LohuisNetworks

Wireless ADSL2/2+Router Modem

MODEL NO.: LH200DRG

User Manual

Version 1.0

Version Date: Sept., 2008

Document Number: TCD-3162UG

Table of Contents

General Information

The 4-Port Wireless Ethernet Router features 4 LAN ports and wireless ability.

Package Contents

The package includes one of each of the following items—

4-Port wireless Ethernet router Modem
12 VAC AC power adapter
RJ-11 telephone cable
RJ-45 Ethernet cable
Splitter
CD for User Manual
Quick Guide

Safety Instructions—please read.

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.

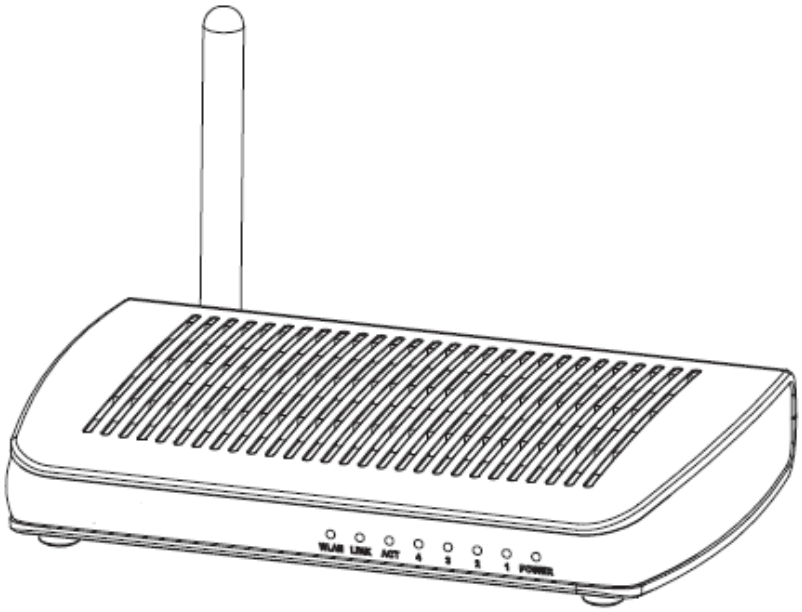
Plug this equipment into a surge protector to reduce the risk of damage from power surges and lightning strikes.

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.

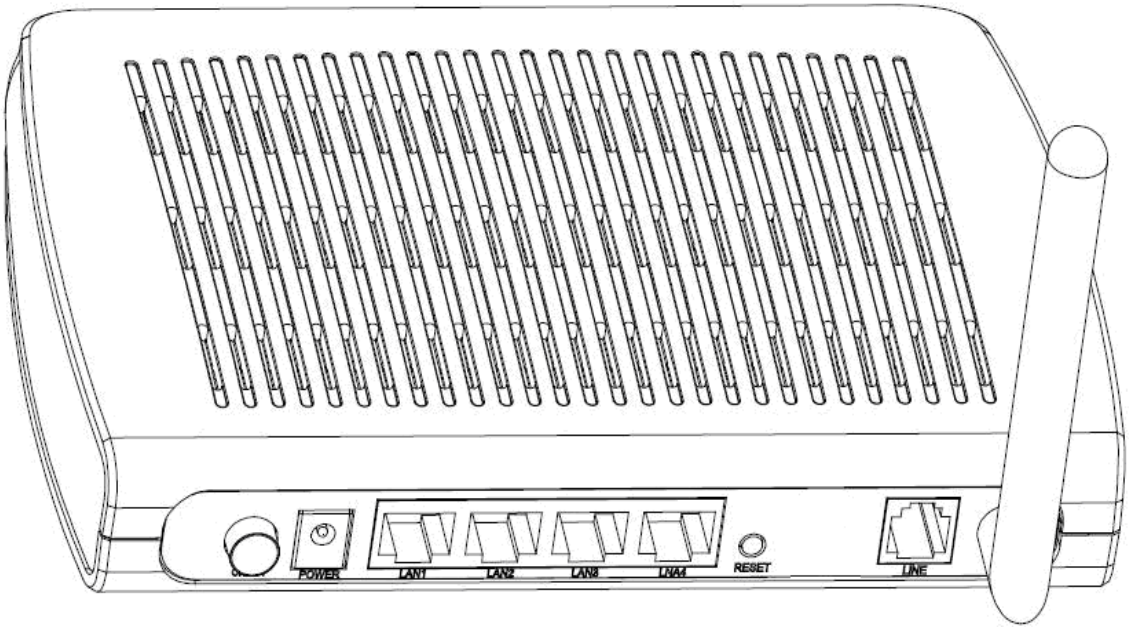
Unplug equipment first before cleaning. A damp cloth can be used to clean the equipment. Do not use liquid / aerosol cleaners or magnetic / static cleaning devices.

Front Panel View



LED	Mode	Indication
WLAN	Off	Wireless is disabled.
	Blinking	Wireless is enabled or wireless traffic.
Link	On	ADSL link established and active.
	Blinking	ADSL is not connected.
	Quick blinking	ADSL is trying to establish link。
ACT	Off	ADSL is not connected.
	blinking	ADSL traffic.
LAN1-LAN4	On	Router is connected to the LAN.
	Off	No connection to the LAN. Check if the LAN cable is connected to the router.
	Blinking	LAN traffic
POWER	On	Router is powered on.
	Off	Router is not powered. Check if the router is plugged in and if the power switch is turned on.

Back Panel View

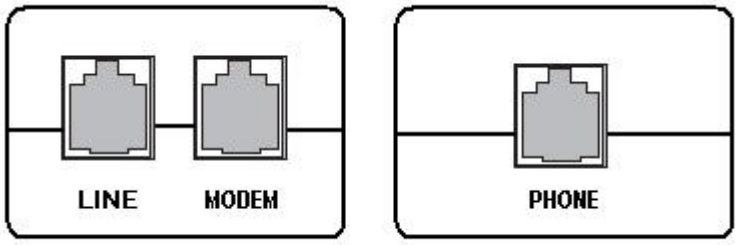


Port	Description
On / Off	Press to turn the router on and off.
Power	Connects to a 12 VAC AC power adapter.
LAN1-LAN4	RJ-45 connects the unit to an Ethernet device such as a PC or a switch.
Reset	Restart—press the button for less than 4 seconds. Default settings—press the button for 4 seconds or longer
Line	RJ-11 cable connects to the splitter provided.

Installing the Router

Connect the ADSL Line and Telephone

An RJ-11 cable will be connected to the wall phone jack and the Line - end of the splitter. Connect another RJ-11 phone wire from the modem-end of the splitter to the port labeled “line” on the router. The third RJ-11 phone wire will be needed to connect the telephone to the phone-end of the splitter.



NOTE: See connections on the installation diagram.

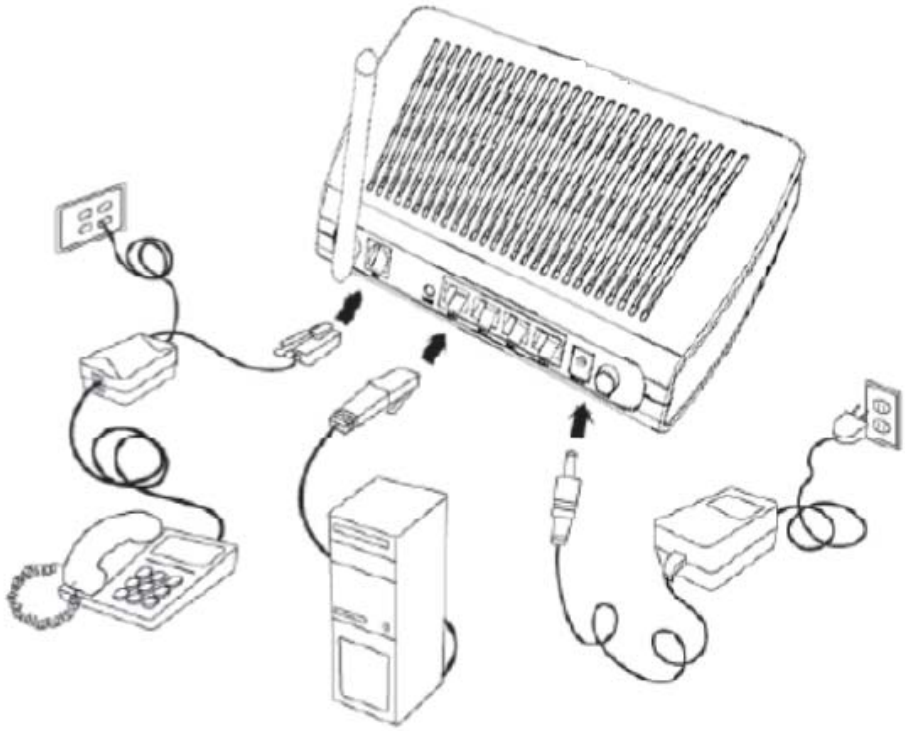
Connect the PC to the Router

Use the Ethernet cable to connect your computer directly to the router. Connect one end of the Ethernet cable to one of the ports labeled LAN on the rear panel of the router and connect the other end to the Ethernet port of your compute. Attach any additional PCs to the router using RJ-45 cables to the port labeled LAN on the rear panel of the router.

Connect the Power Adapter

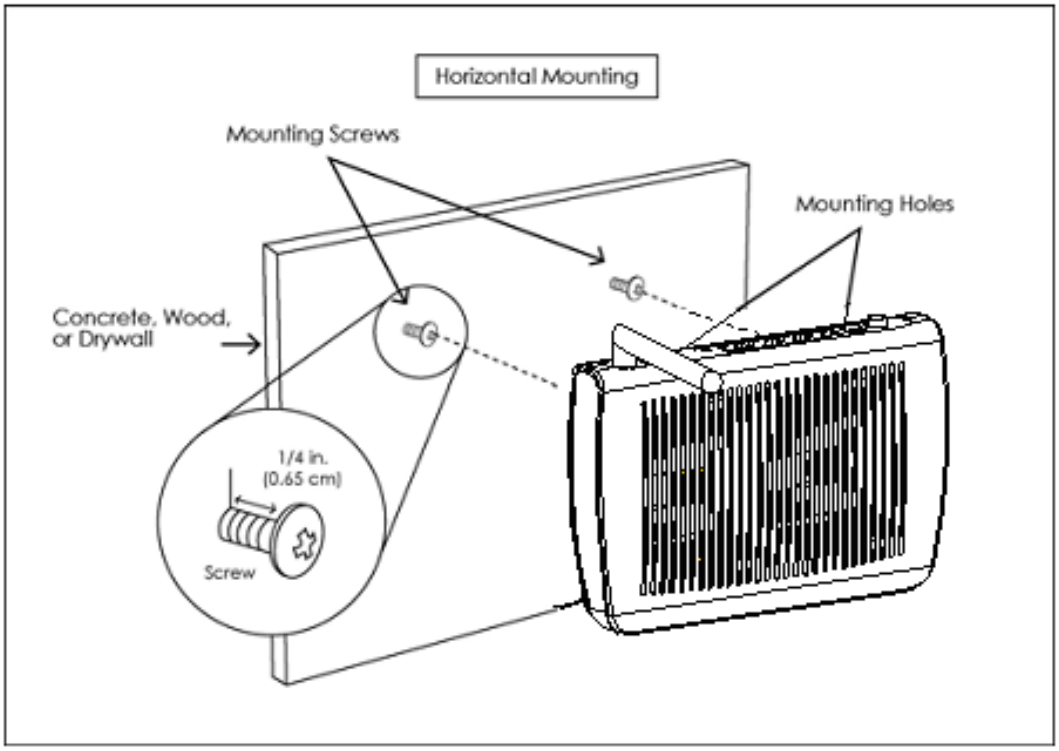
Complete the process by connecting the AC power adapter to the POWER connector on the back of the device and plug the adapter into a wall outlet or power strip. Then turn on and boot up your PC and any LAN devices, such as hubs or switches, and any computers connected to them.

Installation Diagram



Mounting the Router

The router can be mounted on the wall with the screws provided. Mounting can be done on wall material including concrete, wood, or drywall. Select an appropriate location free from obstructions or any possible interference. Make sure the cables can be easily attached to the router without strain. The illustration below shows how to mount the router horizontally on a wall.



Configuring Your Computer

Prior to accessing the router through the LAN port, note the following necessary configurations—

Your PC' s TCP/IP address: 192.168.1.___(The last number is any number between 2 and 254)

The router's default IP address: 192.168.1.1

Subnet mask: 255.255.255.0

Below are the procedures for configuring your computer. Follow the instructions for the operating system that you are using.

Windows 2000

1. In the Windows taskbar, click on the Start button and point to Settings, Control Panel, and Network and Dial-up Connections (in that order).

2. Click on Local Area Connection. When you have the Local Area Connection Status window open, click on Properties.

3. Listed in the window are the installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, and you can skip to Step 10.

4. If Internet Protocol (TCP/IP) does not appear as an installed component, then click on Install.

5. In the Select Network Component Type window, click on protocol and then the Add button.

6. Select Internet Protocol (TCP/IP) from the list and then click on OK.

7. If prompted to restart your computer with the new settings, click OK.

8. After your computer restarts, click on the Network and Dial- up Connections icon again, and right click on the Local Area Connection icon and then select Properties.

9. In the Local Area Connection Properties dialog box, select Internet Protocol (TCP/IP) and then click on Properties.

10. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled Use the following IP address and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.

11. Click on OK twice to save your changes and then close the Control Panel.

Windows XP

1. In the Windows taskbar, click on the Start button and point to Settings and then click Network Connections.

2. In the Network Connections window, right click on the Local Area Connection icon and click on properties.

3. Listed in the Local Area Connection window are the installed network components. Make sure the box for Internet Protocol (TCP/IP) is checked and then click on Properties.

4. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled Use the following IP address and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.

5. Click on OK twice to save your changes and then close the Control Panel.

Logging into the Router

This section explains how to login to your router using the following steps—

1. Launch your web browser.
2. Enter the URL http://192.168.1.1 in the address bar and click on Enter.

A login screen like the one below will be displayed after you connect to the user interface.

3. Enter your user name and password, and then click on OK to display the user interface.

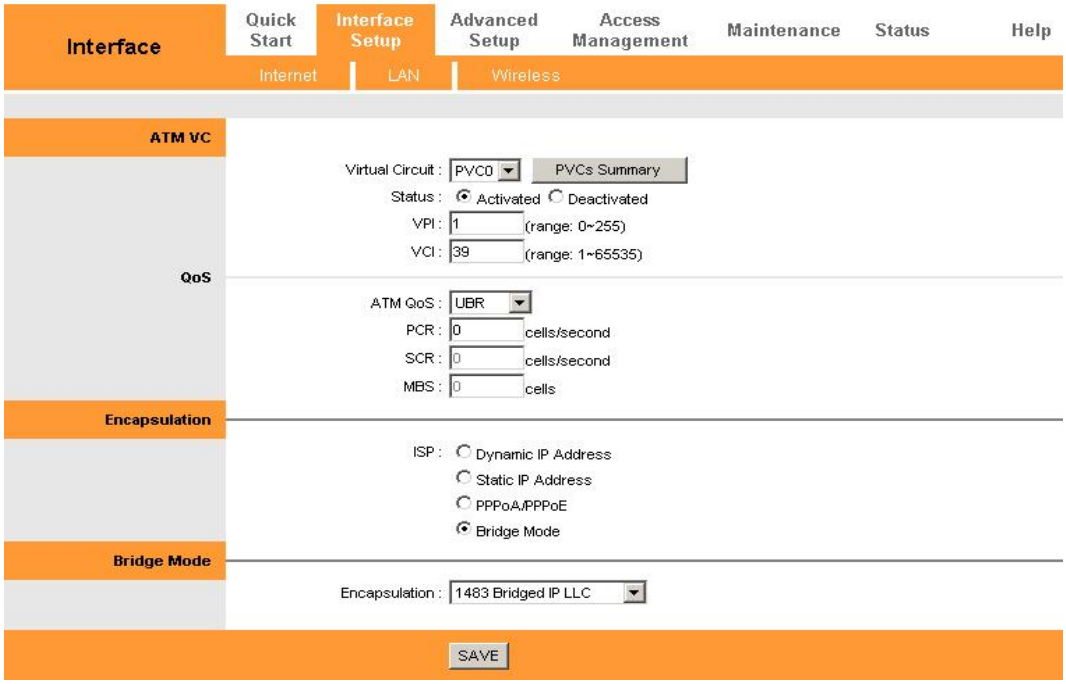
NOTE: There is one default user name and password combinations. The user / user name and password combination can display device status. The admin / admin combination can perform all functions. Passwords can be changed at any time.

Interface Setup

This section of the user manual is on the Interface configurations of the router. The under Interface Setup are Internet, LAN and Wireless.

Internet

The Internet Configuration screen allows you to configure the ATM VC and Encapsulation.



1、ATM VC & QoS

The ATM PVC Configuration screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a ATM QoS service category.

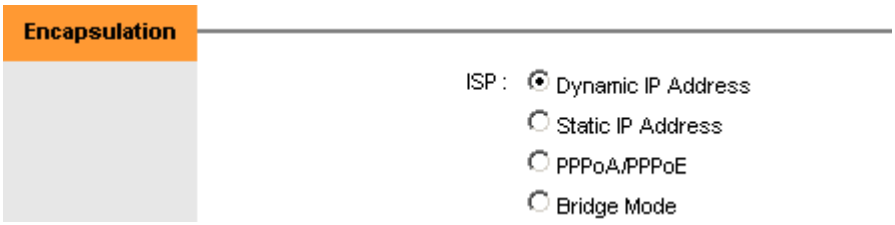
Asynchronous transfer mode (ATM) is a protocol that arranges data into small, uniform-sized cells with VCI data, as opposed to variable-sized data packets. ATM settings are used to connect to your ISP. Your ISP provides your VPI and VCI setting information. You can configure up to 8 virtual circuits (VC), each using different encapsulations, if you apply for 8 different VCs from your ISP. You must activate each VC for it to take effect. For permanent virtual circuit (PVC) management, you can use ATM Quality of Service (QoS) to set up each PVC traffic line's priority.

Verify the following values with your ISP before you change them.

LABEL	DESCRIPTION
Virtual Circuit	Select the PVC you wish to modify.
Status	Each PVC can be toggled Activated or Deactivate.
VPI	Enter the VPI here. VPI can range from 0 to 255.
VCI	Enter the VCI here. VCI can range from 1 to 65535.
ATM QoS	Select the QoS type for the PVC in question from the dropdown list.
PCR	Enter the PCR here. For all QoS types.
SCR	Enter the SCR here. Only for rtVBR and nrtVBR.
MBS	Enter the MBS here. Only for rtVBR and nrtVBR.

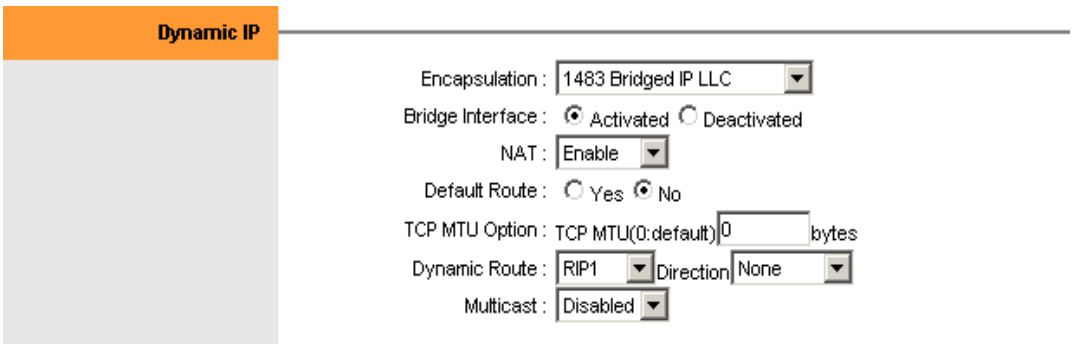
The PVCs Summary button opens a new window that displays the current PVC settings.

2、Encapsulation



Select the encapsulation protocol your ISP uses. The following section will vary depending on which encapsulation protocol you select.

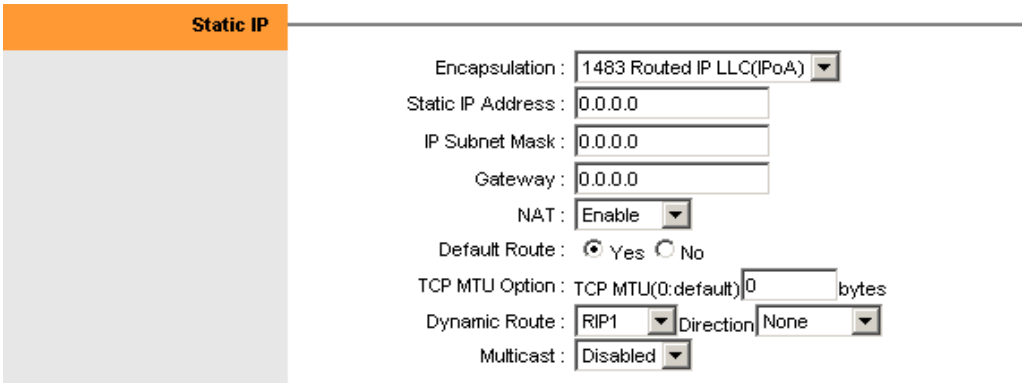
◆ Dynamic IP Address



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet data.
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the dropdown list.

◆ Static IP Address

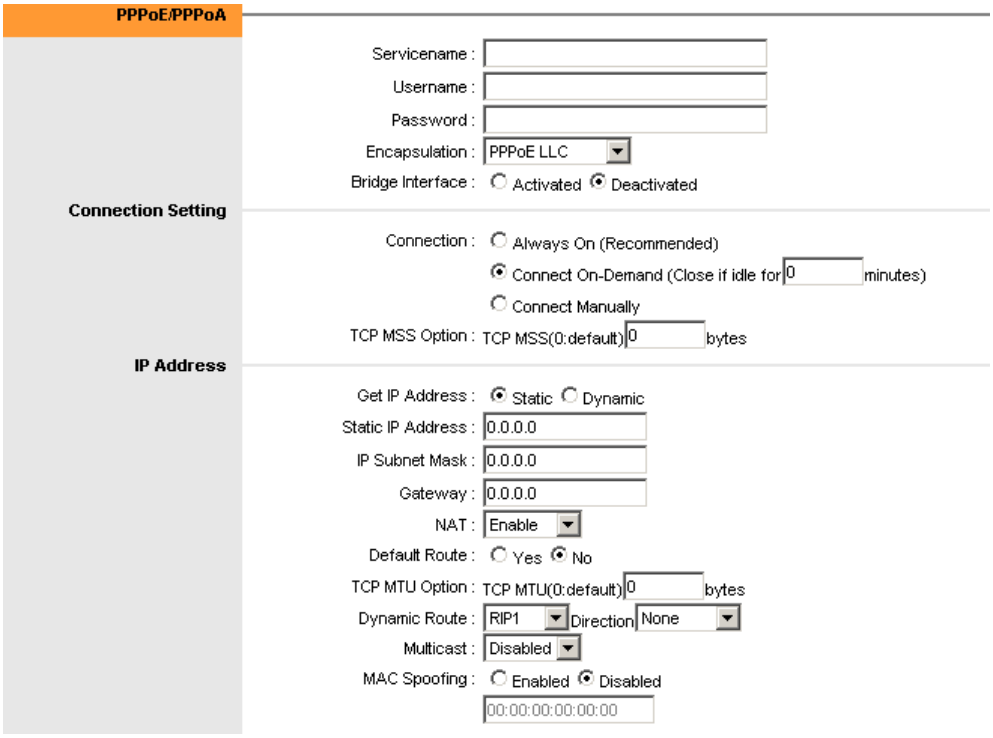


The following table describes the labels in this screen.

LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.
Static IP Address	Enter the static IP Address here.
IP Subnet Mask	Enter the IP Subnet Mask here.
Gateway	Enter the Gateway address here.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the

Your ISP should provide the above information.

- **PPPoE/PPPoA**



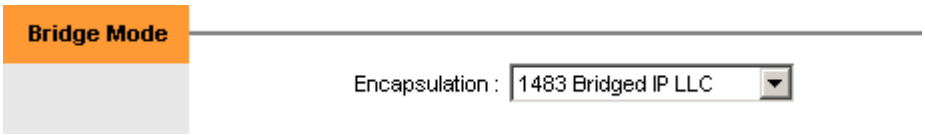
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Username	Enter your username here.
Password	Enter your password here.
Encapsulation	Select your encapsulation type from the dropdown list.
Connection	Select whether your connection is always on or if it connects on demand. If on demand, specify how many minutes the
TCP MSS Option	Enter the TCP MSS you wish to use here.
Get IP Address	Choose whether the device obtains the IP address statically or dynamically.
Static IP Address	Enter the static IP address here. Only if you chose Static
IP Subnet Mask	Enter the IP subnet mask here. Only if you chose Static
Gateway	Enter the gateway here. Only if you chose Static above.
NAT	Select whether NAT is Enabled or Disabled.
Default Route	Select whether this PVC will be the default route for Internet
Dynamic Route	Select the RIP type and direction from the dropdown lists.
Multicast	Select the multicast protocol you wish to use from the

Your ISP should provide the above information. Note that you must enter

the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given.

◆ Bridge Mode

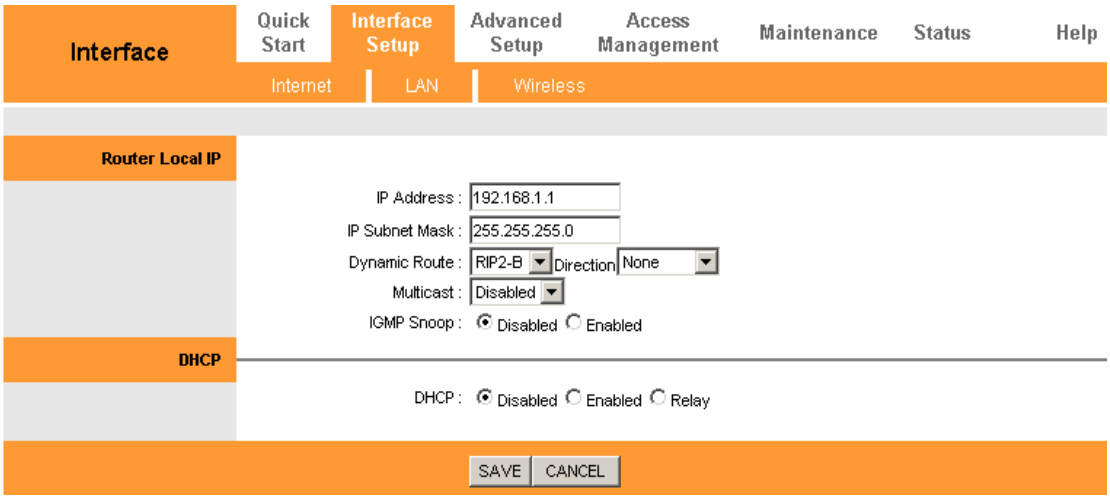


The following table describes the labels in this screen.

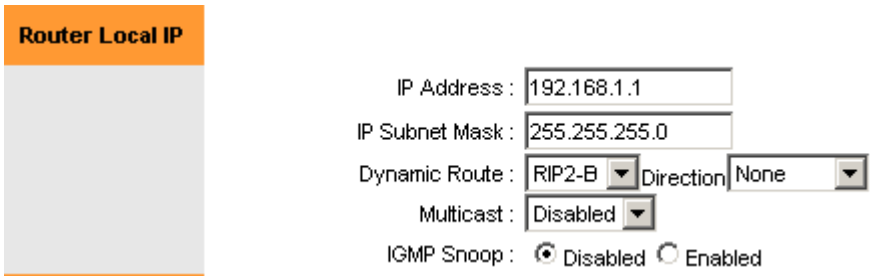
LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.

LAN

You can configure the DSL Router IP address and Subnet Mask for the LAN interface to correspond your LAN's IP Subnet. When you are done making changes, click on SAVE to save your changes or CANCEL to reset the fields to their original states.



1、Router Local IP



The following table describes the labels in this screen.

LABEL	DESCRIPTION
IP Address	Enter the IP address you wish to use with your LAN here.
IP Subnet Mask	Enter the IP subnet mask you wish to use with your LAN here.
Dynamic Route	Select the Routing Information Protocol (RIP) you wish to use from the dropdown list and the direction you want from the dropdown list. The RIP and direction options are described below.
Multicast	Select the multicast protocol you wish to use from the dropdown list.
IGMP Snoop	Select whether IGMP Snoop is Enabled or Disabled.

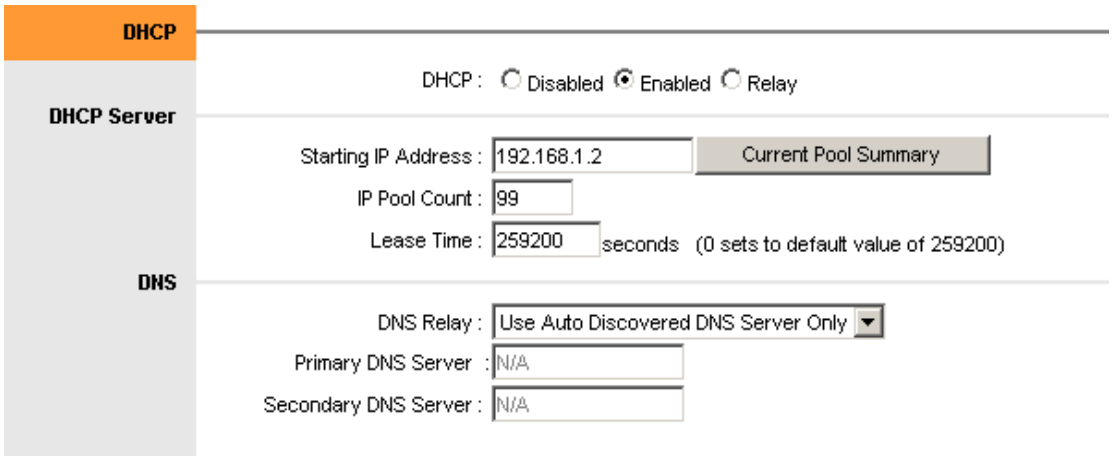
2、DHCP

Dynamic Host Control Protocol (DHCP), when enabled, gives out IP addresses to a device that requests an IP address to be logged on to the network as it boots up. A device must be configured as a DHCP client to obtain the IP address automatically. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

The next screen will vary depending on the **DHCP** option you selected.

◆ Enabled DHCP

The following screen will appear if you selected Enabled in the **DHCP** Server field.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
Starting IP Address	Enter the starting IP address you wish to use as the DHCP server's IP assignment.
IP Pool Count	Enter the maximum user pool size you wish to allow.
Lease Time	Enter the amount of time you wish to lease out a given IP address.
DNS Relay	Select the DNS relay option you wish to use from the dropdown list.
Primary DNS Server	Enter the primary DNS server IP address you wish to use. For user discovered DNS only.
Secondary DNS Server	Enter the secondary DNS server IP address you wish to use. For user discovered DNS only.

The Current Pool Summary button opens a new window that displays the current DHCP IP Pool settings.

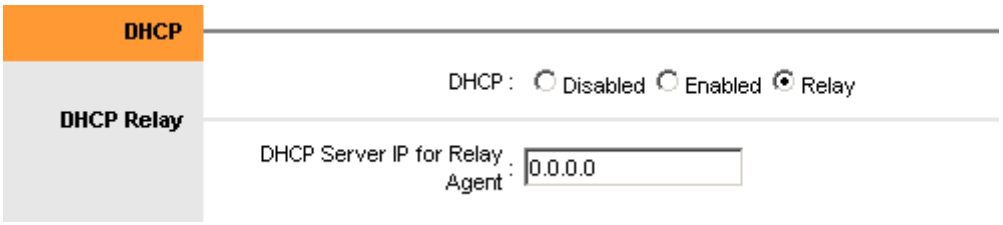
DHCP IP Pool Summary

Host Name	IP Address	MAC Address
164300	192.168.1.2	00-01-36-0A-6D-8A

If you don't want to use the DNS Relay option, set the DNS relay to "Use User Discovered DNS Server Only" and set both Primary and Secondary DNS Servers to "0.0.0.0".

- **Relay DHCP**

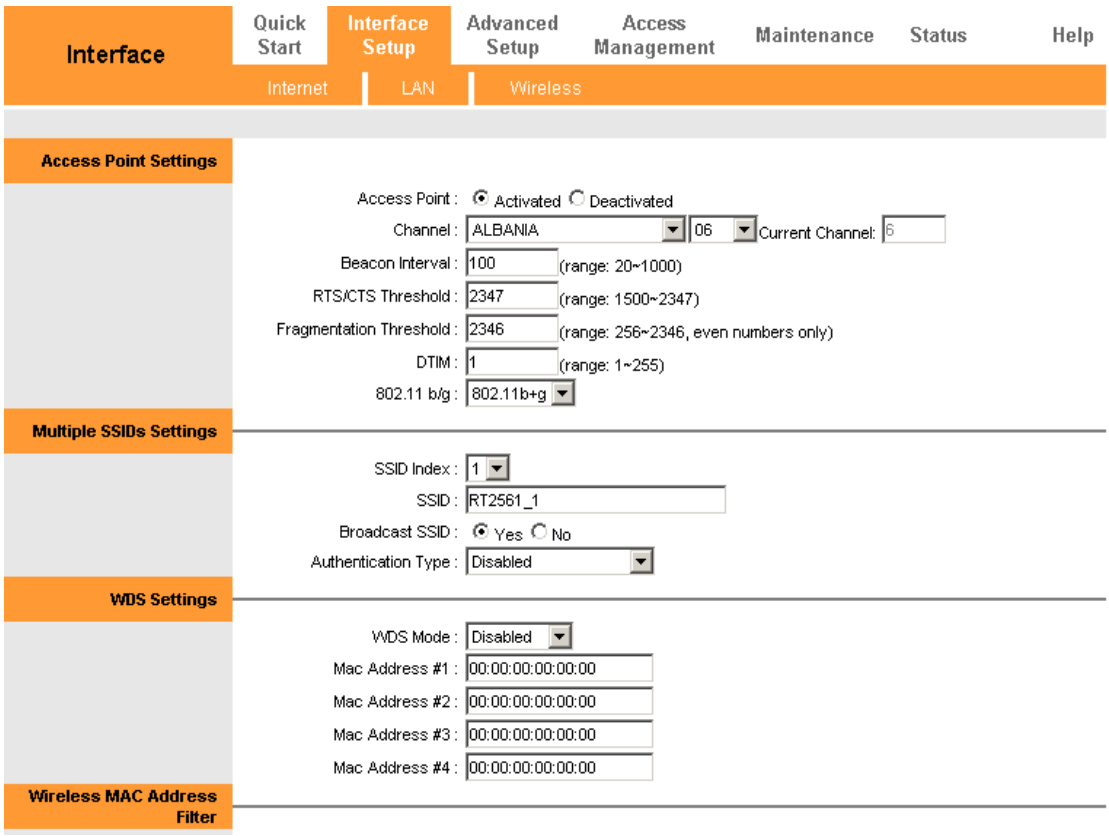
The following screen will appear if you selected Relay in the DHCP Server field.



A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the IP addresses. If the DHCP Relay option is enabled, DHCP requests from local PCs will be forwarded to the DHCP server that runs on WAN side. For this function working properly, you must run it on router mode only; disable the DHCP server on the LAN port and make sure the routing table has the correct routing entry.

Wireless

This section introduces the wireless LAN and some basic configurations. Wireless LANs can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to the wired LAN.



1、Access Point Settings

Access Point: Default setting is set to **Activated**. If you do not have any wireless, both 802.11g and 802.11b, device in your network, select **Deactivated.**

Channel: Select the country or the region from the drop-down list box, and select a channel.

Beacon interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.

RTS/CTS Threshold: The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be

larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake Enter a value between 1500 and 2347.

Fragmentation Threshold: The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.

DMIT: This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

802.11b/g: The default setting is **802.11b+g** (Mixed mode). If you do not know or have both 11g and 11b devices in your network, then keep the default in

2、Multiple SSIDs Settings

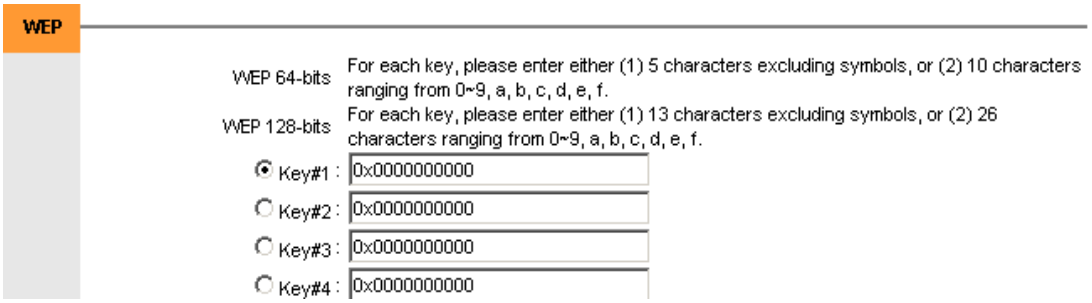
SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default name to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Broadcast SSID: Select **No** to hide the SSID in so a station cannot obtain the SSID through passive scanning. Select **Yes** to make the SSID visible so a station can obtain the SSID through passive scanning.

Authentication Type: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP.&WPA. If you require high security for transmissions, there are five alternatives to select from: **Disabled, WEP-64bits, WEP-128bits, WPA-PSK, WPA2-PSK.**

The next screen will vary depending on the Authentication **T**ype option you selected.

◆ **WEP**

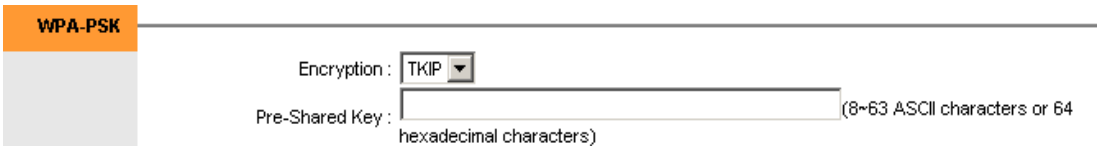


Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bitWEP and 128-bitWEP respectively.

If you chose **WEP 64-bits**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").

If you chose **WEP 128-bits**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.

◆ **WPA-SPK**



.

Encryption: TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

Pre-Shared key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 64 characters.

3、Wireless MAC Address Filter

The MAC filter screen allows you to configure the router to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the router (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your router's MAC filter settings, click Wireless LAN, MAC Filter to open the MAC Filter screen. The screen appears as shown.

.

Active: Select **Activated** to enable MAC address filtering.
Action: Define the filter action for the list of MAC addresses in the MAC address filter table.

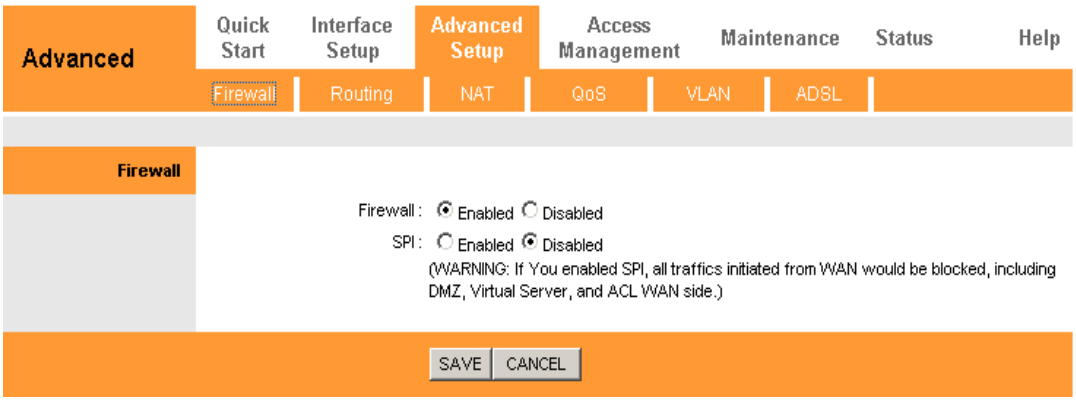
Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the router.

MAC Address: Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the router in these address fields.

Advanced Setup

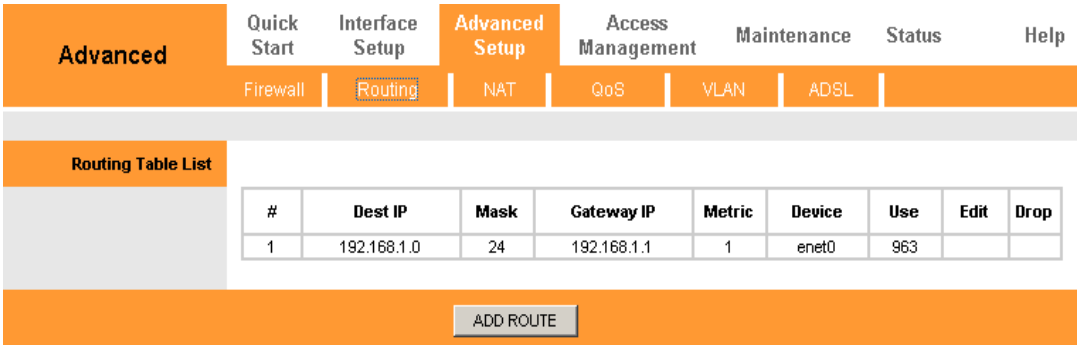
This section of the user manual is on the advanced configurations of the router. The topics under Advanced Setup are Firewall, Routing, NAT, QOS, VLAN and ADSL .

Firewall

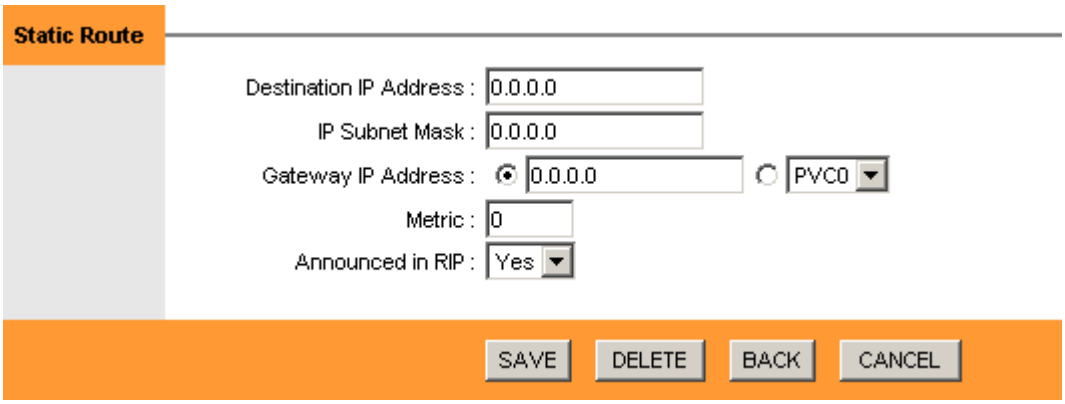


Select whether the Firewall and SPI will be enabled, and click on SAVE.

Routing



This screen shows the routing rules you have already set. A few defaults have been configured for you. To add your own route, click on the Add Route button.



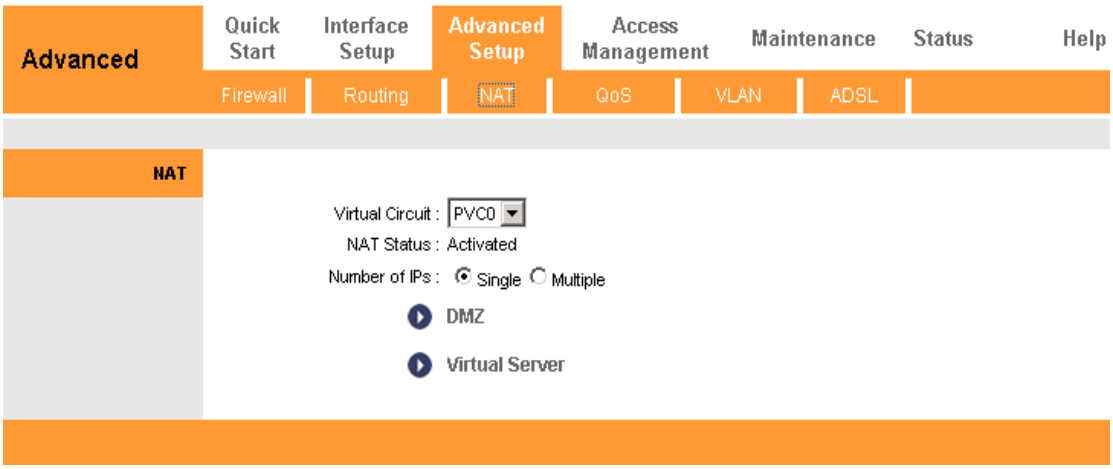
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Destination IP Address	Enter the destination IP address for this routing rule.
IP Subnet Mask	Enter the destination IP subnet mask for this routing rule.
Gateway IP Address	Enter the gateway IP address for this routing rule or select which PVC will be affected by this routing rule.
Metric	Enter the metric for this routing rule.
Announce in RIP	Choose whether this route is included in RIP broadcasts.

When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set, BACK to return to the previous screen or CANCEL to exit without saving.

NAT

Network Address Translation (NAT) translates the host IP address in a packet used within one network to a different IP address known within another network.

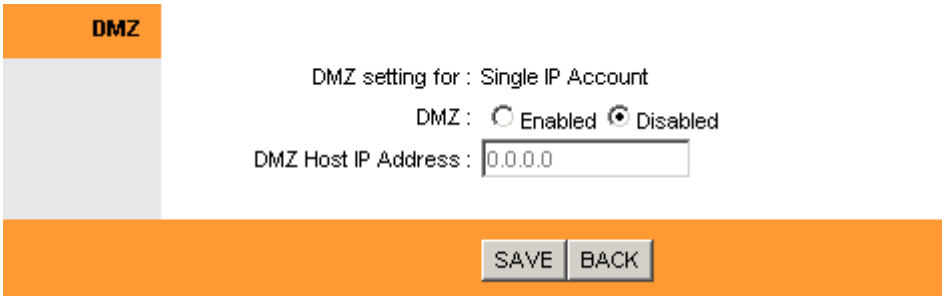


The following table describes the labels in this screen.

LABEL	DESCRIPTION
Virtual Circuit	Select the virtual circuit you wish to edit from the dropdown list.
NAT Status	The NAT status of the selected VC.
Number of IPs	Toggle whether the Virtual Circuit NAT affects a Single IP or Multiple IPs.
DMZ	Click this link to go to the DMZ screen.
Virtual Server	Click this link to go to the Virtual Server screen.

◆ DMZ

A demilitarized zone (DMZ) is a host between a private local network and the outside public network. It prevents outside users from gaining access to a server that you wish to keep private. Users of the public network outside the company can only access the DMZ host.



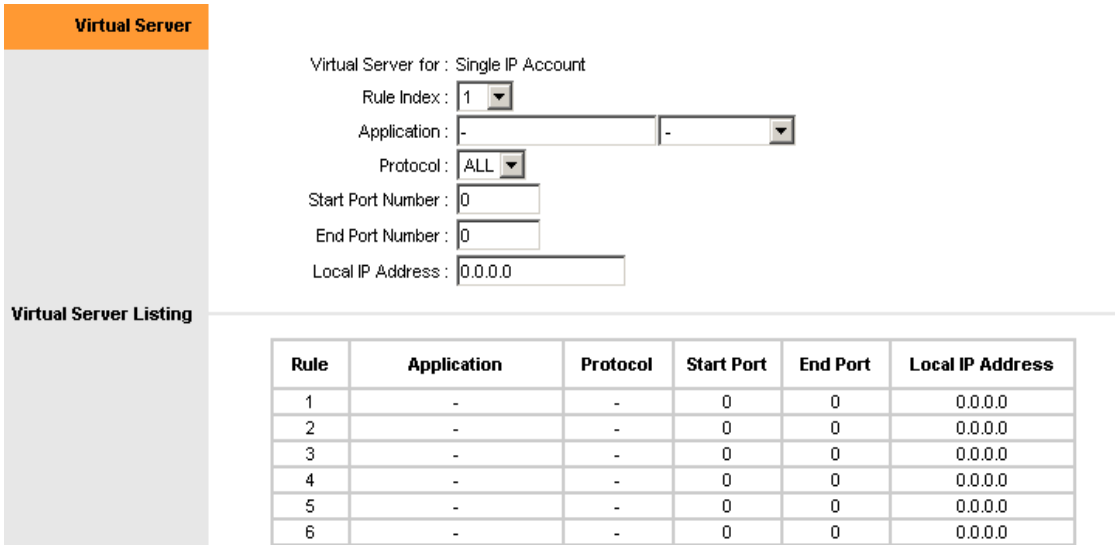
The **f**ollowing table describes the labels in this screen.

LABEL	DESCRIPTION
DMZ	Toggle the DMZ function Enabled or Disabled.
DMZ Host IP Address	Enter the IP address of the DMZ host you wish to use.

When you are done making changes, click on SAVE to save your changes or on BACK to return to the previous screen.

◆ Virtual Server

A virtual server is a server behind NAT (on the LAN), such as a Web server or FTP server, which you can make visible to the outside world while NAT makes your network appear as a single machine.



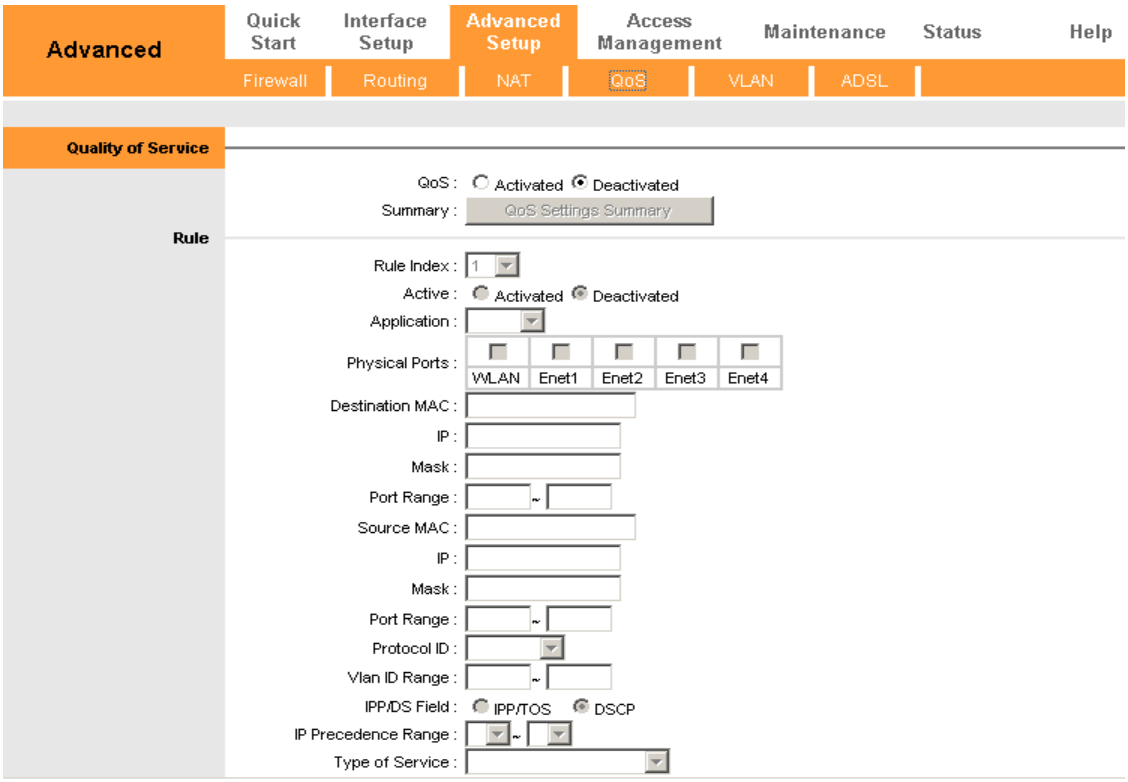
The **f**ollowing table describes the labels in this screen.

LABEL	DESCRIPTION
Rule Index	Select which rule index to use with this virtual circuit. All VCs with the same IP will use the same rules.
Application	Select the Application you wish to use from the dropdown list .
Protocol	Select the the protocol you want from the dropdown list.
Start Port Number	Enter the specific port number you wish to start forwarding at.
End Port Number	Enter the specific port number you wish to end forward at. This
Local IP Address	Enter the IP address of the virtual server on the LAN.
Virtual Server Listing	This is a listing of all virtual servers you have set.

When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set, BACK to return to the previous screen or CANCEL to exit without saving.

QoS

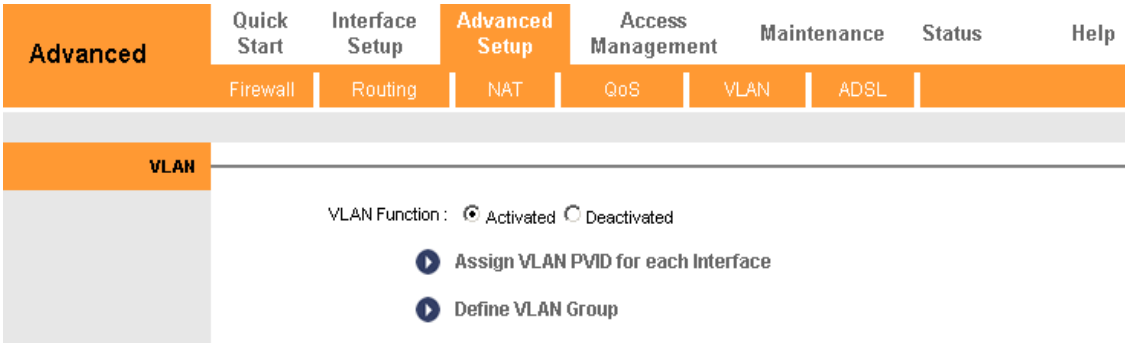
Quality of Service (QoS) helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice data packets given higher priority than Web data packets.
QoS can be toggled Activated and Deactivated. QoS must be activated before you can edit the following options.



On this screen you can ADD and delete QoS settings.

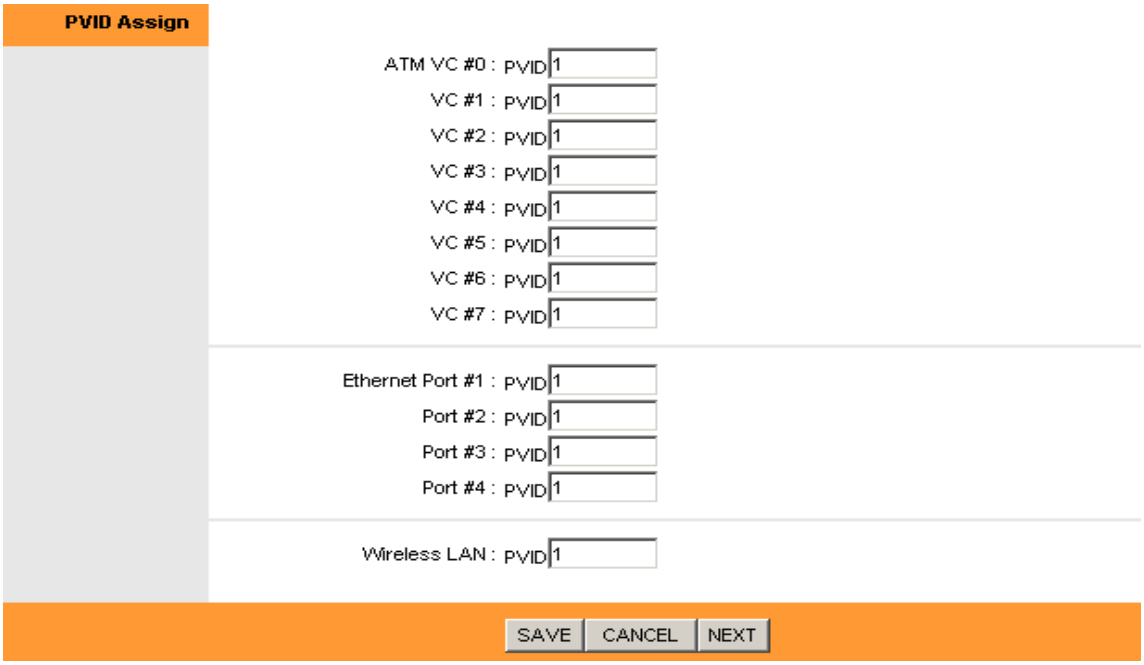
VLAN

A Virtual LAN (VLAN) is a switched network logically segmented by functions, project teams, or applications; the physical location of VLAN members is unimportant. VLANs allow ports on the same or different switches to be grouped so that traffic is confined to members of only that group. In high-traffic networks, VLANs can reduce the amount of data sent to unnecessary destinations.
VLAN can be toggled Activated or Deactivated. Note that VLAN must be activated before you can access the next two screens.

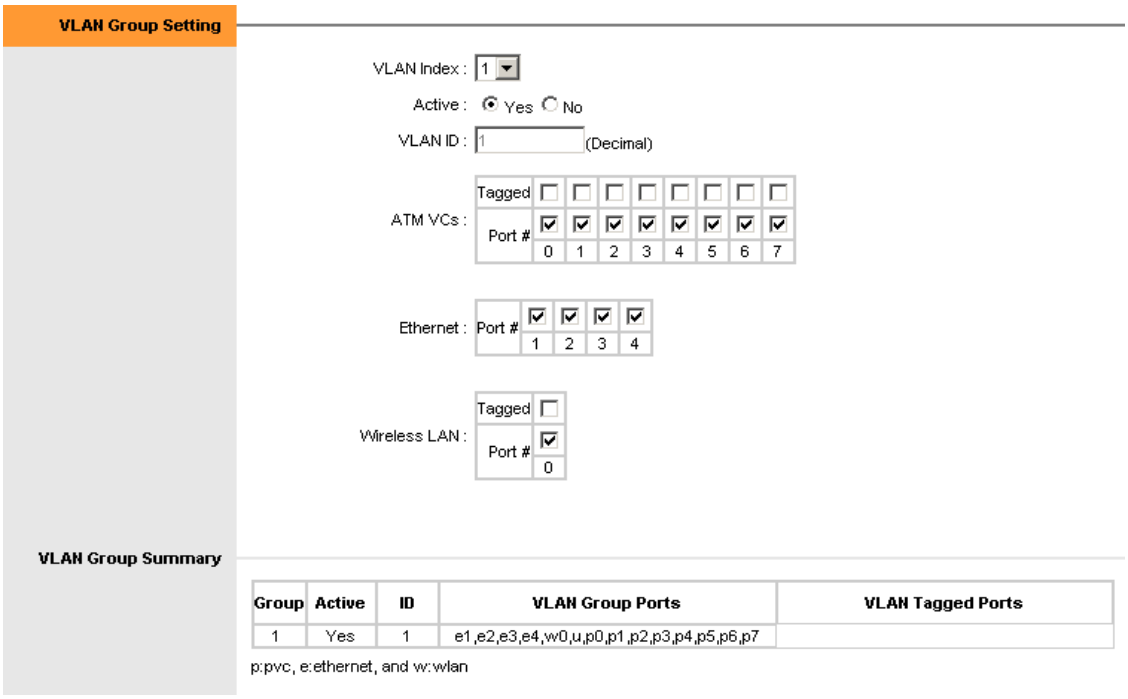


Click on Assign VLAN PVID for each Interface or Define VLAN group to open there spec. screens.

1、Assign VLAN PVID for each Interface



Enter the PVID number you wish to assign to ATM VC, Ethernet Port and Wireless LAN.
When you are done making changes, click on SAVE to save your changes, CANCEL to exit without saving or NEXT to continue to the next screen.

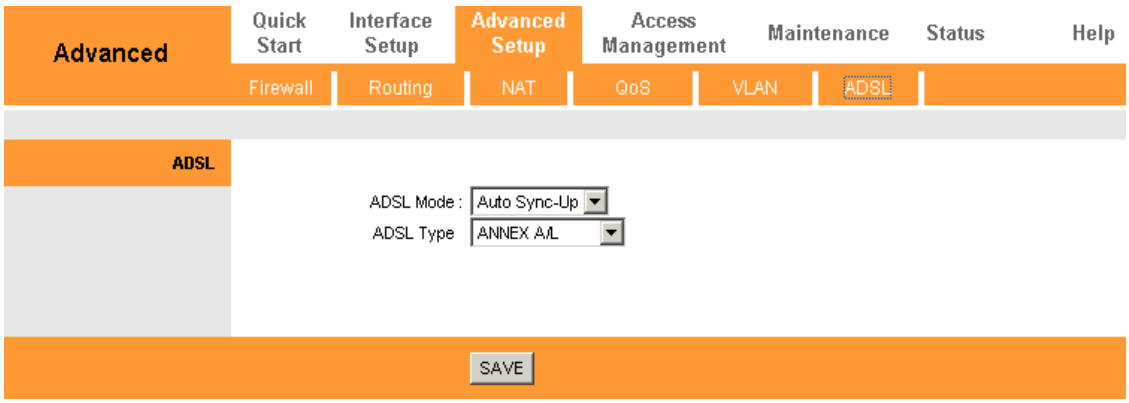


The following table describes the labels in this screen.

LABEL	DESCRIPTION
VLAN Index	The number of the index is determined by the model or IC.
Active	Toggle this index on or off with Yes and No, respectively.
VLAN ID	Enter the VLAN ID number.
ATM VCs	Checking the Tagged and Port # boxes for each port number will add a tag to let other devices know if they need to check the packet and allow the packet through to the port in question, respectively.
Ethernet	Checking the Tagged and Port # boxes for each port number will add a tag to let other devices know if they need to check the packet and allow the packet through to the port in question, respectively.
Wireless LAN	Checking the Tagged and Port # box will add a tag to let other devices know if they need to check the packet and allow the packet through to the port in question, respectively.

When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set or CANCEL to exit without saving.

ADSL



The following table describes the labels in this screen.

LABEL	DESCRIPTION
ADSL Mode	Select which mode your ADSL connection uses from the dropdown list.
ADSL Type	Select the ADSL type you use from the dropdown list.

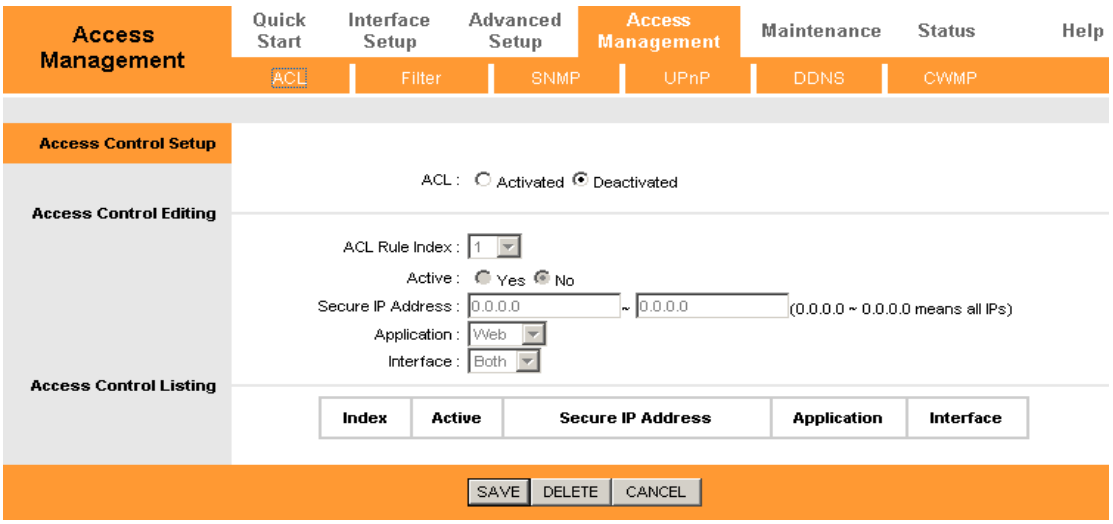
When you are done making changes, click on **SAVE** to save your changes.

Access Management

The access management screens help you manage what can access your network.

ACL

Access Control Listing (ACL) is a management tool that acts as a filter for incoming or outgoing packets, based on application.



The following table describes the labels in this screen.

LABEL	DESCRIPTION
ACL	ACL can be toggled Activated or Deactivated. ACL must be Activated before you can edit the settings.
ACL Rule Index	Select the rule index you wish to edit.
Active	Toggle the rule on or off with Yes or No, respectively.
Secure IP Address	Enter the IP address you wish to give access. Note that entering 0.0.0.0 allows all packets access.
Application	Select the application you wish to give access. Note that the first application you give access should be Web, or you will no longer be able to access the router through the Web configurator.
Interface	Select the interface the above rules should modify.

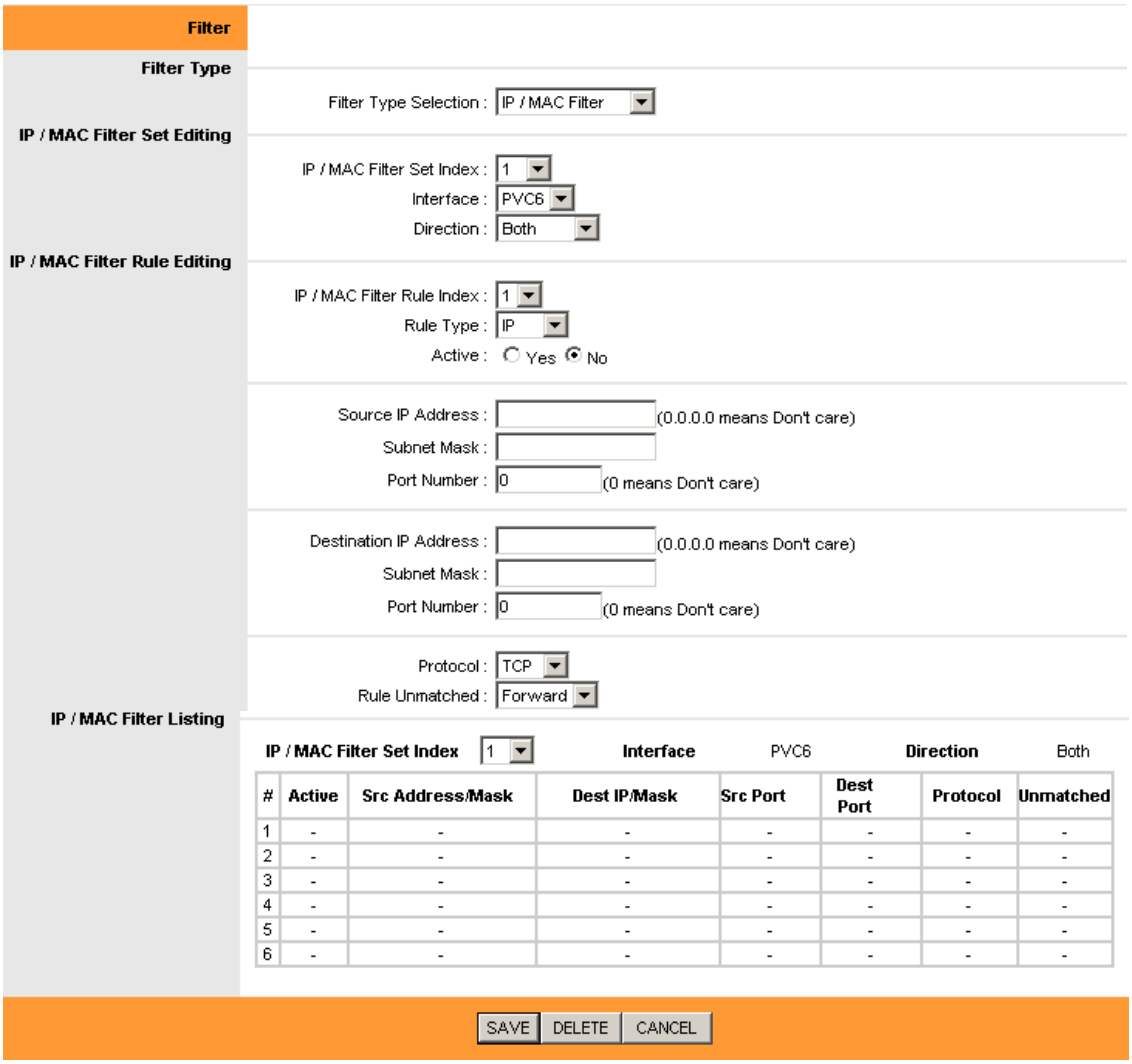
Access Control Listing is a list of all the rules you have set for access control. When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set or CANCEL to exit without saving.

Filter

The next screen will vary depending on the Filter Type option and Rout Type option you selected.

1、Filter Type : IP/MAC Filter

- **Rule Type: IP**

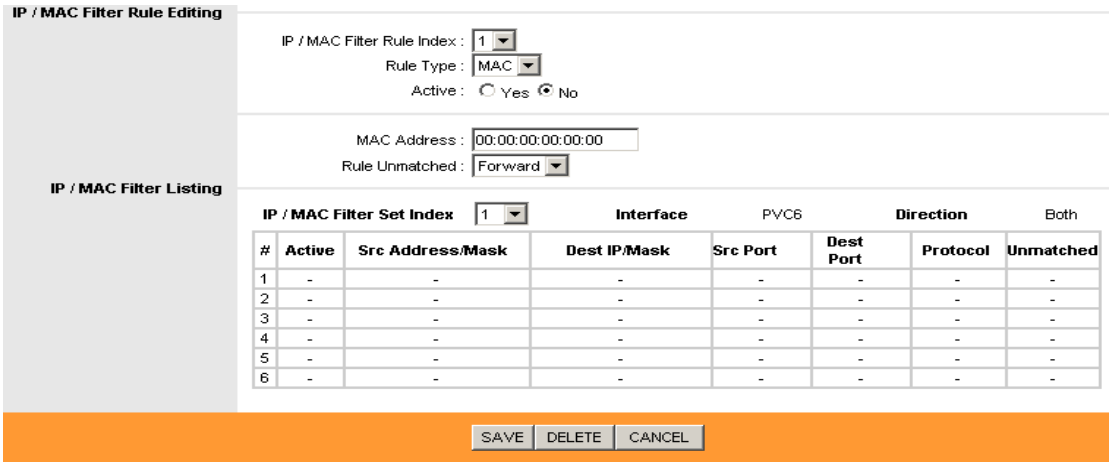


The following table describes the labels in this screen.

LABEL	DESCRIPTION
Filter Type Selection	Select the filter type you wish to apply.
IP Filter Set Index	Select the IP Filter Set Index you wish to modify.
Interface	Select the Interface you wish to modify. PVC0-PVC7 are WAN interfaces
Direction	Select which direction of data flow you wish to apply the filters to. Note that Incoming and Outgoing are from the point of view of your router, relative to the interface you select. For WAN, data coming from outside your system is considered Incoming and data leaving your system is Outgoing. For LAN, data leaving your system is considered Incoming and data entering your system is Outgoing.
IP Filter Rule Index	Select the IP Filter Rule Index you wish to modify.
Rule Type	Select the IP Filter or MAC Filter Rule you wish to modify
Active	Toggle this rule index on or off with Yes or No, respectively.
Source IP Address	Enter the source IP address you wish to deny access to your system.
Subnet Mask	Enter the subnet mask of the source IP address.

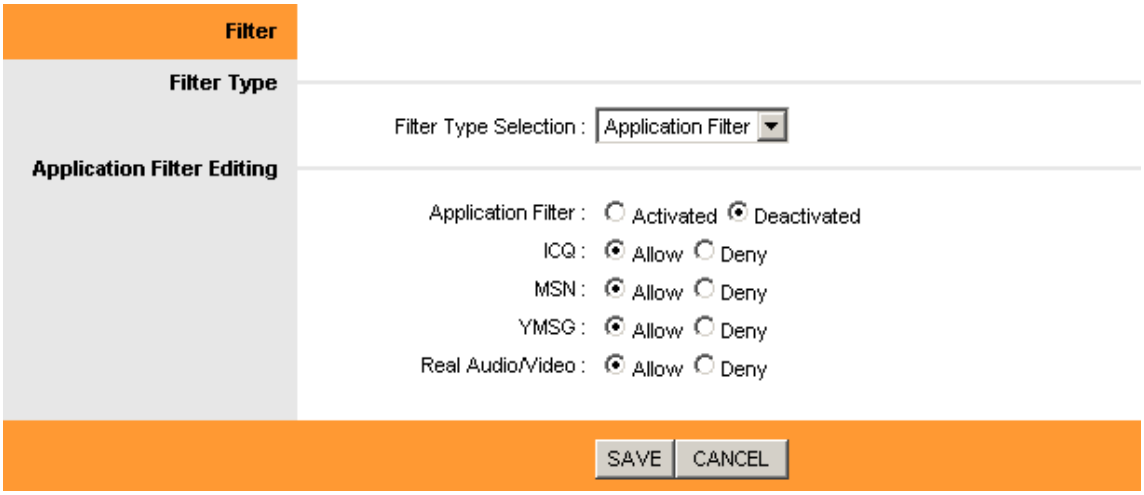
Port Number	Enter the port number of the source IP address. Note that 0 means all that ports are allowed.
Destination IP Address	Enter the destination IP address that you wish to deny access to your system.
Subnet Mask	Enter the subnet mask of the destination IP address.
Port Number	Enter the port number of the destination IP address. Note that 0 means that all ports are allowed.
Protocol	Select the protocol to filter.
Rule Unmatched	Select what happens to the data in question if the rule you are currently editing is unmatched. Next means that the data is then compared to the next IP filter rule. Forward means that the data will be allowed into your system. Note that a Forward rule should be the last rule, as no data will be compared to rules after a Forward rule.
IP Filter Set Index	Select the IP filter set you wish to view.

◆ **Rule Type: MAC**



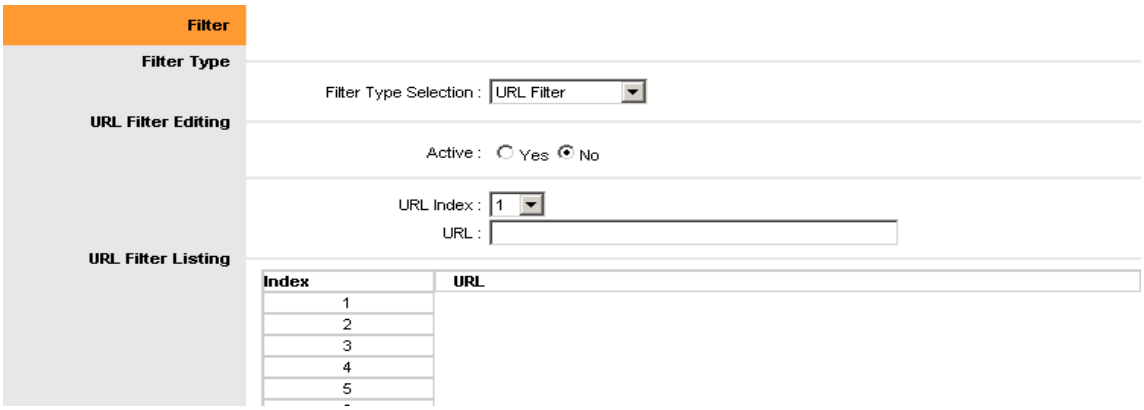
When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set or CANCEL to exit without saving.

2、Filter Type : Application Filter



changes or CANCEL to exit without saving.

3、Filter Type : URL Filter



When you are done making changes, click on SAVE to save your changes, DELETE to delete the rule with the parameters you set or CANCEL to exit without saving.

SNMP

Simple Network Management Protocol (SNMP) is a protocol for exchanging management information between network devices, and is part of the TCP/IP protocol suite.

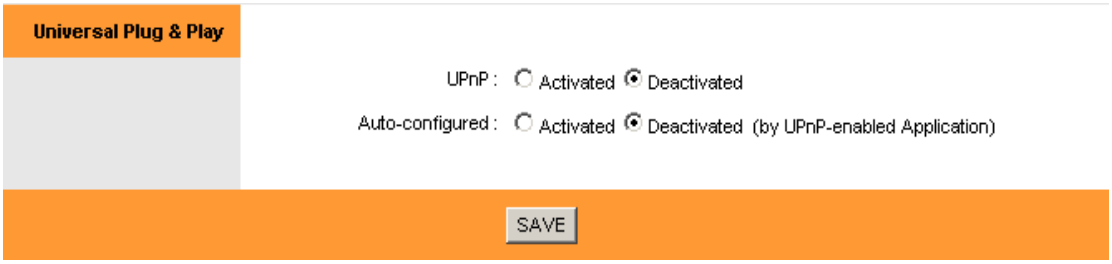
The following table describes the labels in this screen.

LABEL	DESCRIPTION
Get Community	Enter the password for incoming Get and Get Next requests from the management station.
Set Community	Enter the password for incoming Set requests from the management station.

The default password is ‘public’. When you are done making changes, click on SAVE to save your changes.

UPnP

Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. A device can leave a network smoothly and automatically when it is no longer in use.



The **f**ollowing table describes the labels in this screen.

LABEL	DESCRIPTION
UPnP	UPnP can be toggled Activated or Deactivated.
Auto-configured	Auto-configuration can be toggled Activated or Deactivated (by UPnP-enabled Application).

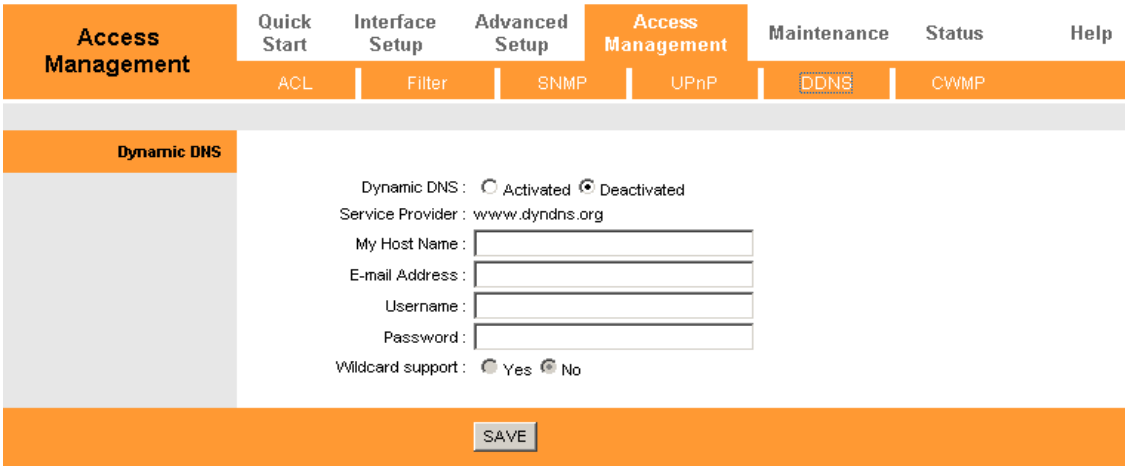
Default setting is set to **Deactivated**. When you are done making changes, click on SAVE to save your changes.

DDNS

Dynamic DNS (DDNS) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you through various applications. You can also access your FTP server or Web site on your own computer using a DNS-like address that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

You need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The Dynamic DNS service provider will give you a password or key.

To change your Router's DDNS, Click on DDNS. The screen appears as shown.



DDNS can be toggled Activated and Deactivated. DDNS must be activated before you can edit the following options.

The following table describes the labels in this screen.

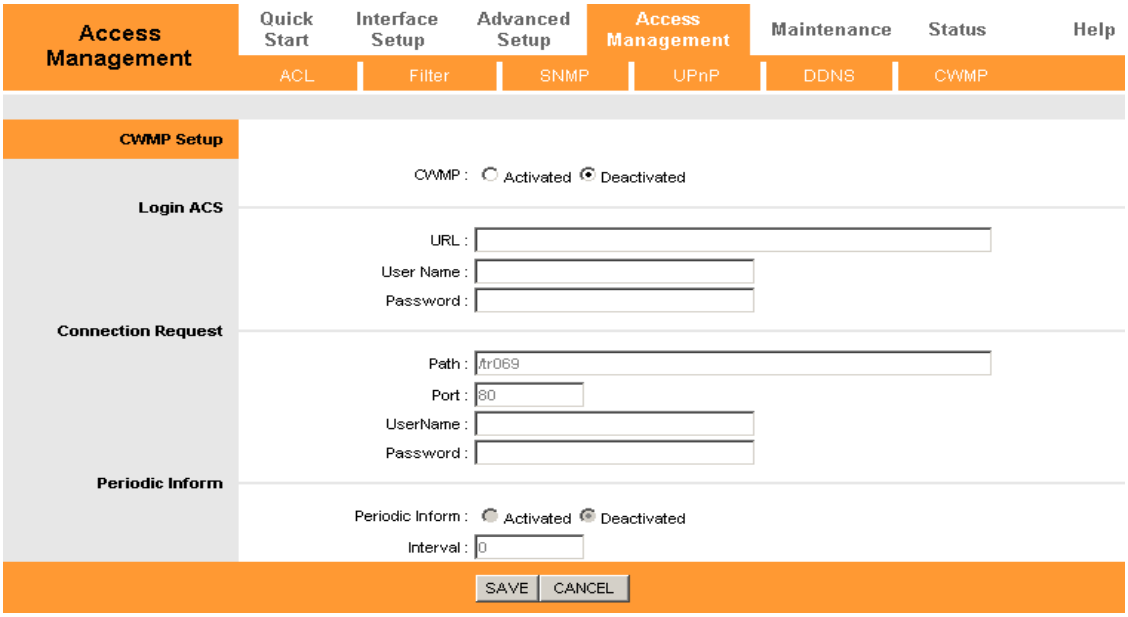
LABEL	DESCRIPTION
Active	Dynamic DNS can be toggled Activated or Deactivated.
Service Provider	Select the name of your Dynamic DNS service provider.
My Host Name	Enter the domain name assigned to your device by your Dynamic DNS provider here.
E-mail Address	Enter your e-mail address here.
Username	Enter your user name here.
Password	Enter the password assigned to you here.
Wildcard support	Choose whether or not you have DYNDNS Wildcard.

Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given. When you are done making changes, click on SAVE to save your changes.

CWMP

To change your Router's CWMP, Click on CWMP. The screen appears as shown.

CWMP can be toggled Activated and Deactivated. CWMP must be activated before you can edit the following options.

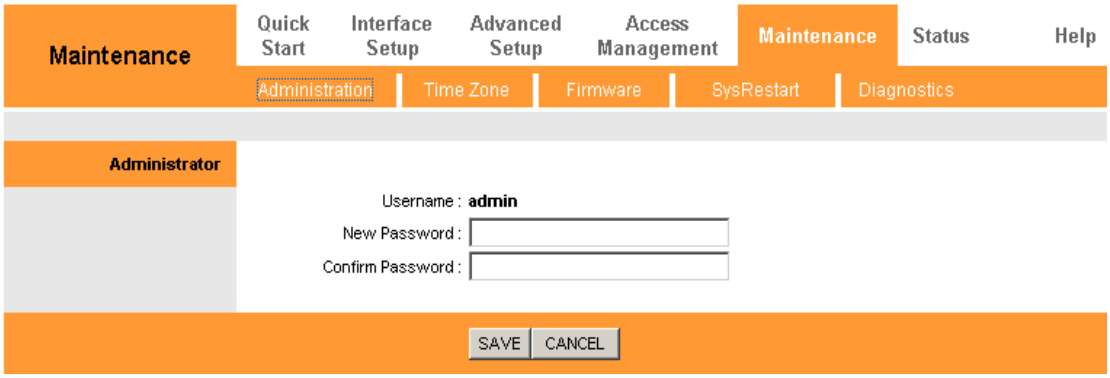


When you are done making changes, click on SAVE to save your changes, CANCEL to exit without saving.

Maintenance

The maintenance screens help you manage your router.

Administration

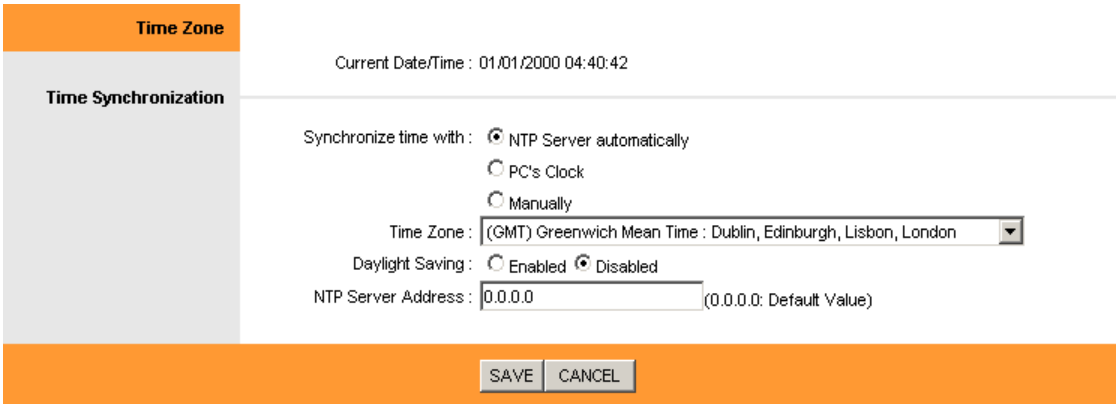


The following table describes the labels in this screen.

LABEL	DESCRIPTION
New Password	Enter the password you wish to use here.
Confirm Password	Enter the password again to confirm it.

Time Zone

Use the Time Zone screen to change your router's time and date.



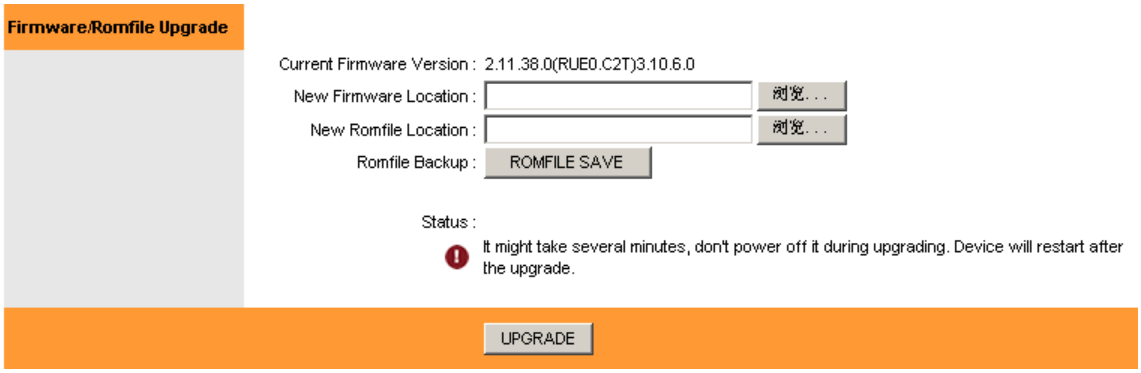
following table describes the labels in this screen.

LABEL	DESCRIPTION
Synchronize time with	Chose how you want your device to obtain the time.
Time Zone	Select your time zone from the dropdown list.
Daylight Saving	Daylight saving can be toggled Enabled or Disabled.
NTP Server Address	Enter the NTP server address you wish to use here.

A Network Time Protocol (NTP) server can automatically set the router's time for you. If you use an NTP server, you will only need to select your time zone. If you manually set the time, you can enable Daylight Saving. The router will automatically adjust when Daylight Saving goes into effect. When you are done making changes, click on SAVE to save your changes or on CANCEL to exit without saving.

Firmware

Use the Firmware screen to view and update your router's firmware.

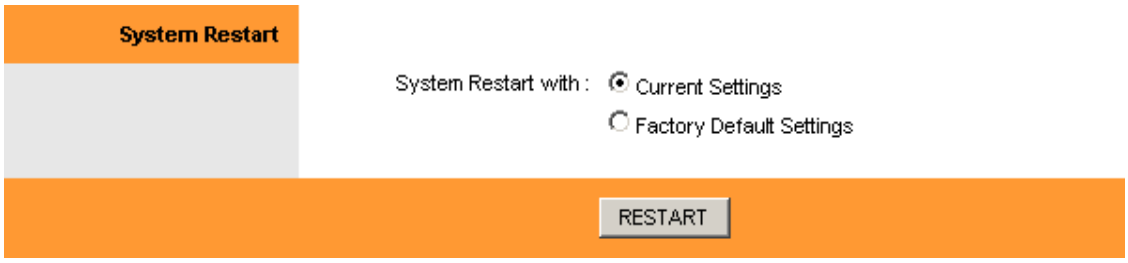


The following table describes the labels in this screen.

LABEL	DESCRIPTION
Current Firmware Ver	The current firmware version your device is using.
New Firmware Location	The location on your computer of the firmware you wish to upload. Enter the location here, or click on Browse… to find it.
Romfile Backup	Backup the current Rom file

Once you have entered the new firmware's location in the field, click on UPGRADE to upload it to your router. Note that upgrading might take several minutes. Do not turn off your router during this time. It will restart automatically after upgrading finishes.

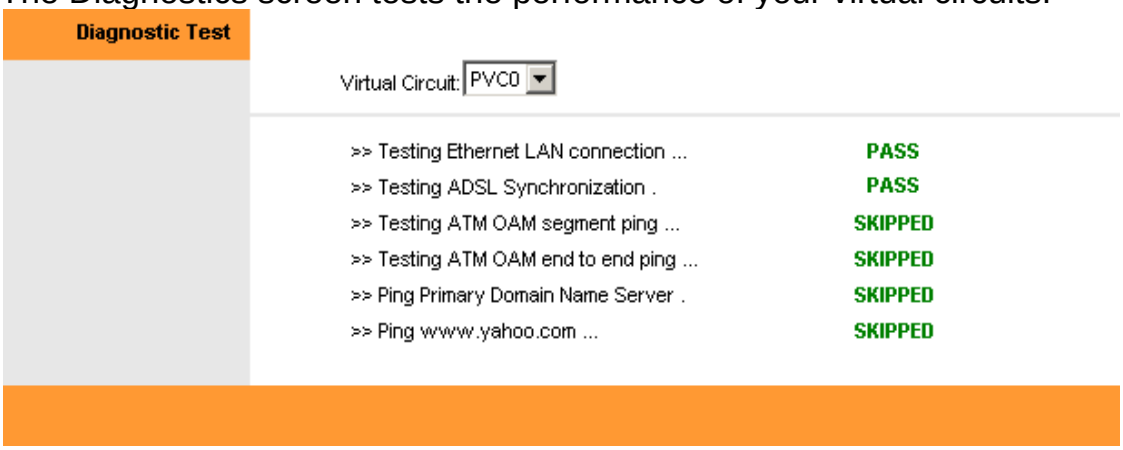
SysRestart



The SysRestart screen allows you to restart your router with either its current settings still in place or the factory default settings.
Once you have selected the settings you wish to use upon restart, click on RESTART to restart the router.

Diagnostics

The Diagnostics screen tests the performance of your virtual circuits.

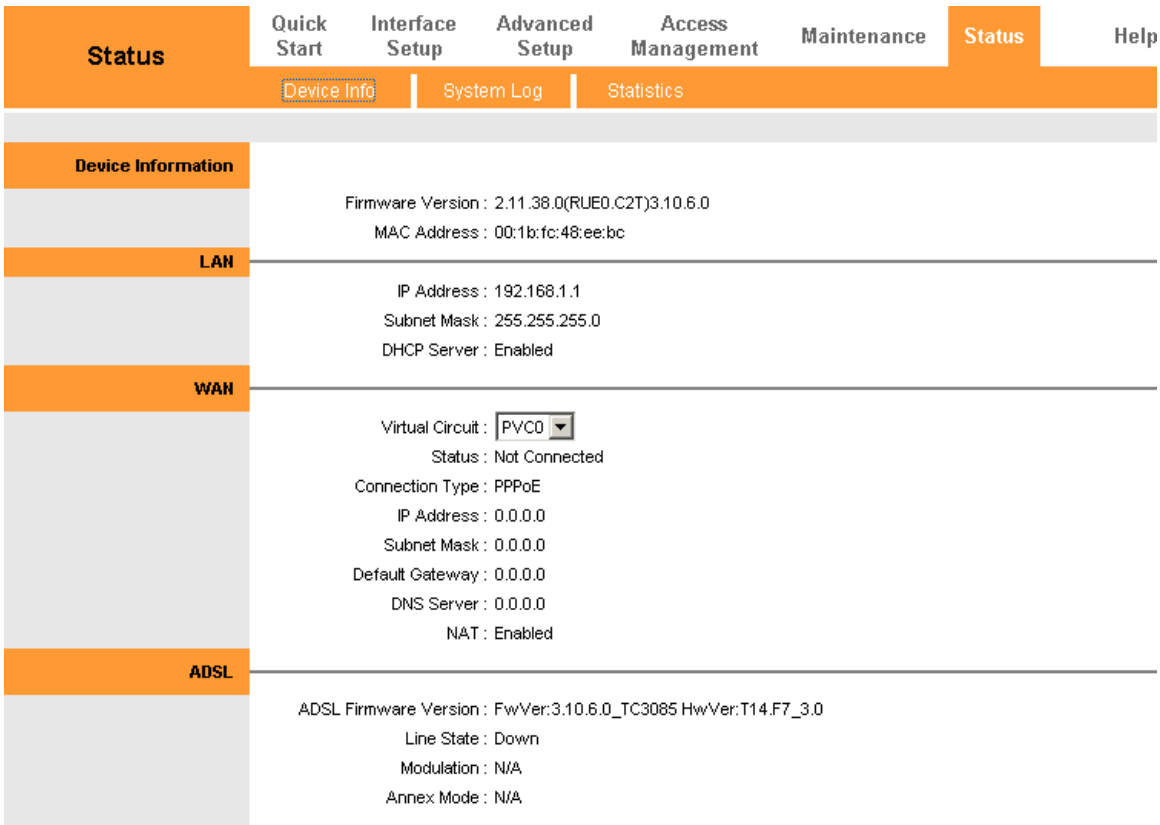


Select which PVC you wish to test from the dropdown list. The router will automatically run diagnostic tests on that circuit. A green PASS means that the given test was passed, a red FAIL means that the test was failed and a green SKIPPED means that the test was skipped.

Status

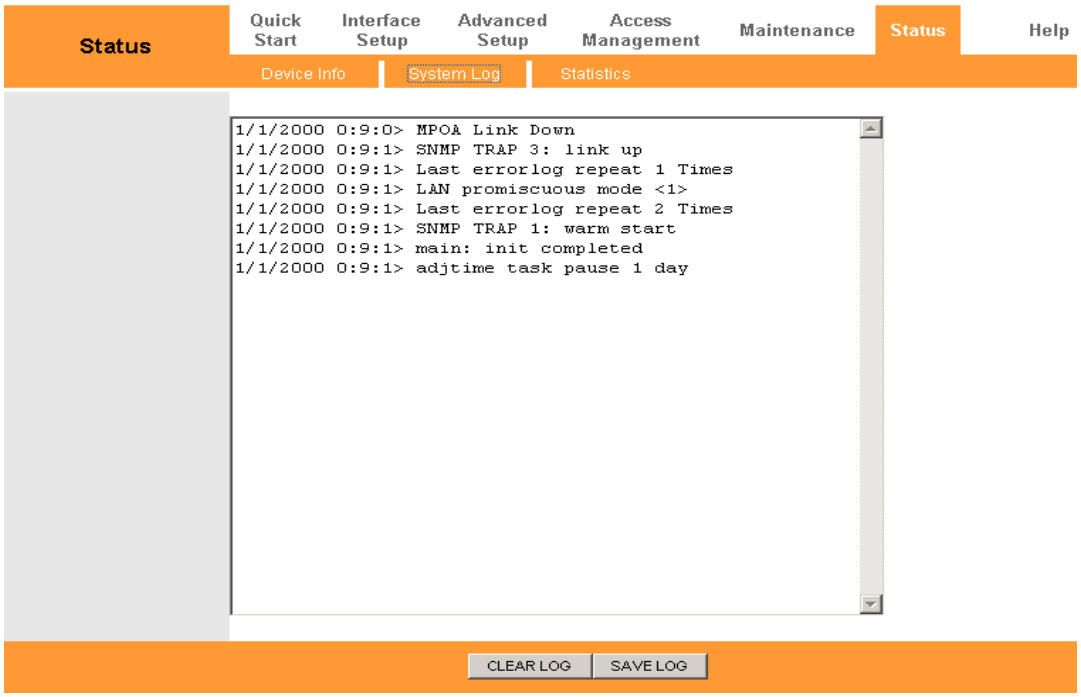
The status screens give you information about various aspects of your router's settings.

Device Info



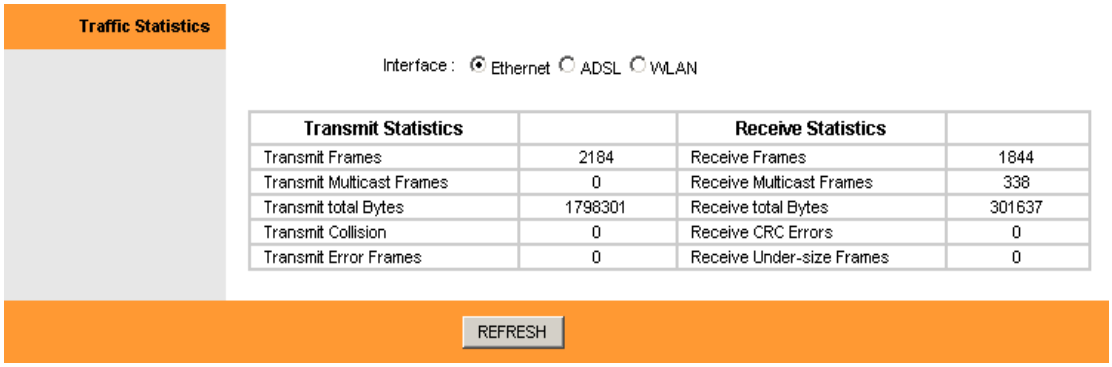
System Log

The system log screen displays a log of the router's functioning. Click on CLEAR LOG to clear the log or on SAVE LOG, which will save the log data to a separate file.



Statistics

The statistics screen gives you information on how much data your router has processed. Choose Ethernet, ADSL or WLAN to view the respective statistics screens. Click on REFRESH to update the screen.



Appendix Troubleshooting

This chapter covers potential problems and the corresponding remedies.

Using LEDs to Diagnose Problems

The Light-Emitting Diodes (LED) are useful aides for finding the possible causes of problems.

◆ **Problem: Power LED Doesn't Light Up**

The Power (PWR) LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Make sure that the router's power adaptor is connected to the router and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the router and the power source are both turned on and the router is receiving sufficient power.
3	Turn the router off and on.
4	If the error persists, you may have a hardware problem. Contact your vendor.

◆ **Problem: LAN LED Doesn't Light Up**

The LAN LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet cable connections between your router and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If the error persists, contact your local distributor for assistance.

◆ Problem: DSL LED Doesn't Light Up

The DSL LED on the front panel does not light up.

STEPS	CORRECTIVE ACTION
1	Check the telephone wire and connections between the router DSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for DSL service.
3	Reset your ADSL line to reinitialize your link to the DSLAM.
4	If the problem persists, contact your local distributor for assistance.

Can't Access Web Configurator

I cannot access the Web configurator.

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the router. Check the IP address of the router.
2	Make sure that a console session isn't running.
3	Check that you have enabled Web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.
4	For WAN access, you must configure remote management to allow server access from the WAN (or all).
5	Your computer's and the router's IP addresses must be on the same subnet for LAN access.
6	If you changed the router's LAN IP address, enter the new one as the URL.
7	Remove any filters in LAN or WAN that block Web service.

The Web configurator does not display properly.

STEPS	CORRECTIVE ACTION
1	Make sure you are using Internet Explorer 5.0 or later versions.
2	Delete the temporary Web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files ...** button. When a **Delete Files** window displays, select **Delete all offline content** and click **OK**. (Steps may vary depending on the version of your Internet browser.)

Forgotten Login Username and Password

I forgot my login username or password.

STEPS	CORRECTIVE ACTION
1	If you have changed the password and forgotten it, you will need to upload the default
	configuration file. This will erase all custom configurations and restore factory defaults, including the password.
2	Press the **RESET** button for five seconds, and then release it. When the **SYS** LED begins to blink, the defaults have been restored and the router restarts. Or refer to the *Resetting the* router section for uploading a configuration file via console port.
3	The default username is “admin”. The default password is “admin”. The **Password** and **Username** fields are case-sensitive. Make sure that you use the proper casing.
4	It is highly recommended to change the default username and password. Make sure you record the username and password in a save place.

Can’t Access LAN Interface

I cannot access the router from the LAN or ping any computer on the LAN.

STEPS	CORRECTIVE ACTION
1	Check the Ethernet LEDs on the front panel. A LAN LED should be on if the port is connected to a computer or hub. If the 10M/100M LEDs on the front panel are both off.
2	Make sure that the IP address and the subnet mask of the router and your computer(s) are on the same subnet.

Can't Access WAN Interface

Initialization of the ADSL connection failed.

STEPS	CORRECTIVE ACTION
1	Check the cable connections between the ADSL port and the wall jack. The DSL LED on the front panel of the router should be on.
2	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as that you obtained from your telephone company and ISP.
3	Restart the router. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP.

STEPS	CORRECTIVE ACTION
1	The ISP provides the WAN IP address after authenticating you. Authentication may be through the username and password, the MAC address or the host name.
2	The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing).

Can't Access the Internet

I cannot access the Internet.

STEPS	CORRECTIVE ACTION
1	Make sure the router is turned on and connected to the network.
2	If the DSL LED is off, refer to *Section A.1.3*.
3	Verify your WAN settings.
4	Make sure you entered the correct username and password.
5	For wireless stations, check that both the router and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).

Internet connection disconnects.

STEPS	CORRECTIVE ACTION
1	Check the schedule rules.
2	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting.
3	Contact your ISP.

Can't Access Remote Management

I cannot remotely manage the ROUTER from the LAN or WAN.

STEPS	CORRECTIVE ACTION
1	Refer to the Remote Management Limitations section in the Firmware and Configuration File Management chapter for scenarios when remote management may not be possible.
2	Use the router's WAN IP address when configuring from the WAN. Use the router's LAN IP address when configuring from the LAN.

Can't Access Remote Node Connection

I cannot connect to a remote node or ISP.

STEPS	CORRECTIVE ACTION
1	Check the WAN screen to verify that the username and password are entered properly.
2	Verify your login name and password for the remote node.
3	If the problem persists, you may need to verify your login and password with your ISP.