

D-Link DSL-2500U

ADSL2/2+ Ethernet Router

User Manual



D-Link[®]
Building Networks for People



RECYCLABLE

2006/08/30

Ver. 1.00

Table of Contents

GENERAL INFORMATION	3
<i>Package Contents</i>	3
<i>Important Safety Instructions</i>	3
<i>Front Panel View</i>	4
<i>Back Panel View</i>	5
CONNECTING THE ROUTER TO YOUR COMPUTER	6
<i>Connect the ADSL Line and Telephone</i>	6
<i>Connect the PC to the Router</i>	6
<i>Connect the Power Adapter</i>	6
CONFIGURING YOUR ROUTER	7
HOME	8
<i>Wizard</i>	8
ATM PVC Configuration	8
Connection Type	10
PPP Username and Password	11
Network Address Translation Settings	12
Device Setup	13
Setup - Summary	14
<i>WAN</i>	15
<i>LAN</i>	21
<i>DNS</i>	23
DNS Server Configuration	23
<i>Dynamic DNS</i>	24
<i>Logout</i>	25
ADVANCED SETUP	26
<i>ADSL</i>	26
ADSL Settings	27
ADSL Tone Settings	27
<i>Virtual Server</i>	28
NAT—Virtual Servers Setup	28
<i>DMZ</i>	31
<i>SNMP</i>	32
SNMP—Configuration	32
<i>IP Filter</i>	32
Incoming IP Filtering Setup	33
Outgoing IP Filtering Setup	35
<i>Bridge Filters</i>	36
MAC Filtering Setup	36
<i>Parental Control</i>	38
Time of Day Restrictions	38
<i>Routing</i>	40
Routing—Static Route	40
Routing—Default Gateway	41
Routing—RIP Configuration	42
<i>Quality of Service</i>	42
<i>Port Mapping</i>	44
TOOLS	46
<i>Access Control</i>	46
Access Control—Admin	47
Access Control—Services	48
Access Control—IP Address	48
<i>Time</i>	50
<i>Remote Log</i>	51
<i>System</i>	52
Save and Reboot	52
Backup Settings	52
Update Settings	54

Restore Default Settings	54
<i>Firmware</i>	55
<i>Test</i>	55
STATUS	57
<i>Device Info</i>	57
<i>DHCP Clients</i>	58
<i>WAN Info</i>	58
<i>Route Info</i>	58
<i>Log</i>	59
<i>LAN</i>	59
<i>WAN</i>	60
<i>ATM</i>	61
<i>ADSL</i>	62
ADSL BER Test	63

General Information

The D-Link DSL-2500U is an ADSL2+ router for the main purpose of connecting to the Internet. This user manual provides 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-2500U ADSL2/2+ Ethernet Router
- Power adapter
- RJ-11 telephone cable
- RJ-45 Ethernet cable
- CD-ROM (*contains 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.
- 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



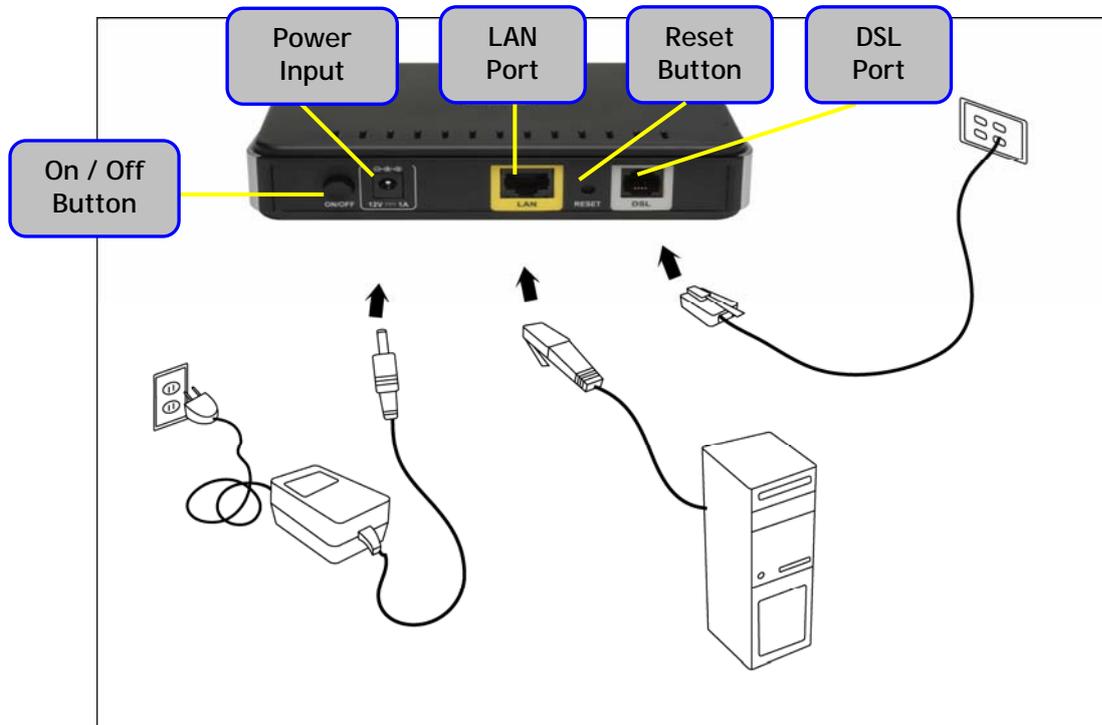
LED	Mode	Indication
Power	Solid Green	The router is powered on. (READY)
	No light	The power is off.
	Solid Red	Failure or device malfunction. (NOT READY)
Status	Blinking Green	Traffic is passing through the device. (INTERNET TRAFFIC)
DSL	Solid Green	DSL is synchronized.
	No Light	No carrier signal.
	Slow Blinking	DSL attempting synch. Trying to detect carrier signal.
	Fast Blinking	Carrier has been detected and modem is trying to train.
LAN	Solid Green	Powered device connected to associated port
	Blinking 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.
	Solid 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.
AC 15V-D.7A	Connects to the power adapter.
LAN	RJ-45 connects the unit to an Ethernet device such as a PC or a switch.
Reset	Resets the router to its default settings.
DSL	RJ-11 telephone port connects telephone cable to telephone or fax machine.

Connecting the Router to Your Computer



Connect the ADSL Line and Telephone

- 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 PC to the Router

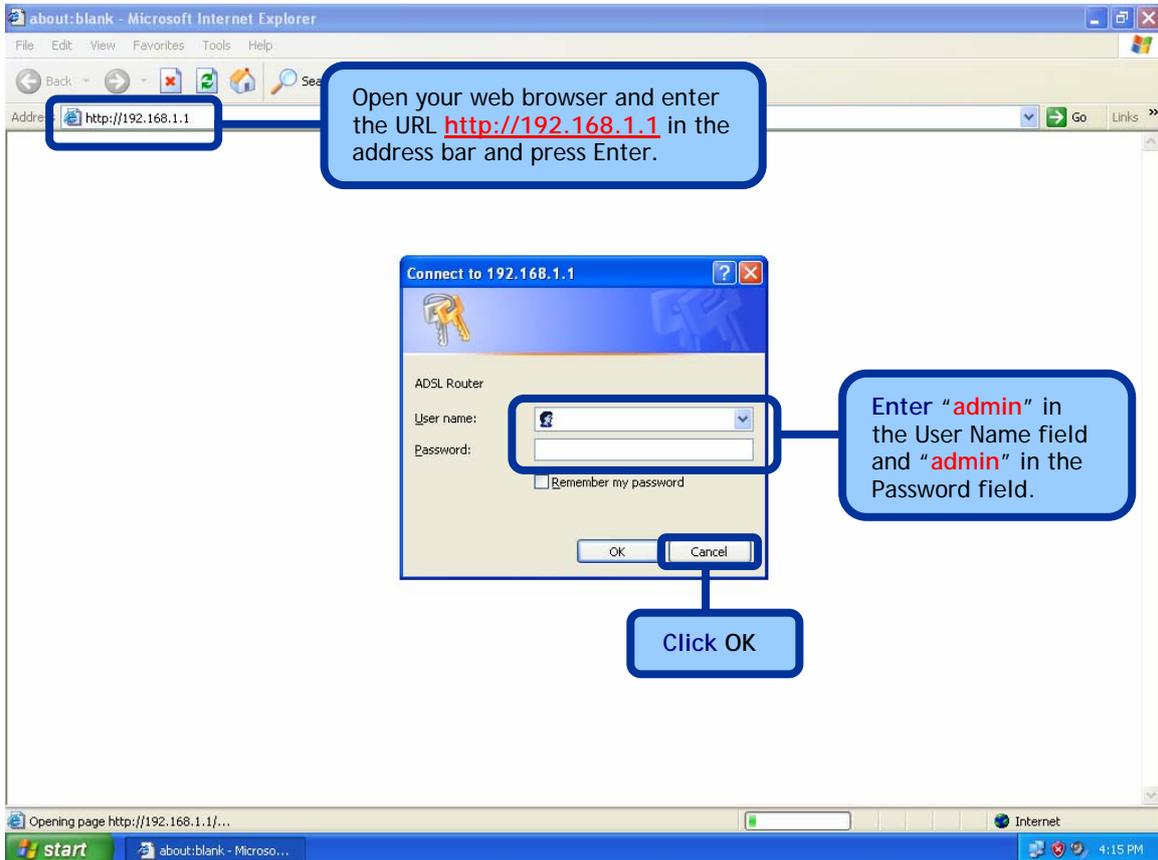
- Connect one end of the Ethernet cable to the **LAN port** on the back of the router and attach the other end to an Ethernet Adapter or available Ethernet port on your computer.

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 Your 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.



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 explain 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, PPPoA, and Bridge Protocol (with DHCP Server available). To continue, click on the Next button.



The screenshot displays the D-Link DSL-2500U web interface. The top left corner features the D-Link logo with the tagline "Building Networks for People". The main title "DSL-2500U" is centered at the top. Below the title, there are four tabs: "Home" (highlighted in yellow), "Advanced", "Tools", and "Status". On the left side, there is a vertical menu with buttons for "Wizard" (highlighted in yellow), "WAN", "LAN", "DNS", "Dynamic DNS", and "Logout". The main content area shows the "Wizard" configuration page. It includes a sub-header "Wizard" and a description: "This Quick Setup will guide you through the steps necessary to configure your DSL Router." Below this, there is a section titled "ATM PVC Configuration." with the instruction: "Select the check box below to enable DSL Auto-connect process." A checkbox labeled "DSL Auto-connect" is checked. At the bottom of the main content area, there is a blue circular button with a right-pointing arrow and the text "Next" below it.

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.

Home **Advanced** **Tools** **Status**

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]

VCI: [32-65535]

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


Next

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.

Home Advanced Tools Status

Wizard

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

Back Next

PPP Username and Password

Enter the PPP username and password as given by your ISP. Then decide if you will be using any features such as *dial on demand*, *PPP IP extension*, *keep alive* and then click on **Next**.

Home **Advanced** **Tools** **Status**

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:

Dial on demand (with idle timeout timer)

PPP IP extension

Keep Alive

Use Static IP Address

Obtain default gateway automatically:

Use the following default gateway:

Use IP Address:

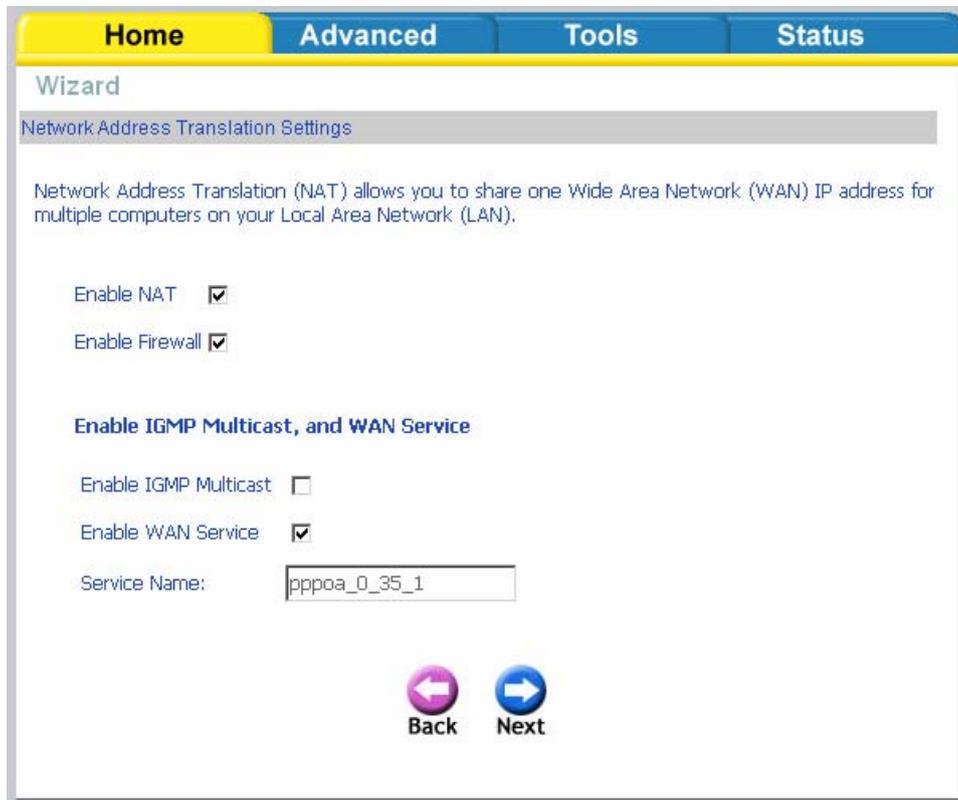
Use WAN Interface:

Back **Next**

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.



The screenshot shows a web-based configuration wizard with a navigation bar at the top containing four tabs: **Home** (highlighted in yellow), **Advanced**, **Tools**, and **Status**. Below the navigation bar, the page title is **Wizard**, and the current step is **Network Address Translation Settings**. A descriptive paragraph states: "Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN)." The configuration options are as follows:

- Enable NAT**:
- Enable Firewall**:
- Enable IGMP Multicast, and WAN Service**:
 - Enable IGMP Multicast**:
 - Enable WAN Service**:
- Service Name**:

At the bottom of the form, there are two navigation buttons: a purple **Back** button with a left-pointing arrow and a blue **Next** button with a right-pointing arrow.

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.

Home **Advanced** **Tools** **Status**

Wizard

Device Setup

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

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

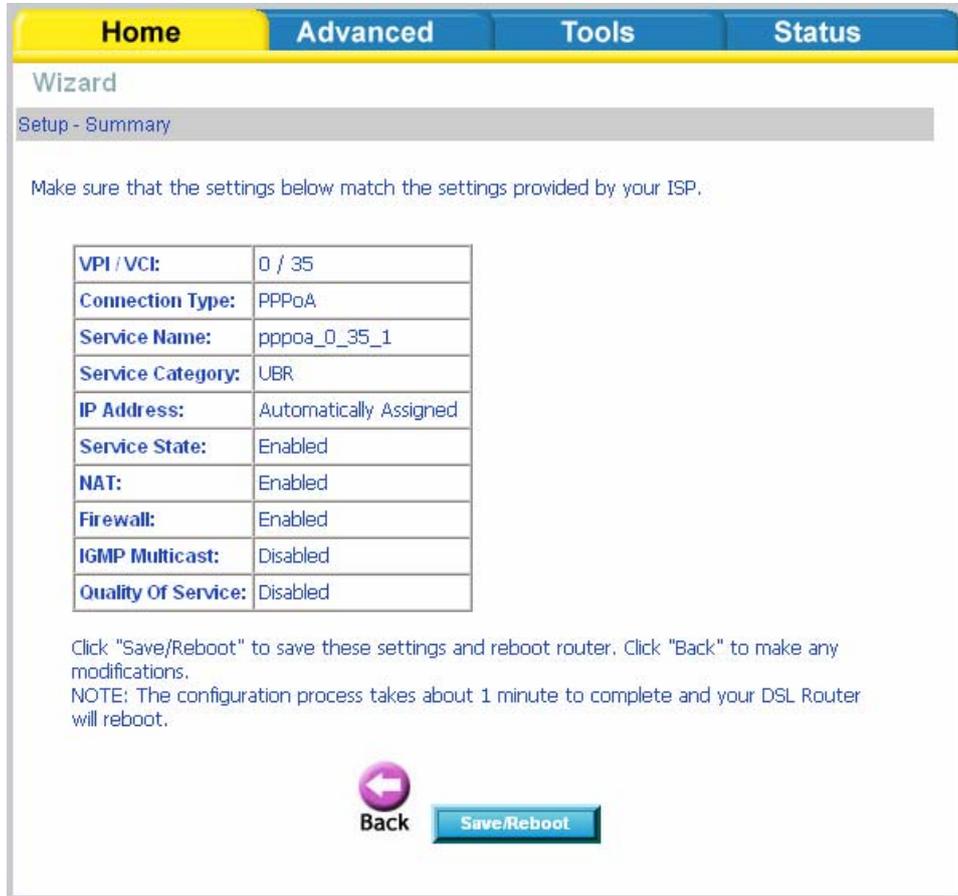
Configure the second IP Address and Subnet Mask for LAN interface

Back **Next**

Setup - Summary

After all of the WAN 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.



The screenshot shows a web interface with a navigation bar at the top containing 'Home', 'Advanced', 'Tools', and 'Status'. Below the navigation bar is a 'Wizard' section with a sub-header 'Setup - Summary'. A message reads: 'Make sure that the settings below match the settings provided by your ISP.' Below this is a table of settings:

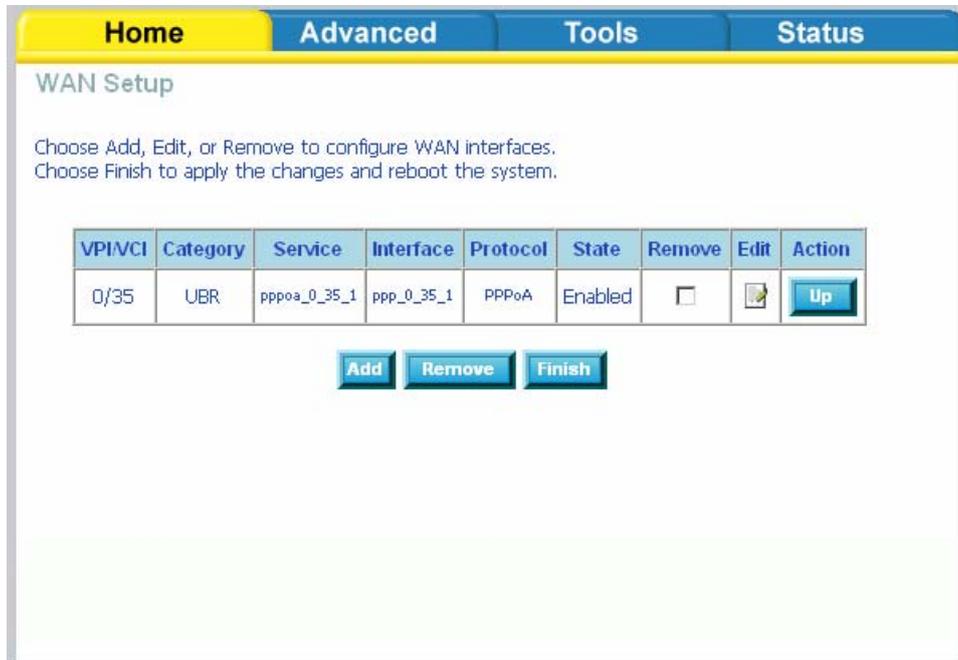
VPI / VCI:	0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Below the table, there is a note: '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.'

At the bottom, there are two buttons: a circular 'Back' button with a left-pointing arrow and a rectangular 'Save/Reboot' button.

WAN

Configure the WAN settings as provided by your ISP.



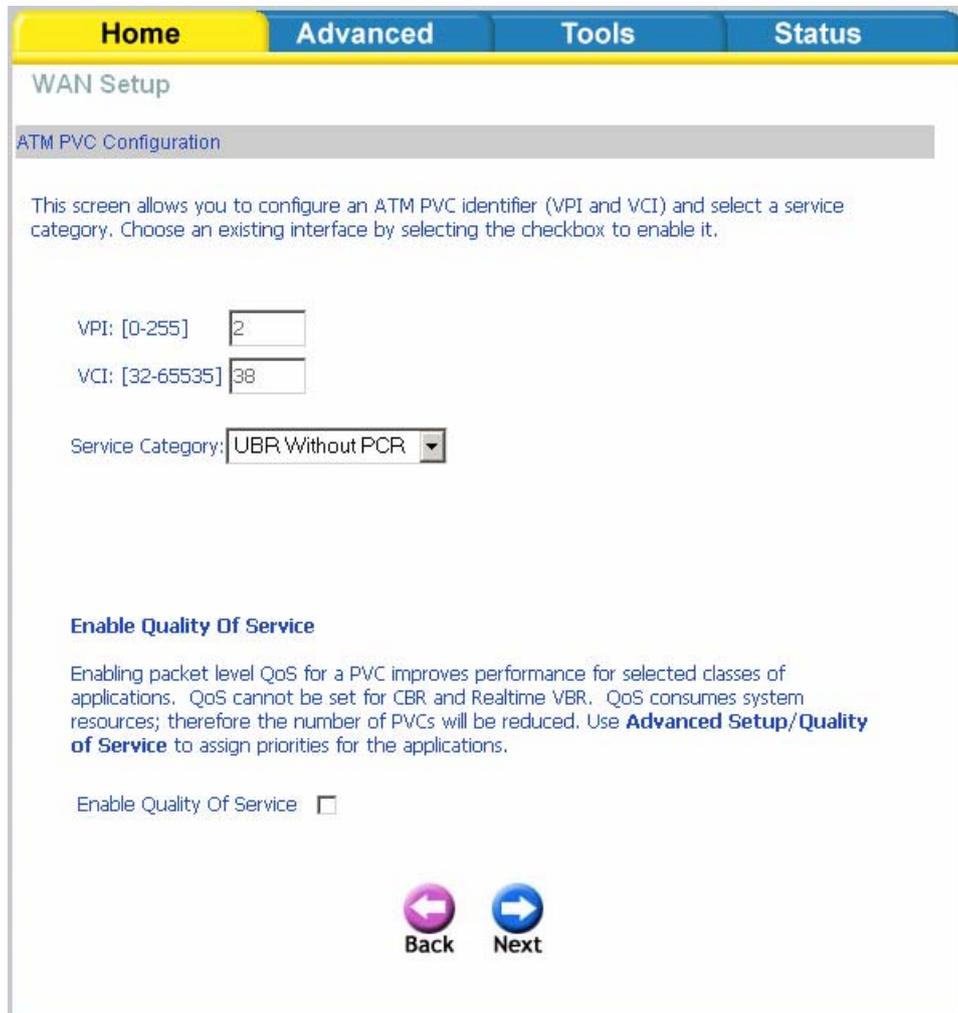
Click on the **Add** button if you want to add a new connection for the WAN interface and to proceed to the ATM PVC Configuration screen as seen below. The ATM PVC Configuration screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

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*.



Home **Advanced** **Tools** **Status**

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]

VCI: [32-65535]

Service Category: ▼

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.

The screenshot shows a web interface for WAN configuration. At the top, there are four tabs: Home (highlighted in yellow), Advanced, Tools, and Status. Below the tabs, the page title is 'WAN'. Underneath, there is a section titled 'Connection Type' with a grey background. Below this, there is a text instruction: '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.' There are five radio button options: 'PPP over ATM (PPPoA)', 'PPP over Ethernet (PPPoE)' (which is selected), 'MAC Encapsulation Routing (MER)', 'IP over ATM (IPoA)', and 'Bridging'. Below these options is a section titled 'Encapsulation Mode' with a dropdown menu currently set to 'LLC/SNAP-BRIDGING'. At the bottom of this section is a checkbox labeled 'Enable 802.1q' which is currently unchecked. At the very bottom of the page are two circular buttons: a purple 'Back' button with a left arrow and a blue 'Next' button with a right arrow.

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:
PPP Password:
Authentication Method:

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:

**Back****Next**

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.

The screenshot shows a web interface with a navigation bar at the top containing 'Home', 'Advanced', 'Tools', and 'Status'. The 'Home' tab is highlighted in yellow. Below the navigation bar, the page title is 'WAN' and the sub-section is 'Network Address Translation Settings'. A descriptive paragraph explains that NAT allows sharing a WAN IP address for multiple LAN computers. There are four checkboxes: 'Enable NAT' (checked), 'Enable Firewall' (checked), 'Enable IGMP Multicast' (unchecked), and 'Enable WAN Service' (checked). Below these is a text input field for 'Service Name' containing 'ppoe_2_38_1'. At the bottom, there are two circular buttons: a pink 'Back' button and a blue 'Next' button.

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.

 **Back**  **Apply**

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.

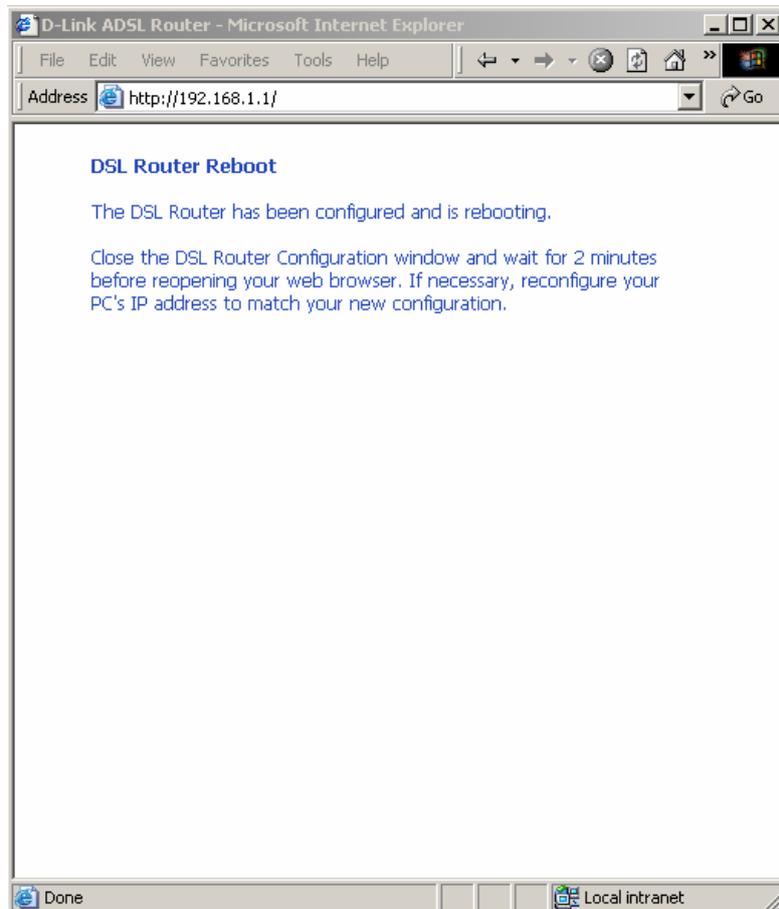
WAN Setup

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	<input type="checkbox"/>		
2/38	UBR	pppoe_2_38_1	ppp_2_38_1	PPPoE	Enabled	<input type="checkbox"/>		

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



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.

Home	Advanced	Tools	Status
------	----------	-------	--------

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:

Subnet Mask:

Enable UPnP

Enable IGMP Snooping

Standard Mode

Blocking Mode

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

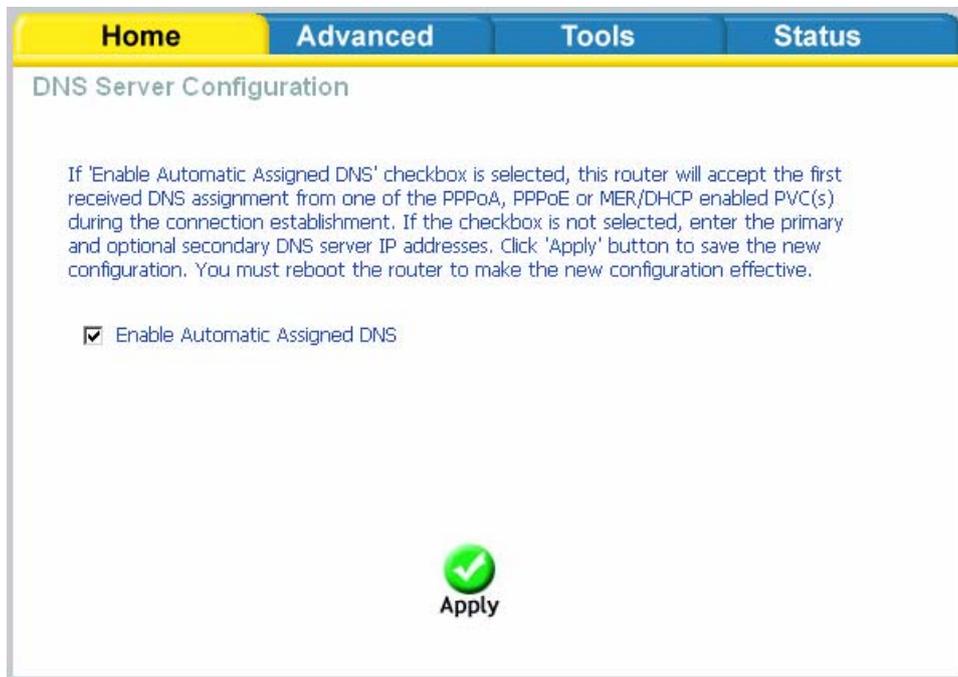
Configure the second IP Address and Subnet Mask for LAN interface

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

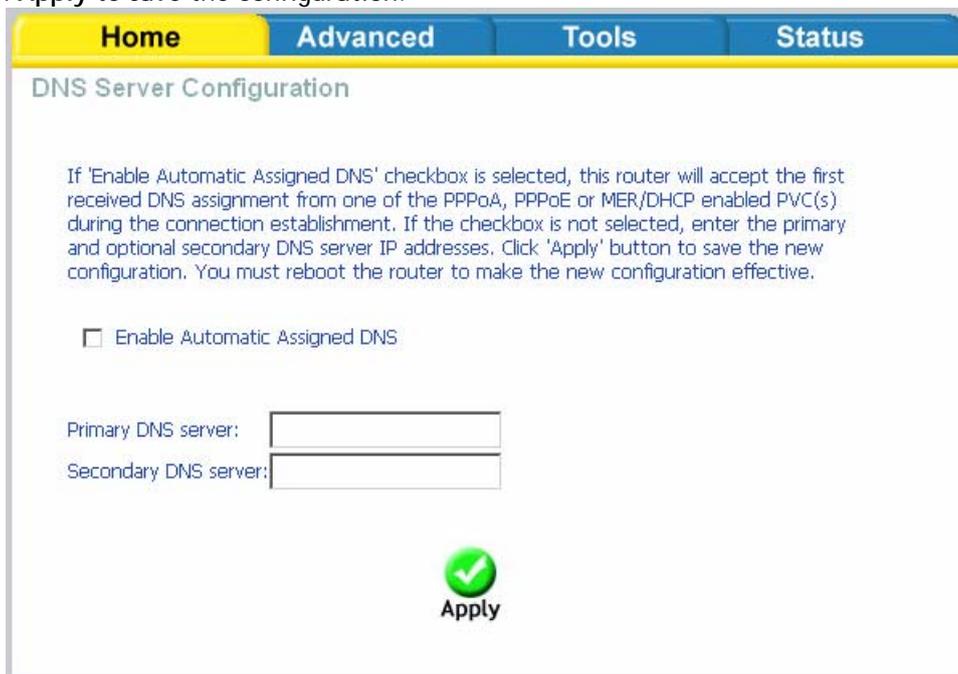
DNS Server Configuration

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



The screenshot shows the 'DNS Server Configuration' page. At the top, there are four tabs: 'Home' (highlighted in yellow), 'Advanced', 'Tools', and 'Status'. Below the tabs, the title 'DNS Server Configuration' is displayed. A paragraph of text explains that if the 'Enable Automatic Assigned DNS' checkbox is selected, the 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, the user must enter the primary and optional secondary DNS server IP addresses. Below this text, the checkbox 'Enable Automatic Assigned DNS' is checked. At the bottom center, there is a green circular icon with a white checkmark and the word 'Apply' below it.

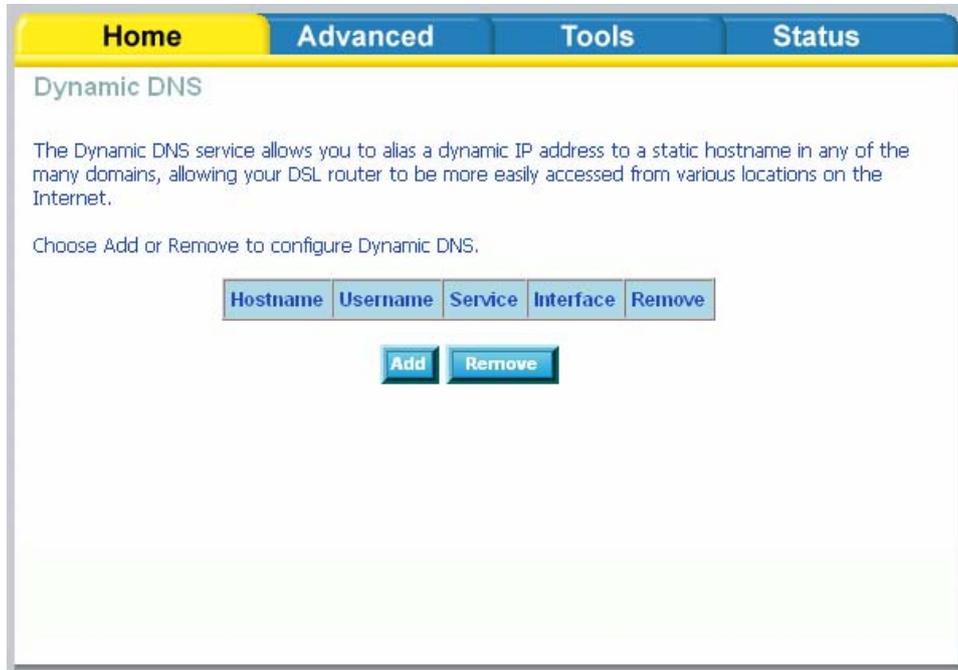
If you uncheck the *Enable Automatic Assigned DNS* checkbox, there will appear two additional fields—primary and secondary DNS server—to enter as seen below. Click on **Apply** to save the configuration.



The screenshot shows the 'DNS Server Configuration' page with the 'Enable Automatic Assigned DNS' checkbox unchecked. Below the checkbox, there are two input fields: 'Primary DNS server:' and 'Secondary DNS server:'. At the bottom center, there is a green circular icon with a white checkmark and the word 'Apply' below it.

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.



The screenshot shows a web interface with a navigation bar at the top containing four tabs: **Home** (highlighted in yellow), **Advanced**, **Tools**, and **Status**. Below the navigation bar, the page title is **Dynamic DNS**. The main content area contains the following text:

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.

Below the text, there is a table with five columns: **Hostname**, **Username**, **Service**, **Interface**, and **Remove**. Below the table, there are two buttons: **Add** and **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.

Home **Advanced** **Tools** **Status**

Add dynamic DDNS

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

D-DNS provider:

Hostname:

Interface:

DynDNS Settings

Username:

Password:

 **Apply**

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.

Home **Advanced** **Tools** **Status**

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.

D-Link
Building Networks for People

DSL-2500U

Home **Advanced** Tools Status

ADSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

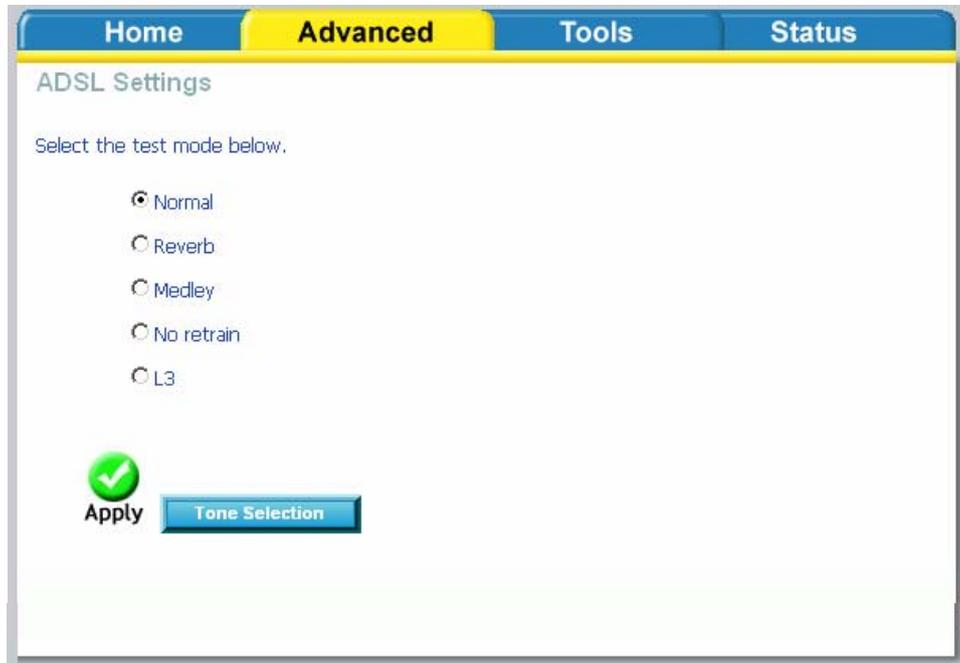
Capability

- Bitswap Enable
- SRA Enable

 **Apply** [Advanced Settings](#)

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*.



Home Advanced Tools Status

ADSL Settings

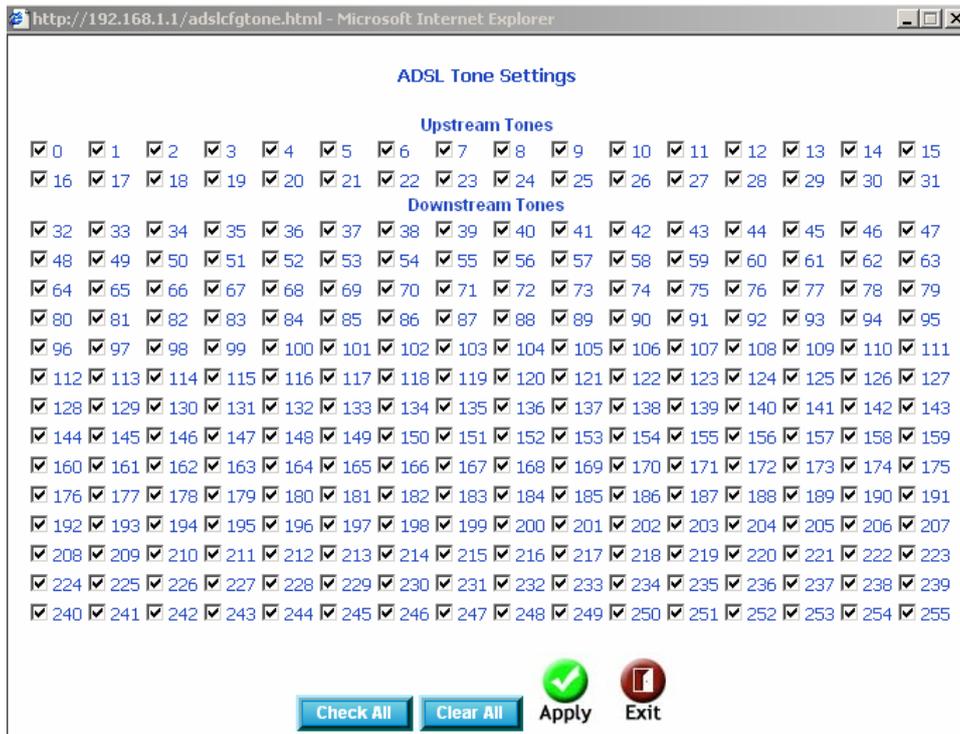
Select the test mode below.

- Normal
- Reverb
- Medley
- No retrain
- L3

 Apply [Tone Selection](#)

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.



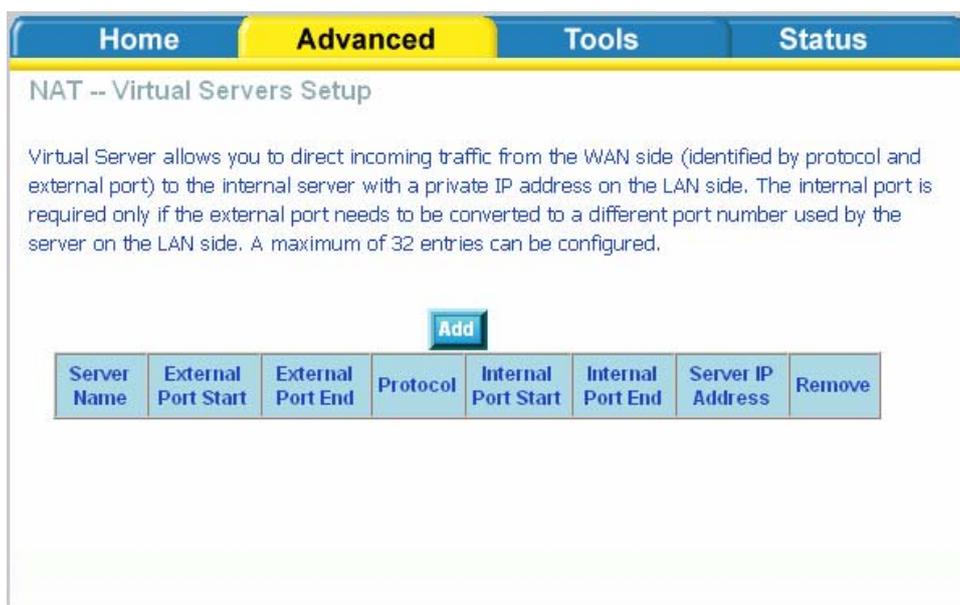
Virtual Server

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.



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:

Custom Server:

Server IP Address:



External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		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.

Add **Remove**

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	<input type="checkbox"/>
Age of Kings	6073	6073	TCP	6073	6073	192.168.1.2	<input type="checkbox"/>
Age of Kings	2300	2400	TCP	2300	2400	192.168.1.2	<input type="checkbox"/>
Age of Kings	2300	2400	UDP	2300	2400	192.168.1.2	<input type="checkbox"/>

DMZ

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

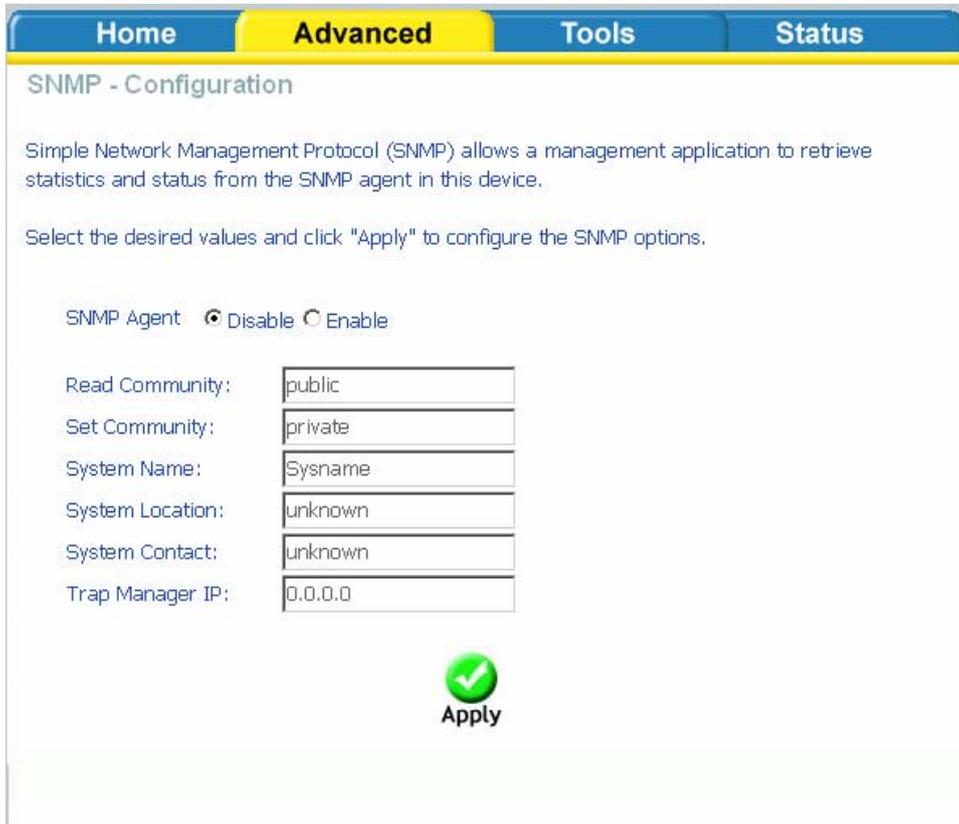
DMZ Host IP Address:

Apply

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.



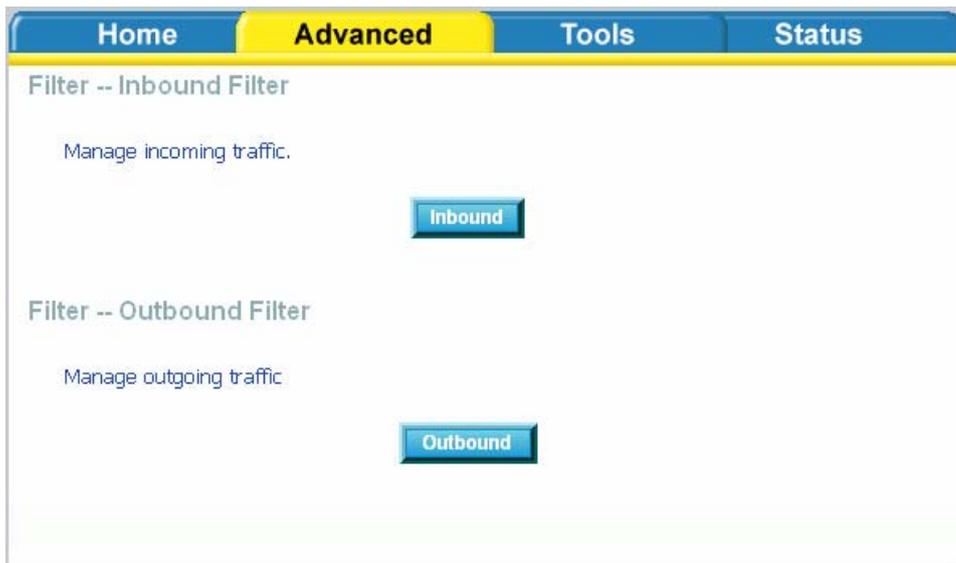
The image shows a web interface for configuring SNMP. At the top, there are four tabs: Home, Advanced (selected), Tools, and Status. Below the tabs, the page title is "SNMP - Configuration". A descriptive paragraph states: "Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device." Below this, a instruction says: "Select the desired values and click 'Apply' to configure the SNMP options." The configuration options are as follows:

SNMP Agent	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Read Community:	public
Set Community:	private
System Name:	Sysname
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

At the bottom center, there is a green circular button with a white checkmark and the text "Apply" below it.

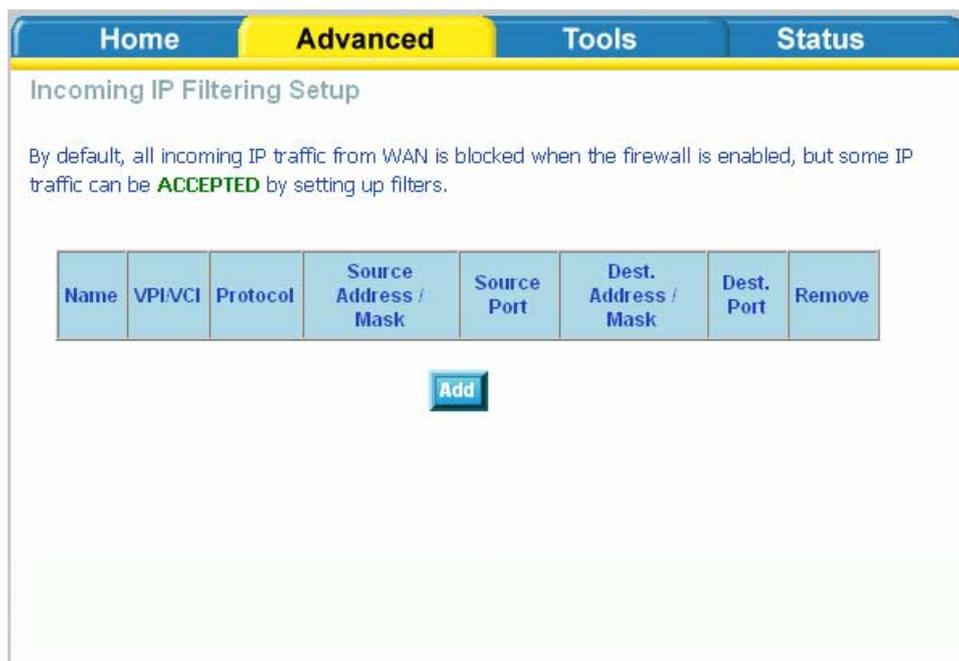
IP Filter

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.



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.



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.

Home **Advanced** **Tools** **Status**

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:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

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
 pppoa_0_35_1/ppp_0_35_1
 pppoe_2_38_1/ppp_2_38_1


Apply

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.

Home **Advanced** Tools Status

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 / 255.255.255.0				<input type="checkbox"/>

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.

Home **Advanced** Tools Status

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.

Home **Advanced** Tools Status

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:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

 Apply

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.

Home **Advanced** Tools Status

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
Test1	TCP	192.168.1.5 / 255.255.255.0		192.168.1.8 / 255.255.255.0		<input type="checkbox"/>

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.

The screenshot shows the 'MAC Filtering Setup' page. At the top, there are navigation tabs: 'Home', 'Advanced' (highlighted in yellow), 'Tools', and 'Status'. Below the tabs, the page title is 'MAC Filtering Setup'. The main content area displays 'MAC Filtering Global Policy: **FORWARDED**' in green text. A blue button labeled 'Change Policy' is centered below this text. Further down, a paragraph explains that MAC filtering is only effective on ATM PVCs in Bridge mode. It defines 'FORWARDED' as allowing all MAC layer frames except those matching specified rules, and 'BLOCKED' as blocking all MAC layer frames except those matching specified rules. Below this, it says 'Choose Add or Remove to configure MAC filtering rules.' and shows a table with columns: 'VPI/VCI', 'Protocol', 'Destination MAC', 'Source MAC', 'Frame Direction', and 'Remove'. A blue 'Add' button is positioned below the table.

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

The screenshot shows a confirmation dialog titled 'Change MAC Filtering Global Policy'. At the top, there are navigation tabs: 'Home', 'Advanced' (highlighted in yellow), 'Tools', and 'Status'. Below the tabs, the page title is 'Change MAC Filtering Global Policy'. A warning message in red text states: '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.' Below the warning, the question 'Are you sure you want to change MAC Filtering Global Policy from **FORWARDED** to **BLOCKED** ?' is displayed in blue text. At the bottom, there are two blue buttons: 'NO' and 'YES'.

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.

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.

After you click you **Add**, you will see the below screen. 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 **Save / 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

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

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>						

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)



Apply

Routing

The screenshot shows a web interface with a navigation bar at the top containing 'Home', 'Advanced' (highlighted), 'Tools', and 'Status'. Below the navigation bar, there are three sections:

- Routing -- Static Route**: A section with the description "Allows you to manually configure special routes that your network might need." and a central button labeled "Static Route".
- Routing -- Default Gateway**: A section with the description "Allows you to configure Default Gateway used by WAN Interface." and a central button labeled "Default Gateway".
- Routing -- RIP**: A section with the description "Allows you to configure RIP (Routing Information Protocol)." and a central button labeled "RIP".

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.

The screenshot shows the 'Routing -- Static Route' configuration page. The navigation bar is the same as in the previous screenshot. The page title is "Routing -- Static Route (A maximum 32 entries can be configured)". Below the title is a table with the following columns: Destination, Subnet Mask, Gateway, Interface, and Remove. Below the table are two buttons: "Add" and "Remove".

Destination	Subnet Mask	Gateway	Interface	Remove
-------------	-------------	---------	-----------	--------

Buttons: Add, Remove

Enter the route information and then apply your configurations.

Home	Advanced	Tools	Status
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:	<input type="text"/>		
Subnet Mask:	<input type="text"/>		
<input type="checkbox"/> Use Gateway IP Address	<input type="text"/>		
<input type="checkbox"/> Use Interface	<input type="text" value="pppoe_0_35_1/ppp_0_35_1"/>		
 Apply			

Routing—Default Gateway

Home	Advanced	Tools	Status
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.			
<input checked="" type="checkbox"/> Enable Automatic Assigned Default Gateway			
 Apply			

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	<input type="checkbox"/>
ppp_0_35_1	0/35	2	Passive	<input type="checkbox"/>
ppp_2_38_1	2/38	2	Passive	<input type="checkbox"/>

Apply

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

Add

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

Home **Advanced** **Tools** **Status**

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 corresponding 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:

Mark IP Precedence:

Mark IP Type Of Service:

Mark 802.1p if 802.1q is enabled on WAN:

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:

Protocol:

Source IP Address:

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

SET-2

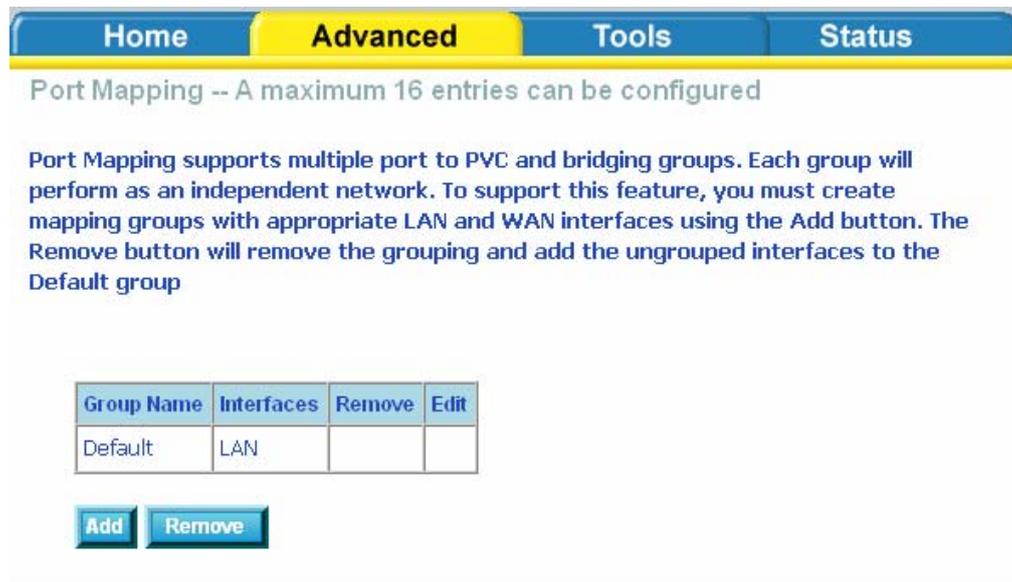
802.1p Priority:


Apply

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.



The screenshot shows a web interface with a navigation bar containing 'Home', 'Advanced' (highlighted), 'Tools', and 'Status'. Below the navigation bar, the page title is 'Port Mapping -- A maximum 16 entries can be configured'. A paragraph explains that port mapping supports multiple port to PVC and bridging groups, each performing as an independent network. It instructs users to use the 'Add' button to create mapping groups with appropriate LAN and WAN interfaces, and the 'Remove' button to remove the grouping and add the ungrouped interfaces to the Default group. Below the text is a table with four columns: 'Group Name', 'Interfaces', 'Remove', and 'Edit'. The first row shows 'Default' in the 'Group Name' column and 'LAN' in the 'Interfaces' column. Below the table are two buttons: 'Add' and 'Remove'.

Group Name	Interfaces	Remove	Edit
Default	LAN		

Add **Remove**

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

**Automatically Add
Clients With the
following DHCP Vendor
IDs**



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.

The screenshot displays the D-Link DSL-2500U web interface. The top navigation bar includes 'Home', 'Advanced', 'Tools' (highlighted), and 'Status'. The left sidebar contains a vertical menu with buttons for 'Access Control' (highlighted), 'Time', 'Remote Log', 'System', 'Firmware', 'Test', and 'Logout'. The main content area is titled 'Access Control -- Admin' and contains three sections:

- Access Control -- Admin:** Manage ADSL router user accounts. Includes an 'Admin' button.
- Access Control -- Services:** A Service Control List ("SCL") enables or disables services from being used.. Includes a 'Services' button.
- Access Control -- IP Address:** Permits access to local management services. Includes an 'IP Address' button.

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.

Home | **Advanced** | **Tools** | **Status**

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:


Apply

Access Control—Services

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

Service	LAN	WAN
FTP	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
HTTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
ICMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
SNMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
TELNET	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
TFTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

 Apply

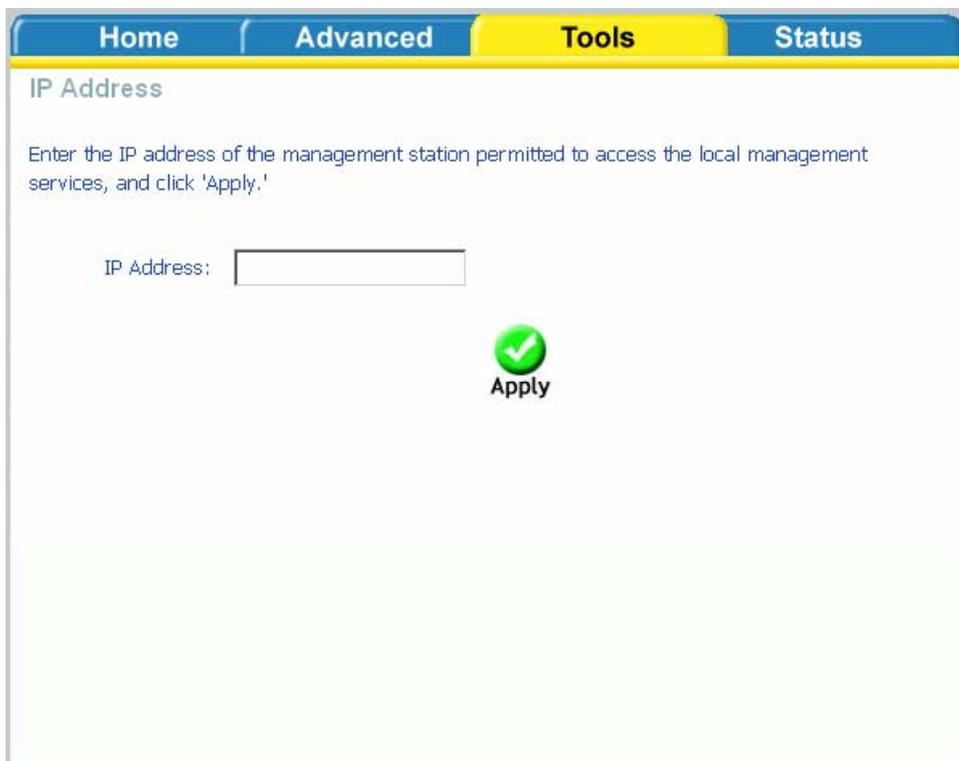
Access Control—IP Address

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.

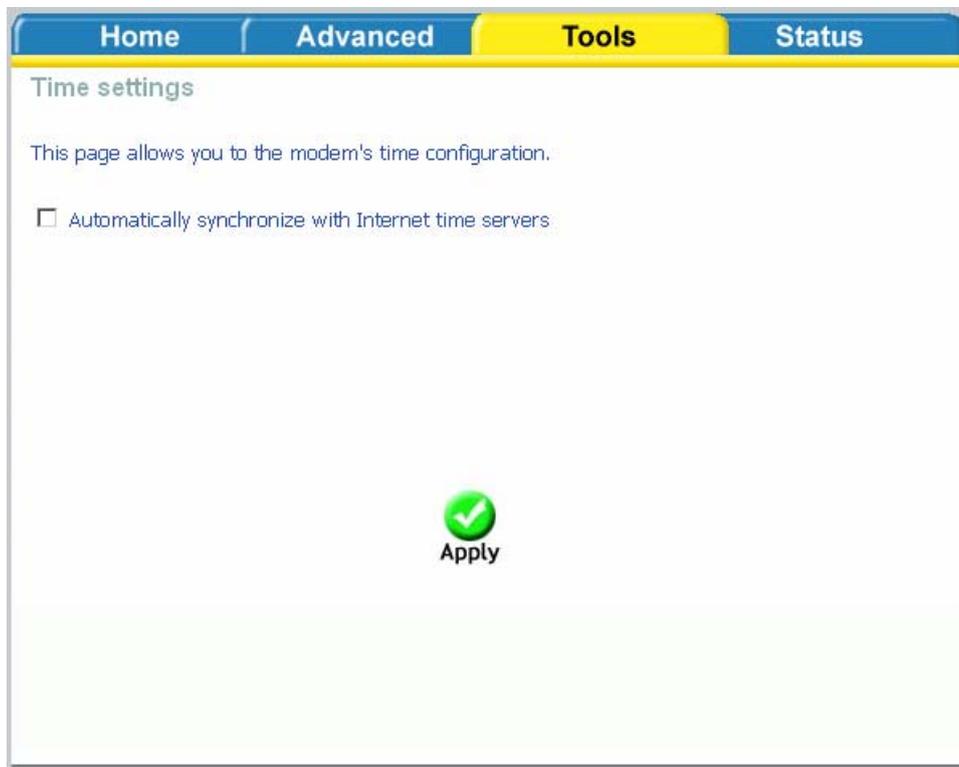


To assign the IP address of the management station that is permitted to access the local management services, enter the IP address in the box and click on the **Apply** button.



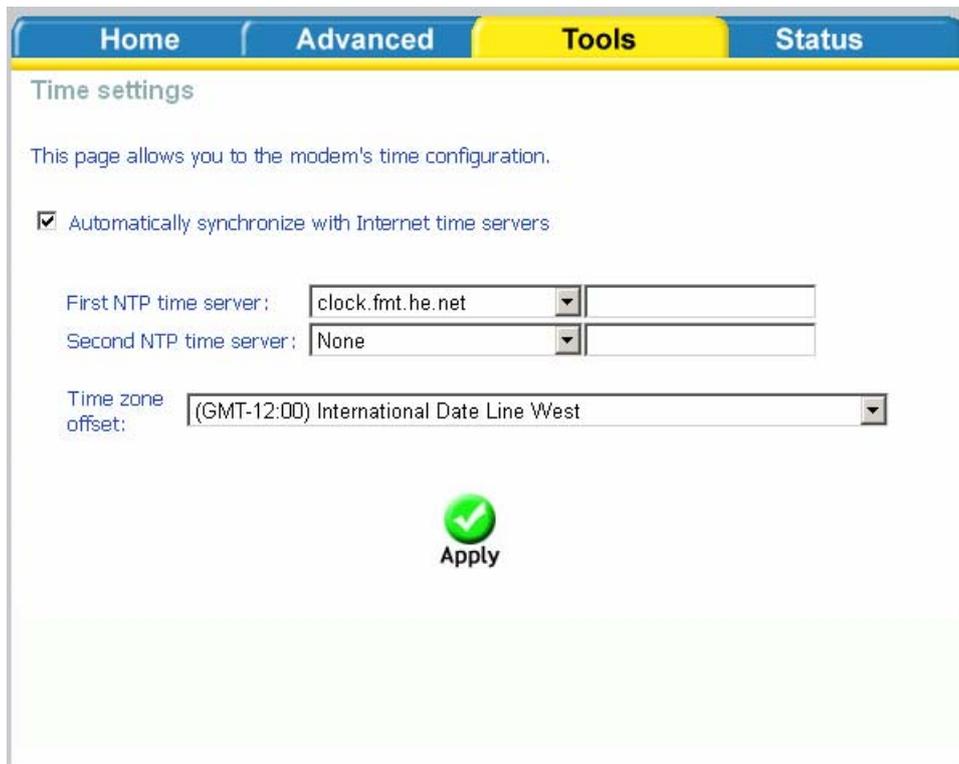
Time

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



The screenshot shows the 'Time settings' page in a web interface. At the top, there are four tabs: 'Home', 'Advanced', 'Tools' (which is highlighted in yellow), and 'Status'. Below the tabs, the page title is 'Time settings'. A descriptive text reads: 'This page allows you to the modem's time configuration.' Below this text is a single checkbox labeled 'Automatically synchronize with Internet time servers', which is currently unchecked. At the bottom center of the page, there is a green circular icon with a white checkmark and the word 'Apply' underneath it.

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



This screenshot shows the 'Time settings' page after the checkbox has been checked. The 'Tools' tab remains highlighted. The checkbox 'Automatically synchronize with Internet time servers' is now checked. Below the checkbox, three input fields have appeared: 'First NTP time server' with a dropdown menu showing 'clock.fmt.he.net', 'Second NTP time server' with a dropdown menu showing 'None', and 'Time zone offset' with a dropdown menu showing '(GMT-12:00) International Date Line West'. At the bottom center, the green 'Apply' button is still present.

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.



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** →



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** →



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

Home	Advanced	Tools	Status
System Log -- Configuration			
<p>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.</p>			
<p>Select the desired values and click 'Apply' to configure the system log options.</p>			
Log:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		
Log Level:	<input type="text" value="Debugging"/>		
Display Level:	<input type="text" value="Error"/>		
Mode:	<input type="text" value="Local"/>		
 Apply			

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.

System

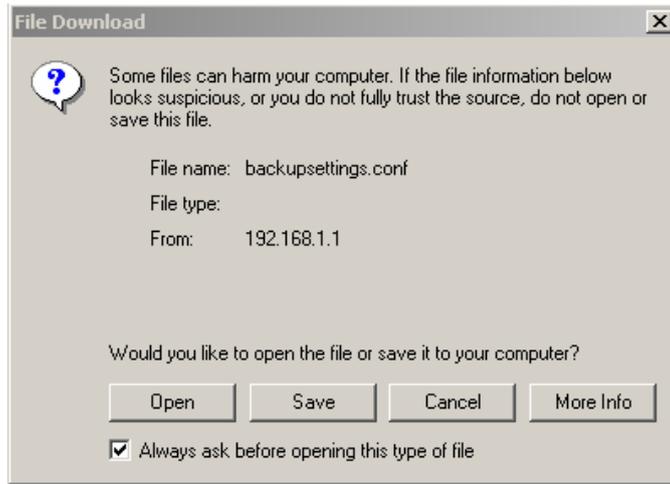
The system section includes several tools on one page, including save and reboot, backup settings, update settings, and restore default settings.

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.

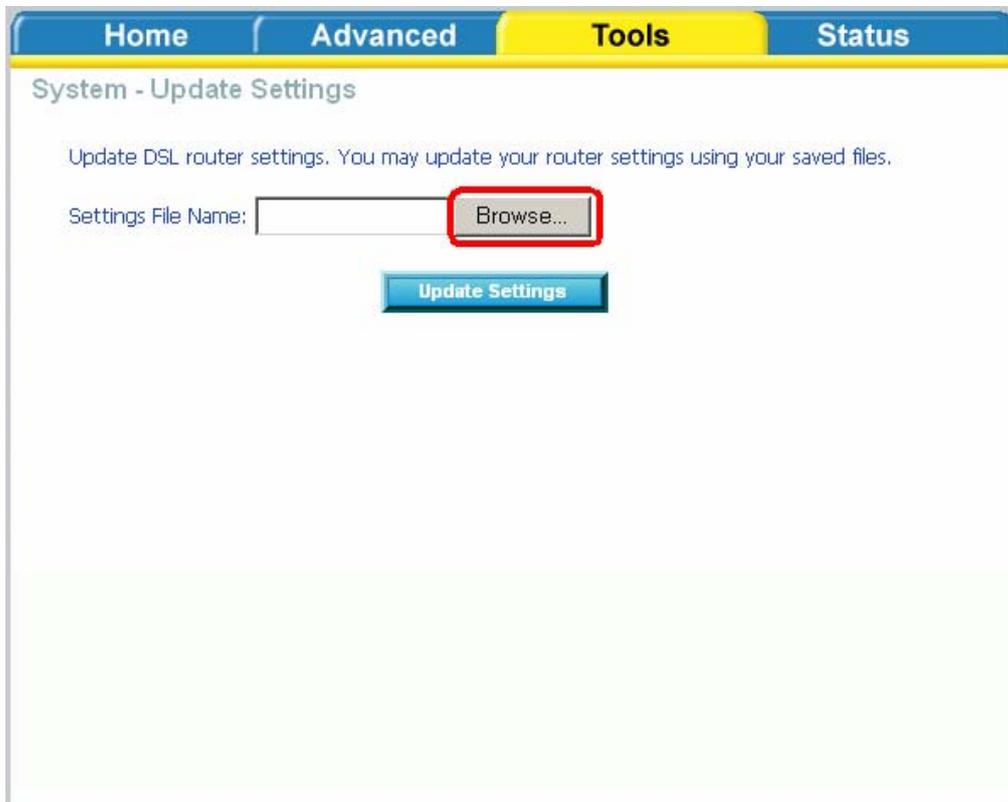
Backup Settings

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.



Update Settings

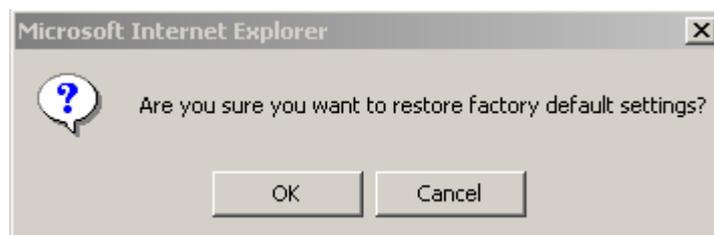
To load a previously saved configuration file onto your router, click **Browse** and select the file on your computer and then click on **Update Settings**.



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

Restore Default Settings

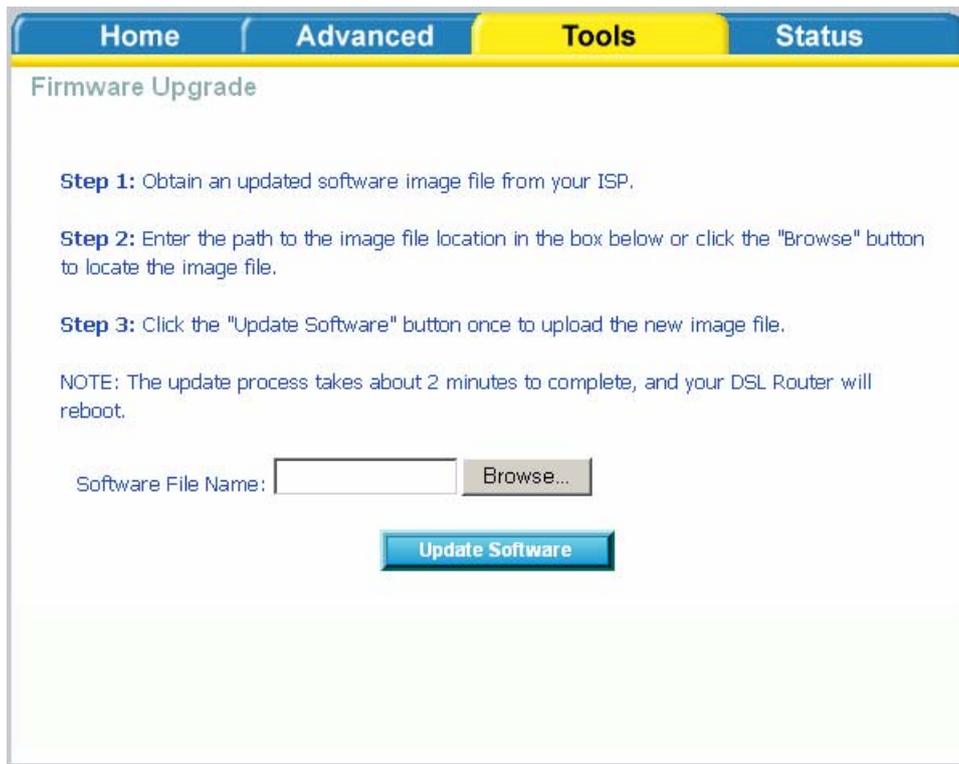
Restore Default will delete all current settings and restore the router to factory default settings. Click on the **Restore Default Settings** button to proceed. The following confirmation dialog will appear confirming your decision to restore default settings. Click on **OK** to continue.



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.



The screenshot shows a web interface with a navigation bar at the top containing 'Home', 'Advanced', 'Tools' (highlighted in yellow), and 'Status'. Below the navigation bar is a section titled 'Firmware Upgrade'. The page contains three numbered steps: 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. Below the steps is a note: NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. At the bottom of the page, there is a text input field labeled 'Software File Name:' followed by a 'Browse...' button and a large blue 'Update Software' button.

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.

pppoe_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(1-4) 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 connection:	FAIL	Help
Test authentication with ISP:	PASS	Help
Test the assigned IP address:	FAIL	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	PASS	Help

[Test](#) [Test With OAM F4](#)

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—

D-Link
Building Networks for People

DSL-2500U

Home | Advanced | Tools | **Status**

Device Info

Board ID:	D-1P
Software Version:	RU_DSL-2500U_3-06-04-0Z00.A2pB021c.d19b
Bootloader (CFE) Version:	1.0.37-6.5

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

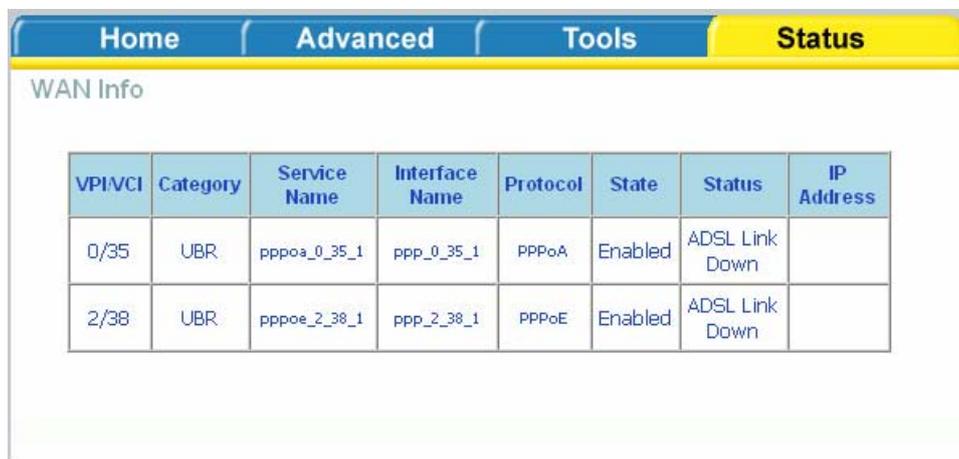
Access the DHCP Leases screen by clicking "DHCP" under "Statistics". This shows the computers, identified by the hostname and MAC address that have acquired IP addresses by the DHCP server with the time that the lease for the IP address is up.



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*.



VPI/VCI	Category	Service Name	Interface Name	Protocol	State	Status	IP Address
0/35	UBR	pppoe_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.

Home | Advanced | Tools | **Status**

Device Info -- Route

Flags: U - up, I - 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.

Home | Advanced | Tools | **Status**

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.

[Refresh](#)

LAN

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

Home | Advanced | Tools | **Status**

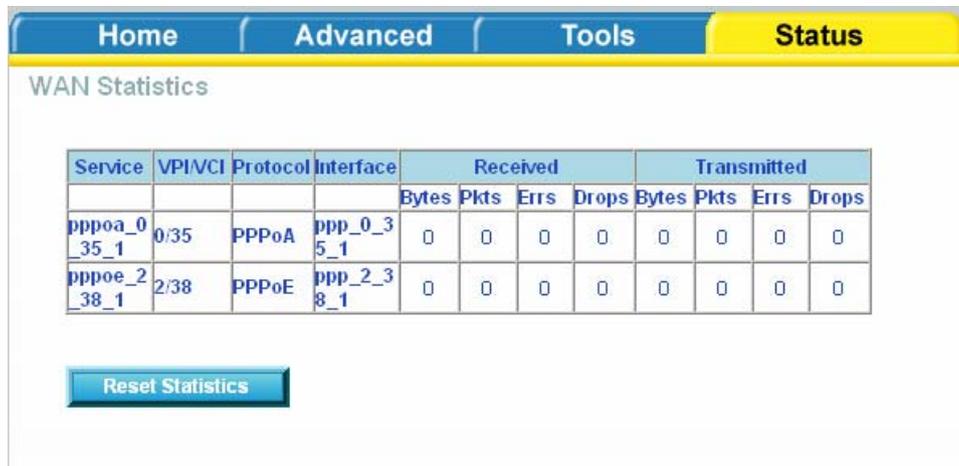
LAN Statistics

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	244894	2224	0	0	1145170	2289	0	0

[Reset Statistics](#)

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.



The screenshot shows a web interface with four navigation tabs: Home, Advanced, Tools, and Status. The Status tab is selected and highlighted in yellow. Below the tabs, the page title is "WAN Statistics". A table displays statistics for two WAN services. The table has columns for Service, VPI/VCI, Protocol, Interface, and two groups of four columns each for Received and Transmitted data (Bytes, Pkts, Errs, Drops). All values in the table are 0. Below the table is a "Reset Statistics" button.

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0a_0_35_1	0/35	PPPoA	ppp_0_35_1	0	0	0	0	0	0	0	0
ppp0e_2_38_1	2/38	PPPoE	ppp_2_38_1	0	0	0	0	0	0	0	0

[Reset Statistics](#)

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.

Home Advanced Tools Status

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

Reset Statistics

ADSL

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

HomeAdvancedToolsStatus

ADSL Statistics

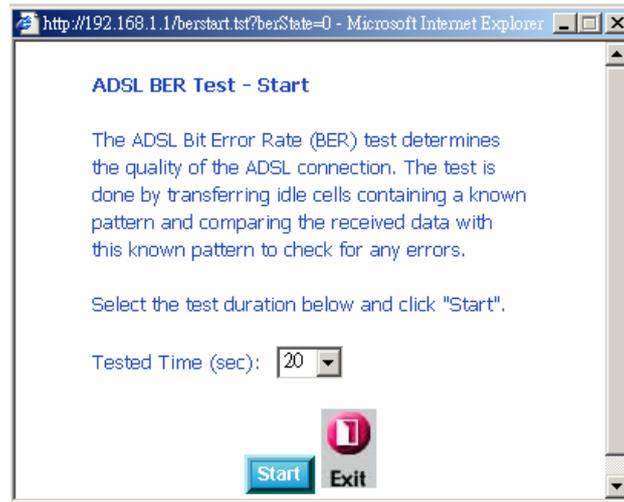
Mode:	G.DMT	
Type:	Fast	
Line Coding:	Trellis On	
Status:	No Defect	
Link Power State:	LO	
	Downstream	Upstream
SNR Margin (dB):	11.9	12.0
Attenuation (dB):	0.0	1.0
Output Power (dBm):	7.8	12.5
Attainable Rate (Kbps):	9568	1056
Rate (Kbps):	8000	800
K (number of bytes in DMT frame):	251	26
R (number 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 TestReset Statistics

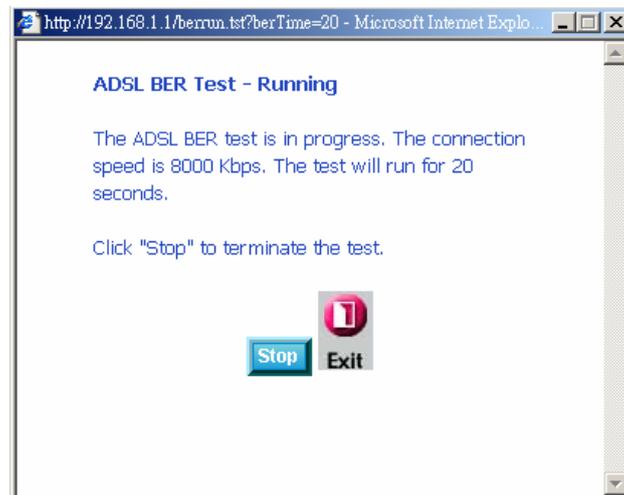
ADSL BER Test

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.



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.



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.

