

## Route

To access the **Device Info – Route** window, click the **Route** button in the **Device Info** directory.

This read-only window displays routing info.

Device Info -- Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.0.0.0	0.0.0.0	255.0.0.0	U	0		br0

## ARP

To access the **Device Info – ARP** window, click the **ARP** button in the **Device Info** directory.

This read-only window displays Address Resolution Protocol info.

Device Info -- ARP			
IP address	Flags	HW Address	Device
192.168.1.100	Complete	00:0C:6E:AA:B9:C0	br0

## DHCP

To access the **Device Info – DHCP Leases** window, click the **DHCP** button in the **Device Info** directory.

This read-only window displays DHCP lease info.

Device Info -- DHCP Leases			
Hostname	MAC Address	IP Address	Expires In

# Advanced Setup

This chapter includes the more advanced features used for network management and security as well as administrative tools to manage the Router, view status and other information used to examine performance and for troubleshooting.

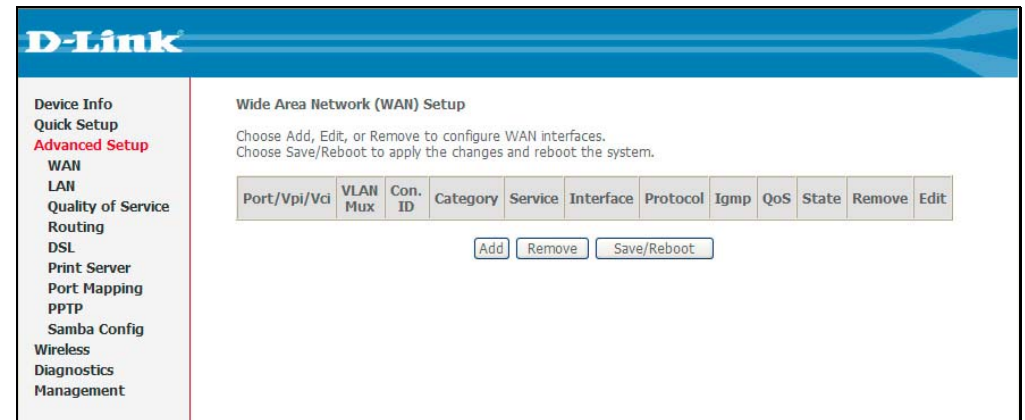
## WAN

To access the **Wide Area Network (WAN) Setup** window, click the **WAN** button in the **Advanced Setup** directory.

This window is used to configure the WAN interface. You can add, delete, and modify WAN interfaces on this window.

Once the desired changes to the WAN interface are complete, click the **Save/Reboot** button.

If you are setting up the WAN interface for the first time, click the **Add** button.



## Section 3 – Configuration

---

The **ATM PVC** Configuration window allows you to set up ATM PVC configuration. Enter a Port Identifier, Virtual Path Identifier, and Virtual Channel Identifier. The VPI and VCI values should be provided by your ISP. This window also allows you to enable QoS by ticking the Enable Quality of Service check box. Click the **Next** button to continue.

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

PORT: [0-3]

VPI: [0-255]

VCI: [32-65535]

VLAN Mux - Enable Multiple Protocols Over a Single PVC

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

## Section 3 – Configuration

This window allows you to select the appropriate connection type. The choices include PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), MAC Encapsulation Routing (MER), IP over ATM (IPoA), and Bridging (default).

This window also allows you to use the drop-down menu to select the desired Encapsulation Mode. Click the **Next** button to continue.

For further information about each of the five connection types available on the Router, please go to the Quick Setup section earlier in this manual as all of the windows are identical.

If the connection type of WAN interface is in Bridging, **Security IP Filtering** with the **MAC Filtering** and **Parental Control** sub-menus will appear in the **Advanced Setup** directory.

If the connection type of WAN Interface is not in Bridging, **NAT** and **Security** with **IP Filtering** and **Parental Control** will appear in the **Advanced Setup** directory.

**Connection Type**

Select the type of network protocol for IP over Ethernet as WAN interface

PPP over ATM (PPPoA)

PPP over Ethernet (PPPoE)

MAC Encapsulation Routing (MER)

IP over ATM (IPoA)

Bridging

**Encapsulation Mode**

LLC/SNAP-BRIDGING ▾

# LAN

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

To access the **Local Area Network (LAN) Setup** window, click the **LAN** button in the **Advanced Setup** directory.

This window allows you to set up a LAN interface. When you are finished, click either the **Save** or **Save/Reboot** button.

**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:

Subnet Mask:

Leased Time (hour):

Configure the second IP Address and Subnet Mask for LAN interface

## NAT

To access the **Network Address Translation (NAT) Setup** window, click the **NAT** button in the **Advanced Setup** directory. The **NAT** button appears when configuring WAN interface in PPPoA, PPPoE, MER or IPoA.

## Virtual Servers

This window is used to configure virtual server. You can add, delete, and modify virtual server on this window.

If you are setting up the virtual server, click the **Add** button.

**NAT -- Virtual Servers Setup**

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with 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 32 entries can be configured.

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

## Section 3 – Configuration

You can configure the service settings on this window by clicking the **Select a Service** radio button and then using the drop-down list to choose an existing service, or by clicking the **Custom Server** radio button and entering your own Application Rule in the field provided.

Click **Save/Apply** when you are finished with the virtual server configuration.

**NAT -- Virtual Servers**

Select the service name, and enter the server IP address and click "Save/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
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>

## Port Triggering

Some applications require that the remote parties open specific ports in the Router's firewall for access. Port Trigger dynamically opens the Open Ports in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using Trigger Ports. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the Open Ports.

Applications such as games, video conferencing, and other remote access applications require that specific ports in the Router's firewall be opened for access by applications.

Click the **Add** button to configure port triggering.

### NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application	Trigger		Open		Remove		
Name	Protocol	Port Range		Protocol	Port Range		
		Start	End		Start	End	



## Section 3 – Configuration

You can configure the port settings on this window by clicking the **Select an application** radio button and then using the drop-down list to choose an existing application, or by clicking the **Custom application** radio button and entering your own Application Rule in the field provided.

Click **Save/Apply** when you are finished with the port setting configuration. The new Application Rule will appear in the Port Triggering table.

**NAT -- Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

**Remaining number of entries that can be configured:32**

Application Name:

Select an application:  ▼

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>
<input type="text"/>	<input type="text"/>	TCP <span>▼</span>	<input type="text"/>	<input type="text"/>	TCP <span>▼</span>

## DMZ Host

Since some applications are not compatible with NAT, the Router supports use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and will therefore be visible to agents on the Internet with the right type of software. Keep in mind that any client PC in the DMZ will be exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through the DMZ.

To designate a DMZ IP address, type in the IP Address of the server or device on your LAN, and click the **Save/Apply** button.

**NAT -- 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:

## Security

To access the **Security** window, click the **Security** button in the **Advanced Setup** directory. The **Security** button appears after configuring WAN interface.

## IP Filtering

The **IP Filtering** button appears when configuring WAN interface in PPPoA, PPPoE, MER or IPoA.

### IP Filtering - Outgoing

This window allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Filters are used to allow or deny LAN or WAN users from accessing the Internet or your internal network.

If you are setting up the outgoing IP filtering, click the **Add** button.

**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.

Choose Add or Remove to configure outgoing IP filters.

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

## Section 3 – Configuration

Enter the information in the section. Explanations of parameters are described below. Click the **Save/Apply** button to add the entry in the Active Outbound IP Filtering table.

**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 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Select IP Range by:

Source Port (port or port:port):

Select IP Range by:

Destination Port (port or port:port):

Filters Parameter	Description	
Filter Name	Enter a name for the new filter.	
Protocol	Select the transport protocol (Any, TCP/UDP, TCP, UDP or ICMP) that will be used for the filter rule.	
Select IP Range by	Select either <b>IP address</b> or <b>Netmask</b> to show different items.	
	Source IP Address	Enter the start and end IP address for the range of IP addresses which you are creating the filter rule.
	Source IP Address & Source Subnet Mask	This is the IP address and their associated subnets for which you are creating the filter rule.
Source Port	The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule.	
Destination Port	The Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule.	

### IP Filtering – Incoming

The Inbound Filter allows you to create a filter rule to allow incoming IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. By default, all incoming IP traffic from the Internet is blocked when the firewall is enabled.

If you are setting up the incoming IP filtering, click the **Add** button.

Enter the information in the section. Explanations of parameters are described below. Click the **Save/Apply** button to add the entry in the Active Inbound IP Filtering table.

**Incoming IP Filtering Setup**

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

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

**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 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol: Any

Select IP Range by:

Source Port (port or port:port):

Select IP Range by:

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

pppoe\_1\_1\_35\_1/ppp\_1\_1\_35\_1

Filters Parameter	Description	
Filter Name	Enter a name for the new filter.	
Protocol	Select the transport protocol (Any, TCP/UDP, TCP, UDP or ICMP) that will be used for the filter rule.	
Select IP Range by	Select either <b>IP address</b> or <b>Netmask</b> to show different items.	
	Source IP Address	Enter the start and end IP address for the range of IP addresses which you are creating the filter rule.
	Source IP Address & Source Subnet Mask	This is the IP address and their associated subnets for which you are creating the filter rule.
Source Port	The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule.	
Destination Port	The Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule.	

## MAC Filtering

The **MAC Filtering** button appears when configuring WAN interface in Bridging.

MAC filtering are used to block or allow various types of packets through the WAN/LAN interface. This may be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address. Filter rules can be set up for source, destination or both. You can set up filter rules and disable the entire set of rules without losing the rules that have been configured.

Click **Change Policy** to configure the global policy as **Forwarded** or **Blocked**.

If you are setting up the MAC filtering, click the **Add** button.

**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
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

## Section 3 – Configuration

Select a protocol (All, PPPoE, IPv4, IPv6, Apple Talk, IPX, NetBEUI or IGMP) in the **Protocol Type** list, type in a Destination MAC, a Source MAC or both in the entry fields. Select a direction (LAN=>WAN, WAN=>LAN, or LAN<=>WAN) in the **Frame Direction** list. Click the **Save/Apply** button to add the entry in the Active Bridge Filters table.

### 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:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Select All

br\_0\_0\_35/nas\_0\_0\_35

## Quality of Service

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

To access the **QoS – Queue Management Configuration** window, click the **Quality of Service** button in the **Advanced Setup** directory.

This window allows you to set up QoS on the Router. When you are finished, click on the **Save/Apply** button.

**QoS -- Queue Management Configuration**

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.

**Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.**

**Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.**

Enable QoS



## Queue Config

Click the **Add** button to add a QoS Queue Configuration table entry.

**QoS Queue Configuration -- A maximum 24 entries can be configured.**  
**If you disable WMM function in Wireless Page, queues related to wireless will not take effects**  
**The QoS function has been disabled. Queues would not take effects.**

Interfacename	Description	Precedence	Queue Key	Enable	Remove
wireless	WMM Voice Priority	1	1		
wireless	WMM Voice Priority	2	2		
wireless	WMM Video Priority	3	3		
wireless	WMM Video Priority	4	4		
wireless	WMM Best Effort	5	5		
wireless	WMM Background	6	6		
wireless	WMM Background	7	7		
wireless	WMM Best Effort	8	8		

This window allows you to configure a QoS queue entry and assign it a specific network interface.

Click the **Save/Apply** button to save and activate the filter.

**QoS Queue Configuration**

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Save/Apply' to save and activate the filter.

Queue Configuration Status

Queue:

Queue Precedence:



# QoS Classification

Choose **Add** or **Remove** to configure network traffic classes.

Use this window to create a traffic class rule to classify the upstream traffic, assign a queue that defines the precedence and the interface, and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. Please remember that all of the specified conditions on this window must be met for the rule to take effect.

Click the **Save/Apply** button to save and activate this rule.

Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects  
The QoS function has been disabled. Classification rules would not take effects.

MARK				TRAFFIC CLASSIFICATION RULES													
Class Name	DSCP Mark	Queue ID	802.1P Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Order	Enable/Disable	Remove	Edit
<input type="button" value="Add"/> <input type="button" value="Save/Apply"/>																	

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP 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 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

**Assign ATM Priority and/or DSCP Mark for the class**  
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the corresponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled:

**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:

Differentiated Services Code Point (DSCP) Check:

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):

Source MAC Address:  (The MAC address format is xx:xx:xx:xx:xx:xx)

Source MAC Mask:

Destination MAC Address:  (The MAC address format is xx:xx:xx:xx:xx:xx)

Destination MAC Mask:

**SET-2**

802.1p Priority:

# Routing

To access the **Routing** windows, click the **Routing** button in the **Advanced Setup** directory.

## Default Gateway

If the **Enable Automatic Assigned Default Gateway** checkbox is ticked, the Router will accept the first default gateway assignment received from one of the enabled PPPoA, PPPoE, or MER/DHCP enabled PVC(s). If this checkbox is not ticked, enter the static default gateway and/or a WAN interface. Click the **Save/Apply** button when you are finished.

**Routing -- 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 'Save/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

Set PPTP to Default Route

Save/Apply

## Static Route

Click the **Add** button on the **Routing – Static Route** window to access the following window displayed on the next page.

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

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

Add Remove

Enter the static routing information for an entry to the routing table.  
Click the **Save/Apply** button when you are finished.

**Routing -- Static Route Add**

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

Destination Network Address:

Subnet Mask:

Use Gateway IP Address

Use Interface

## RIP

The **RIP** button appears when configuring WAN interface in **Advanced Setup -> WAN -> Routing**.

The Router supports both RIP-1 and RIP-2 exchanges with other routers.

Click the **Enabled** radio button in **Global RIP Mode** to active the function.

You can also configure individual interface in the table below.

**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 'Save/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_10_70_1	0/10/70	2	Passive	<input type="checkbox"/>

## DNS

To access the **DNS** windows, click the **DNS** button in the **Advanced Setup** directory. The **NAT** button appears when configuring WAN interface in PPPoA, PPPoE, MER or IPoA.

### DNS Server

If you have not been given specific DNS server IP addresses or if the Router is not pre-configured with DNS server information, tick the **Enable Automatic Assigned DNS** checkbox. Auto discovery DNS instructs the Router to automatically obtain the DNS IP address from the ISP through DHCP. If your WAN connection uses a Static IP address, auto discovery for DNS cannot be used.

If you have DNS IP addresses provided by your ISP, deselect the **Enable Automatic Assigned DNS** checkbox and enter these IP addresses in the available entry fields for the Primary DNS Server and the Secondary DNS Server. Click the **Save** button when you are finished.

**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 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

Enable Automatic Assigned DNS

Save

### Dynamic DNS

The Router supports Dynamic DNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form [hostname.dyndns.org](http://hostname.dyndns.org), Many ISPs assign public IP addresses using DHCP, this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS providers.

Click **Add** to see the Add DDNS Settings section.

**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

Add Remove

Enter the required DDNS information, click the **Save/Apply** button to save the information.



**Note**

*DDNS requires that an account be setup with one of the supported DDNS servers prior to engaging it on the Router. This function will not work without an accepted account with a DDNS server.*

**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