use of the router to help control traffic flow.
- **DTIM Interval**—sets the Wake-up interval for clients in power-saving mode.
- **Beacon Interval**—a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).
- **Xpress Technology—**a technology that utilizes standards based on framebursting to achieve higher throughput. With Xpress Technology enabled, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by up to 25% in 802.11g only networks and up to 75% in mixed networks comprised of 802.11g and 802.11b device.
- **54g Mode—** 54g is a Broadcom Wi-Fi technology.
- **54g Protection**—the 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS (Request to Send / Clear to Send) to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
- **Preamble Type**— this is the length of the CRC (Cyclic Redundancy Check) block for communication between the router and wireless clients. High network traffic areas should select Short preamble type.

- **Transmit Power**— this is the percentage of power that should be transmitted from your wireless router. Select from 20%, 40%, 60%, 80%, and 100%.



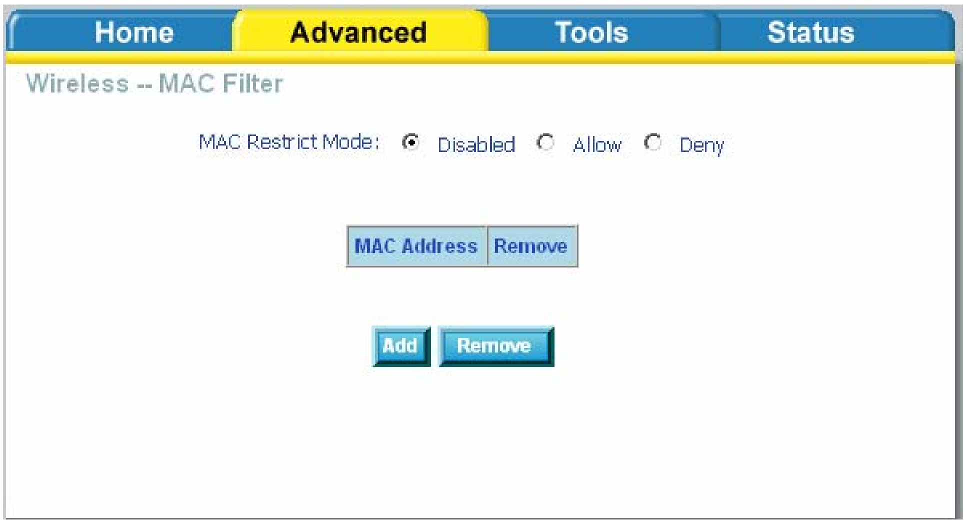
Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply" to configure the advanced wireless options.

AP Isolation:	Off	
Band:	2.4GHz	
Channel:	11	Current: 11
Auto Channel Timer(min)	0	
54g™ Rate:	Auto	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
XPress™ Technology:	Disabled	
54g™ Mode:	54g Auto	
54g™ Protection:	Auto	
Preamble Type:	long	
Transmit Power:	100%	

Wireless—MAC Filter

The MAC Filter feature allows you to disable, allow or deny users access to the wireless router based on their MAC address. To add MAC addresses, click on **Add** to continue. Click on **Remove** if you want to take out a MAC address from the MAC filter list.

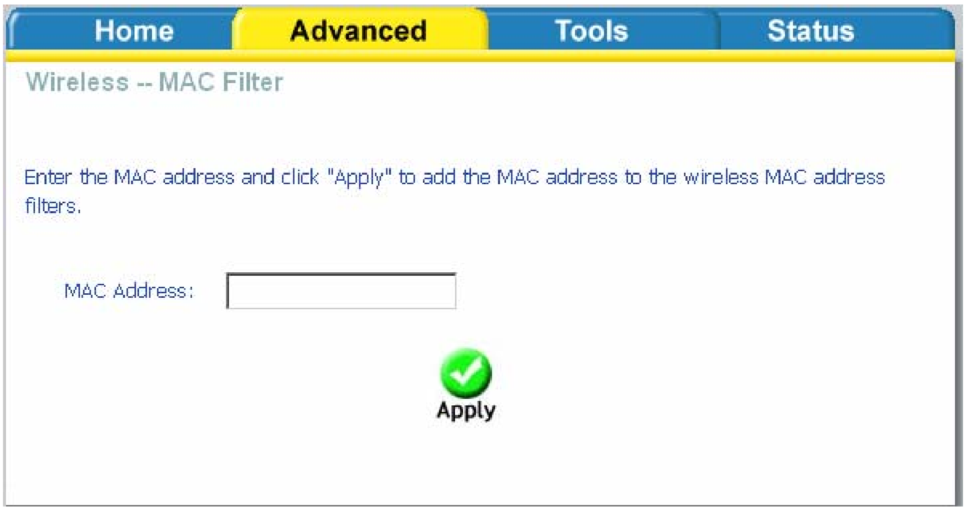


Wireless -- MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

The MAC filter screen allows you to manage MAC address filters. Add the MAC addresses that you want to manage and then select the mode that you want to use to manage them. You can disable this feature or you can allow or deny access to the MAC addresses that you add to the list.



Wireless -- MAC Filter

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

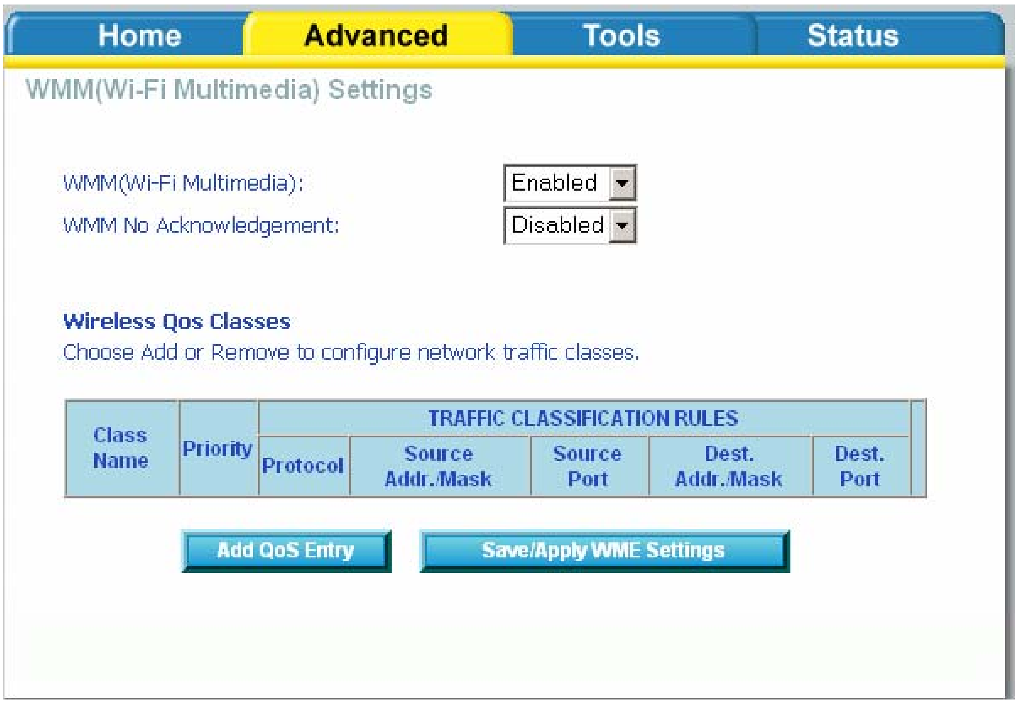
MAC Address:

Wireless—QoS

WMM (Wi-Fi Multimedia) technology is available on the wireless router, allowing you to give multimedia applications a higher quality of service and priority in a wireless network so applications such as videos will be of higher quality. Enabling WMM may delay the network traffic of other lower assigned quality applications.

WMM No Acknowledgement can be enabled if you enable WMM which refers to the acknowledgement policy used at the MAC level.

To create a QoS entry, click the **Add QoS Entry** button to proceed to add or remove traffic class rules for your network. Click on **Save/Apply WME Settings**.



WMM(Wi-Fi Multimedia) Settings

WMM(Wi-Fi Multimedia): Enabled

WMM No Acknowledgement: Disabled

Wireless Qos Classes

Choose Add or Remove to configure network traffic classes.

Class Name	Priority	TRAFFIC CLASSIFICATION RULES					
		Protocol	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	

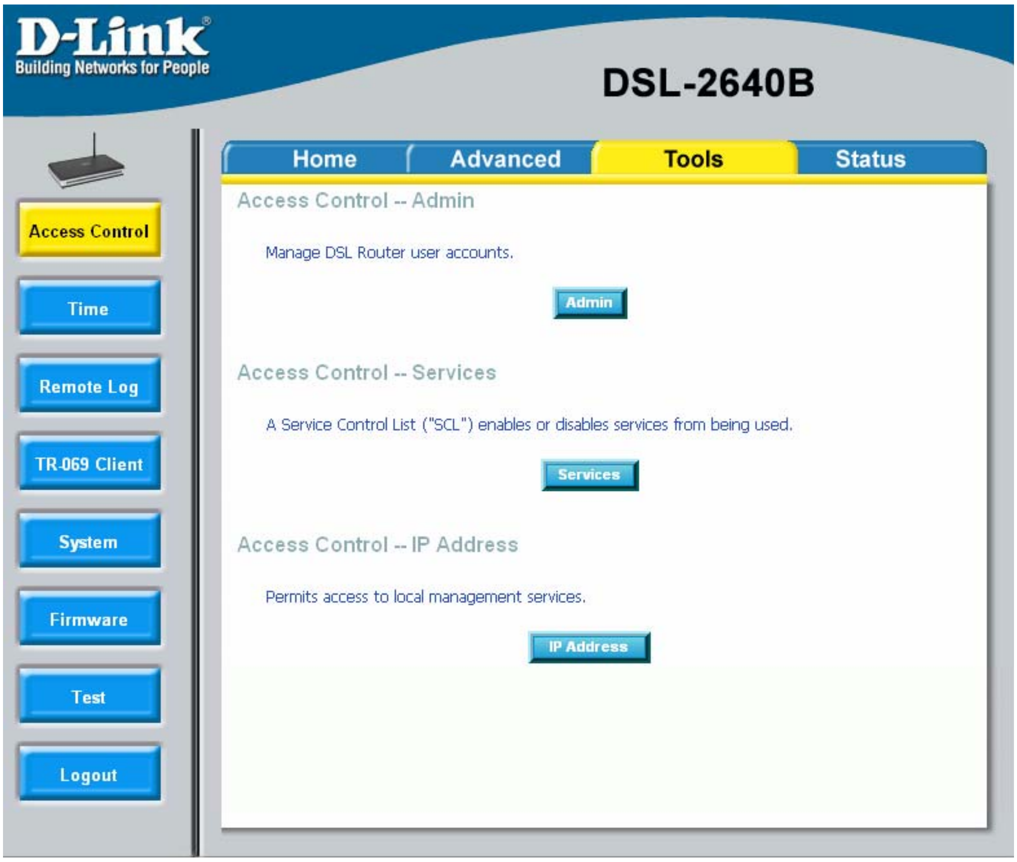
Tools

The tools section contains various administrator functions to maintain your router. Sections include the following—Admin, Time, Remote Log, System, Firmware, and Test.

- **Admin:** Allows you to change the password for the various user names available
- **Time:** Allows you to set the router's time
- **Remote Log:** Allows you to view logs of the router's activities
- **System:** Allows you to perform functions such as save / reboot, backup, update settings, and restore default settings
- **Firmware:** Allows you to upgrade your router with new available firmware versions
- **Test:** Allows you to view test information for your Internet connection

Access Control

You can enable or disable some services of your router by LAN or WAN. If no WAN connection is defined, only the LAN side can be configured.



Access Control -- Admin

Manage DSL Router user accounts.

Access Control -- Services

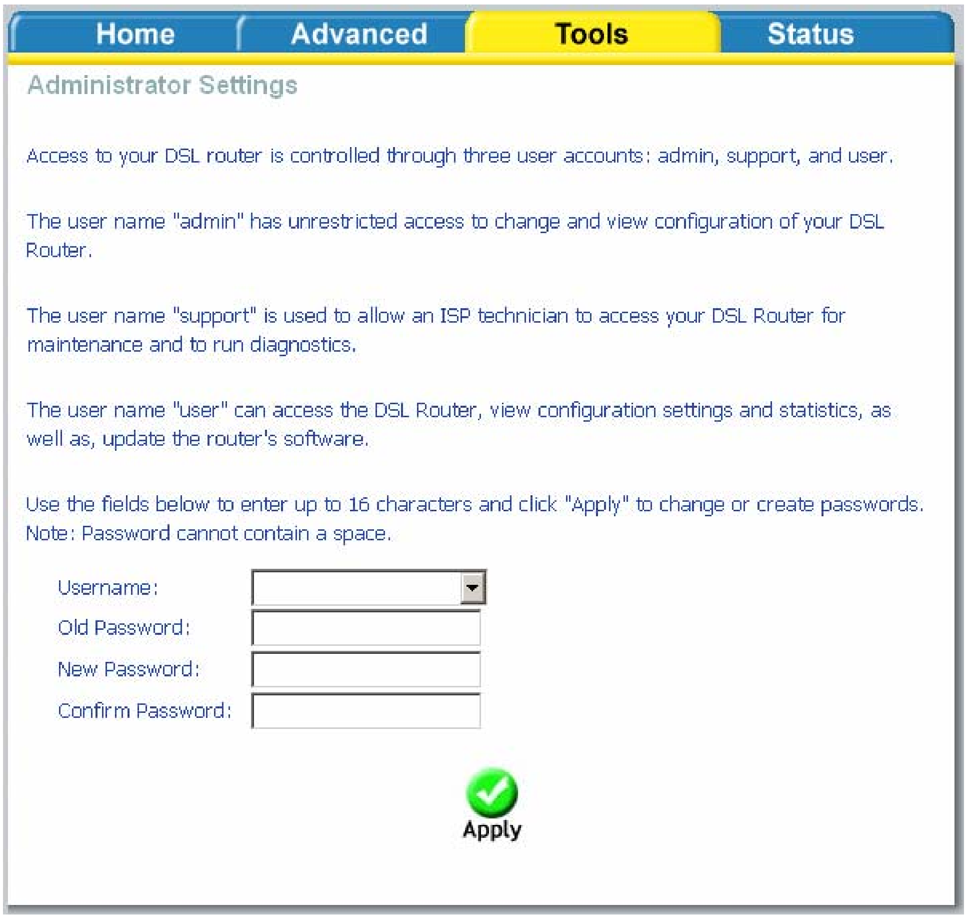
A Service Control List ("SCL") enables or disables services from being used.

Access Control -- IP Address

Permits access to local management services.

Access Control—Admin

Three user names and passwords—**admin**, **support**, and **user**—can be used to control your router. The passwords for these user names can be changed on the following screen. Enter the user name followed by the old password and the new password that you wish to change to.



Administrator Settings

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

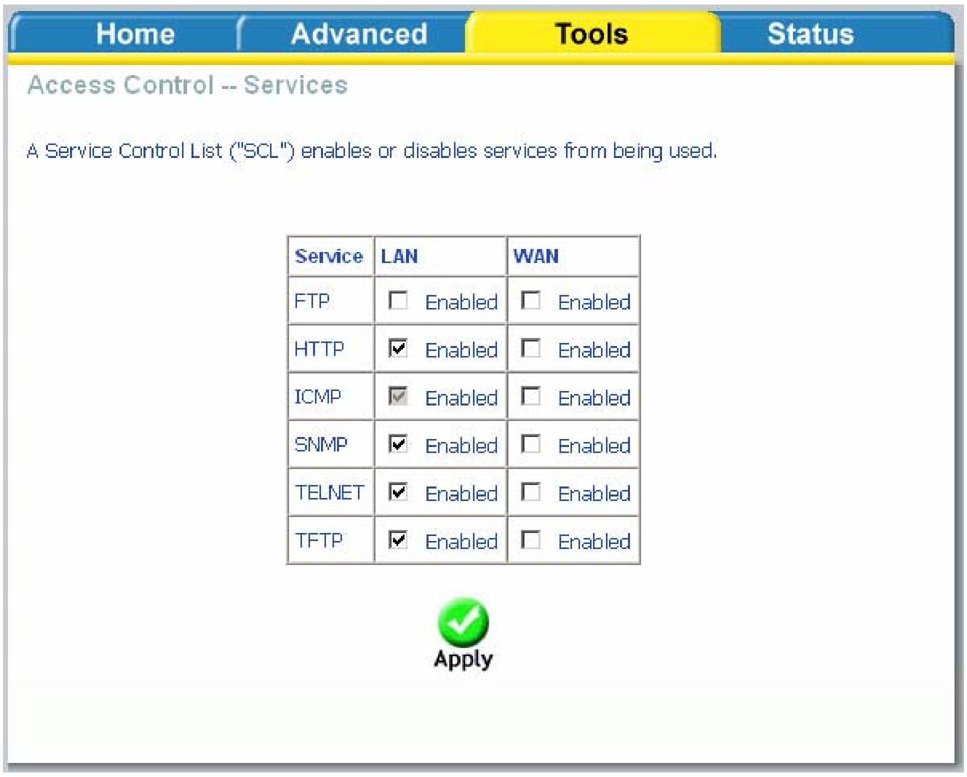
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:	
Old Password:	
New Password:	
Confirm Password:	

Access Control—Services

Services that can be enabled / disabled on the LAN / WAN are FTP, HTTP, ICMP, SNMP, Telnet, and TFTP.



Access Control -- Services

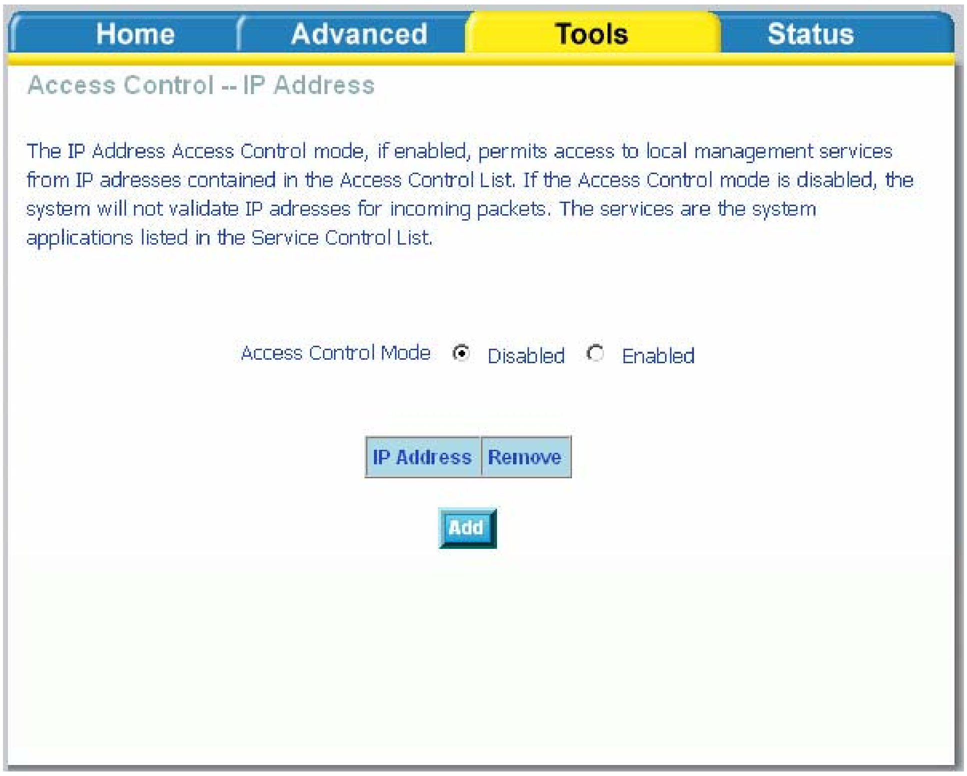
A Service Control List ("SCL") enables or disables services from being used.

Service	LAN	WAN
FTP	□ Enabled	□ Enabled
HTTP	☑ Enabled	□ Enabled
ICMP	☑ Enabled	□ Enabled
SNMP	☑ Enabled	□ Enabled
TELNET	☑ Enabled	□ Enabled
TFTP	☑ Enabled	□ Enabled

Access Control—IP Address

Web access to the router can be limited when Access Control Mode is enabled. The IP addresses of allowed hosts can be added using Access Control→IP Address.

Add the IP address to the IP address list by clicking on the **Add** button, then select "**Enabled**" to enable Access Control Mode.



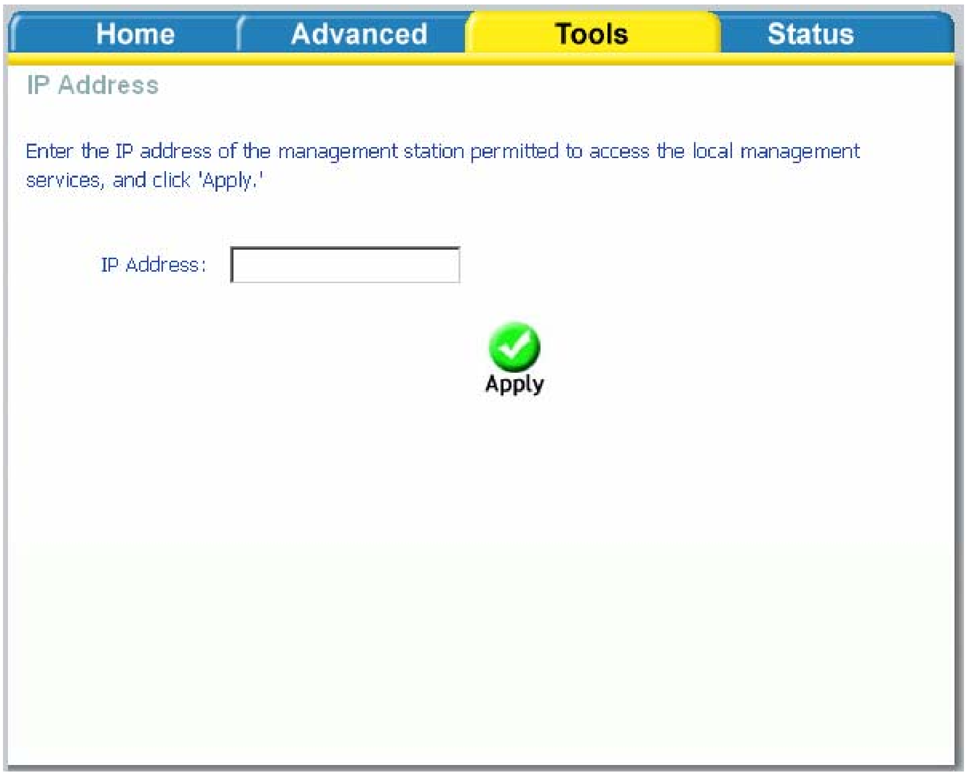
Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP adresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP adresses for incoming packets. The services are the system applications listed in the Service Control List.

Access Control Mode ● Disabled ○ Enabled

IP Address	Remove

To assign the IP address of the management station that is permitted to access the local management services, enter the IP address in the box and click on the **Apply** button.



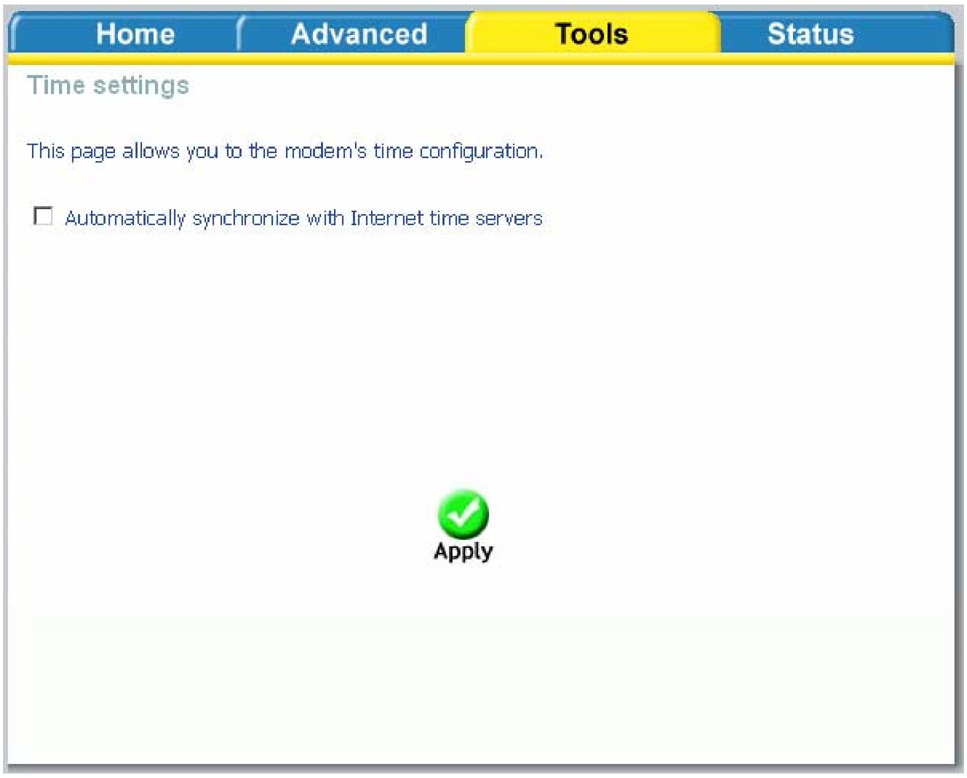
IP Address

Enter the IP address of the management station permitted to access the local management services, and click 'Apply.'

IP Address:

Time

The Time Settings page allows you to automatically synchronize your time with a time server on the Internet.

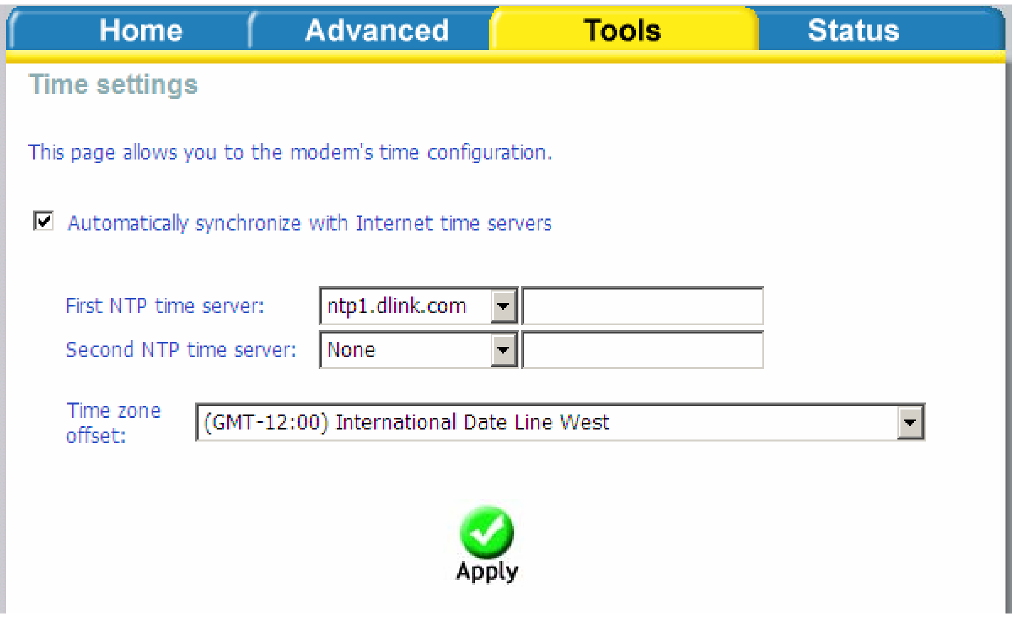


Time settings

This page allows you to the modem's time configuration.

□ Automatically synchronize with Internet time servers

If you choose to set the router's time, click on the "automatically synchronize with Internet time servers" checkbox and the below fields appear.



Time settings

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

First NTP time server: ntp1.dlink.com

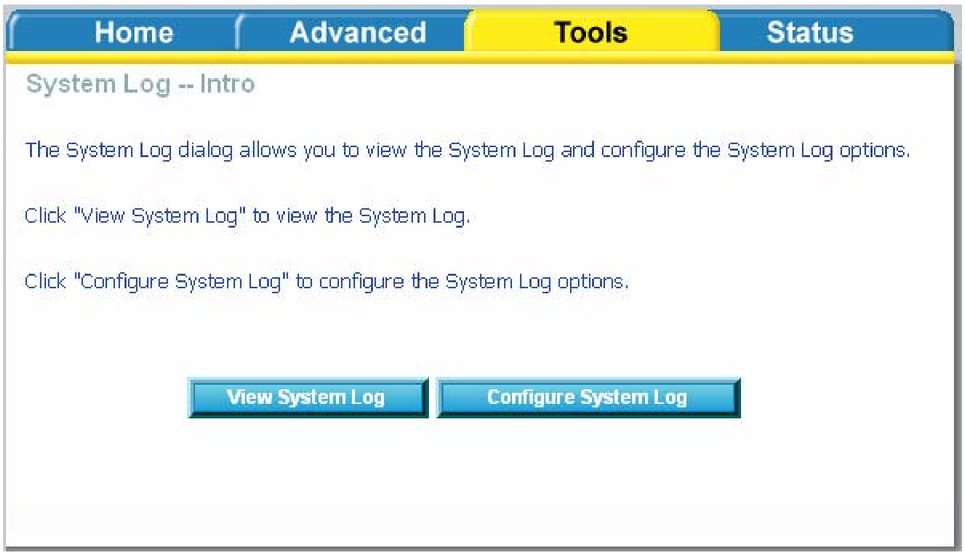
Second NTP time server: None

Time zone offset: (GMT-12:00) International Date Line West

Select from the list of NTP (Network Time Protocol) time servers. Then select the time zone that you are in and click on **Apply** to save.

Remote Log

The Log dialog allows you to view and configure the log. To view the log, click on the **View System Log** button.



System Log -- Intro

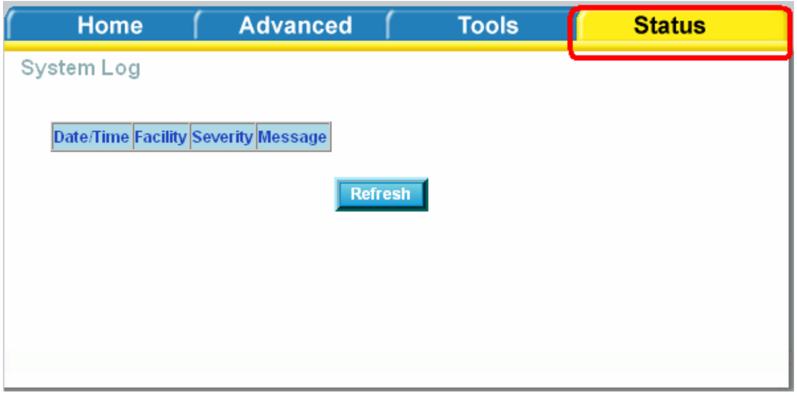
The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

Below is the **System Log** screen which shows the date/time of the log, the facility that was logged, the severity level and the log message. Click on **Refresh** to view any new information that is logged.

System Log when log mode is DISABLED →

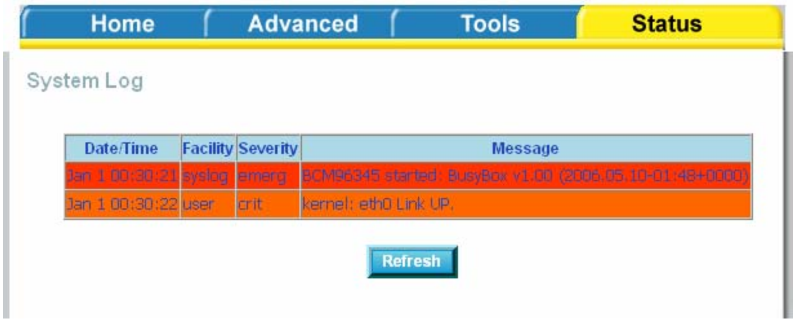


System Log

Date/Time	Facility	Severity	Message

⚠ ***NOTE:*** *When you click on the* ***View System Log*** *button, the* ***System Log*** *screen that you access will be located under the* ***Status*** *section (see screen on left). To return to the previous screen to configure system log, remember to click on the* ***Tools*** *tab (located on top row) first and then click on* ***Remotelog****.*

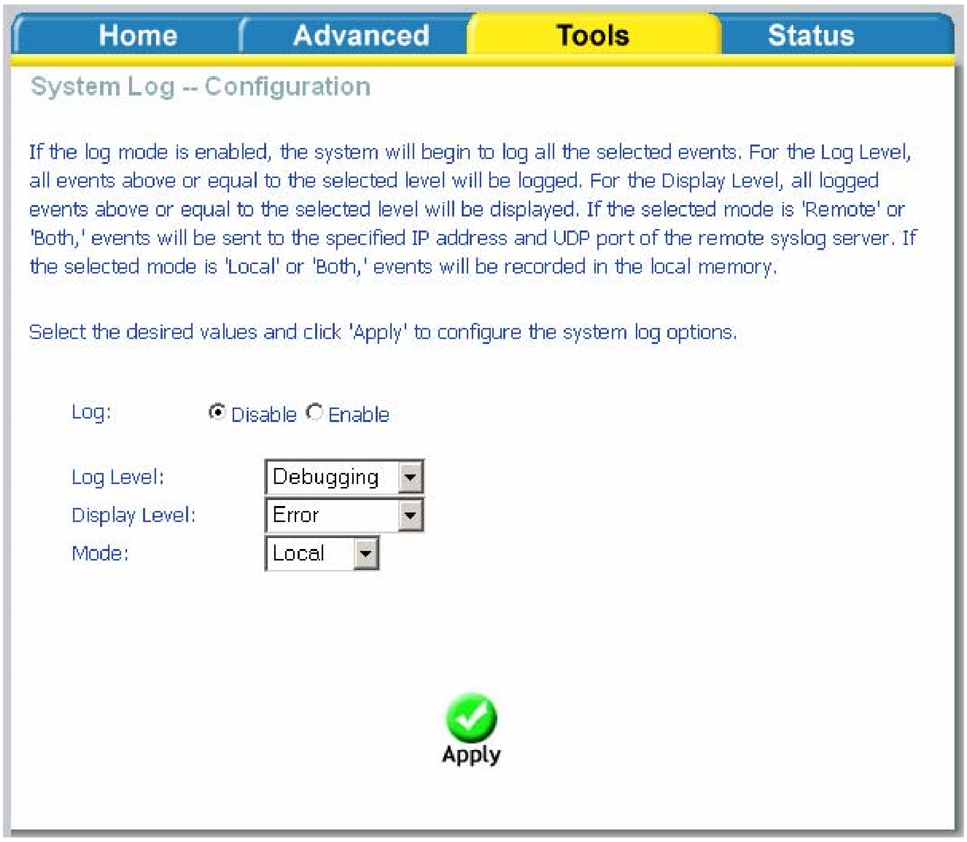
System Log when log mode is ENABLED →



System Log

Date/Time	Facility	Severity	Message
Jan 1 00:30:21	syslog	emerg	BCM96345 started: BusyBox v1.00 (2006.05.10-01:48+0000)
Jan 1 00:30:22	user	crit	kernel: eth0 Link UP.

To configure the system log settings, click on the **Configure System Log** button to view the following screen.



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply' to configure the system log options.

Log: ● Disable ○ Enable

Log Level: Debugging

Display Level: Error

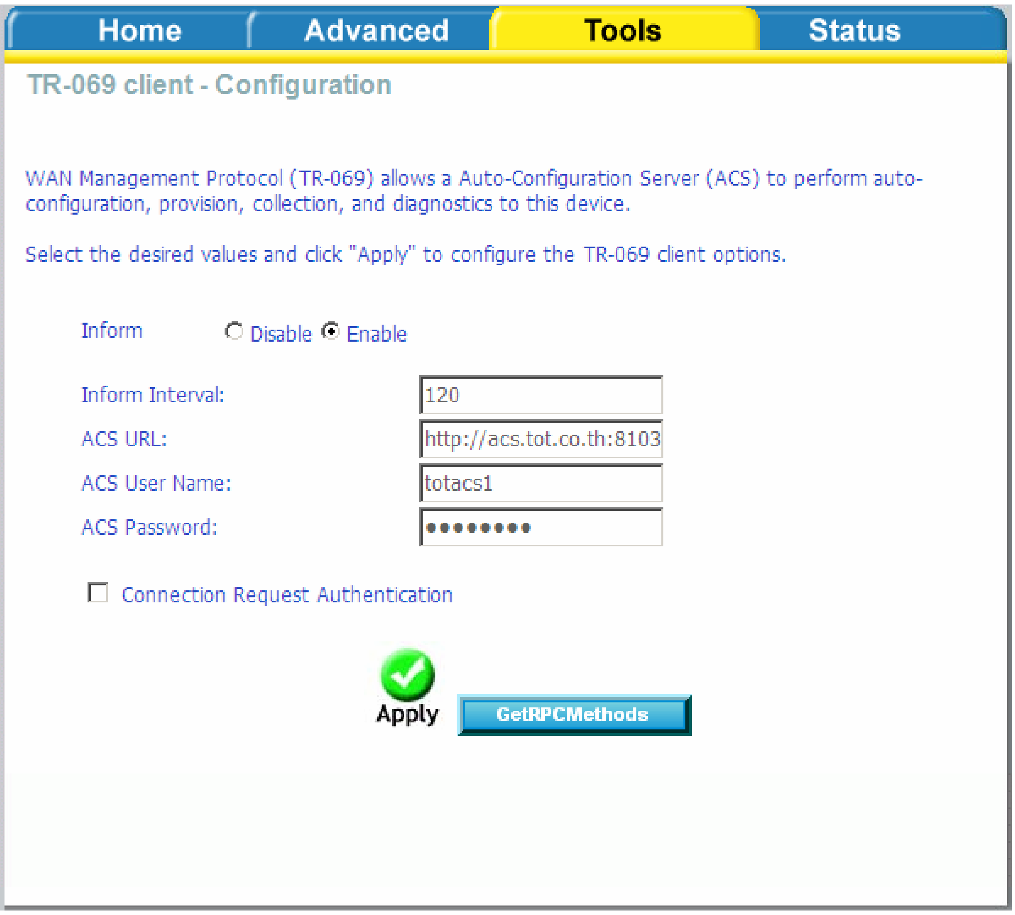
Mode: Local

If the log is enabled, the system will log selected events including *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Informational*, and *Debugging*. All events above or equal to the selected log level will be logged and displayed.

If the selected mode is “Remote” or “Both”, events will be sent to the specified IP address and UDP port of a remote system log server. If the selected mode is “Local” or “Both”, events will be recorded in the local memory. Select the desired values and click on **Apply** to configure the system log options.

TR-069 Client

The router includes a TR-069 client, a WAN management protocol. All the values are already filled in. If you wish to enable this protocol, then select *enable*.
If the **Connection Request Authentication** checkbox is checked, enter the *Connection Request Username* / *Password*. You must click on the **Apply** button for the setting to take place.



TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

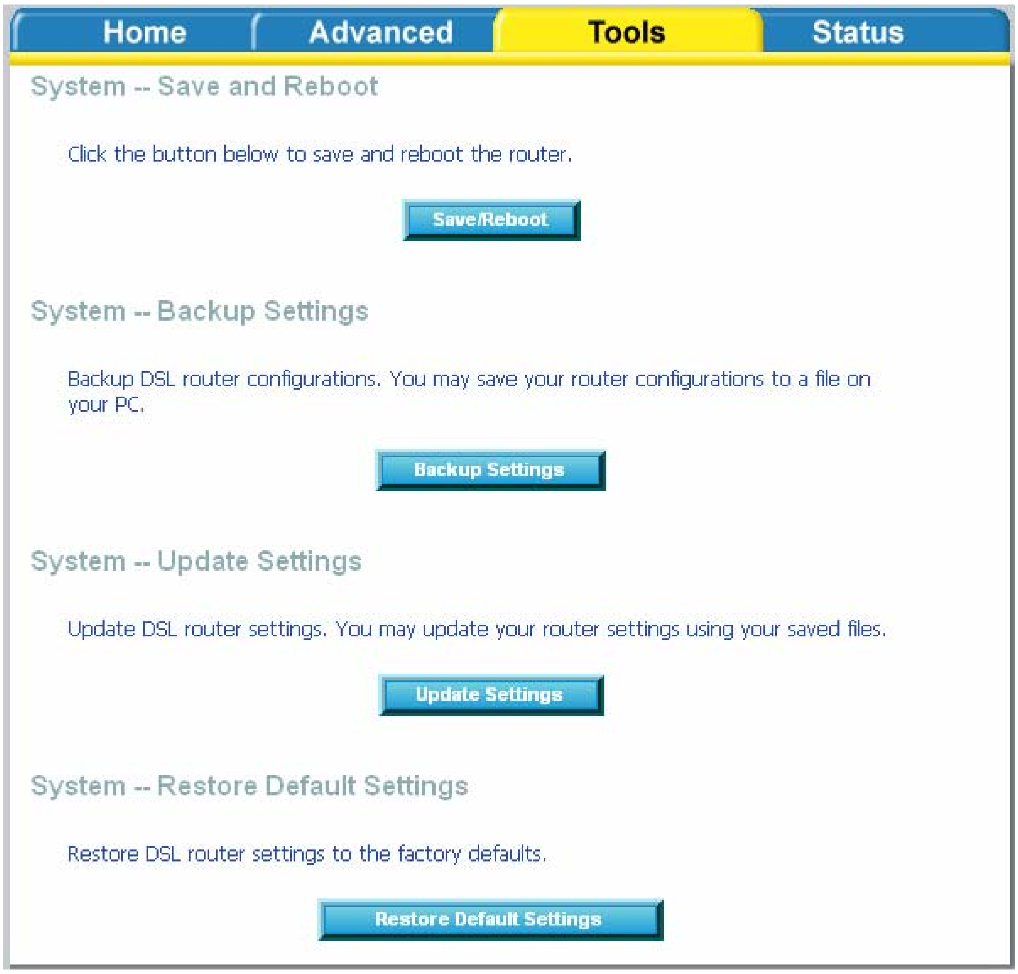
Inform ○ Disable ● Enable

Inform Interval:	120
ACS URL:	http://acs.tot.co.th:8103
ACS User Name:	totacs1
ACS Password:	●●●●●●●●●

□ Connection Request Authentication

System

The system section includes several tools on one page, including save and reboot, backup settings, update settings, and restore default settings.



System -- Save and Reboot

Click the button below to save and reboot the router.

System -- Backup Settings

Backup DSL router configurations. You may save your router configurations to a file on your PC.

System -- Update Settings

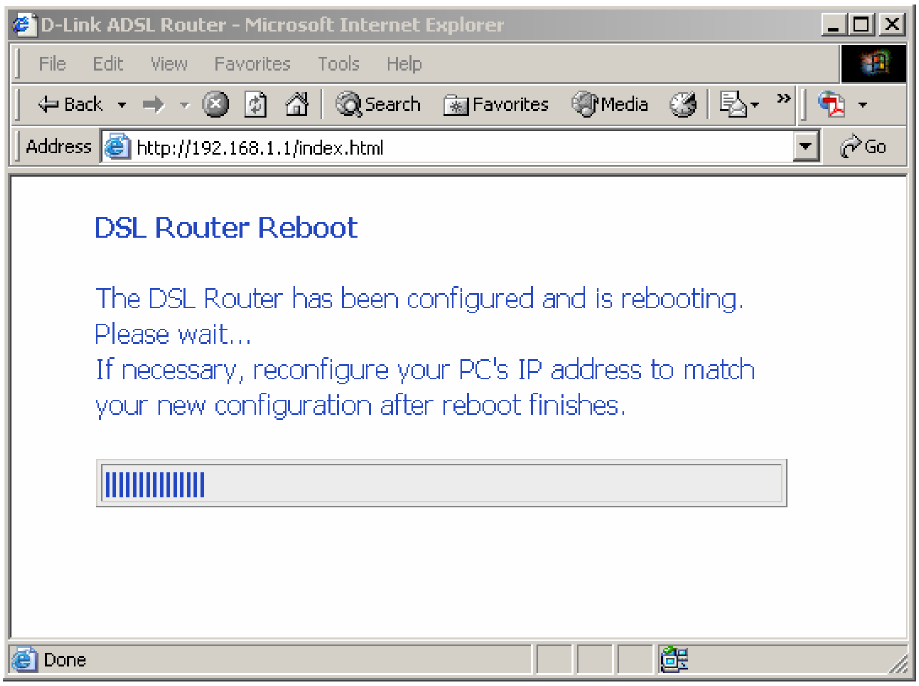
Update DSL router settings. You may update your router settings using your saved files.

System -- Restore Default Settings

Restore DSL router settings to the factory defaults.

Save and Reboot

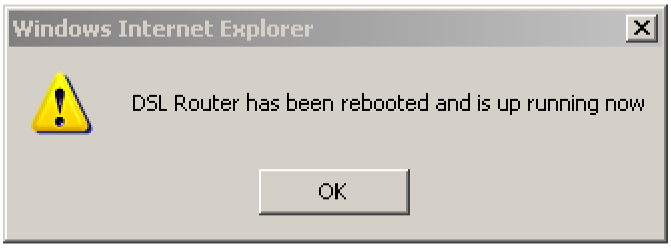
To save all configurations made, click on the **Save/Reboot** button. This will save all your settings and restart the router for the settings to take effect.


D-Link ADSL Router - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/index.html
Go
Done

DSL Router Reboot

The DSL Router has been configured and is rebooting.
Please wait...
If necessary, reconfigure your PC's IP address to match your new configuration after reboot finishes.

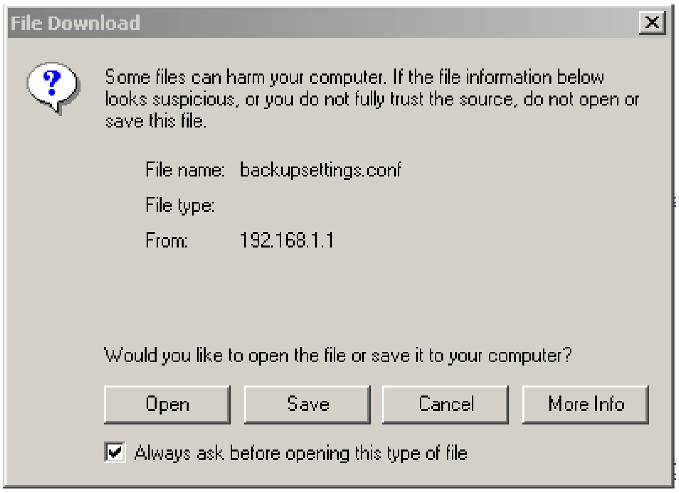
When completed, the below pop-up window will appear confirming that the router has been rebooted.



DSL Router has been rebooted and is up running now

Backup Settings

To save your configurations in a file on your computer so that it may be accessed again later if your current settings are changed, click on the **Backup Settings** button. The below pop-up screen will appear with a prompt to open or save the file to your computer.



Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

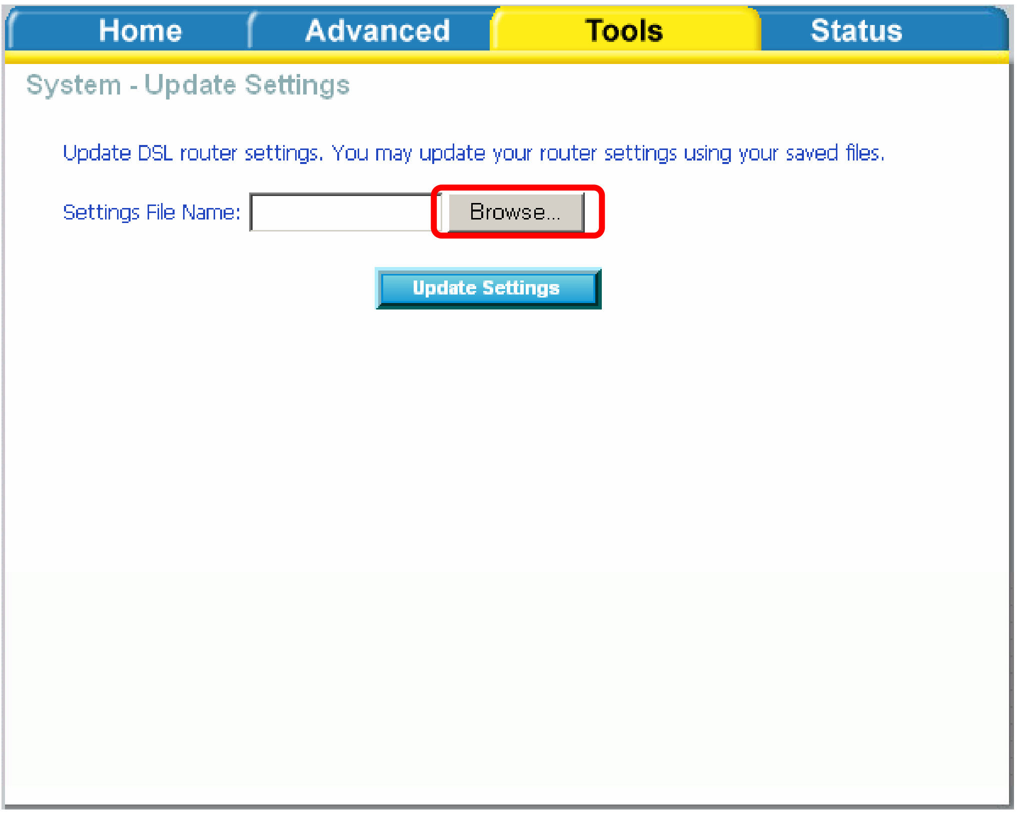
File name: backupsettings.conf
File type:
From: 192.168.1.1

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Update Settings

To load a previously saved configuration file onto your router, click **Browse** and select the file on your computer and then click on **Update Settings**.



System - Update Settings

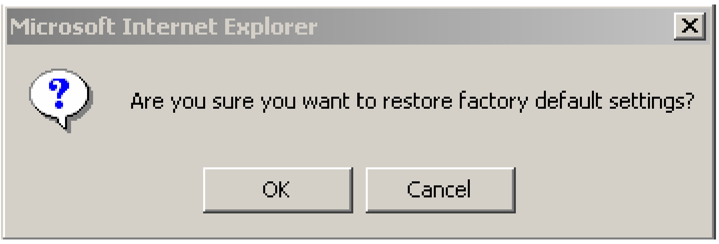
Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

The router will restore settings and reboot to activate the restored settings.

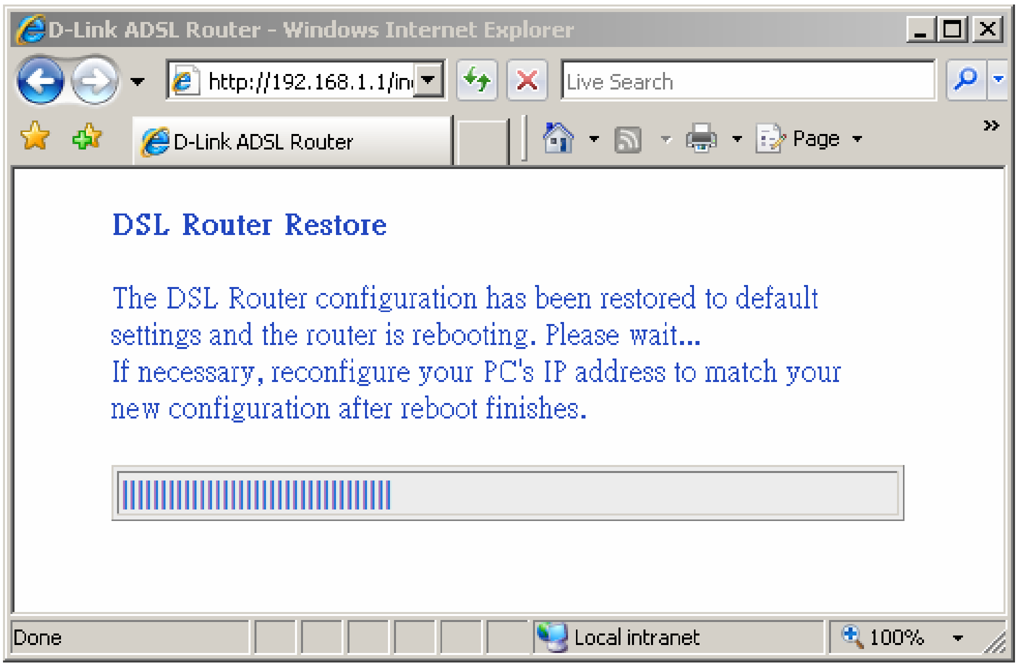
Restore Default Settings

Restore Default will delete all current settings and restore the router to factory default settings. Click on the **Restore Default Settings** button to proceed. The following confirmation dialog will appear confirming your decision to restore default settings. Click on **OK** to continue.



Are you sure you want to restore factory default settings?

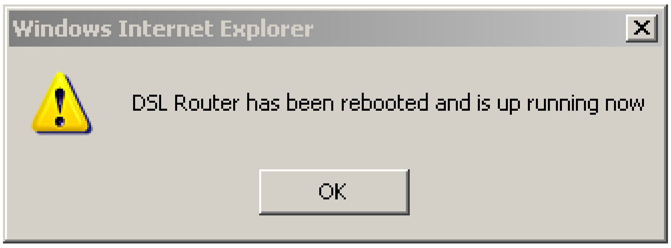
Click on the **OK** button to start. The below screen will appear with the progress of restoring the default settings.



DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting. Please wait...
If necessary, reconfigure your PC's IP address to match your new configuration after reboot finishes.

When completed, the below pop-up window will appear confirming that the router has been rebooted.

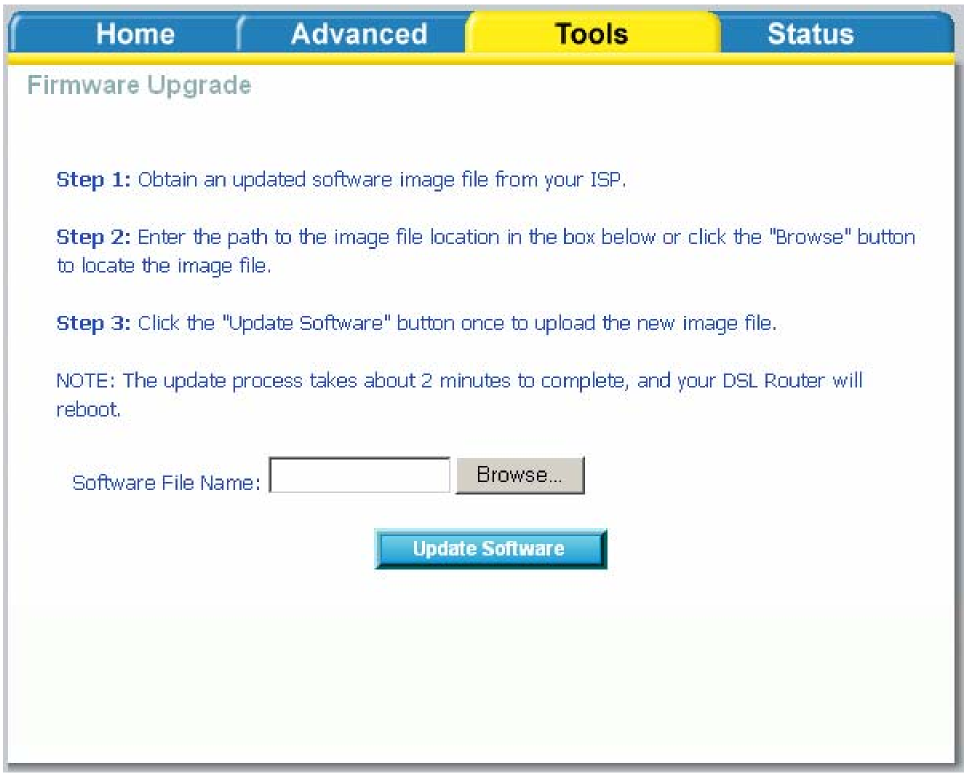


DSL Router has been rebooted and is up running now

Firmware

If your ISP releases new software for this router, follow these steps to perform an upgrade.

1. Obtain an updated software image file from your ISP.
2. Enter the path to the image file location or click on the **Browse** button to locate the image file.
3. Click the **Update Software** button once to upload the new image file.



Firmware Upgrade

Step 1: Obtain an updated software image file from your ISP.

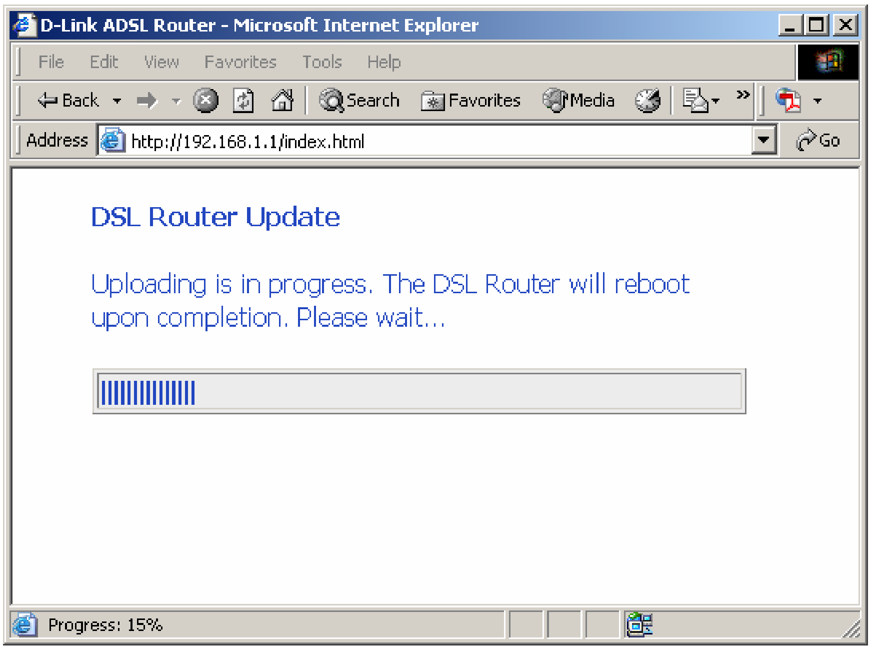
Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

The below page will appear when you click on the **Update Software** button.

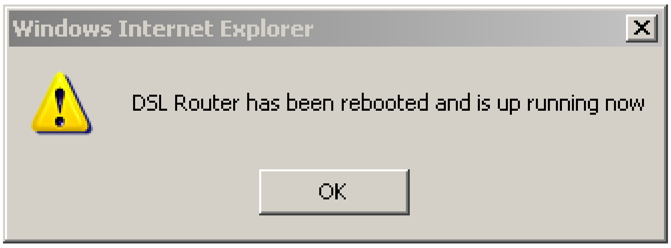

D-Link ADSL Router - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/index.html
Go

DSL Router Update

Uploading is in progress. The DSL Router will reboot upon completion. Please wait…

Progress: 15%

When completed, the below pop-up window will appear confirming that the router has been rebooted.



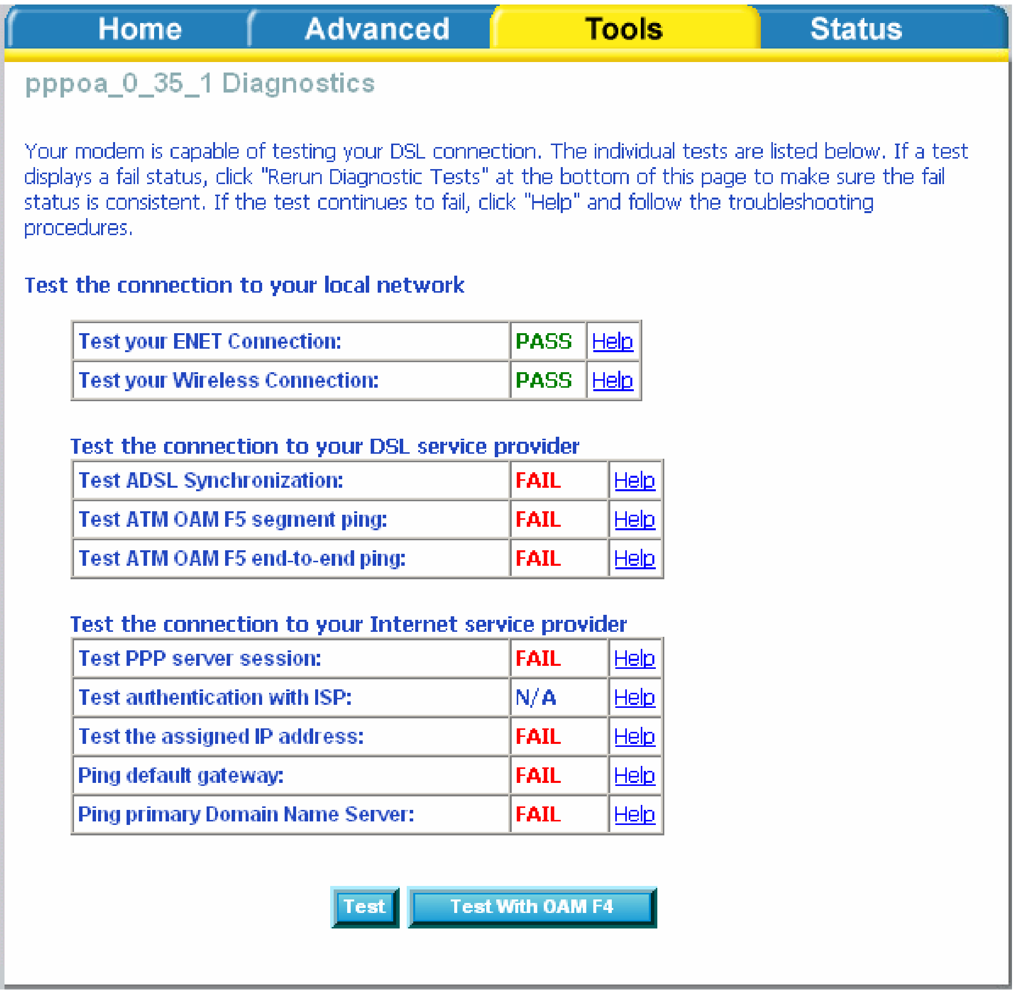
DSL Router has been rebooted and is up running now

Test

The diagnostics screen allows you to run diagnostic tests to check your DSL connection. The results will show test results of three connections—

- Connection to your local network
- Connection to your DSL service provider
- Connection to your Internet service provider

There are three buttons at the bottom of the page—**Next Connection** (appears only if you have created more than one connection)**, Test** and **Test with OAM F4**—which will allow you to retest if necessary.



pppoa_0_35_1 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ENET Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	FAIL	Help
Test ATM OAM F5 end-to-end ping:	FAIL	Help

Test the connection to your Internet service provider

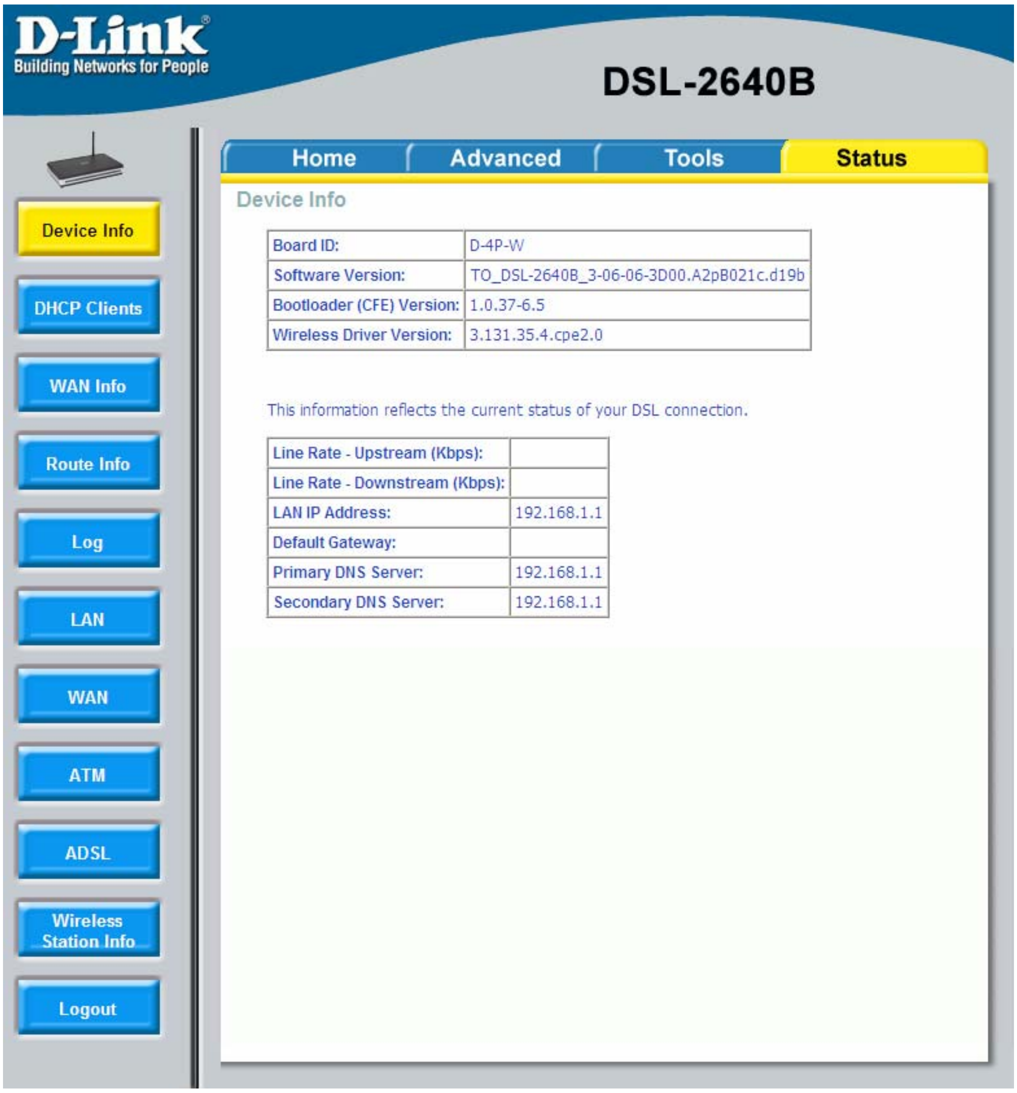
Test PPP server session:	FAIL	Help
Test authentication with ISP:	N/A	Help
Test the assigned IP address:	FAIL	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

Status

The status section allows you to view general and status information for your router’s connection.

Device Info

It shows details of the router such as the version of the software, bootloader, LAN IP address, etc. It also displays the current status of your DSL connection as shown below—



Device Info

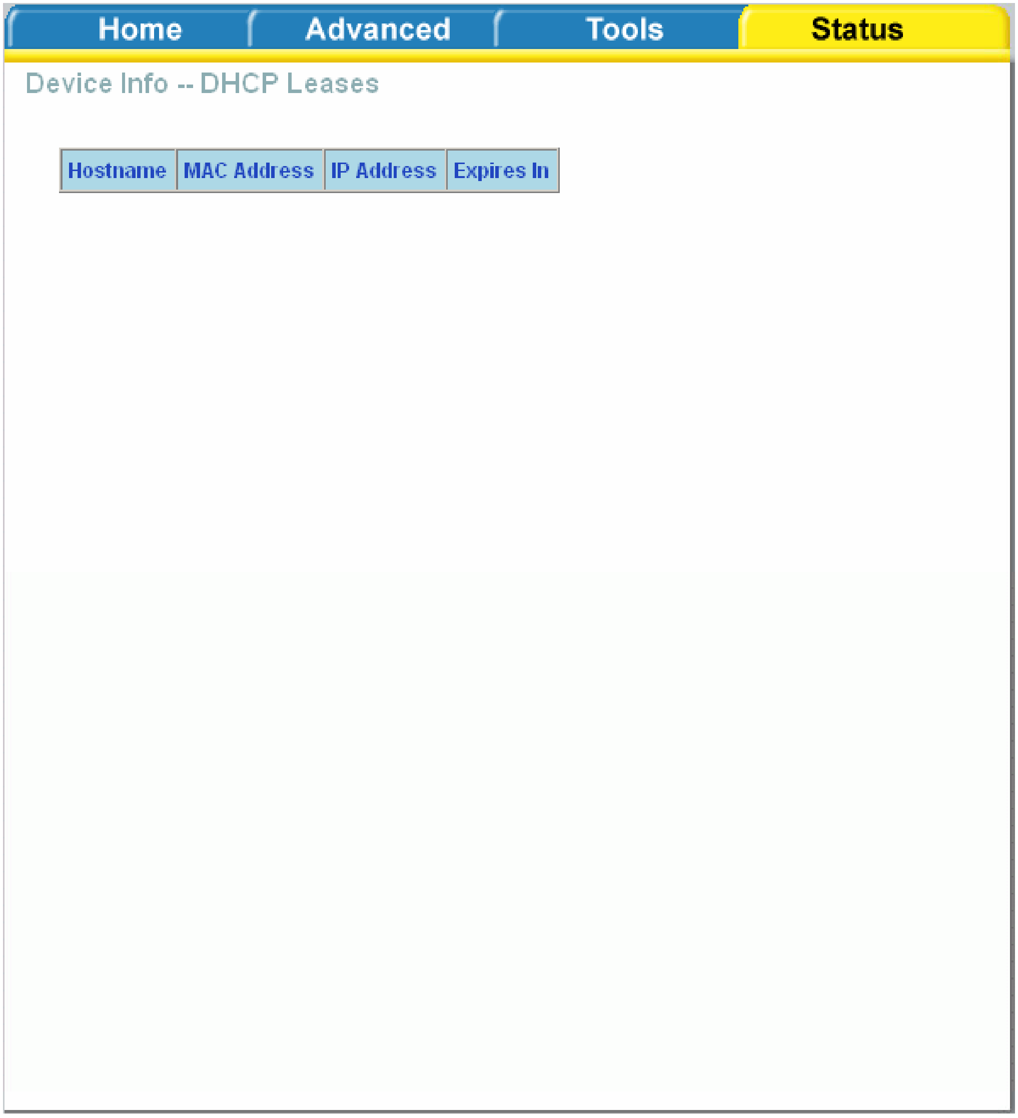
Board ID:	D-4P-W
Software Version:	TO_DSL-2640B_3-06-06-3D00.A2pB021c.d19b
Bootloader (CFE) Version:	1.0.37-6.5
Wireless Driver Version:	3.131.35.4.cpe2.0

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

DHCP Clients

Access the DHCP Leases screen by clicking “**DHCP**” under “**Statistics**”. This shows the computers, identified by the hostname and MAC address that have acquired IP addresses by the DHCP server with the time that the lease for the IP address is up.

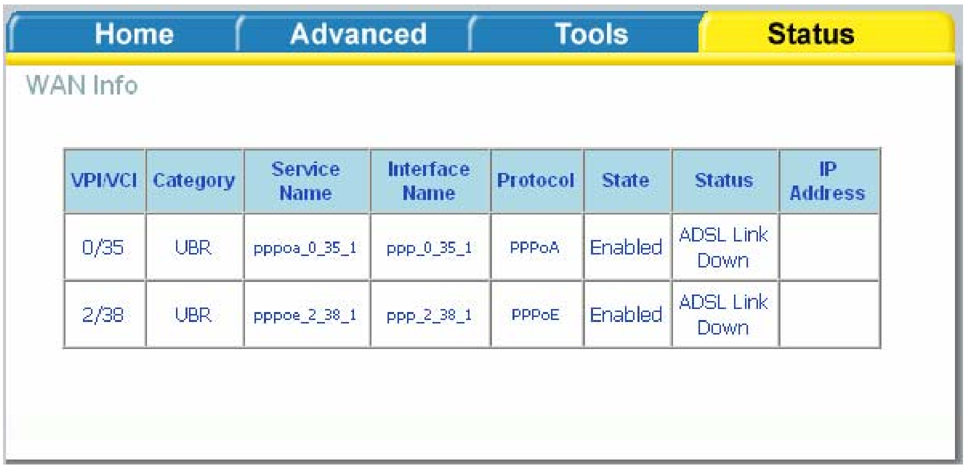


Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

WAN Info

The WAN Info screen displays WAN connections previously set up in the Home section. The information added in the status section is the extra column for connection status information, displaying either *ADSL Link Down* or *ADSL Link Up*.

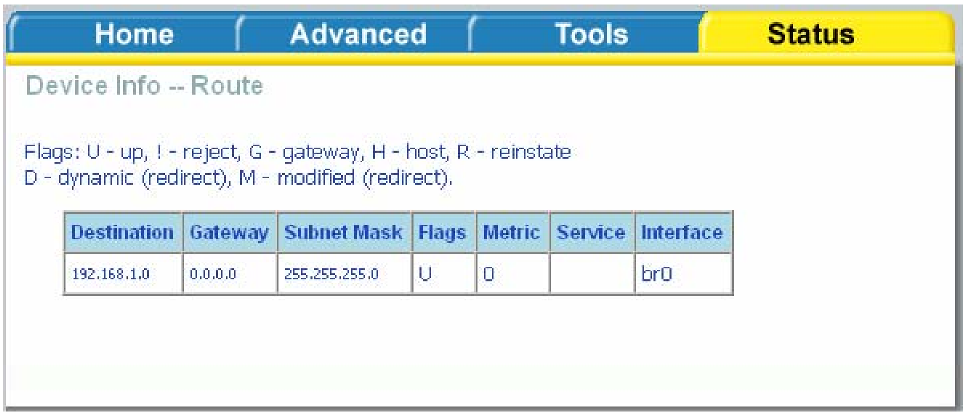


WAN Info

VPI/VCI	Category	Service Name	Interface Name	Protocol	State	Status	IP Address
0/35	UBR	pppoa_0_35_1	ppp_0_35_1	PPPoA	Enabled	ADSL Link Down	
2/38	UBR	pppoe_2_38_1	ppp_2_38_1	PPPoE	Enabled	ADSL Link Down	

Route Info

The Route Info section displays route information showing the IP addresses of the destination, gateway, and subnet mask as well as other route information.



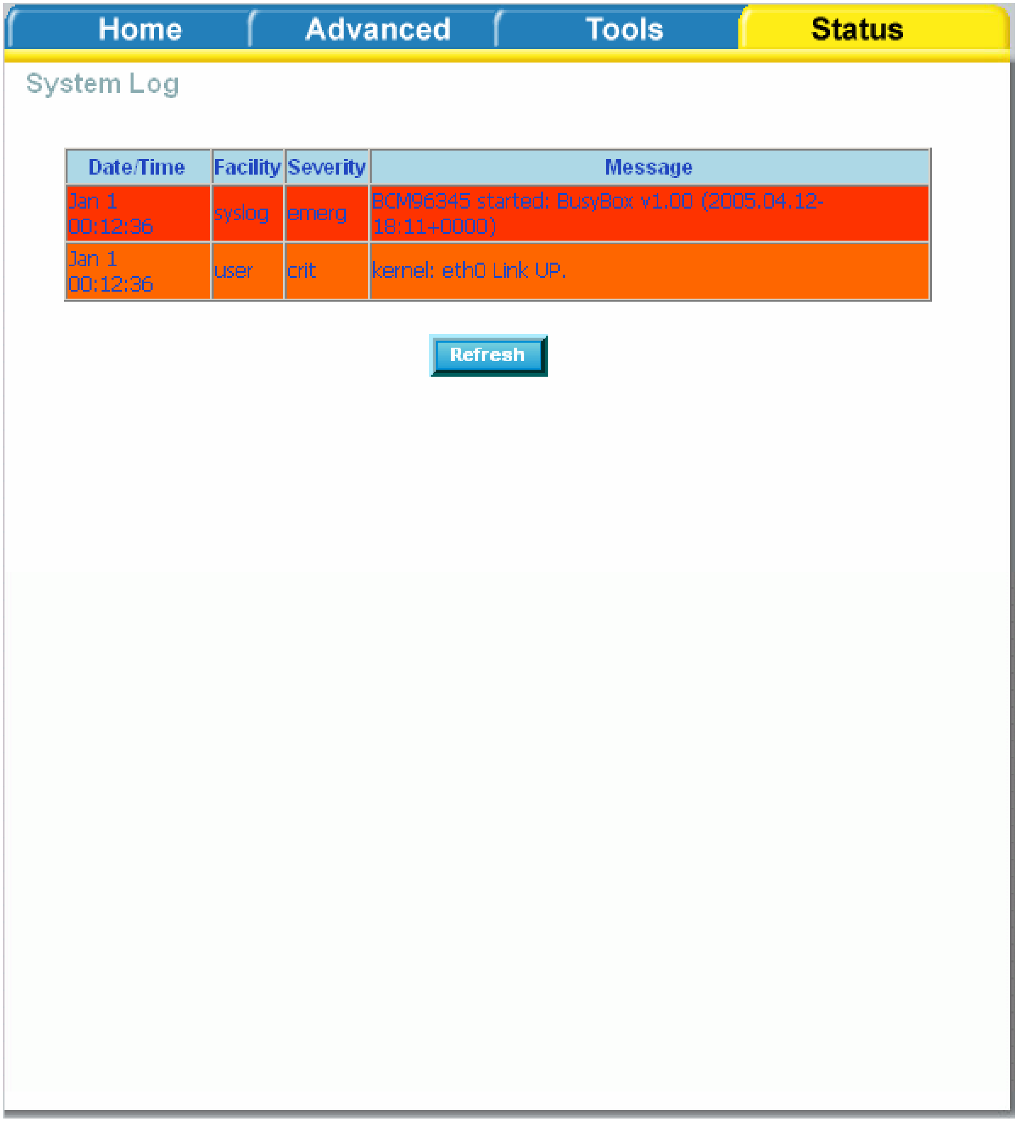
Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Log

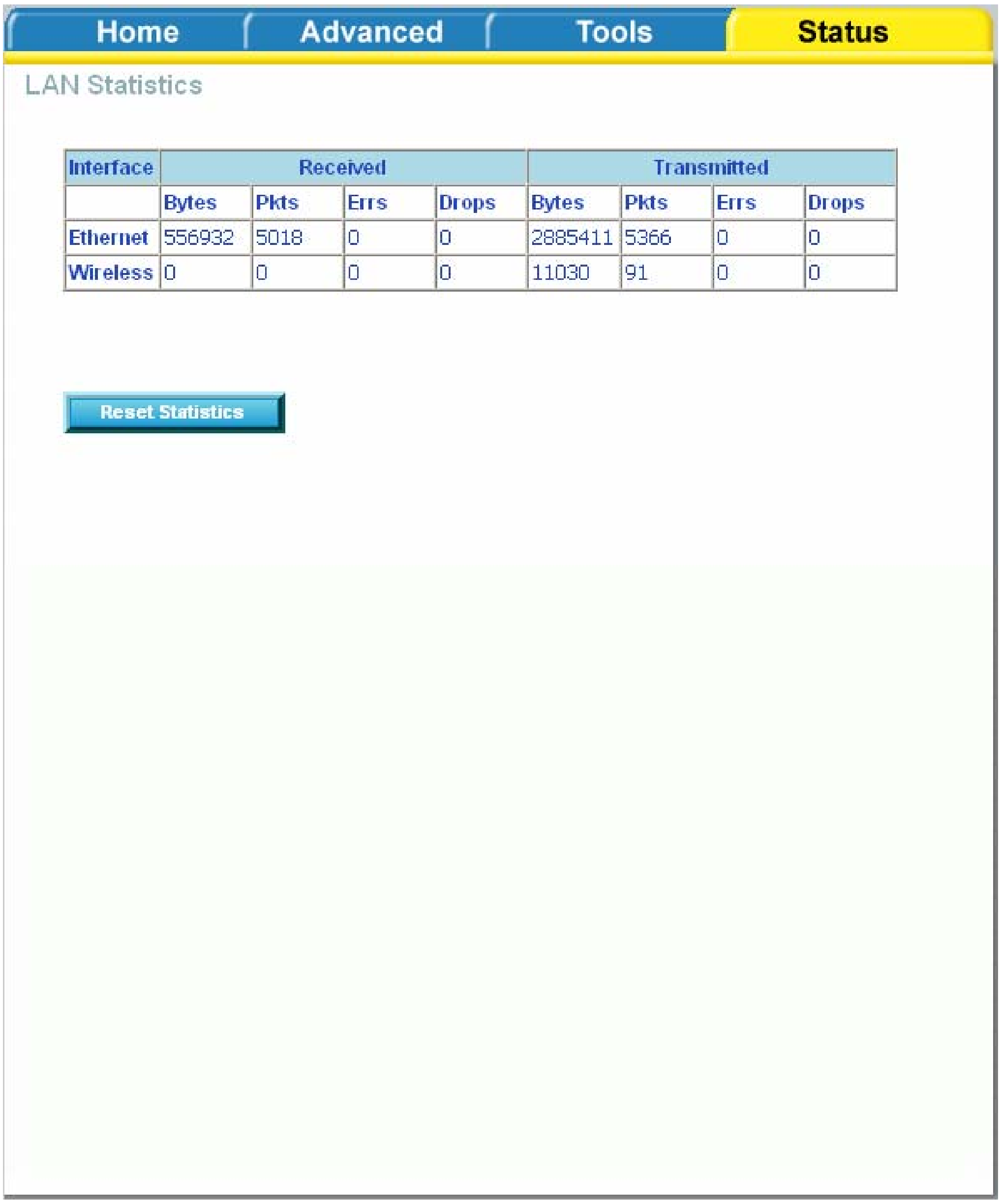
This is the same screen as seen in the Remotelog section under tools.



Date/Time	Facility	Severity	Message
Jan 1 00:12:36	syslog	emerg	BCM96345 started: BusyBox v1.00 (2005.04.12-18:11+0000)
Jan 1 00:12:36	user	crit	kernel: eth0 Link UP.

LAN

The LAN section shows received and transmitted packet information for the Ethernet interfaces. Click on **Reset Statistics** to renew the information.

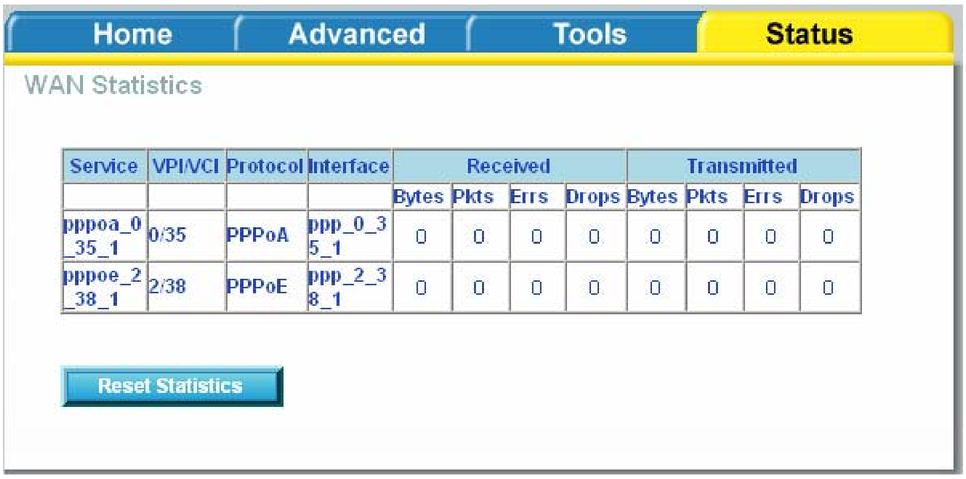


LAN Statistics

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	556932	5018	0	0	2885411	5366	0	0
Wireless	0	0	0	0	11030	91	0	0

WAN

The WAN section shows received and transmitted packet information for the WAN connections that you have set up. Click on **Reset Statistics** to renew the information.

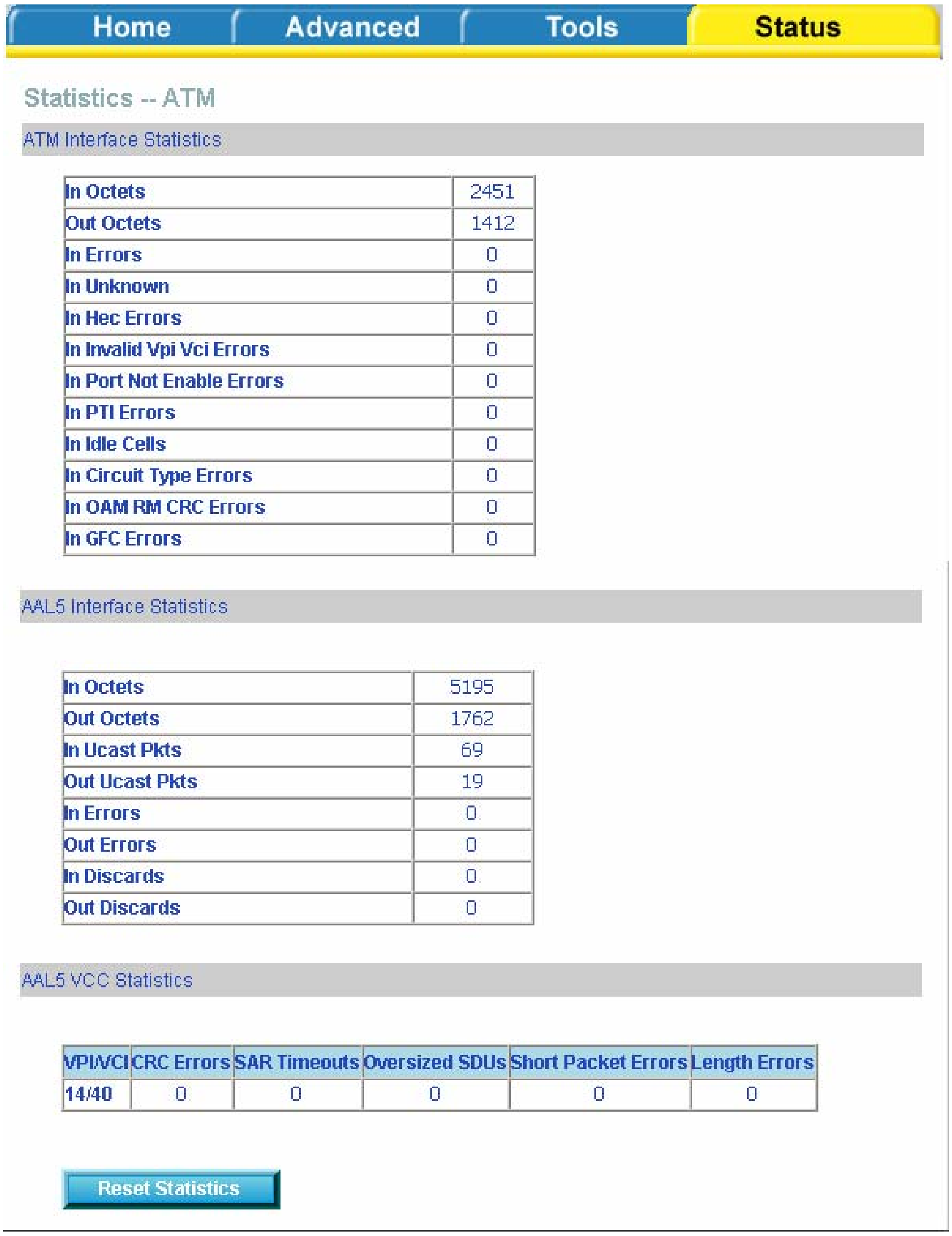


WAN Statistics

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoa_0_35_1	0/35	PPPoA	ppp_0_35_1	0	0	0	0	0	0	0	0
pppoe_2_38_1	2/38	PPPoE	ppp_2_38_1	0	0	0	0	0	0	0	0

ATM

The ATM section displays statistical values for your ATM interface as well as for AAL5 and AAL5 VCC. Click on **Reset Statistics** to renew the values.



Statistics -- ATM

ATM Interface Statistics

In Octets	2451
Out Octets	1412
In Errors	0
In Unknown	0
In Hec Errors	0
In Invalid Vpi Vci Errors	0
In Port Not Enable Errors	0
In PTI Errors	0
In Idle Cells	0
In Circuit Type Errors	0
In OAM RM CRC Errors	0
In GFC Errors	0

AAL5 Interface Statistics

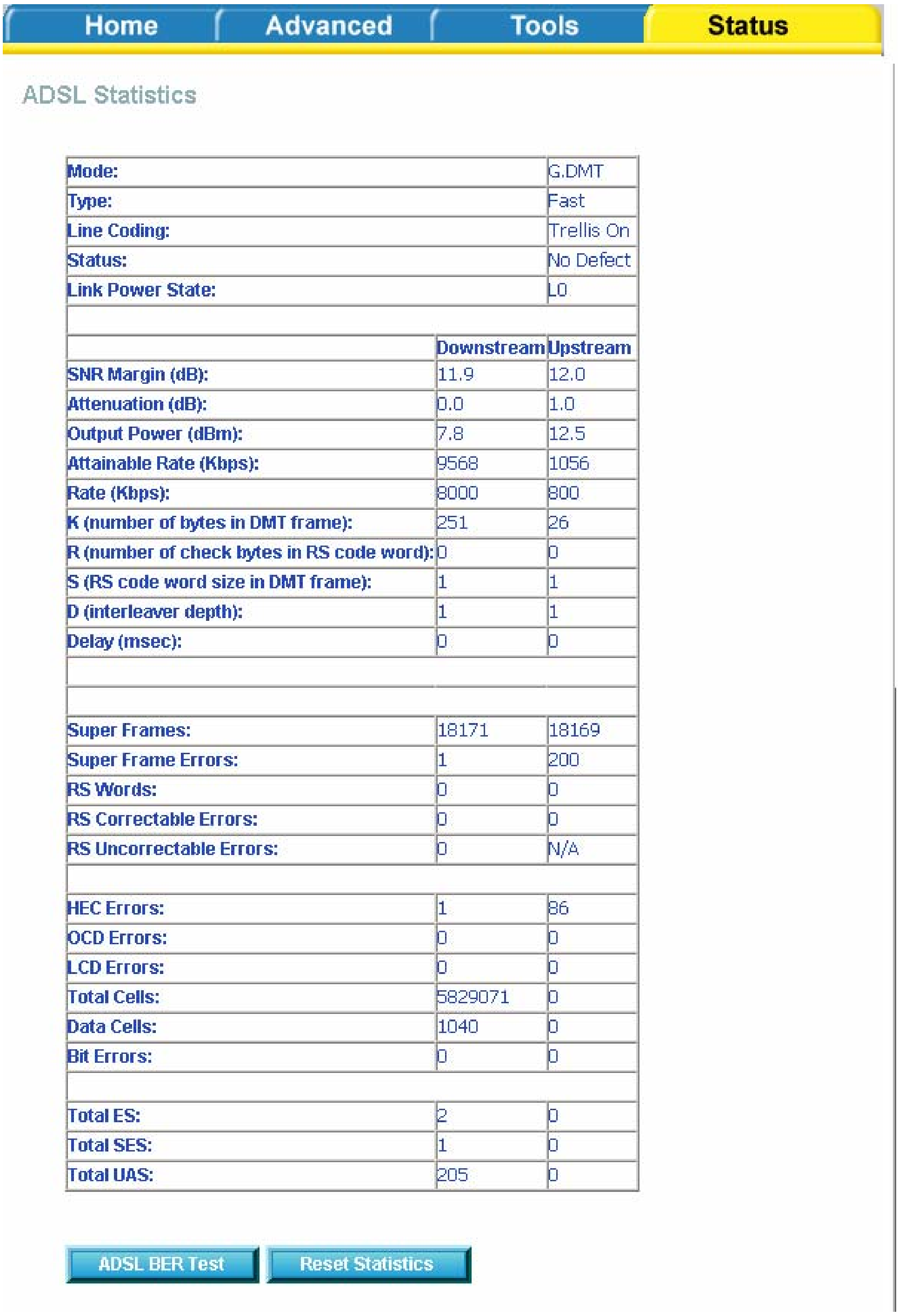
In Octets	5195
Out Octets	1762
In Ucast Pkts	69
Out Ucast Pkts	19
In Errors	0
Out Errors	0
In Discards	0
Out Discards	0

AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
14/40	0	0	0	0	0

ADSL

Information contained in the ADSL screen is useful for troubleshooting and diagnostics of connection problems.



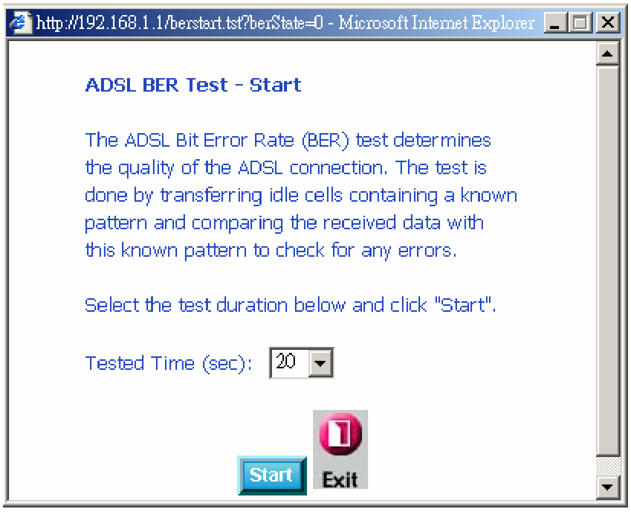
ADSL Statistics

Mode:		G.DMT
Type:		Fast
Line Coding:		Trellis On
Status:		No Defect
Link Power State:		L0
	Downstream	Upstream
SNR Margin (dB):	11.9	12.0
Attenuation (dB):	0.0	1.0
Output Power (dBm):	7.8	12.5
Attainable Rate (Kbps):	9568	1056
Rate (Kbps):	8000	800
K (number of bytes in DMT frame):	251	26
R (number of check bytes in RS code word):	0	0
S (RS code word size in DMT frame):	1	1
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	18171	18169
Super Frame Errors:	1	200
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	1	86
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	5829071	0
Data Cells:	1040	0
Bit Errors:	0	0
Total ES:	2	0
Total SES:	1	0
Total UAS:	205	0

ADSL BER Test

A **Bit Error Rate Test (BER Test)** is a test that reflects the ratio of error bits to the total number transmitted.

If you click on the **ADSL BER Test** button at the bottom of the ADSL Statistics page, the following pop-up screen will appear allowing you to set the tested time and to begin the test.



http://192.168.1.1/berstart.tst?berState=0 - Microsoft Internet Explorer

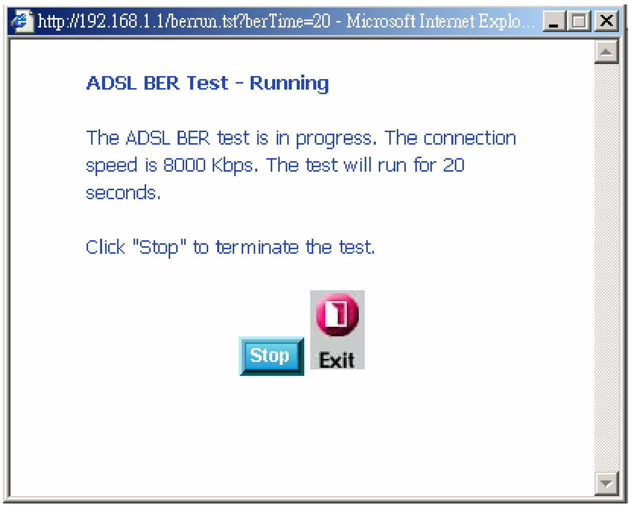
ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): 20

When you start the ADSL BER Test, the following progress window will display the connection speed as well as the length of time that the test will run for. At any time during the test, click on the **Stop** button to terminate the test.



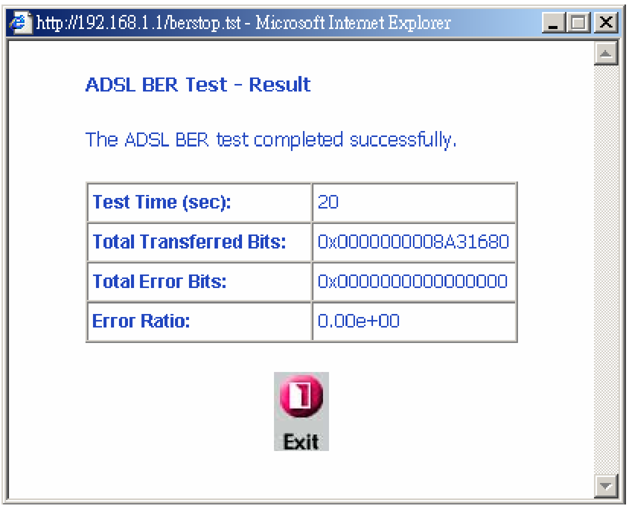
http://192.168.1.1/berrun.tst?berTime=20 - Microsoft Internet Explo...

ADSL BER Test - Running

The ADSL BER test is in progress. The connection speed is 8000 Kbps. The test will run for 20 seconds.

Click "Stop" to terminate the test.

When the test is complete, the following window will display the test results showing the test time, total transferred bits, total error bits and error ratio.


http://192.168.1.1/berstop.tst - Microsoft Internet Explorer

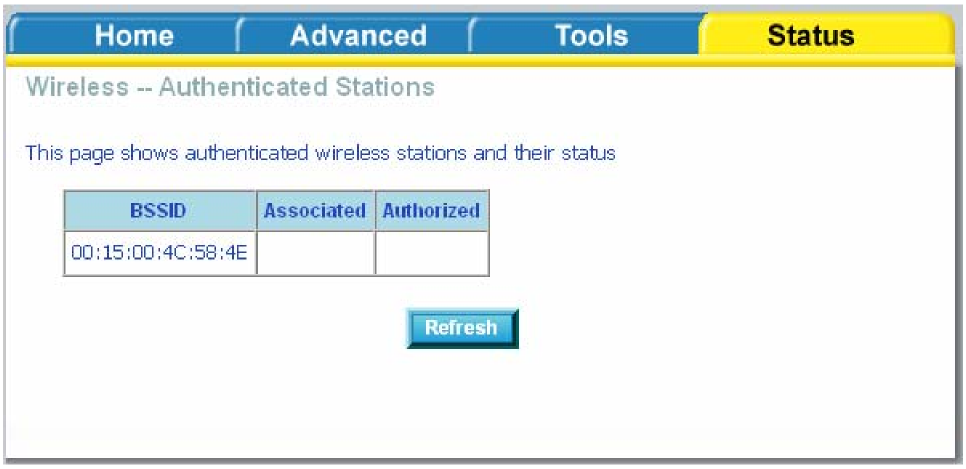
ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x0000000008A31680
Total Error Bits:	0x0000000000000000
Error Ratio:	0.00e+00

Wireless Station Info

This page displays the stations (identified by their BSSID) that are associated with your wireless router. Click on **Refresh** to renew the page for new wireless stations.



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status

BSSID	Associated	Authorized
00:15:00:4C:58:4E		