PLANET
Networking & Communication

802.11g Wireless ADSL 2/2+ Router

ADW-4401A/Bv2

User's Manual

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Revision

User's Manual for 802.11g Wireless ADSL 2/2+ Router

Model: ADW-4401 A/Bv2

Rev: 1.0 (Dec. 2006)

Part No. EM-ADW4401v2_v1

Table of Contents

1. Introduction

The PLANET 802.11g Wireless ADSL 2/2+ Router, ADW-4401v2, provides office and residential users the ideal solution for sharing a high-speed ADSL 2/2+ broadband Internet connection on a 54Mbps wireless network and a 10/100Mbps Fast Ethernet backbone. It can support downstream transmission rates of up to 24Mbps and upstream transmission rates of up to 3.5Mbps. The product supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 2684 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1483) to establish a connection with ISP.

Via the user-friendly management interface, ADW-4401v2 can be managed by workstations running standard web browsers. Furthermore, ADW-4401v2 provides DHCP server, NAT, virtual server, DMZ, access control, IP filter, PPTP/IPSec/L2TP pass-through, DNS Proxy, DDNS, and UPnP capability.

The ADW-4401v2 also serves as an Internet firewall, protecting your network from being accessed by outside users. It provides the natural firewall function (Network Address Translation, NAT). All incoming and outgoing IPs are monitored and filtered. Moreover, it can be configured to block internal users from accessing to the Internet.

1.1 Feature

Internet Access Features

- ***Shared Internet Access.*** All users on the LAN or WLAN can access the Internet through the ADW-4401v2 using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***Built-in ADSL 2/2+ Modem.*** The ADW-4401v2 provides ADSL 2/2+ modem, and supports all common ADSL connections.
- ***IPoA, PPPoE, PPPoA, Direct Connection Support.*** Various WAN connections are supported by ADW-4401v2.
- ***Auto-detection of Internet Connection Method.*** In most situations, the ADW-4401v2 can test your ADSL and Internet connection to determine the connection method used by your ISP.
- ***Fixed or Dynamic IP Address.*** On the Internet (WAN port) connection, the ADW-4401v2 supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***Firewall.*** Supports simple firewall with NAT technology and provides option for blocking access from Internet, like Web, FTP, Telnet, SNMP, and ICMP.
- ***Universal Plug and Play (UPnP)*** UPnP allows automatic discovery and configuration of the Broadband Router. UPnP is supported by Windows ME, XP, or later.
- ***Dynamic DNS Support.*** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.

- ***VPN Pass through Support.*** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.
- ***RIP1/2 Routing.*** It supports RIP1/2 routing protocol for routing capability.
- ***Simple Network Management Protocol (SNMP).*** It is an easy way to remotely manage the router via SNMP.

Wireless Features

- ***Standards Compliant.*** The ADW-4401v2 complies with the IEEE802.11g (DSSS) specifications for Wireless LANs. Maximum of 54Mbps are supported.
- ***Supports both 802.11b and 802.11g Wireless Stations.*** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported.
- ***WPA-PSK support.*** WPA-PSK_TKIP and WAP-PSK_AES encryption are supported.
- ***Wireless MAC Access Control.*** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.

LAN Features

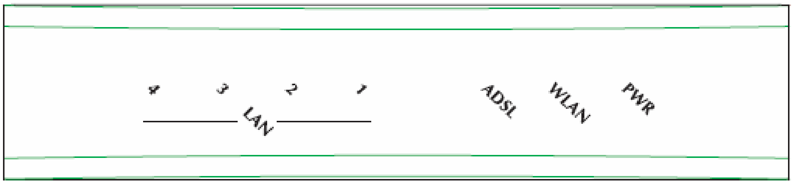
- ***4-Port Switch.*** The ADW-4401v2 incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The ADW-4401v2 can act as a DHCP Server for devices on your local LAN and WLAN.

1.2 Package Contents

- ADW-4401v2 Unit
- Power Adapter
- Quick Installation Guide
- User's Manual CD
- RJ-11 (ADSL) cable
- RJ-45 cable

1.3 Physical Details

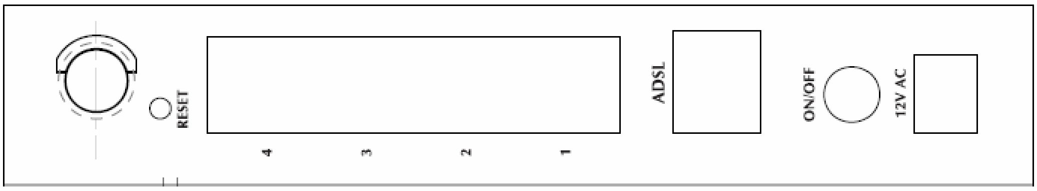
Front Panel



Front Panel LED definition

LED	State	Description
PWR	ON	When the router is powered on and in ready state
	OFF	When the router is powered off.
WLAN	Flashing	When wireless AP is ready
ADSL	ON	Successful connection between ADSL modem and telecom's network
	Flashing	Modem is trying to establish a connection to telecom's network
LAN 1-4	ON	Link
	Flashing	TX or RX activity
	OFF	No Link These four LAN (Local Area Network) ports are where you will connect networked devices, such as PCs, print servers remote hard drives, and anything else you want to put on your network

Rear Panel



Rear panel Port and Button Definition

Connector	Description
POWER	Power connector with 12V AC 1.0 A
POWER Button	The power button is for turn on or turns off the router.
ADSL Connector	The RJ-11 connector allows data communication between the modem and the ADSL network through a twisted-pair phone wire
LAN (1-4)	Router is successfully connected to a device through the corresponding port (1, 2, 3, or 4). If the LED is flashing, the Router is actively sending or receiving data over that port.
Reset Button	The reset button, the router restore the default settings when press this button until reboot

■ 2. Installation

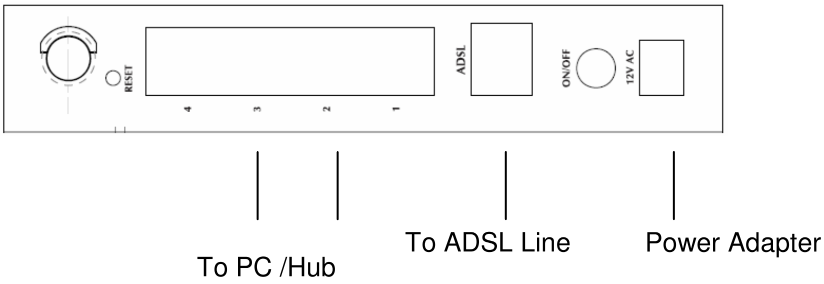
This chapter offers information about installing your router. If you are not familiar with the hardware or software parameters presented here, please consult your service provider for the values needed.

■ 2.1 System Requirement

1. Personal computer (PC)
2. Pentium III 266 MHz processor or higher
3. 128 MB RAM minimum
4. 20 MB of free disk space minimum
5. RJ45 Ethernet Port

■ 2.2 Hardware Installation

This section describes how to connect and configure the ADW-4401.



Step 1. Connect the ADSL Line

Connect the router directly to the wall jack using the included ADSL cable.

Step 2. Connect a Workstation to the Router's LAN port

There are two methods to connect the router and workstation. The one use the crossover Ethernet cable to connect directly between them. The other use straight Ethernet cable to connect router with hub (or switch), then go to the workstation.

Step 3. Connect the Power Adapter to the Router

Connect the power adapter to the port labeled POWER on the rear panel of router.

Step 4. Connect All Cables to the Network

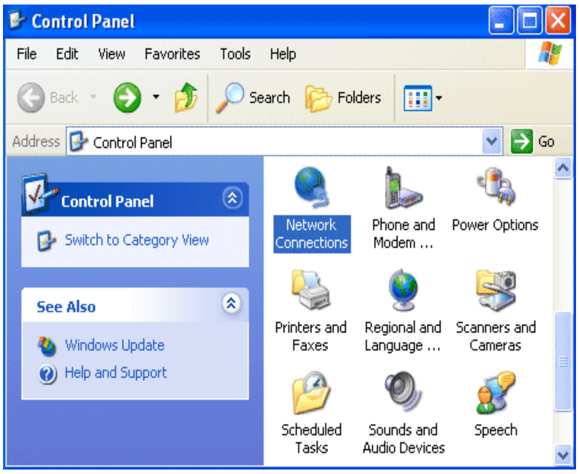
The procedure for connecting cables differs depending on whether or not your telephone equipment is connected to a POTS splitter.

▪ 2.3 Configuring the Network Properties

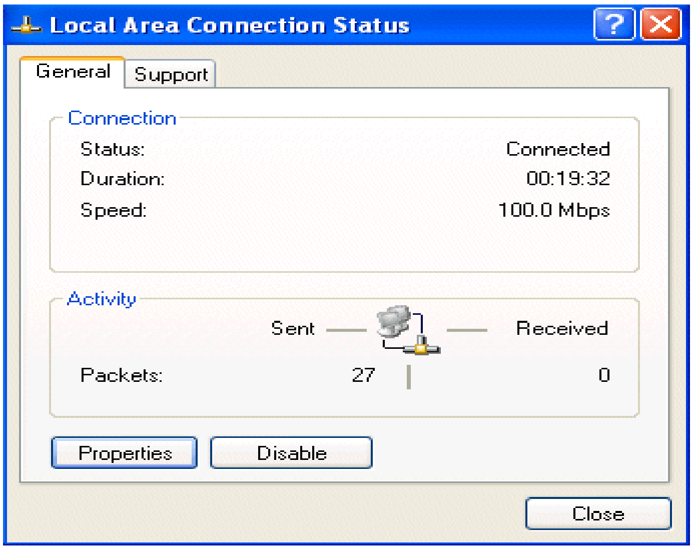
Configuring PC in Windows XP

1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**

2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.


Local Area Connection Status

Connection

Status: Connected

Duration: 00:19:32

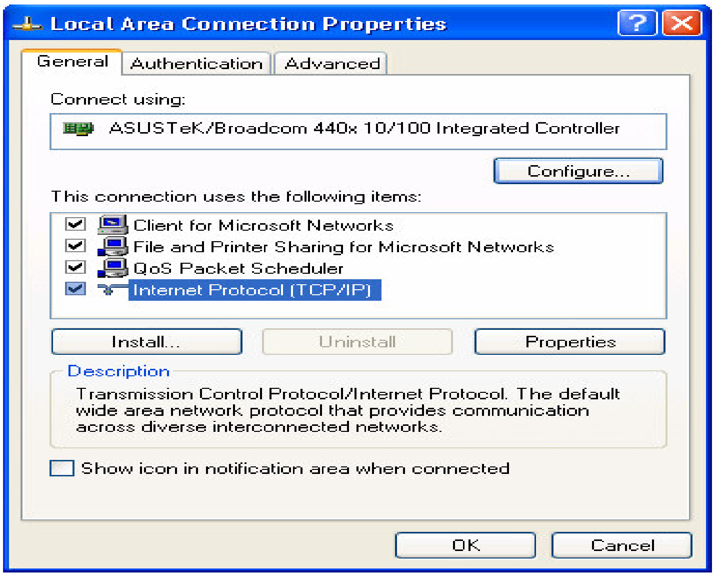
Speed: 100.0 Mbps

Activity

Sent — Received

Packets: 27 | 0

4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

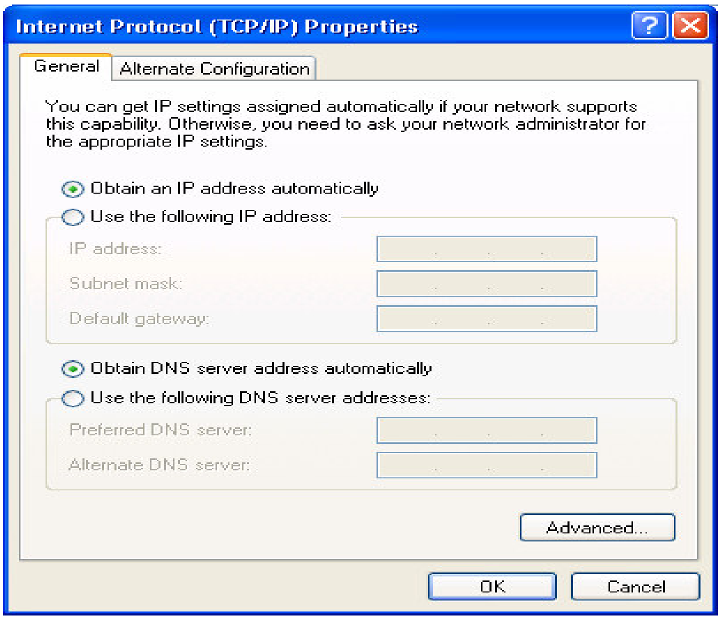
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address:
Subnet mask:
Default gateway:

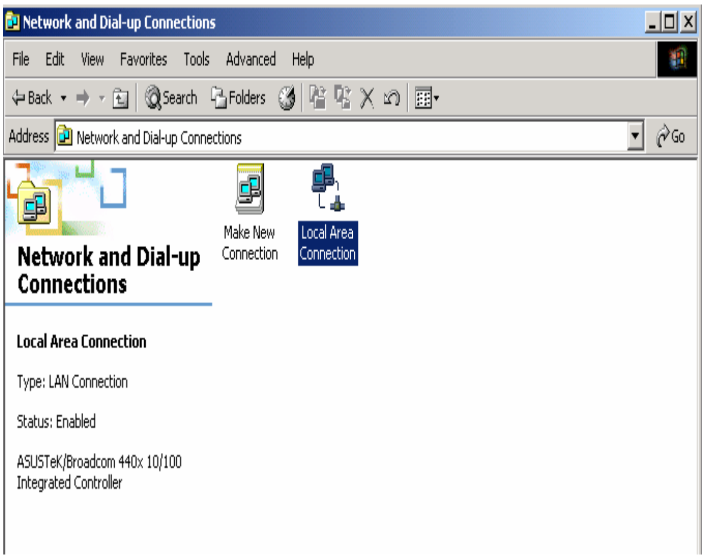
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

Configuring PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

2. Double-click **Local Area Connection**.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
Make New Connection
Local Area Connection

Local Area Connection

Type: LAN Connection

Status: Enabled

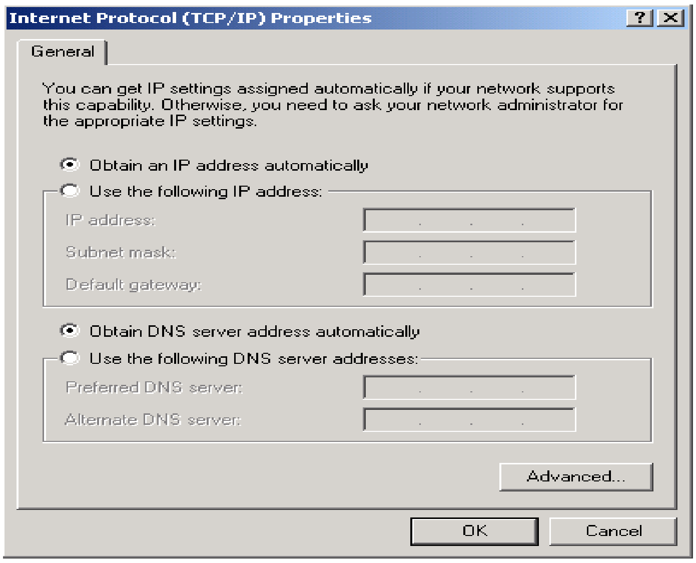
ASUSTeK/Broadcom 440x 10/100 Integrated Controller

3. In the **Local Area Connection Status** window click **Properties**.

4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

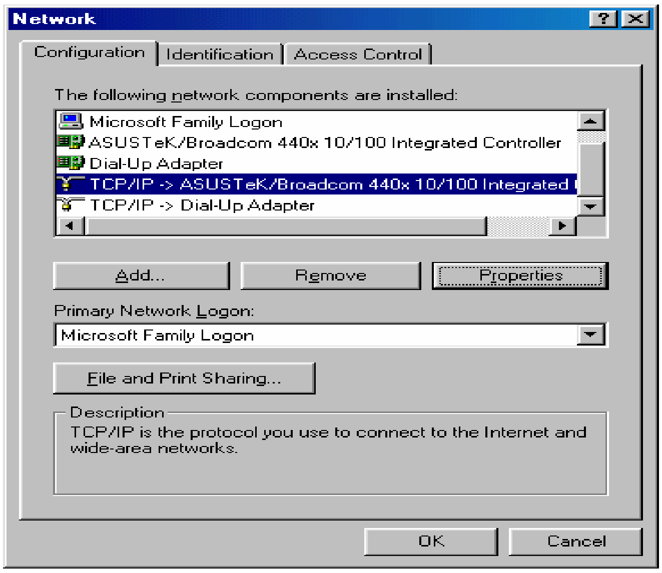
Preferred DNS server: . . .

Alternate DNS server: . . .

Configuring PC in Windows 98/Me

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.

2. Select **TCP/IP ->** **NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.



The following network components are installed:

- Microsoft Family Logon
- ASUSTeK/Broadcom 440x 10/100 Integrated Controller
- Dial-Up Adapter
- TCP/IP -> ASUSTeK/Broadcom 440x 10/100 Integrated
- TCP/IP -> Dial-Up Adapter

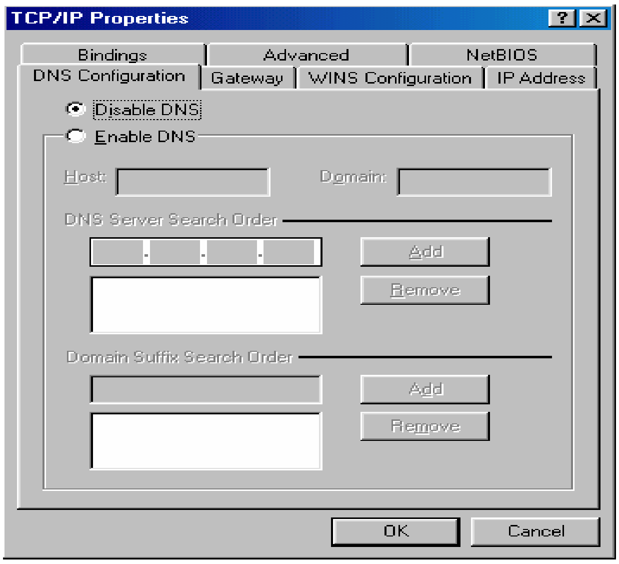
Primary Network Logon: Microsoft Family Logon

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

3. Select the **Obtain an IP address automatically** radio button.

4. Then select the **DNS Configuration** tab.

5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

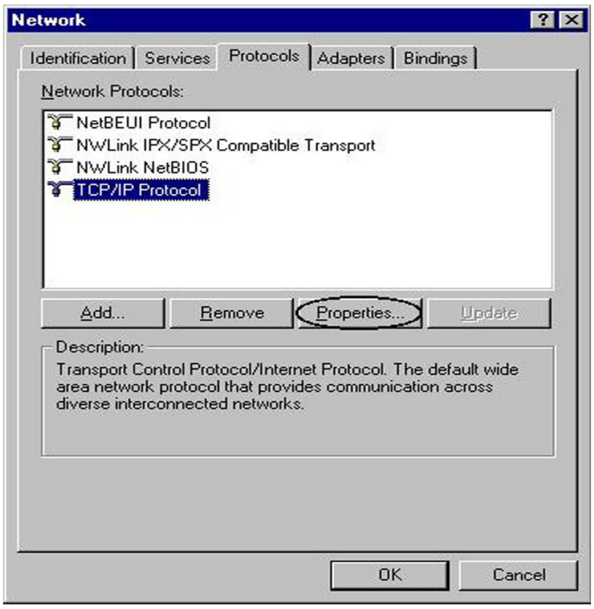


● Disable DNS
○ Enable DNS

Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.

2. Select **TCP/IP Protocol** and click **Properties**.



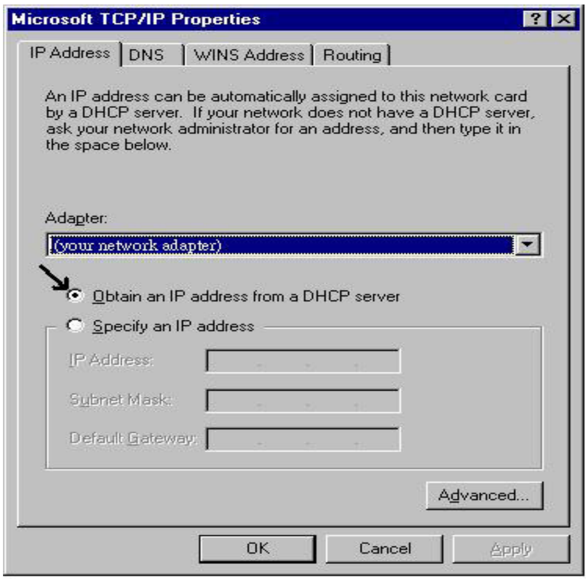
Network

Network Protocols:

- NetBEUI Protocol
- NWLink IPX/SPX Compatible Transport
- NWLink NetBIOS
- TCP/IP Protocol

Description:
Transport Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



Microsoft TCP/IP Properties

An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter: (your network adapter)

● Obtain an IP address from a DHCP server

○ Specify an IP address

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

▪ 3 Configuration

▪ 3.1 Determine your connection settings

Before you configure the router, you need to know the connection information supplied by your ADSL service provider.

▪ 3.2 Connecting the ADSL Router to your network

Unlike a simple hub or switch, the setup of the ADSL Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to assign them.

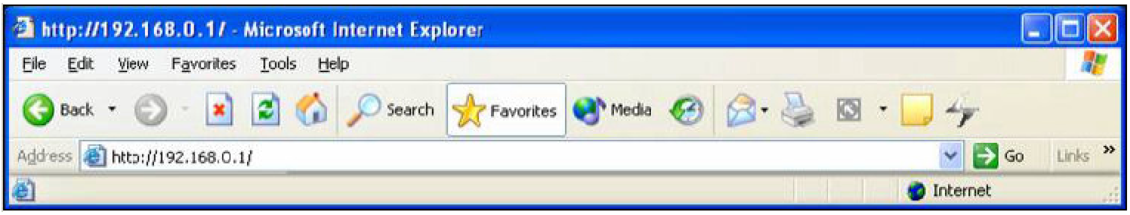
Generally there are several different operating modes for your applications. And you can know which mode is necessary for your system from ISP. These modes are router, bridge, PPPoE+NAT, and PPPoA+NAT.

▪ 3.3 Configuring with Web Browser

It is advisable to change the administrator password to safeguard the security of your network.

To configure the router, open your browser, type '**http: //192.168.0.1**' into the address bar and click 'Go' to get to the login page.

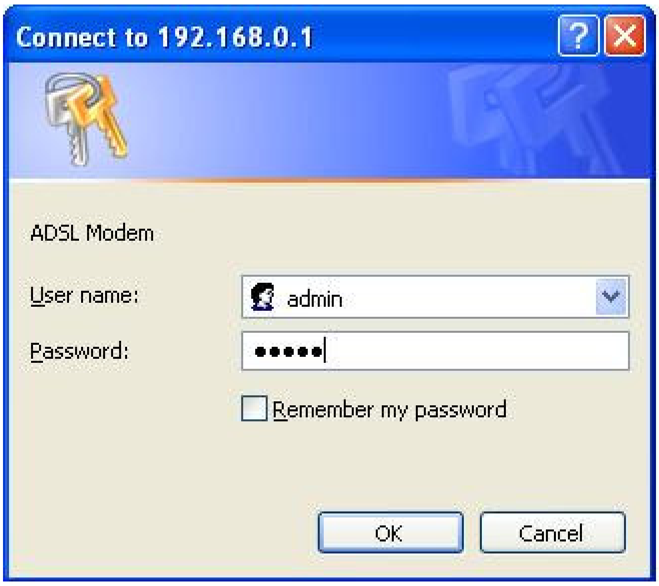
Save this address in your Favorites for future reference.



http://192.168.0.1/ - Microsoft Internet Explorer

Address http://192.168.0.1/

At the User name prompt, type '**admin**'. And the Password prompt, type '**admin**'. You can change these later if you wish. Click **'OK**'.



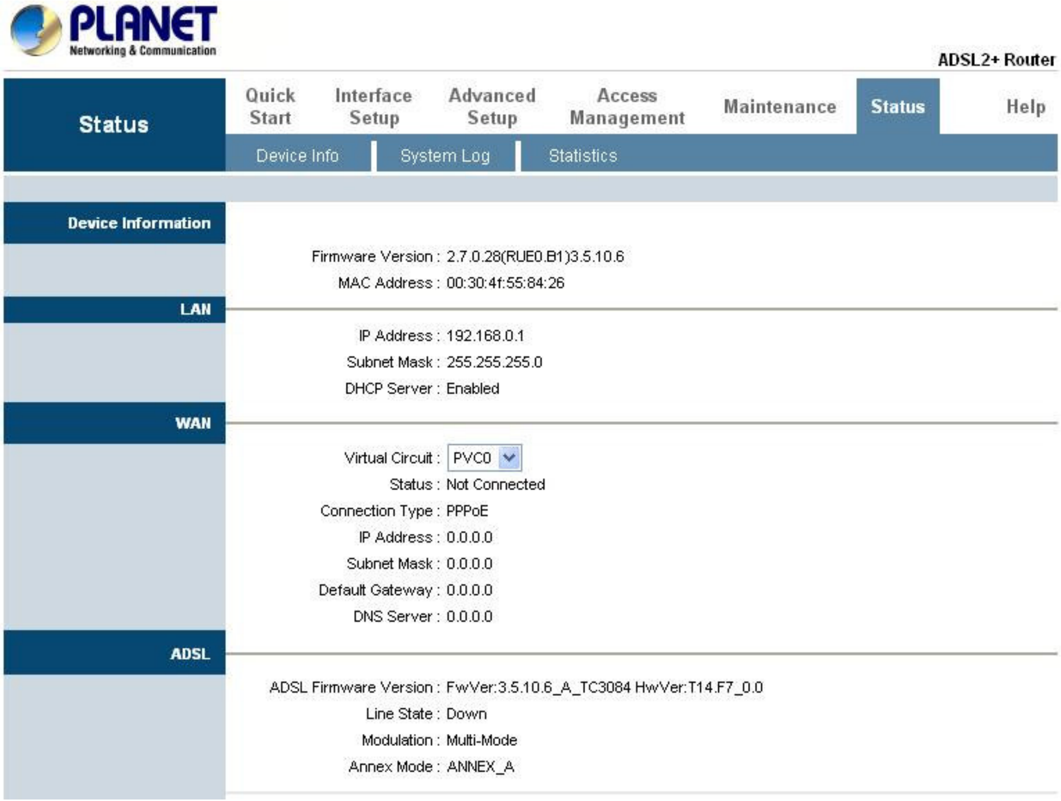
Connect to 192.168.0.1

ADSL Modem

User name: admin

Password: •••••

□ Remember my password



Device Information

Firmware Version : 2.7.0.28(RUE0.B1)3.5.10.6
MAC Address : 00:30:4f:55:84:26

LAN

IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WAN

Virtual Circuit : PVC0
Status : Not Connected
Connection Type : PPPoE
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS Server : 0.0.0.0

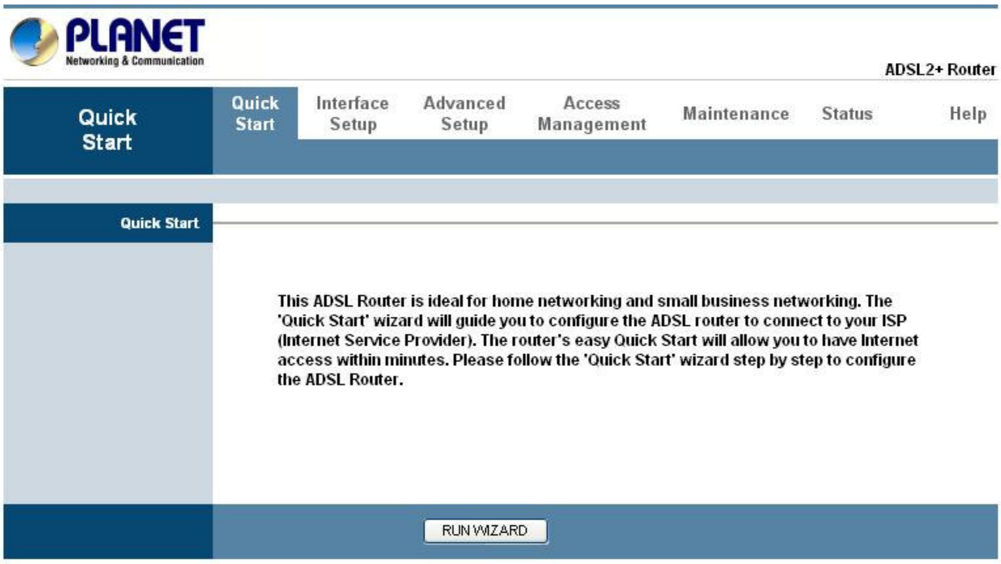
ADSL

ADSL Firmware Version : FwVer:3.5.10.6_A_TC3084 HwVer:T14.F7_0.0
Line State : Down
Modulation : Multi-Mode
Annex Mode : ANNEX_A

■ 3.3.1 Quick Setup Guide

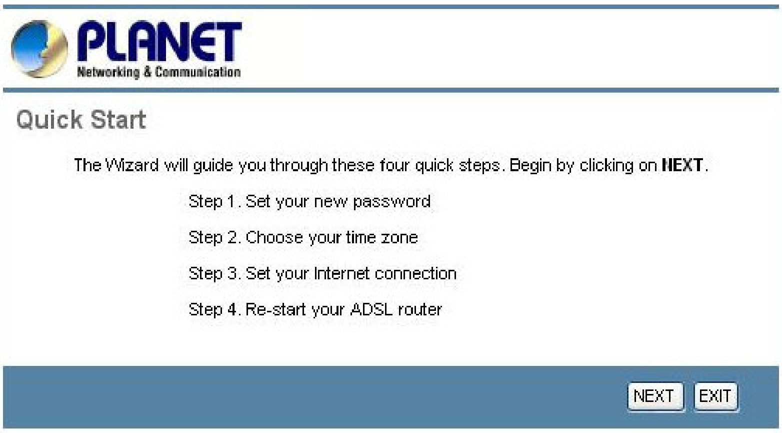
You can use "**Quick Setup**" to setup the router as follows, and the router will connect to the Internet via ADSL line.

Click "**Quick Start**" to get into the quick setup procedures.



This ADSL Router is ideal for home networking and small business networking. The 'Quick Start' wizard will guide you to configure the ADSL router to connect to your ISP (Internet Service Provider). The router's easy Quick Start will allow you to have Internet access within minutes. Please follow the 'Quick Start' wizard step by step to configure the ADSL Router.

Click "**RUN WIZARD**" to start up this procedure.



Quick Start

The Wizard will guide you through these four quick steps. Begin by clicking on **NEXT**.

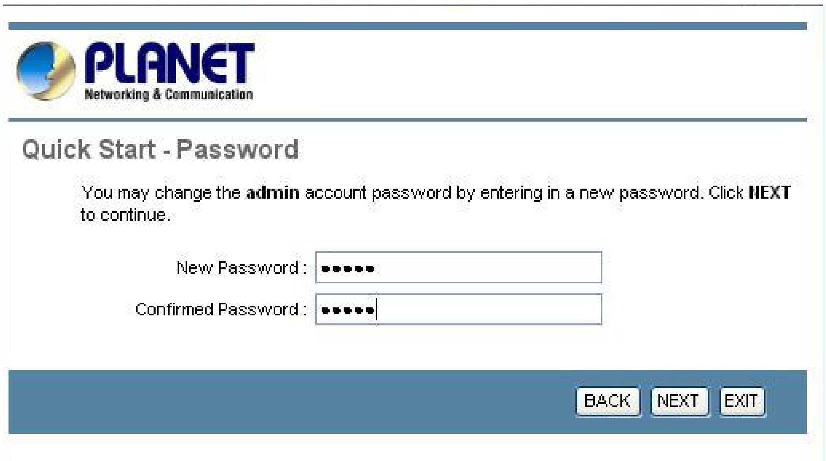
Step 1. Set your new password

Step 2. Choose your time zone

Step 3. Set your Internet connection

Step 4. Re-start your ADSL router

Step 1 - Click "Next" to setup your new administrator's password.



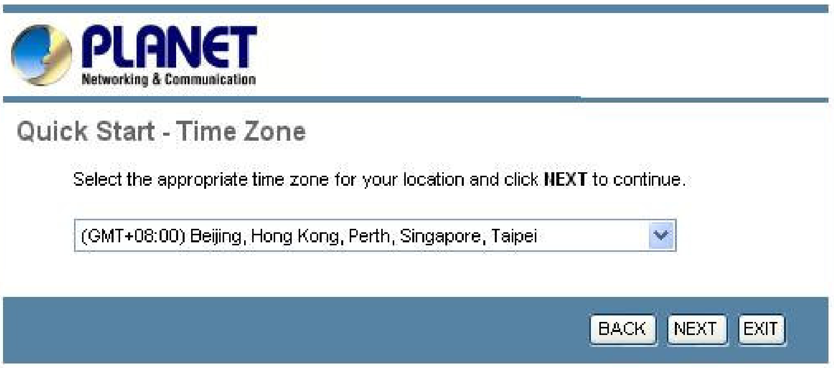
Quick Start - Password

You may change the **admin** account password by entering in a new password. Click **NEXT** to continue.

New Password : •••••

Confirmed Password : •••••

Step 2 - Click "**Next**" to setup your time zone.

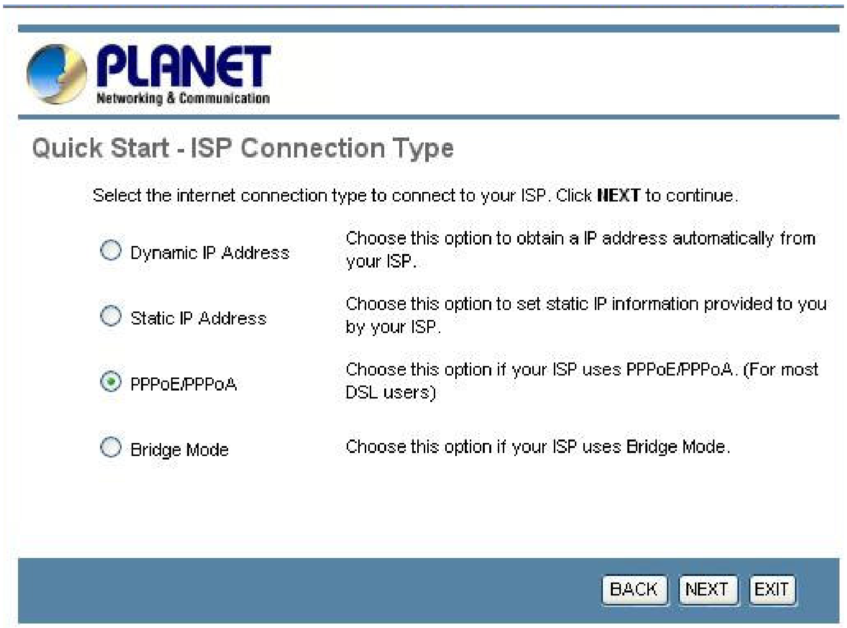


Quick Start - Time Zone

Select the appropriate time zone for your location and click **NEXT** to continue.

(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei

Step 3 - Click "**Next**" to setup your Internet connection type. You can have this information from your Internet Service Provider.



Quick Start - ISP Connection Type

Select the internet connection type to connect to your ISP. Click **NEXT** to continue.

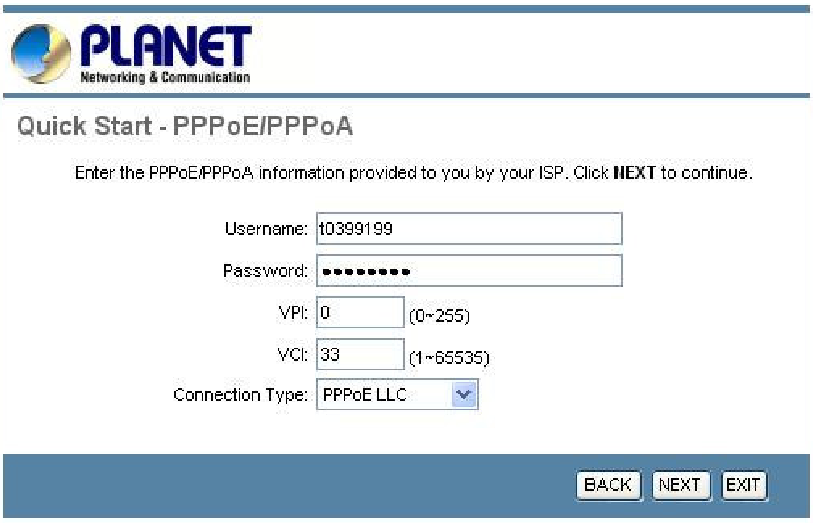
○ Dynamic IP Address — Choose this option to obtain a IP address automatically from your ISP.

○ Static IP Address — Choose this option to set static IP information provided to you by your ISP.

● PPPoE/PPPoA — Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)

○ Bridge Mode — Choose this option if your ISP uses Bridge Mode.

Enter the connection information provided by your ISP.



Quick Start - PPPoE/PPPoA

Enter the PPPoE/PPPoA information provided to you by your ISP. Click **NEXT** to continue.

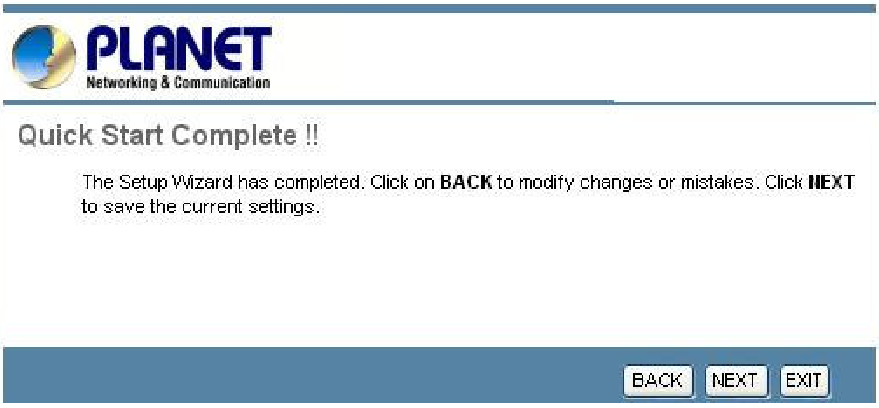
Username: t0399199

Password: ●●●●●●●●●

VPI: 0 (0~255)

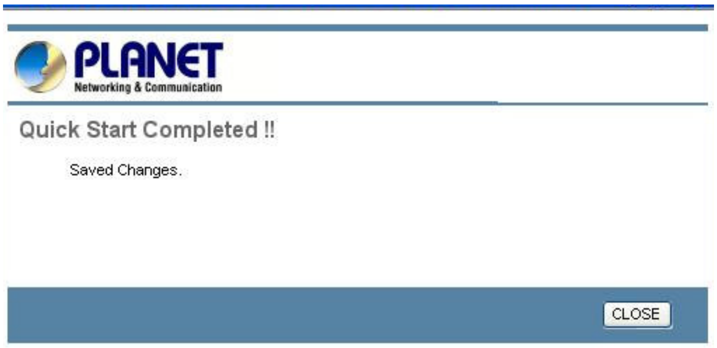
VCI: 33 (1~65535)

Connection Type: PPPoE LLC



Quick Start Complete !!

The Setup Wizard has completed. Click on **BACK** to modify changes or mistakes. Click **NEXT** to save the current settings.



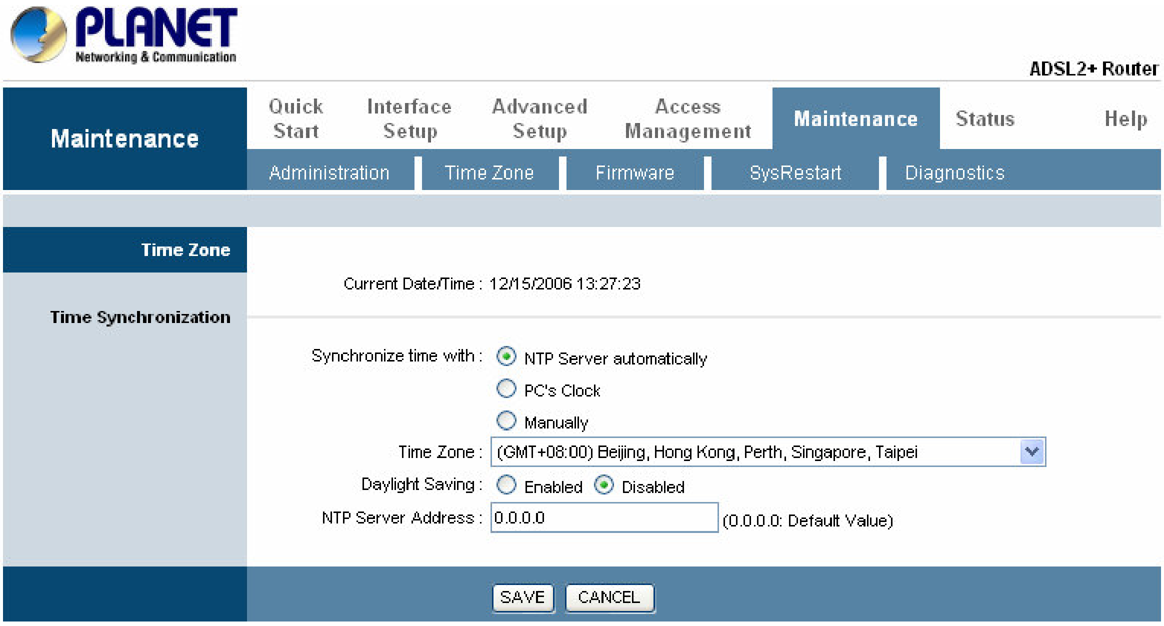
Quick Start Completed !!

Saved Changes.

- **3.4 Maintenance**
- **3.4.1 System Time**

Go to **Maintenance->Time Zone** and select system time as you wish.

The system time is the time used by the device for scheduling services. You can manually set the time or connect to a NTP (Network Time Protocol) server. If an NTP server is set, you will only need to set the time zone. If you manually set the time, you may also set Daylight Saving dates and the system time will automatically adjust on those dates.



Time Zone

Current Date/Time : 12/15/2006 13:27:23

Time Synchronization

Synchronize time with : ● NTP Server automatically ○ PC's Clock ○ Manually

Time Zone : (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei

Daylight Saving : ○ Enabled ● Disabled

NTP Server Address : 0.0.0.0 (0.0.0.0: Default Value)

Current Date/Time: This field displays an updated Date and Time when you reenter this menu.

[Time Synchronization]

Synchronize time with: You can choose ***"NTP Server automatically", "PC's Clock", or "Manually"*** to coordinate the time.

Time Zone: Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Daylight Saving: Choose **"Enabled"** or **"Disabled"** to use daylight savings time.

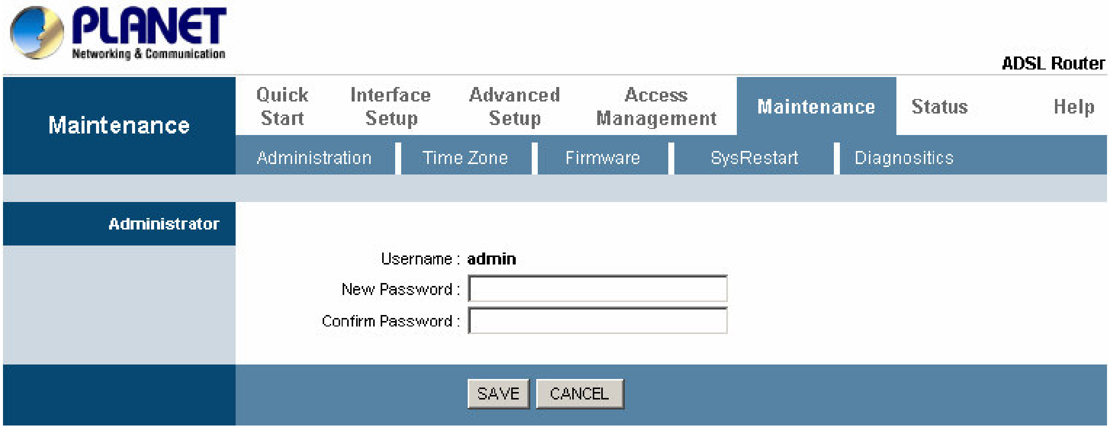
NTP Server Address: Type the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information.

A ***Network Time Protocol (NTP)*** server can automatically set the router 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.

▪ 3.4.2 Admin Setting

Go to **Maintenance-> Administration** to set a new user's name and password to restrict management access to the router.
The default is **admin (User's name)** and **admin (Password)**



Username : admin
New Password :
Confirm Password :

New Password: Type the new password in this field.

Confirm Password: Type the new password again in this field.

Note:* *If you ever forget the password to log in, you may press the RESET button up to 6 second to restore the factory default settings. The Factory Default Settings for User Name & Password are admin & admin.

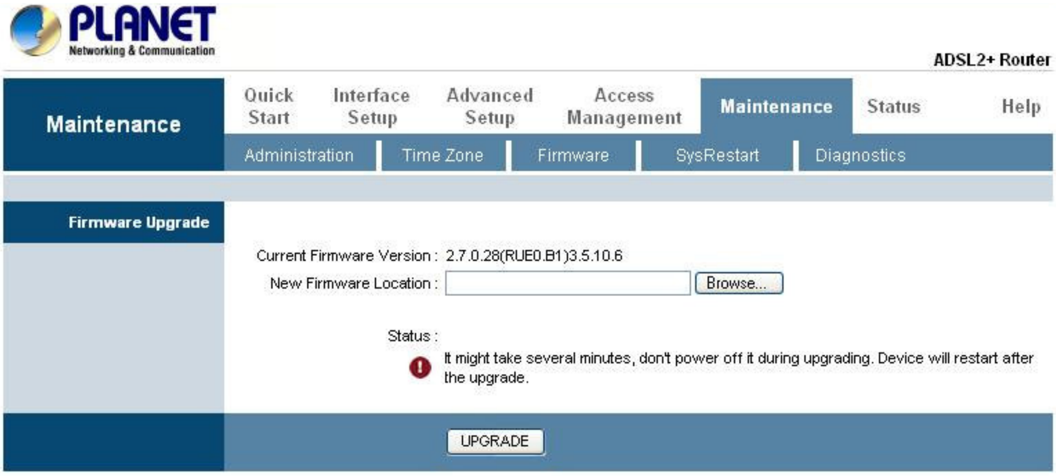
▪ 3.4.3 Firmware

Go to **Maintenance** -> **Firmware** to upgrade the firmware.

You can upgrade the **firmware** of the router in this page. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to browse the local had drive and locate the firmware to be used for the update. Then press **UPGRADE** to upload new Firmware.

It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade!!

After a success upload, the system automatically restarts. Please wait for the device to finish restarting. This should take about 2 minutes or more. You need to log in again if you want to access the device.



Current Firmware Version : 2.7.0.28(RUE0.B1)3.5.10.6

New Firmware Location :

Status :

It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.

Current Firmware Version: This filed displays the current firmware version.

New Firmware Location: Type in the location of the file you want to upload in this field or click **Browse…** to find it.

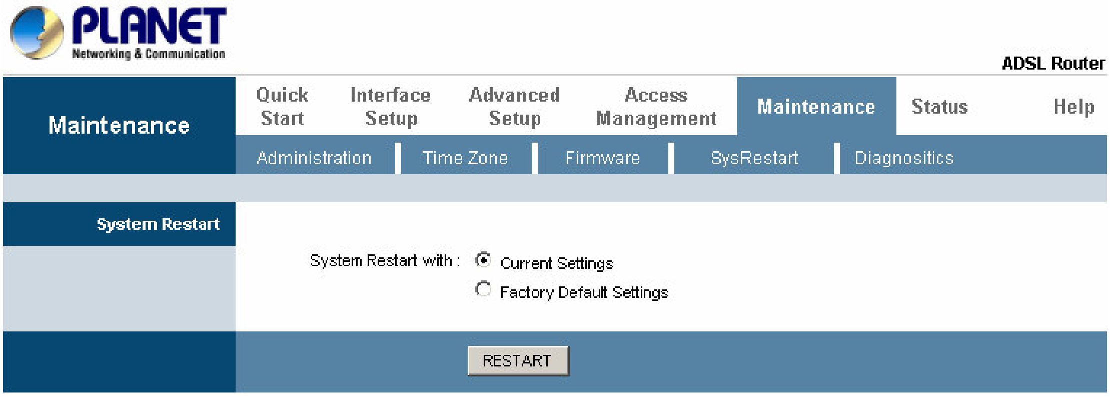
UPGRADE: Click **UPGRADE** to begin the upload process.

▪ 3.4.4 SysRestart

Go to **Maintenance->SysRestart** to do system restart.

The **SysRestart** screen allows you to restart your router with either its current settings still in place or the factory default settings.

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings. Otherwise, you can select **Current Settings**. You may also reset your router to factory settings by holding the **DEFAULT** button on the back panel of your router in for 10-12 second while the router is turned on.



System Restart with : ● Current Settings

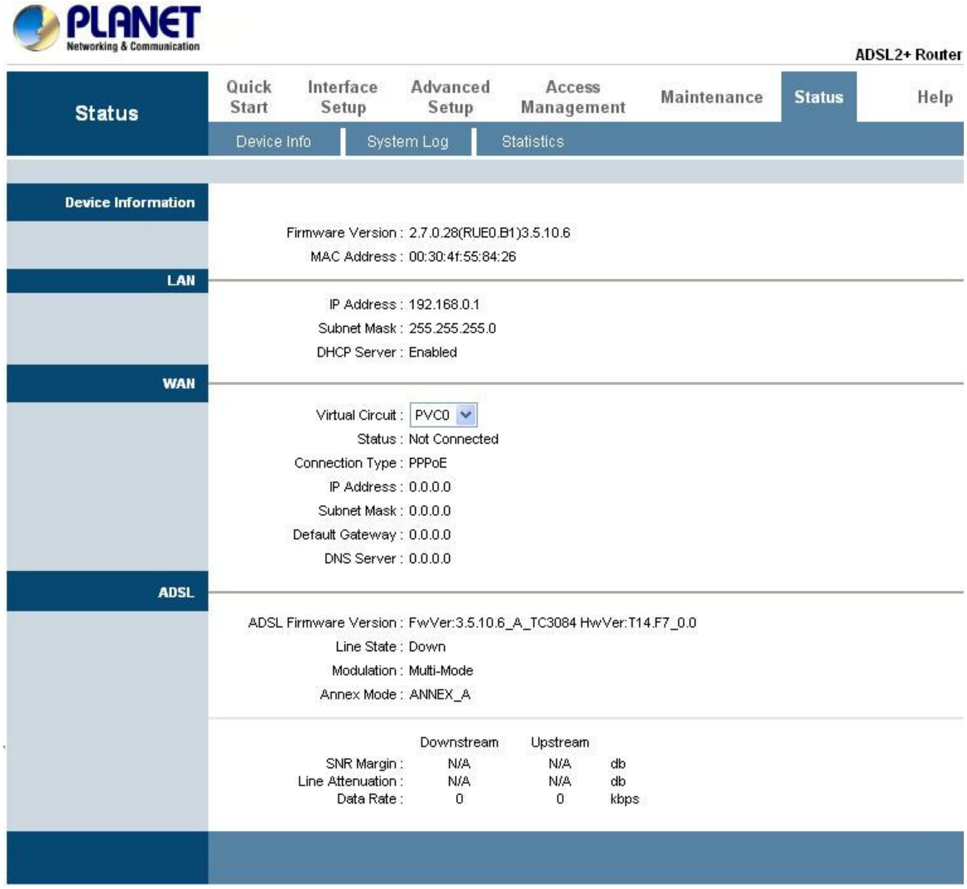
○ Factory Default Settings

■ 3.5 Status

■ 3.5.1 Device Info

Go to **Status->Device Info** to check system information**.**

The **Device Info** screen is a tool that you use to monitor your ADSL Router. It shows the Firmware Version, WAN, LAN, and MAC address information. Note that these fields are read-only and are not meant for diagnostic purposes. Except the Virtual Circuit, click the drop-down list and select the name of the Virtual Circuit on which the system status is to be shown.



Firmware Version : 2.7.0.28(RUE0.B1)3.5.10.6
MAC Address : 00:30:4f:55:84:26

IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

Virtual Circuit : PVC0
Status : Not Connected
Connection Type : PPPoE
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS Server : 0.0.0.0

ADSL Firmware Version : FwVer:3.5.10.6_A_TC3084 HwVer:T14.F7_0.0
Line State : Down
Modulation : Multi-Mode
Annex Mode : ANNEX_A

	Downstream	Upstream	
SNR Margin :	N/A	N/A	db
Line Attenuation :	N/A	N/A	db
Data Rate :	0	0	kbps

[Device Information]

Firmware Version: This filed displays current firmware version.

MAC Address: The MAC (Media Access Control) or Ethernet address unique to your modem.

[LAN]

IP Address: The LAN port IP address

Subnet Mask: The LAN port IP subnet mask.

DHCP Server: The status of **DHCP** Server (Enabled or Disabled)

[WAN]

Virtual Circuit: Click the drop-down list and select the name of the Virtual Circuit on which the system status is to be shown.

Status: Connected or Not Connected

Connection Type: The WAN Connection Type.

IP Address: The WAN port IP address

Subnet Address: The WAN port IP subnet mask.

Default Gateway: The IP address of the default gateway, if applicable.

DNS Server: The IP address of the DNS Server

[ADSL]

ADSL Firmware Version: This field displays current ADSL firmware version.

Line States: This field displays the ADSL connection process and status.

Modulation: This field displays the ADSL modulation status for G.dmt or T1.413.

Annex Mode: This field displays the ADSL annex modes for Annex A or Annex B.

Downstream and Upstream: Status of SNR Margin, Line Attenuation and Data Rate

SNR Margin: Amount of increased noise that can be tolerated while maintaining the designed BER (bit error rate). The SNR Margin is set by Central Office DSLAM. If the SNR Margin is increased, bit error rate performance will improve, but the data rate will decrease. Conversely, if the SNR Margin is decreased, bit error rate performance will decrease, but the data rate will increase.

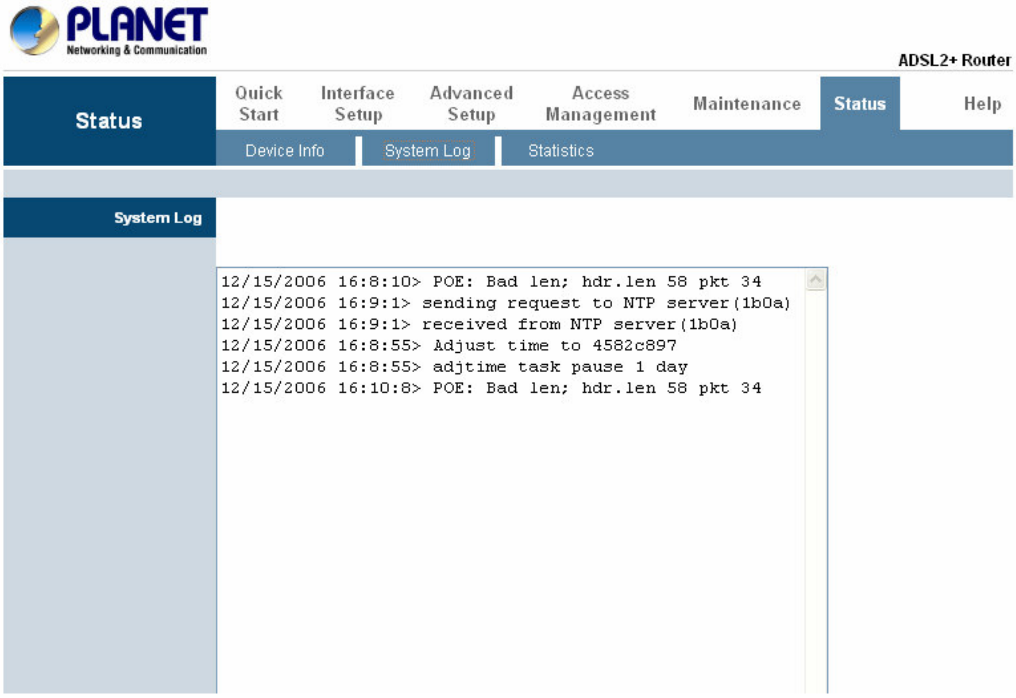
Line Attenuation: Attenuation is the decrease in magnitude of the ADSL line signal between the transmitter (Central Office DSLAM) and the receiver (Client ADSL Modem), measured in dB. It is measured by calculating the difference in dB between the signal power level received at the Client ADSL Router and the reference signal power level transmitted from the Central Office DSLAM.

Data Rate: This field displays the ADSL data rate.

▪ 3.5.2 System Log

Go to **Status -> System Log** and you can see the system log file. Click "**Save Log**" to save system log file.

The **System Log** displays data generated or acquired by routine system communication with other devices, such as the results of negotiations with the ISP's computers for DNS and gateway IP addresses. The device keeps a running log of events and activities occurring on the Router. You can click **Save Log** to display a Windows File Download dialog box that enables opening or saving the contents of the log to your PC. To remove all entries from the list, click **Clear Log**. New entries will begin accumulating. If the device is rebooted, the logs are automatically cleared.



```
12/15/2006 16:8:10> POE: Bad len; hdr.len 58 pkt 34
12/15/2006 16:9:1> sending request to NTP server(1b0a)
12/15/2006 16:9:1> received from NTP server(1b0a)
12/15/2006 16:8:55> Adjust time to 4582c897
12/15/2006 16:8:55> adjtime task pause 1 day
12/15/2006 16:10:8> POE: Bad len; hdr.len 58 pkt 34
```

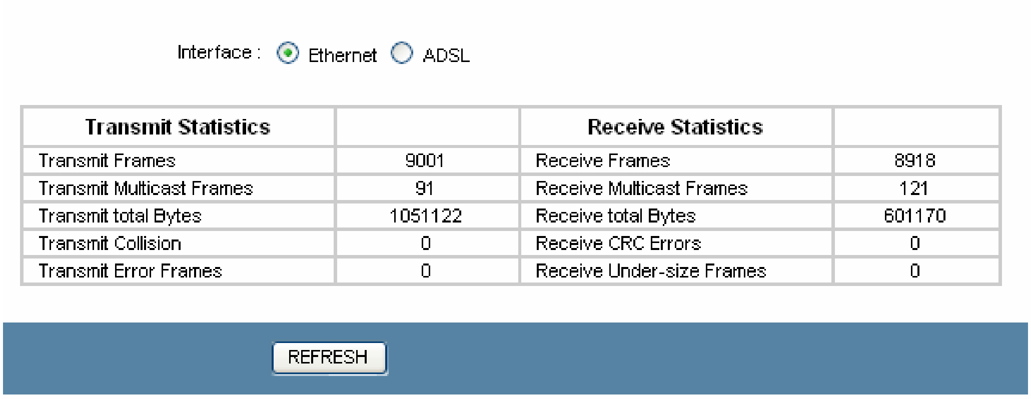
▪ 3.5.3 Statistics

Go to **Status-> Statistics** and select **ADSL** or **Ethernet** interface.

The ADSL Router keeps **statistic** of traffic that passes through it. You are able to view the amount of packets that passes through the Router on both the WAN port & the LAN port. The traffic counter will reset if the device is rebooted. You can select **Ethernet/ADSL** to view the statistics report of LAN/WAN.

[Ethernet]

The Ethernet screen gives you information on how much data your router has transmitted and received across the Ethernet connection. Click on REFRESH to update the screen.

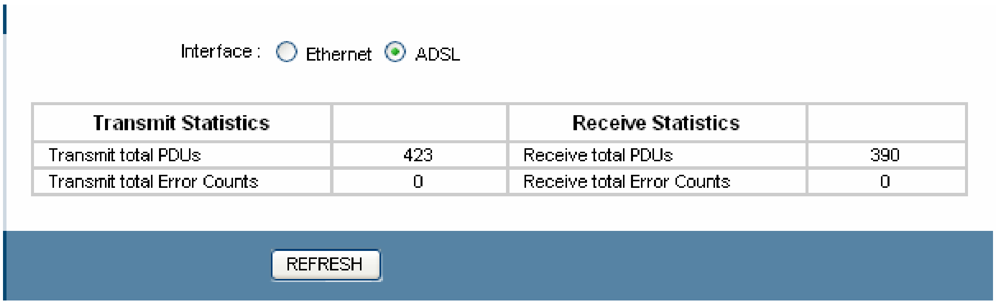


Interface : ● Ethernet ○ ADSL

Transmit Statistics		Receive Statistics	
Transmit Frames	9001	Receive Frames	8918
Transmit Multicast Frames	91	Receive Multicast Frames	121
Transmit total Bytes	1051122	Receive total Bytes	601170
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

[ADSL]

The ADSL screen gives you information about how much data your router has transmitted or received across the ADSL connection. Click on REFRESH to update the screen.



Interface : ○ Ethernet ● ADSL

Transmit Statistics		Receive Statistics	
Transmit total PDUs	423	Receive total PDUs	390
Transmit total Error Counts	0	Receive total Error Counts	0

▪ 3.6 WAN Configuration

▪ 3.6.1 VC Configuration

Go to **Interface Setup -> Internet**. To add or delete ADSL VC configuration, these information provide by ISP.

ATM settings are used to connect to your ISP. Your ISP provides VPI, VCI, settings to you. In this Device, you can totally setup 8 PVCs on different encapsulations if you apply 8 different virtual circuits from your ISP. You need to activate the VC to take effect. For PVCs management, you can use ATM QOS to setup each PVC traffic line's priority.

Virtual Circuit: Select the VC number you want to setup.

VPI: Virtual Path Identifier. The valid range for the VPI is 0 to 255.

VCI: Virtual Channel Identifier. The valid range for the VCI is 1 to 65635 (0 to 31 is reserved for local management of ATM traffic).

ATM QoS: Select the Quality of Service types for this Virtual Circuit. The ATM QoS types include CBR(Constant Bit Rate), VBR(Variable Bit Rate) and UBR (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR, and MBS.

PCR: Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832 Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

SCR: Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

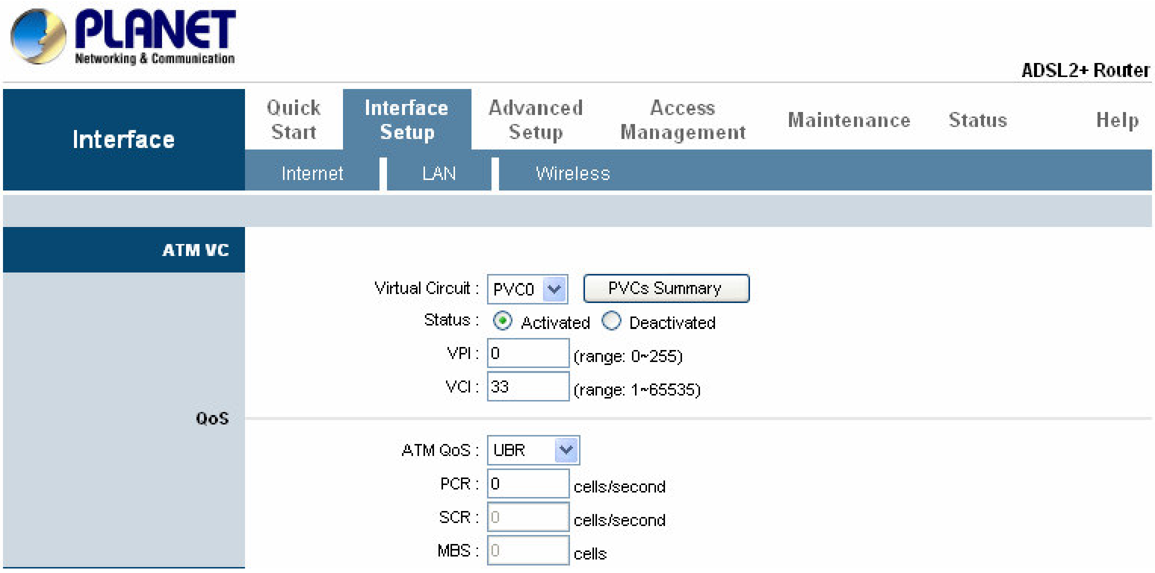
MBS: Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

CBR is for connections that support constant rates of data transfer. The only parameter you need to worry about in CBR is PCR.

UBR is for connections that have variable traffic. The only parameter you need to worry about in UBR is PCR.

rtVBR is for connections that, while having variable traffic, require precise timing between traffic source and destination. PCR, SCR and MBS must all be set for rtVBR.

nrtVBR is for connections that have variable traffic, do not require precise timing, but still require a set bandwidth availability. PCR, SCR and MBS must all be set for nrtVBR.



Virtual Circuit : PVC0
Status : ● Activated ○ Deactivated
VPI : 0 (range: 0~255)
VCI : 33 (range: 1~65535)

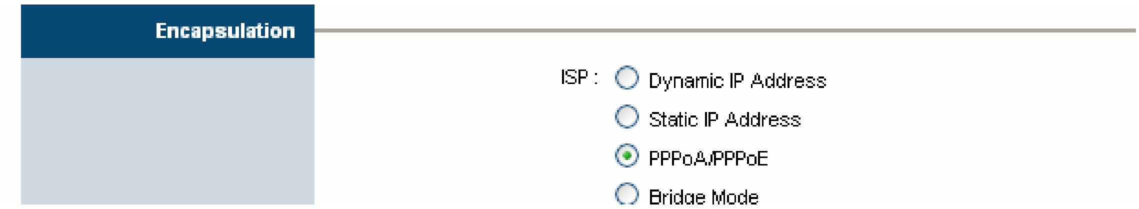
ATM QoS : UBR
PCR : 0 cells/second
SCR : 0 cells/second
MBS : 0 cells

■ 3.6.2 WAN Configuration

Go to **Interface Setup -> Internet**. The router can be connected to your service provider in any of the following ways.

■ 3.6.2.1 Encapsulation

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

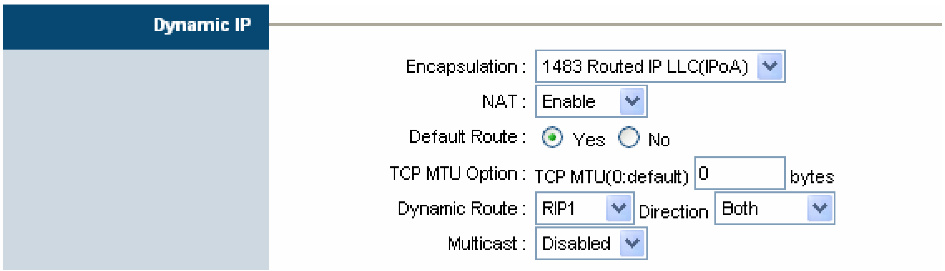


Encapsulation

ISP : ○ Dynamic IP Address
○ Static IP Address
● PPPoA/PPPoE
○ Bridge Mode

(1) Dynamic IP Address

Select this option if your ISP provides you an IP address automatically. Please enter the Dynamic IP information accordingly.



Dynamic IP

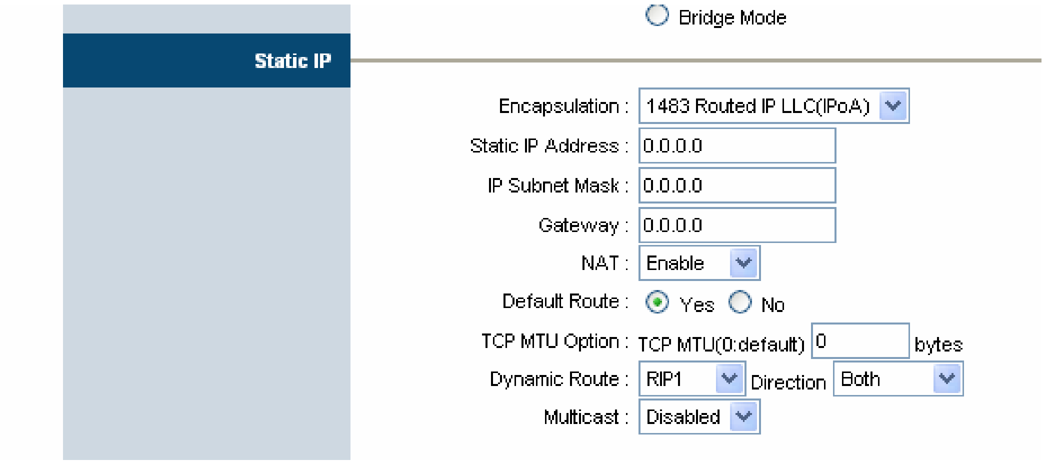
Encapsulation : 1483 Routed IP LLC(IPoA)
NAT : Enable
Default Route : ● Yes ○ No
TCP MTU Option : TCP MTU(0:default) 0 bytes
Dynamic Route : RIP1 Direction Both
Multicast : Disabled

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.
TCP MTU Option	Enter TCP MTU Value here
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.

(2) Static IP Address

Select this option to set static IP information. You will need to enter in the encapsulation type (1483 Bridged IP LLC, 1483 Bridged IP VC-Mux, 1483 Routed IP LLC (IPoA), 1483 Routed IP VC-Mux), IP address, subnet mask, and gateway address provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is 4 IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



○ Bridge Mode

Static IP

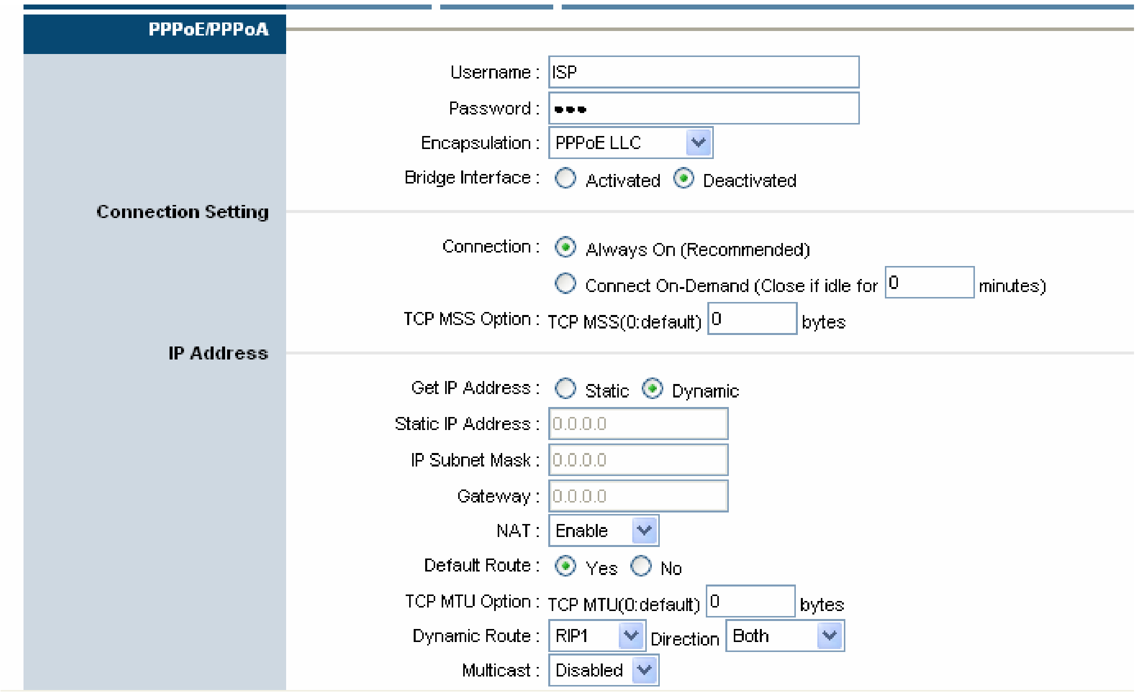
Encapsulation :	1483 Routed IP LLC(IPoA)
Static IP Address :	0.0.0.0
IP Subnet Mask :	0.0.0.0
Gateway :	0.0.0.0
NAT :	Enable
Default Route :	● Yes ○ No
TCP MTU Option :	TCP MTU(0:default) 0 bytes
Dynamic Route :	RIP1 Direction Both
Multicast :	Disabled

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 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.

(3) PPPoA / PPPoE

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL service. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Selection Static PPPoE to use static IP address for your PPPoE connection. Please enter the information accordingly.



PPPoE/PPPoA

Connection Setting

Username : ISP
Password : ●●●
Encapsulation : PPPoE LLC
Bridge Interface : ○ Activated ● Deactivated

Connection : ● Always On (Recommended)
○ Connect On-Demand (Close if idle for 0 minutes)
TCP MSS Option : TCP MSS(0:default) 0 bytes

IP Address

Get IP Address : ○ Static ● Dynamic
Static IP Address : 0.0.0.0
IP Subnet Mask : 0.0.0.0
Gateway : 0.0.0.0
NAT : Enable
Default Route : ● Yes ○ No
TCP MTU Option : TCP MTU(0:default) 0 bytes
Dynamic Route : RIP1 Direction Both
Multicast : Disabled

LABEL	DESCRIPTION
Username	Enter your username for your PPPoE/PPPoA connection.
Password	Enter your password for your PPPoE/PPPoA connection.
Encapsulation	Select your encapsulation type from the dropdown list.
Bridge Interface	Select whether the Interface will be Activated or Deactivated.
Connection	Select whether your connection is always on or if it connects on demand. If on demand, specify how many minutes the connection may be idle before it disconnects.
TCP MSS Option	Enter the TCP MSS you wish to use here.
Get IP Address	Choose whether the ROUTER obtains the IP address statically or dynamically.
Static IP Address	Enter the static IP address here. Only if you chose Static above.
IP Subnet Mask	Enter the IP subnet mask here. Only if you chose Static above.
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 data.
TCP MTU Option	Enter TCP MTU Value here.
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.

***Connection Setting*:** For PPPoE/PPPoA connection, you can select Always on or Connect on-demand. Connect on demand is dependent on the traffic. If there is no traffic (or Idle) for a pre-specified period of time, the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.

***IP Address*:** For PPPoE/PPPoA connection, you need to specify the public IP address for this ADSL Router. The IP address can be either dynamically (via DHCP) or given IP address provide by your ISP. For Static IP, you need to specify the IP address, Subnet Mask and Gateway IP address.

NAT: Select this option to Activate/Deactivated the NAT (Network Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis.

[Dynamic Route]

RIP (Routing Information Protocol): Select this option to specify the RIP version, including ***RIP1***, ***RIP2-B*** and ***RIP2-M***. RIP2-B & RIP2-M are both sent in RIP-2 format, the difference is that RIP2-M using Multicast and RIP2-B using Broadcast format.

RIP Direction: Select this option to specify the RIP direction. ***None*** is for disabling the RIP function. ***Both*** means the ADSL Router will periodically send routing information and accept routing information then incorporate into routing table. ***IN only*** means the ADSL router will only accept but will not send RIP packet. ***OUT only*** means the ADSL router will only sent but will not accept RIP packet.

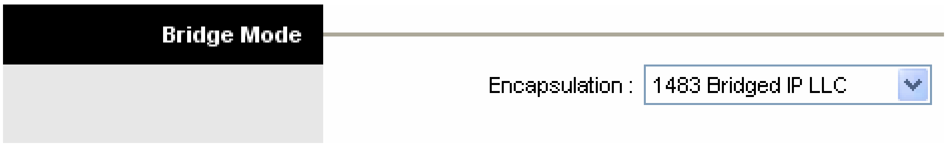
[Multicast]

IGMP (Internet Group Multicast Protocol): It is a session-layer protocol used to establish membership in a multicast group. The ADSL supports both IGMP version ***IGMP-v1*** & ***IGMP-v2***. Select ***None*** to disable it.

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.

(4) Bridge Mode

The modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable 2 or more networks to communicate as if they are 2 segments of the same physical LAN. Please set the Connection type.



Bridge Mode

Encapsulation : 1483 Bridged IP LLC

The following table describes the labels in this screen.

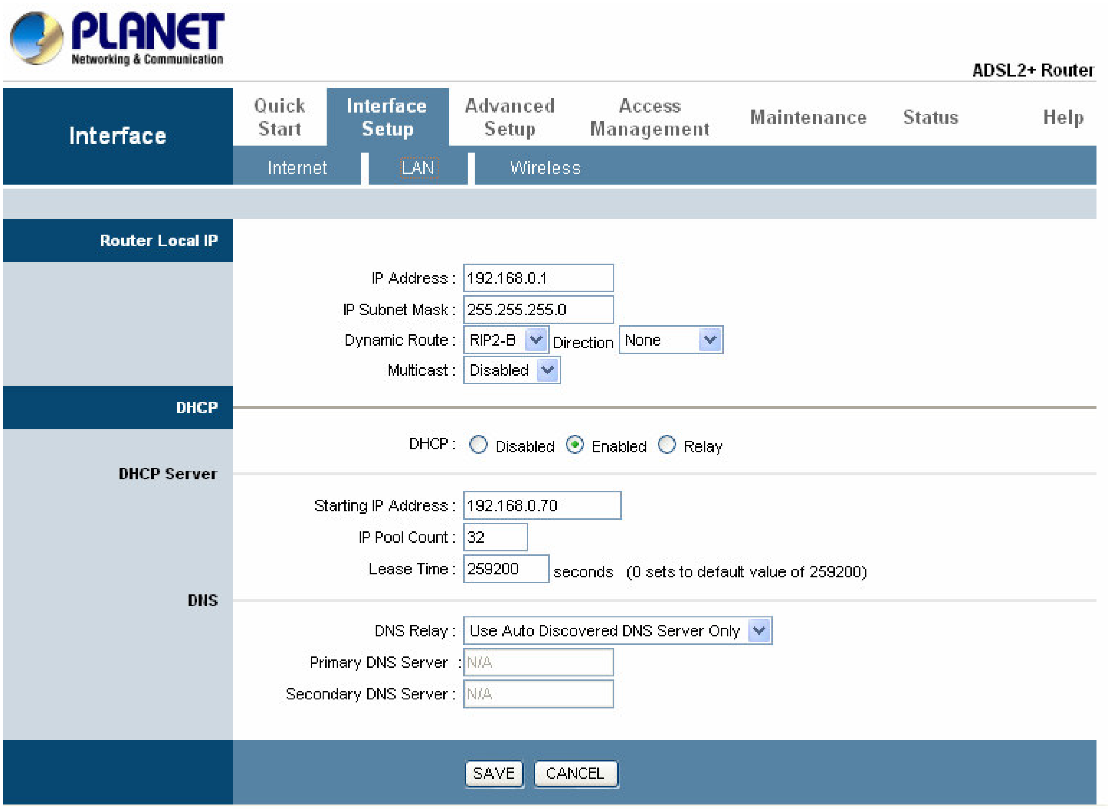
LABEL	DESCRIPTION
Encapsulation	Select your encapsulation type from the dropdown list.

▪ 3.7 LAN Configuration

▪ 3.7.1 LAN Configuration

Go to **Interface Setup** -> **LAN**. The **LAN** option enables you to configure the LAN port.

There are the IP settings of the LAN Interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is provided to your internal network and cannot be seen on the Internet.



Router Local IP

IP Address : 192.168.0.1

IP Subnet Mask : 255.255.255.0

Dynamic Route : RIP2-B Direction None

Multicast : Disabled

DHCP

DHCP : ○ Disabled ● Enabled ○ Relay

DHCP Server

Starting IP Address : 192.168.0.70

IP Pool Count : 32

Lease Time : 259200 seconds (0 sets to default value of 259200)

DNS

DNS Relay : Use Auto Discovered DNS Server Only

Primary DNS Server : N/A

Secondary DNS Server : N/A

■ 3.7.1.1 Router Local IP

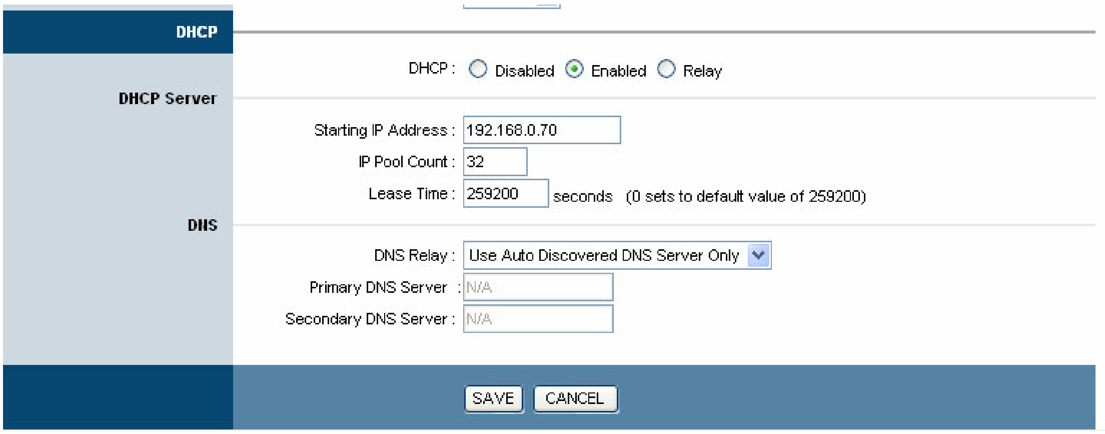
IP Address: Enter the IP address of your ADSL router in dotted decimal notation, for example, 192.168.1.1 (default setting).

IP Subnet Mask: Your ADSL router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing sub netting, use the subnet mask computed by the ADSL router.

Dynamic Route: Select the Dynamic Route from **RIP1**, **RIP2-B**, and **RIP2-M**. Please refer to **Dynamic Routing.** The only difference is the interface.

■ 3.7.1.2 DHCP Server

The DHCP Server gives out IP addresses when a device is booting up and request an IP to be logged on to the network. It must be set as a DHCP client to obtain the IP address automatically. By default, the DHCP Server is enabled. The DHCP address pool contains the range of the IP address that will automatically be assigned to the client on the network.



DHCP : ○ Disabled ● Enabled ○ Relay

Starting IP Address : 192.168.0.70

IP Pool Count : 32

Lease Time : 259200 seconds (0 sets to default value of 259200)

DNS Relay : Use Auto Discovered DNS Server Only

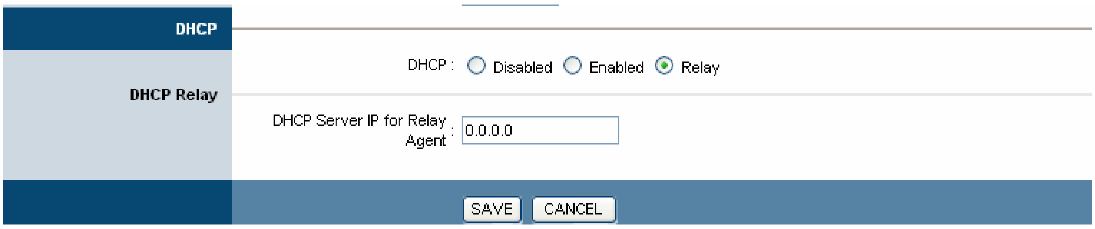
Primary DNS Server : N/A

Secondary DNS Server : N/A

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.

■ 3.7.1.3 DHCP Relay

A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enable, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.



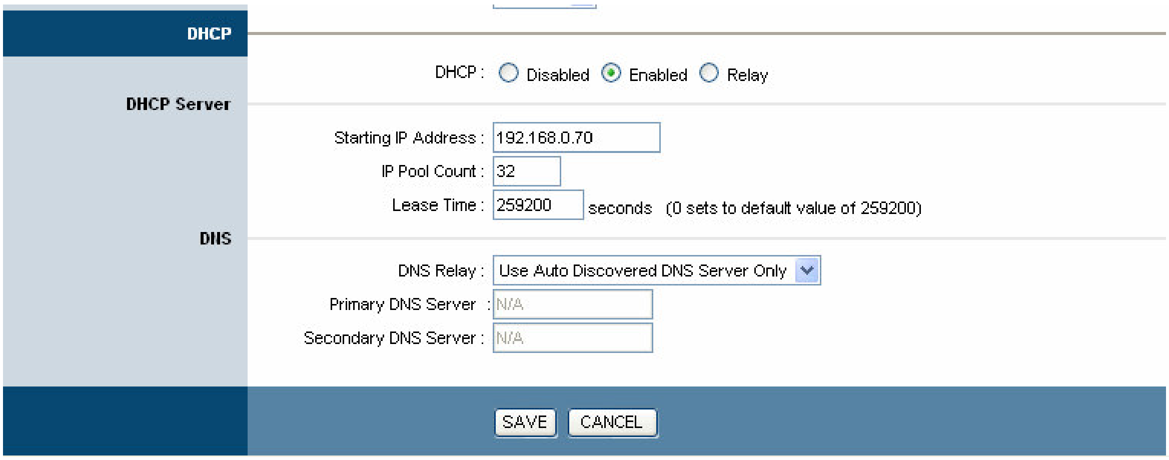
DHCP : ○ Disabled ○ Enabled ● Relay

DHCP Server IP for Relay Agent : 0.0.0.0

DHCP Server IP for relay agent: The DHCP server IP Address runs on WAN side.

- **3.7.1.4 DNS Relay**

The DNS Configuration allows the user to set the configuration of DNS.



DHCP : ○ Disabled ● Enabled ○ Relay

Starting IP Address : 192.168.0.70

IP Pool Count : 32

Lease Time : 259200 seconds (0 sets to default value of 259200)

DNS Relay : Use Auto Discovered DNS Server Only

Primary DNS Server : N/A

Secondary DNS Server : N/A

DNS Rely Selection: If user wants to disable this feature, he just needs to set both Primary & Secondary DNS to 0.0.0.0. Using DNS relay, users can setup DNS server IP to 192.168.1.1 on their computer. If not, device will perform as NO DNS relay.

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**".

▪ 3.8 Wireless Configuration

▪ 3.8.1 Wireless Configuration

Go to **Interface -> Wireless** to setup the wireless parameters.

SSID: The SSID is a unique name to identify the ADSL Router in the Wireless LAN. Wireless Clients associating to the ADSL Router must have the same SSID.

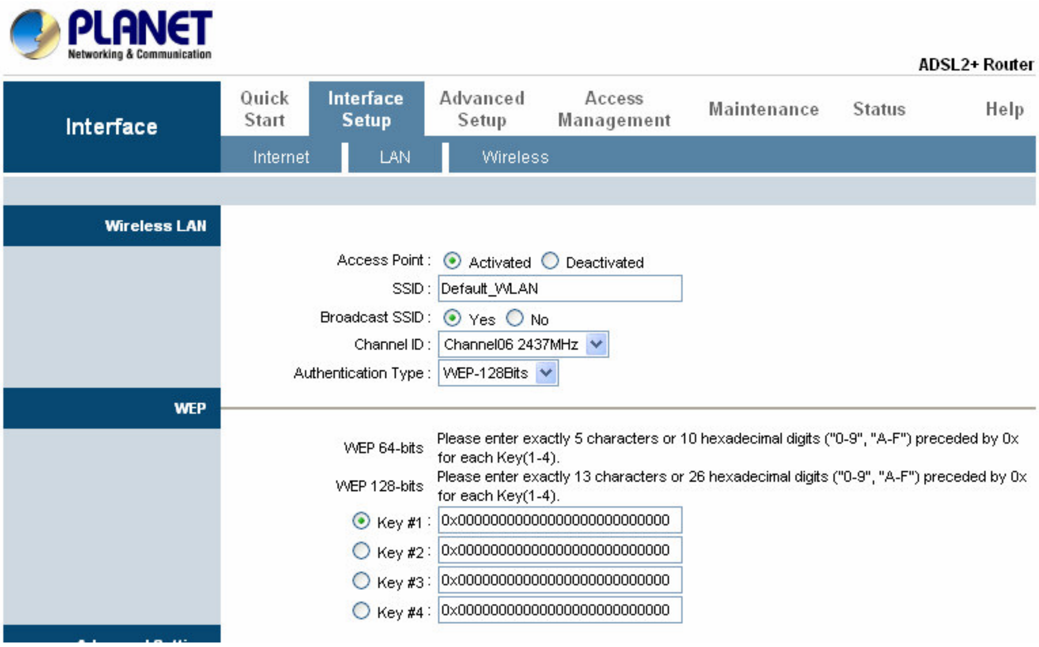
Broadcast SSID: Select **No** to hide the SSID such that a station can not obtain the SSID through passive scanning. Select **Yes** to make the SSID visible so a station can obtain in the SSID through Passive scanning.

Channel ID: The range of radio frequencies used by IEEE 802.11b/g wireless devices us called a channel.

■ 3.8.1.1 Wireless Security

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select **Disable** to allow all wireless computers to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to use data encryption.

Key#1~Key#4 The WEP keys are used to encrypt data. Both the ADSL Router and the wireless clients must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4). If you choose **1280bit WEP**, then enter 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4). The values must be set up exactly the same on the Access Points as they are on the wireless client stations. The same value must be assigned to Key 1 on both access point (your ADSL Router) and the client adapters, the same value must be assigned to Key 2 on both access point and the client stations and so on, for all four WEP keys.



Access Point : ● Activated ○ Deactivated

SSID : Default_WLAN

Broadcast SSID : ● Yes ○ No

Channel ID : Channel06 2437MHz

Authentication Type : WEP-128Bits

WEP 64-bits Please enter exactly 5 characters or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).

WEP 128-bits Please enter exactly 13 characters or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).

● Key #1 : 0x00000000000000000000000000

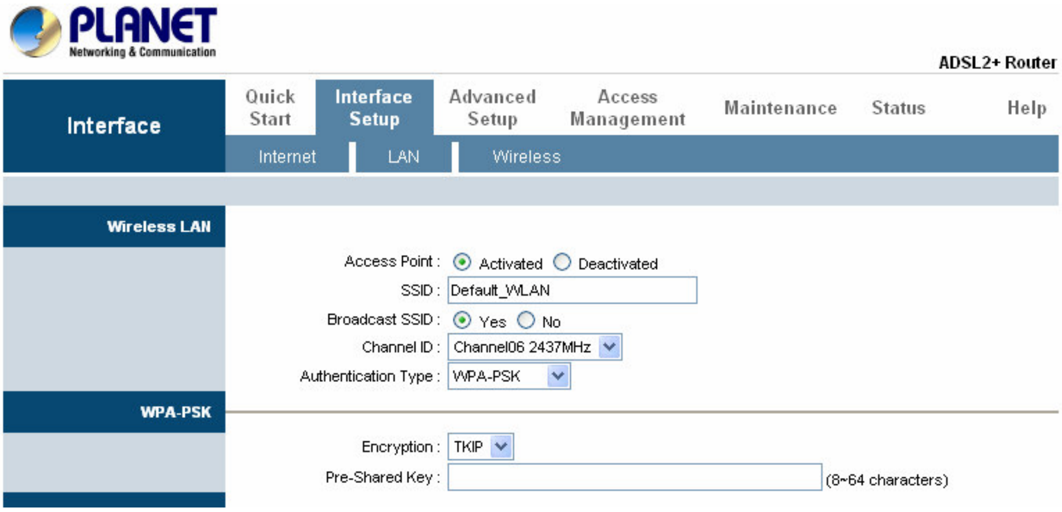
○ Key #2 : 0x00000000000000000000000000

○ Key #3 : 0x00000000000000000000000000

○ Key #4 : 0x00000000000000000000000000

WPA-PSK Wi-Fi Protected Access, pre-shared key. Encrypts data frames before transmitting over the wireless network.

Pre-shared Key is used to encrypt data. Both the ADSL Router and the wireless clients must use the same WPA-PSK Key for data transmission.



Access Point : ● Activated ○ Deactivated

SSID : Default_WLAN

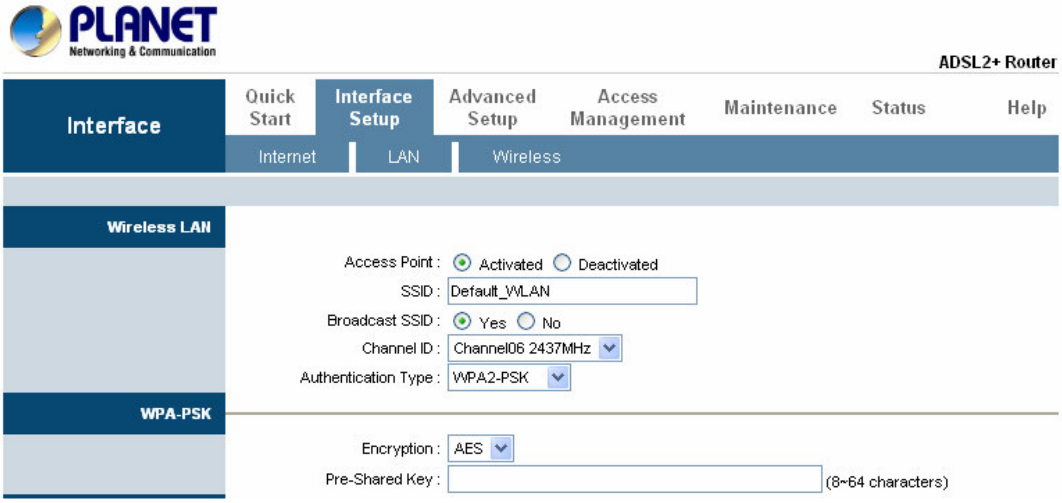
Broadcast SSID : ● Yes ○ No

Channel ID : Channel06 2437MHz

Authentication Type : WPA-PSK

Encryption : TKIP

Pre-Shared Key : (8~64 characters)



Access Point : ● Activated ○ Deactivated

SSID : Default_WLAN

Broadcast SSID : ● Yes ○ No

Channel ID : Channel06 2437MHz

Authentication Type : WPA2-PSK

Encryption : AES

Pre-Shared Key : (8~64 characters)

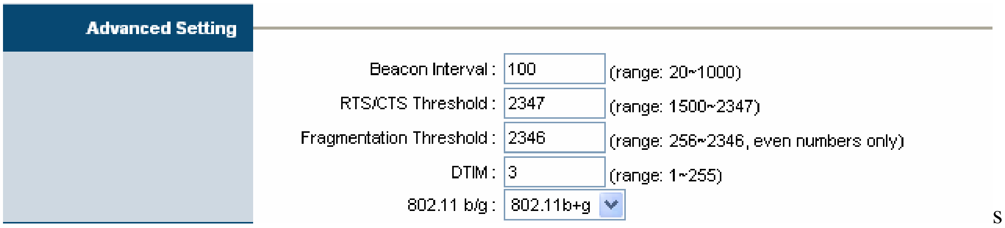
- ### 3.8.1.2 Advanced Setting

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 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. Set this attribute to be larger than the **maximum MSDU** (MAC Service Data Unit) size **TURNS OFF** the RTS/CTS handshake. Set this attribute to **ZERO** **TURNS ON** the RTS/CTS handshake. Enter a value between 0 and 2432.

Fragment 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 2432.

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



Beacon Interval : 100 (range: 20~1000)

RTS/CTS Threshold : 2347 (range: 1500~2347)

Fragmentation Threshold : 2346 (range: 256~2346, even numbers only)

DTIM : 3 (range: 1~255)

802.11 b/g : 802.11b+g

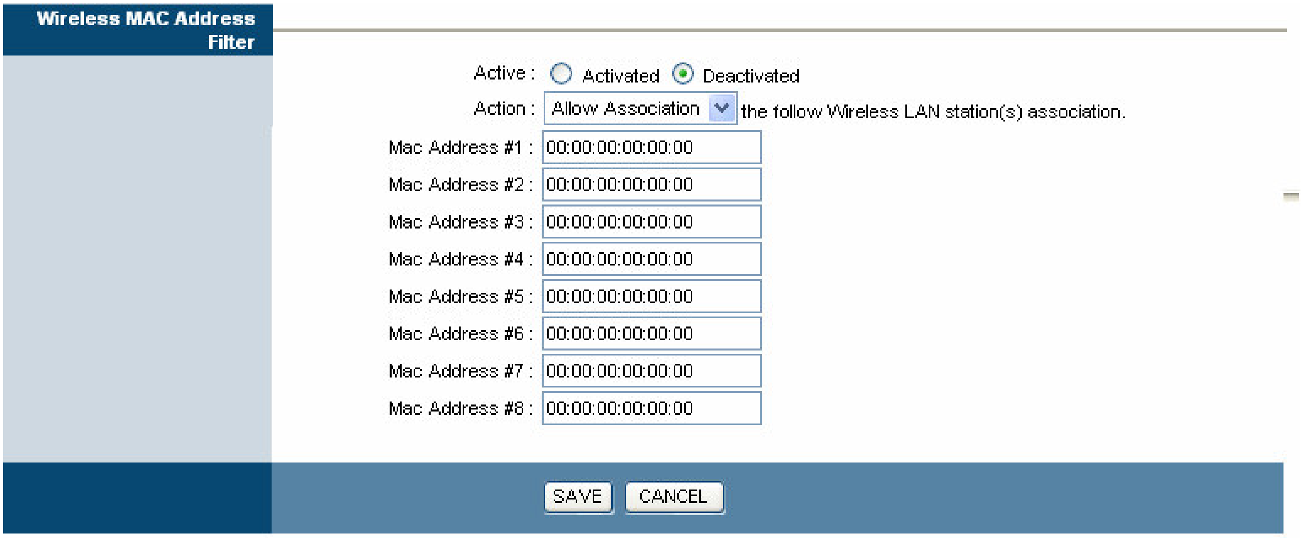
s

■ 3.8.1.3 MAC Address Filter

You can allow or deny a lust of MAC addresses associated with the wireless stations access to the ADSL Router.

Status: Use the drop down list box to enable or disable MAC address filtering.

Action: 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 lusted will be denied access to the router.



Active : ○ Activated ● Deactivated

Action : Allow Association the follow Wireless LAN station(s) association.

Mac Address #1 : 00:00:00:00:00:00

Mac Address #2 : 00:00:00:00:00:00

Mac Address #3 : 00:00:00:00:00:00

Mac Address #4 : 00:00:00:00:00:00

Mac Address #5 : 00:00:00:00:00:00

Mac Address #6 : 00:00:00:00:00:00

Mac Address #7 : 00:00:00:00:00:00

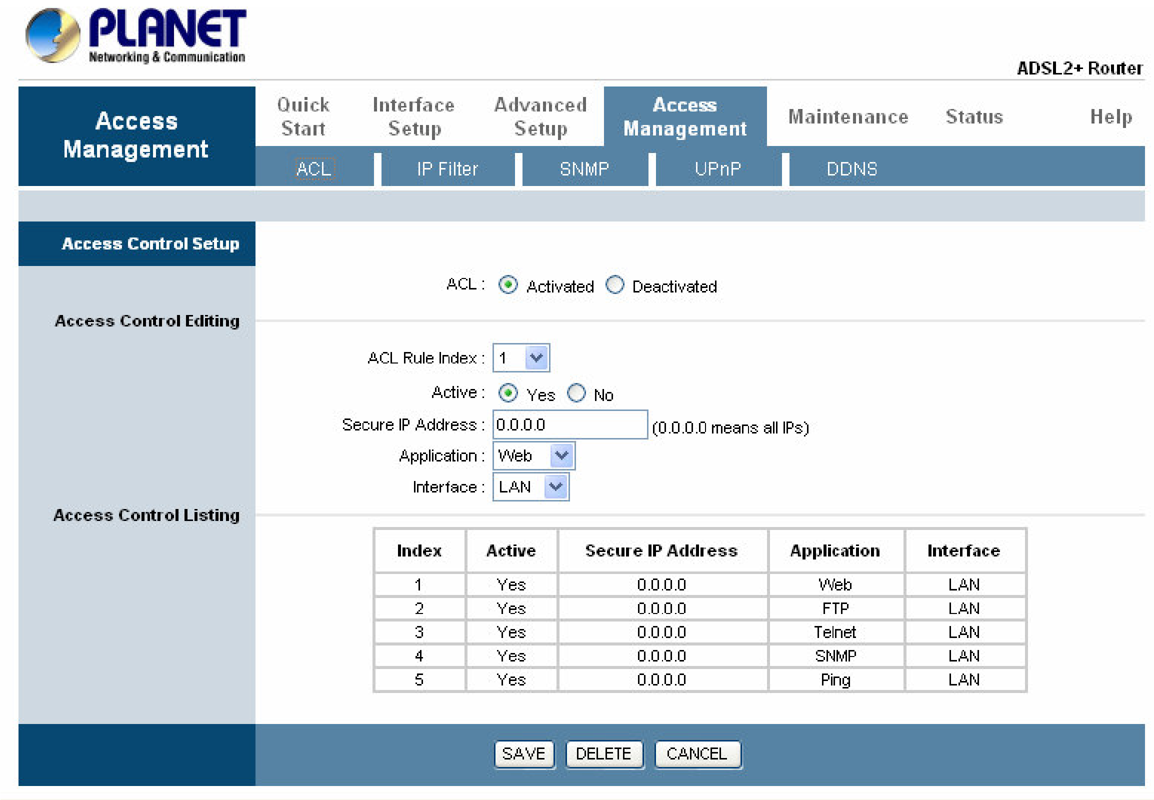
Mac Address #8 : 00:00:00:00:00:00

■ 3.9 Access Management

■ 3.9.1 ACL

Go to **Access Management -> ACL** to enable remote management.

Access Control Listing (ACL) is a management tool that acts as a filter for incoming or outgoing packets, based on application. You may use telnet or Web to remotely manage the ADSL Router. User just needs to enable Telnet or Web and give it an IP address that wants to access the ADSL Router. The default IP 0.0.0.0 allows any client to use this service to remotely manage the ADSL Router.



ACL : ● Activated ○ Deactivated

ACL Rule Index : 1

Active : ● Yes ○ No

Secure IP Address : 0.0.0.0 (0.0.0.0 means all IPs)

Application : Web

Interface : LAN

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0	Web	LAN
2	Yes	0.0.0.0	FTP	LAN
3	Yes	0.0.0.0	Telnet	LAN
4	Yes	0.0.0.0	SNMP	LAN
5	Yes	0.0.0.0	Ping	LAN

ACL: There has **Activated** & **Deactivated** option. The default setting is **Deactivated** which means all IP can access via router. If you choose **Activated**, you only can access via router by listed IP addresses.

ACL Rule Index: Index number from 1 and up to 16.

Active: Once you choose **Yes** then you can access the IP via router.

Application: Each of these labels denotes a service that you may use to remotely manage the Router. Choices are **Web, FTP, Telnet, SNMP, Ping, ALL**.

Interface: Select the access interface. Choices are **WAN, LAN** and **Both.**

■ 3.9.2 IP Filtering

Go to **Access Management -> IP Filtering** to block some packets form WAN.

The Router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attackers. Go to **Access Management ->IP Filtering** to set different IP filter rules of a given protocol (TCP, UDP, or ICMP) and a specific direction (incoming, outgoing, or both) to filter the packets.

IP Filter is a more complex filtering tool, based more on IP and custom rules. Each of the indices can hold six rules, and each interface can have four associated indices, allowing 24 rules per interface. If all six rules in an index are Next rules, the data will be sent to the next index for filtering.

IP Filter Set Index: The IP Filter Set Index from 1 to 12 and each index can set up to 6 IP Filter.

Interface: Choices from **PVC0** to **PVC7** and **LAN**.

Direction: Choices are **Both**, **Incoming** and **Outgoing**. 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 Editing: Select the IP Filter Rule Index 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.

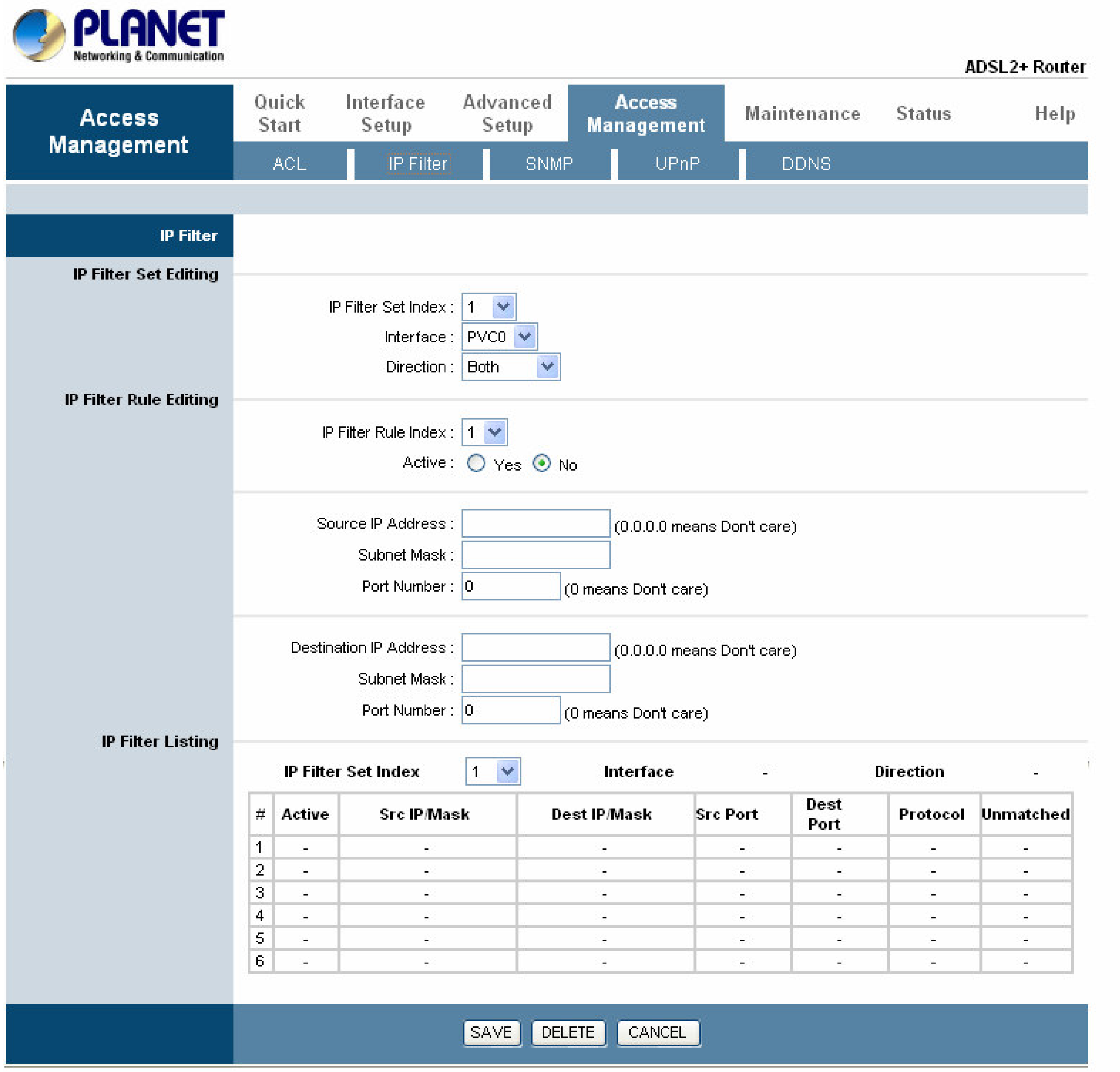
Subnet Mask: Enter the subnet mask of the destination IP address

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. Choices are TCP, UDP, and ICMP.

Rule Unmatched: Choices are **Forward** and **Next.** 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.



IP Filter

IP Filter Set Editing

IP Filter Set Index : 1

Interface : PVC0

Direction : Both

IP Filter Rule Editing

IP Filter Rule Index : 1

Active : ○ Yes ● No

Source IP Address : (0.0.0.0 means Don't care)

Subnet Mask :

Port Number : 0 (0 means Don't care)

Destination IP Address : (0.0.0.0 means Don't care)

Subnet Mask :

Port Number : 0 (0 means Don't care)

IP Filter Listing

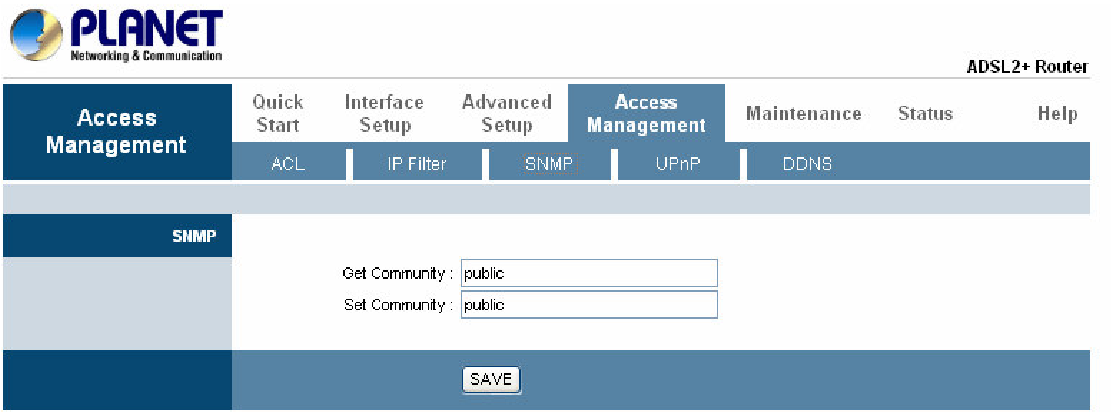
IP Filter Set Index 1 Interface - Direction -

#	Active	Src IP/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-

■ 3.9.3 SNMP

Go to **Access Management** -> **SNMP** to set SNMP.

The **Simple Network Management Protocol (SNMP)** is used for exchanging information between network devices. It enables a host computer to access configuration, performance, and other system data that resides in a database on the modem. The host computer is called a *management station* and the modem is called an *SNMP agent*. The data that can be accessed via SNMP is stored in a *Management Information Database* (MIB) on the modem.



Get Community : public

Set Community : public

Get Community: Select to set the password for incoming Get- and GetNext request from management station.

Set Community: Select to set the password for incoming Set request from management station.

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

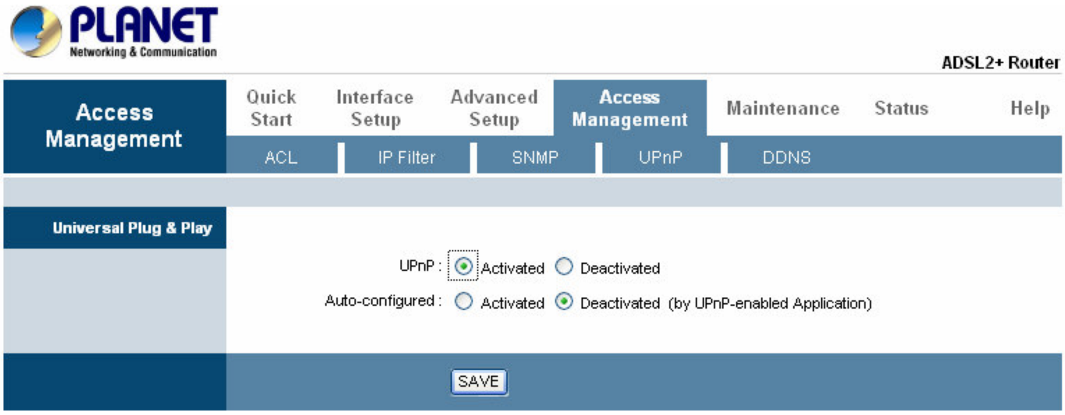
▪ 3.9.4 UPNP

Go to **Access Management -> UPNP** to set UPNP.

UPnP (Universal Plug and Play) is a distributed, 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. In turn, a device can leave a network smoothly an automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN.

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (in Windows XP & Windows ME). Each UPnP-compatible device that is installed on your network will appear as a separate icon.



UPnP : ● Activated ○ Deactivated

Auto-configured : ○ Activated ● Deactivated (by UPnP-enabled Application)

UPnP (Universal Plug and Play): You can choose **"Activated"** or **"Deactivated"** option from this session.

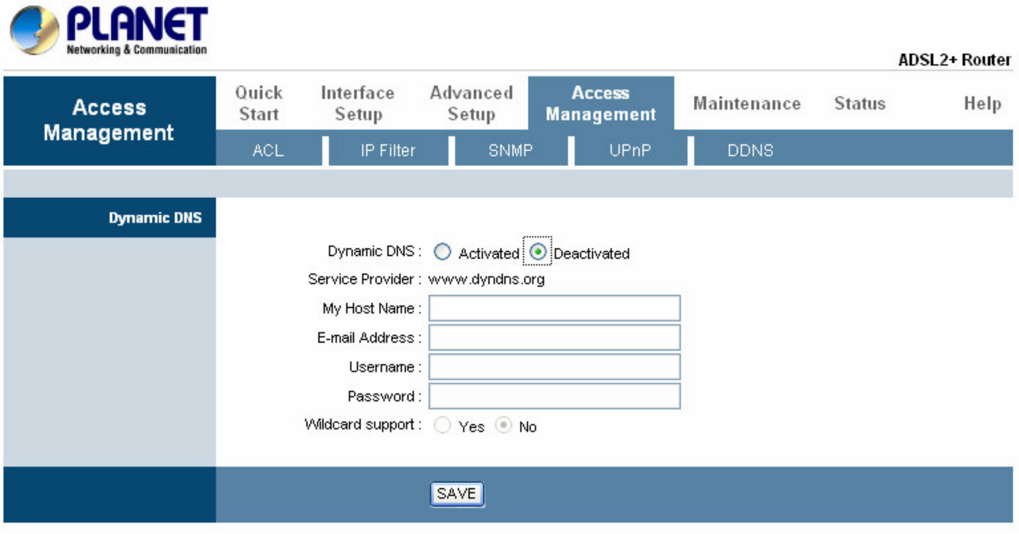
Auto-Configured (by UPnP Application): UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. Choose **"Activated"** option to allow UPnP-enabled applications to automatically configure the ADSL Router so that they can communicate through the ADSL Router, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPP enabled application. If you don't want to make configuration changes through UPnP, just choose **"Deactivated"**.

SAVE: Click **SAVE** to save the setting to the ADSL Router.

▪ 3.9.5 DDNS

Go to **Access Management-> DDNS** to set DDNS account.

The **Dynamic Domain Name System** allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a DNS-like address (for instance myhost.dhs.org, where my host is a name of your choice) 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. First of all, 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.



Dynamic DNS : ○ Activated ● Deactivated

Service Provider : www.dyndns.org

My Host Name :

E-mail Address :

Username :

Password :

Wildcard support : ○ Yes ● No

Dynamic DNS: Choose the option for **Activated** or **Deactivated** DDNS.

Service Provider: The default Dynamic DNS service provider is **www.dyndns.org**.

My Host Name: Type the domain name assigned to your ADSL by your Dynamic DNS provider.

E-mail Address: Type your e-mail address.

Username: Type your user name.

Password: Type the password assigned to you.

Wildcard support: Select **Yes** or **No** to turn on DYNDNS Wildcard.

DYNDNS Wildcard --> Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

SAVE: Click **SAVE** to save your changes.

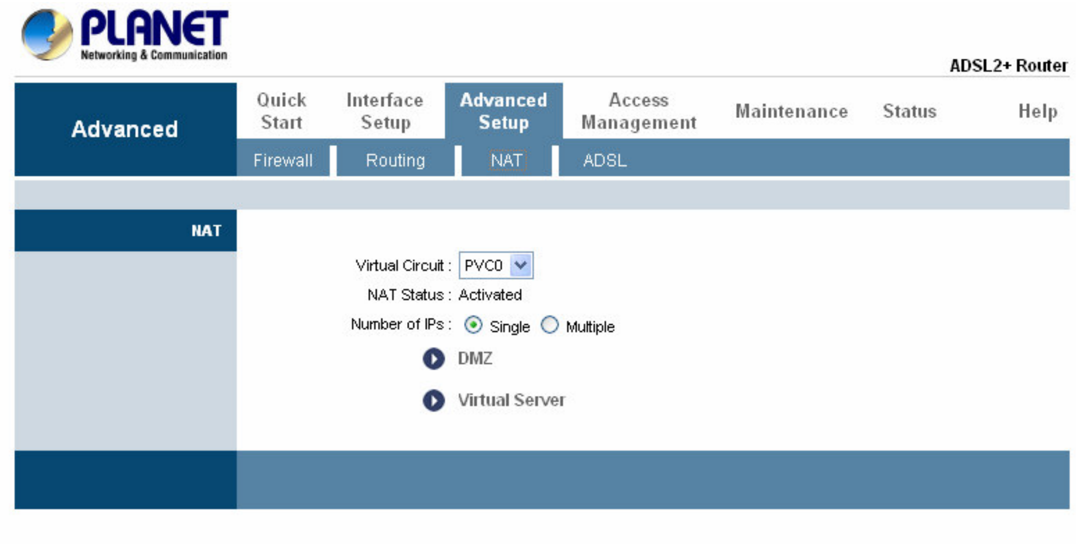
Note that you must enter the user name exactly as your ISP assigned it. If the assigned name is in the form of user@domain where domain identifies a service name, enter it exactly as given. When you are done making changes, click on SAVE to save your changes.

■ 3.10 Advanced Setup

■ 3.10.1 NAT Setting

Go to **Advanced Setup->NAT** to setup the NAT features.

Network Address Translation (NAT) is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses. Simply select this option to setup the NAT function for your ADSL router.



Virtual Circuit : PVC0

NAT Status : Activated

Number of IPs : ● Single ○ Multiple

DMZ

Virtual Server

Virtual Circuit (VC): The Virtual Circuit (VC) properties of the ATM VC interface identify a unique path that your ADSL/Ethernet router uses to communicate via the ATM-based network with the telephone company central office equipment.

NAT Status: This filed shows the current status of the NAT function for the current VC.

Number of IPs: This field is to specify how many IPs are provided by your ISP for current VC. It can be single IP or multiple IPs.

Note: For VCs with single IP, they share the same DMZ & Virtual servers; for VCs with multiple IPs, each VC cab set DMZ and Virtual servers. Furthermore, for VCs with multiple IPs, they can define the Address Mapping rules; for VCs with single IP, since they have only one IP, there is no need to individually define the Address Mapping rule.

What NAT Does

NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. You may also designate servers, such as a Web server and a telnet server, on your local network and make them accessible to the outside world. With no servers defined, your ROUTER filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

Inside/outside indicates where a host is located relative to the ROUTER. The computers hosts of your LAN are inside, while the Web servers on the Internet are outside.

Global/local indicates the IP address of a host in a packet as the packet traverses a router. The local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host of a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side.

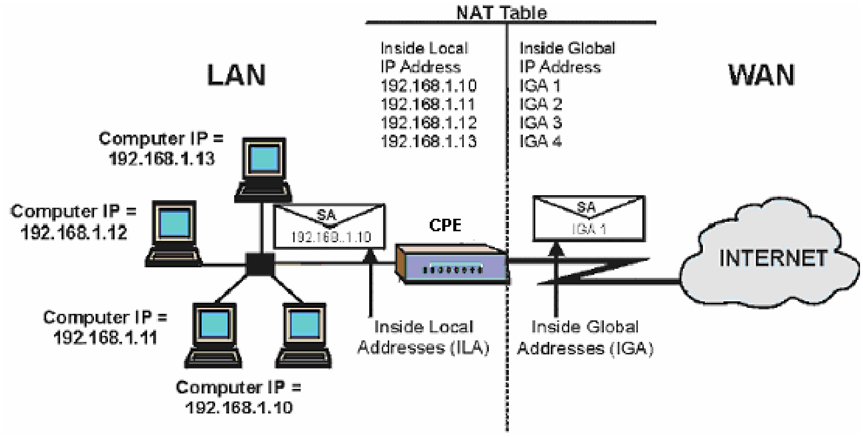
The following table summarizes this information.

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

How NAT Works

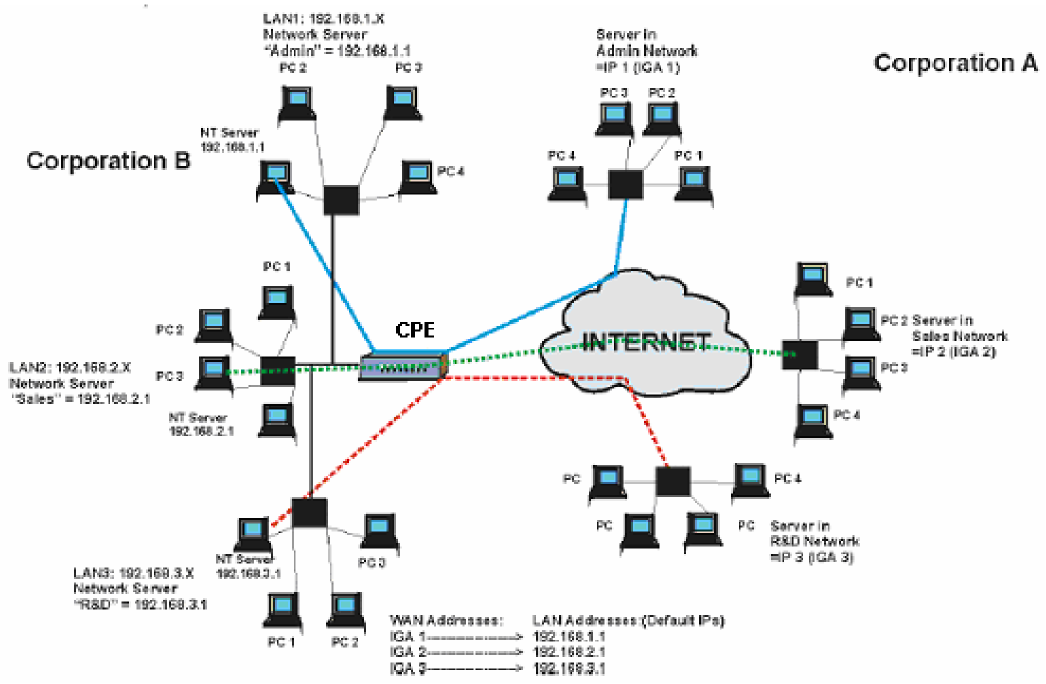
Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA is the source address on the LAN, and the IGA is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ROUTER keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

The following figure illustrates this.



NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the router can communicate with three distinct WAN networks. More examples follow at the end of this chapter.



NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

a. **One-to-One**: In One-to-One mode, the TC3162 EVM maps one local IP address to one global IP address.

b. **Many-to-One**: In Many-to-One mode, the TC3162 EVM maps multiple local IP addresses to one global IP address.

c. **Many-to-Many Overload**: In Many-to-Many Overload mode, the TC3162 EVM maps multiple local IP addresses to shared global IP addresses.

d. **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the TC3162 EVM maps each local IP address to a unique global IP address.

e. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

The following table summarizes these types.

TYPE	IP MAPPING
One-to-One	ILA1 IGA1
Many-to-One (SUA/PAT)	ILA1 IGA1 ILA2 IGA1 …
Many-to-Many Overload	ILA1 IGA1 ILA2 IGA2 ILA3 IGA1 ILA4 IGA2 …
Many-to-Many No Overload	ILA1 IGA1 ILA2 IGA2 ILA3 IGA3 …
Server	Server 1 IP IGA1 Server 2 IP IGA1 Server 3 IP IGA1

■ 3.10.1.1 Virtual Server

Go to **Advanced Setup ->NAT -> Virtual Server** to set virtual server as you need. (known as Port Mapping).

The Virtual Server is the server or server(s) behind NAT (on the LAN), for example, Web server or FTP server, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

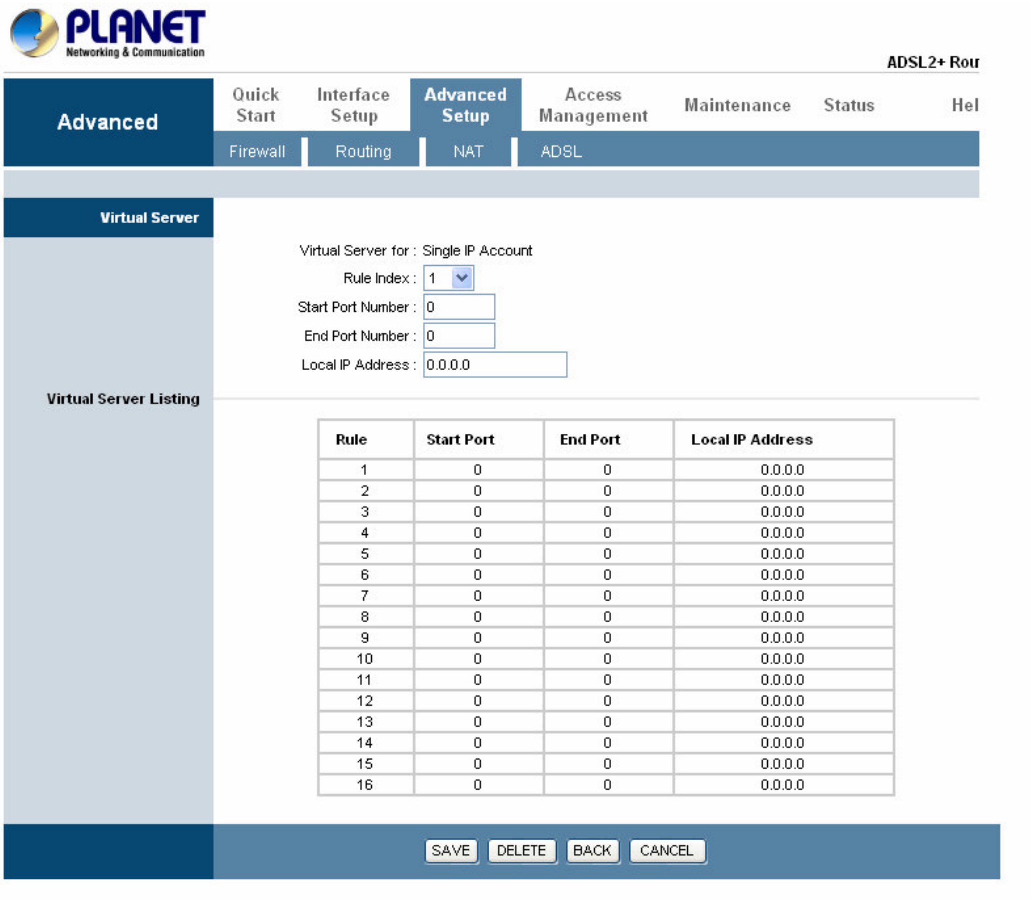
Rule Index: The Virtual server rule index for this VC. You can specify up to 10 rules. All the VCs with single IP will use the same Virtual Server rules.

Start & End port number: Enter the specific Start and End Port number you want to forward. If it is one port only, you can enter the End port number the same as Start port number. For example, set the FTP Virtual server, you can set the start and end port number to 21.

Local IP Address: Enter the IP Address for the Virtual Server in LAN side.

Virtual Server Listing: This is a listing of all virtual servers your 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.



Virtual Server for : Single IP Account
Rule Index : 1
Start Port Number : 0
End Port Number : 0
Local IP Address : 0.0.0.0

Rule	Start Port	End Port	Local IP Address
1	0	0	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0
13	0	0	0.0.0.0
14	0	0	0.0.0.0
15	0	0	0.0.0.0
16	0	0	0.0.0.0

■ 3.10.1.2 DMZ Setting

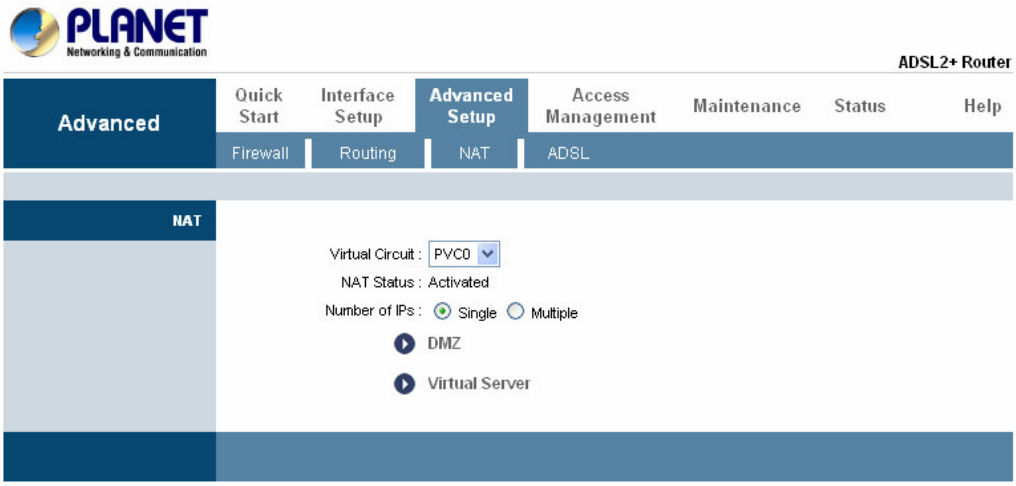
Go to **Advanced Setup ->NAT -> DMZ** to set DMZ parameters.

A ***DMZ*** (de-militarized zone) is a host between a private local network and the outside public network. It prevents outside users from getting direct access to s server that has company data. Users of the public network outside the company can access only the DMZ host.

DMZ: Toggle the DMZ function Enabled or Disabled.

DMZ Host IP Address: Enter the specified IP Address for DMZ host on the LAN side

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



Virtual Circuit : PVC0

NAT Status : Activated

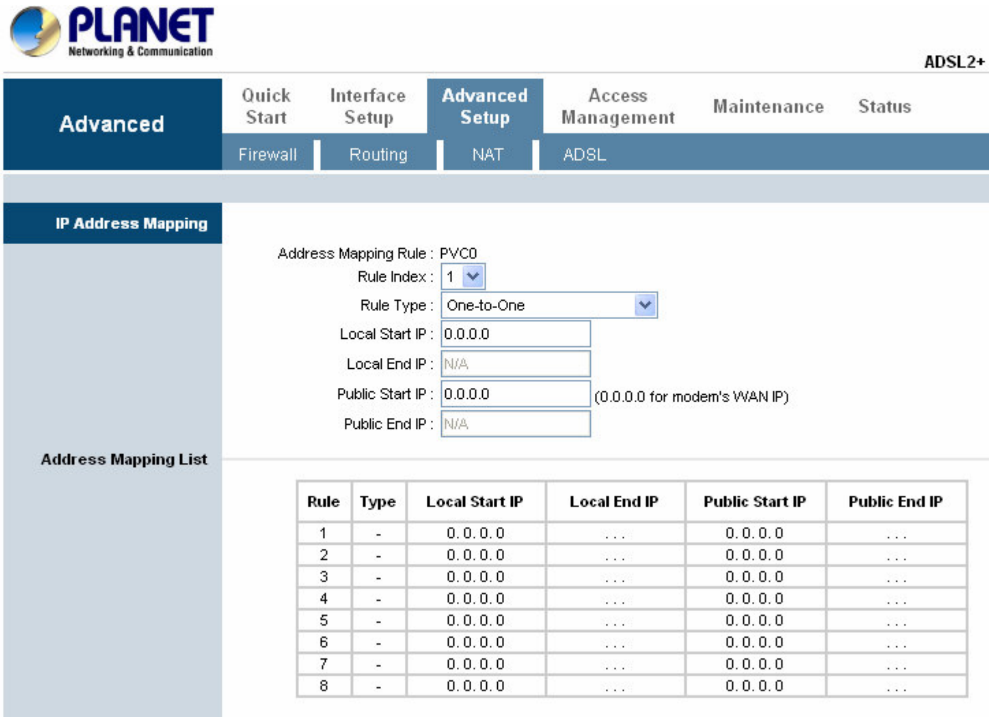
Number of IPs : ● Single ○ Multiple

DMZ

Virtual Server

■ 3.10.1.3 IP Address Mapping

Go to **Advanced Setup ->NAT -> Multiple ->IP Address mapping** to set IP Address mapping parameters.



Address Mapping Rule : PVC0

Rule Index : 1

Rule Type : One-to-One

Local Start IP : 0.0.0.0

Local End IP : N/A

Public Start IP : 0.0.0.0 (0.0.0.0 for modem's WAN IP)

Public End IP : N/A

Rule	Type	Local Start IP	Local End IP	Public Start IP	Public End IP
1	-	0. 0. 0. 0	. . .	0. 0. 0. 0	. . .
2	-	0. 0. 0. 0	. . .	0. 0. 0. 0	. . .
3	-	0. 0. 0. 0	. . .	0. 0. 0. 0	. . .
4	-	0. 0. 0. 0	. . .	0. 0. 0. 0	. . .
5	-	0. 0. 0. 0	. . .	0. 0. 0. 0	. . .
6	-	0. 0. 0. 0	. . .	0. 0. 0. 0	. . .
7	-	0. 0. 0. 0	. . .	0. 0. 0. 0	. . .
8	-	0. 0. 0. 0	. . .	0. 0. 0. 0	. . .

The IP Address Mapping is for those VCs that with multiple IPs. The IP Address Mapping rule is per-VC based. (only for Multiple IPs' VCs).

Rule Index: The Virtual server rule index for this VC. You can specify up to 10 rules. All the VCs with single IP will use the same Virtual Server rules.

Rule Type: There are 4 types of One-to-One, Many-to-One, Many-to-Many Overload, and Many-to Many No-Overload.

Local Start & End IP: Enter the local IP address you plan to map to. Local Start IP is the starting local IP address & Local End IP is the ending local IP address. If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.

Public Start & End IP: Enter the Public IP Address you want to do NAT. Public Start IP is the starting Public IP Address and Public End IP is the ending Public IP Address. If you have a Dynamic IP, enter 0.0.0.0 as the Public Start IP.

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.

3.10.2 ADSL Type Setting

Go to **Advanced Setup ->ADSL** to set different ADSL connection

Select this option to set ADSL Mode and ADSL Type information.

ADSL Mode: Select which mode your ADSL connection uses from the dropdown list.

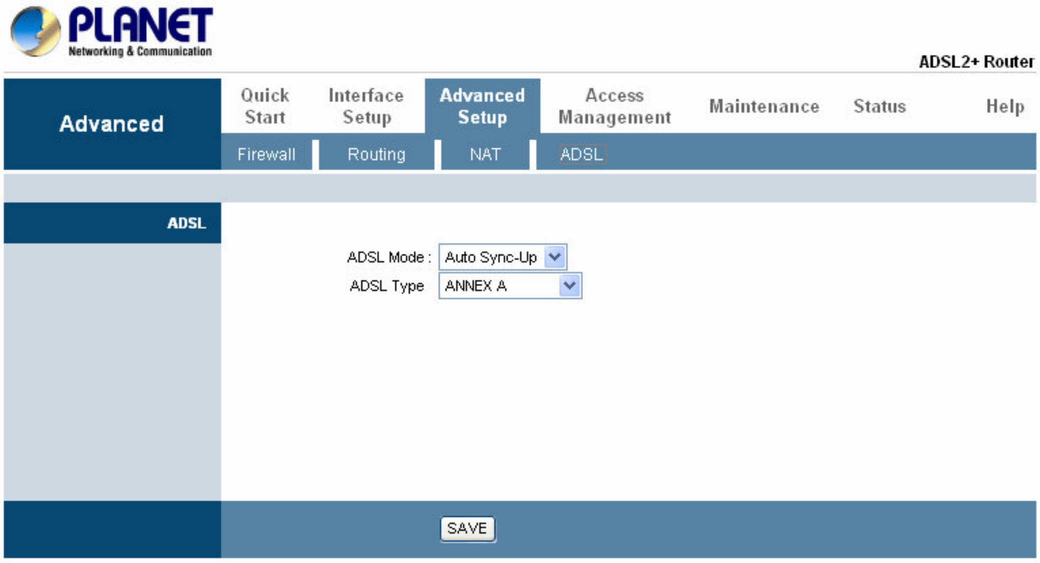
The option has Auto Sync-up, ADSL2+, ADSL2, G.DMT, T1.413, G.LITE

ADSL Type: Select the ADSL type you use from the dropdown list.

ANNEX A, ANNEX I, ANNEX A/L, ANNEX M, ANNEX A/I/J/L/M

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

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



ADSL Mode : Auto Sync-Up

ADSL Type ANNEX A

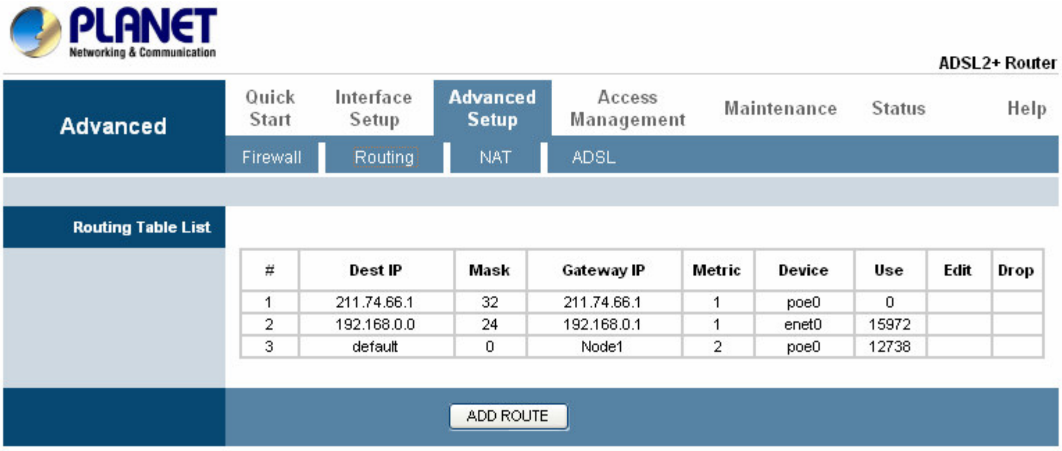
■ 3.10.3 Routing

■ 3.10.3.1 Static Routing

Go to **Advance Setup-> Routing** to see the Routing Table

Routing Table List

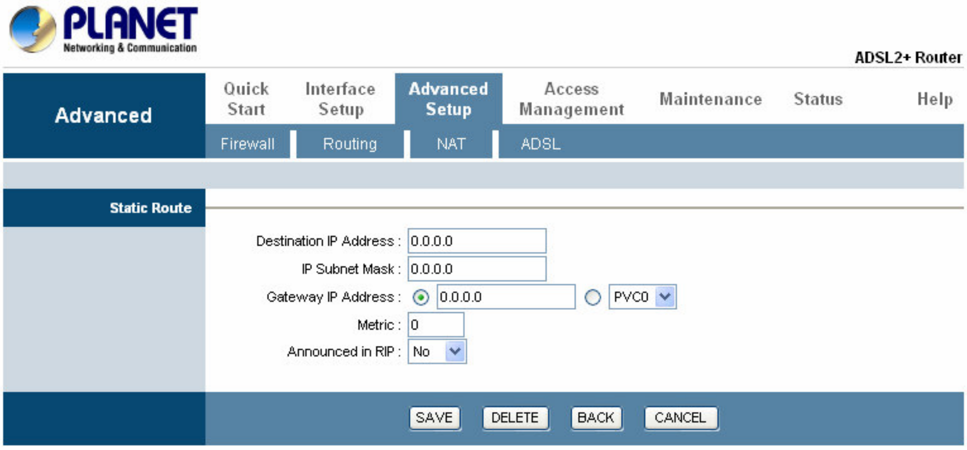
This table lists IP address of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Gateway IP to identify the first Internet router it should contact to route the data most efficiently. Select this option will list the routing table information. You can press **ADD ROUTE** to edit the static route. (As below screen)



#	Dest IP	Mask	Gateway IP	Metric	Device	Use	Edit	Drop
1	211.74.66.1	32	211.74.66.1	1	poe0	0		
2	192.168.0.0	24	192.168.0.1	1	enet0	15972		
3	default	0	Node1	2	poe0	12738		

[Static Route]

Select this option to set Static Routing information.



Destination IP Address : 0.0.0.0

IP Subnet Mask : 0.0.0.0

Gateway IP Address : ● 0.0.0.0 ○ PVC0

Metric : 0

Announced in RIP : No

Destination IP Address: This parameter specifies the IP network address of the final destination of packets routed by this rule.

IP Subnet Mask: Enter the subnet mask for this destination.

Gateway IP Address: Enter the IP address of the gateway. A **gateway** does the actual forwarding of the packets. Enter the gateway's IP address in the field or select which PVC you wish to act as a gateway.

The gateway is an immediate neighbor of your ADSL Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Router; over Internet (WAN), the gateway must be the IP address of one of the remote nodes.

Metric: Metric represents the "cost" of transmission for routing purposes. IP Routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not to be precise, but it must between 1 and 15. In practice, 2 or 3 is usually a good number.

Announced in RIP: This parameter determines if the ADSL router includes the router to this remote node in its RIP broadcasts. If you choose **Yes**, the router in this remote node will be propagated to other hosts through RIP broadcasts. If you choose **No**, this route is kept private and is not included in the 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.

■ 3.10.3.2 Dynamic Routing

Go to **Interface Setup -> LAN** to select the Dynamic Route from **RIP1**, **RIP2-B**, and **RIP2-M**.

Explaining RIP Setup

Routing Information Protocol (RIP) allows a router to exchange routing information with other routers. The RIP Direction field controls how RIP packets are allowed to enter and leave the router. Selecting **Both** means the router will broadcast its routing table and incorporate the RIP information that it receives. Selecting **In Only** means the router will only accept RIP packets received, not send RIP packets. Selecting **Out Only** means the router will only send RIP packets, not accept any RIP packets received. Selecting **None** means the router will not send any RIP packets nor will it accept any RIP packets received.

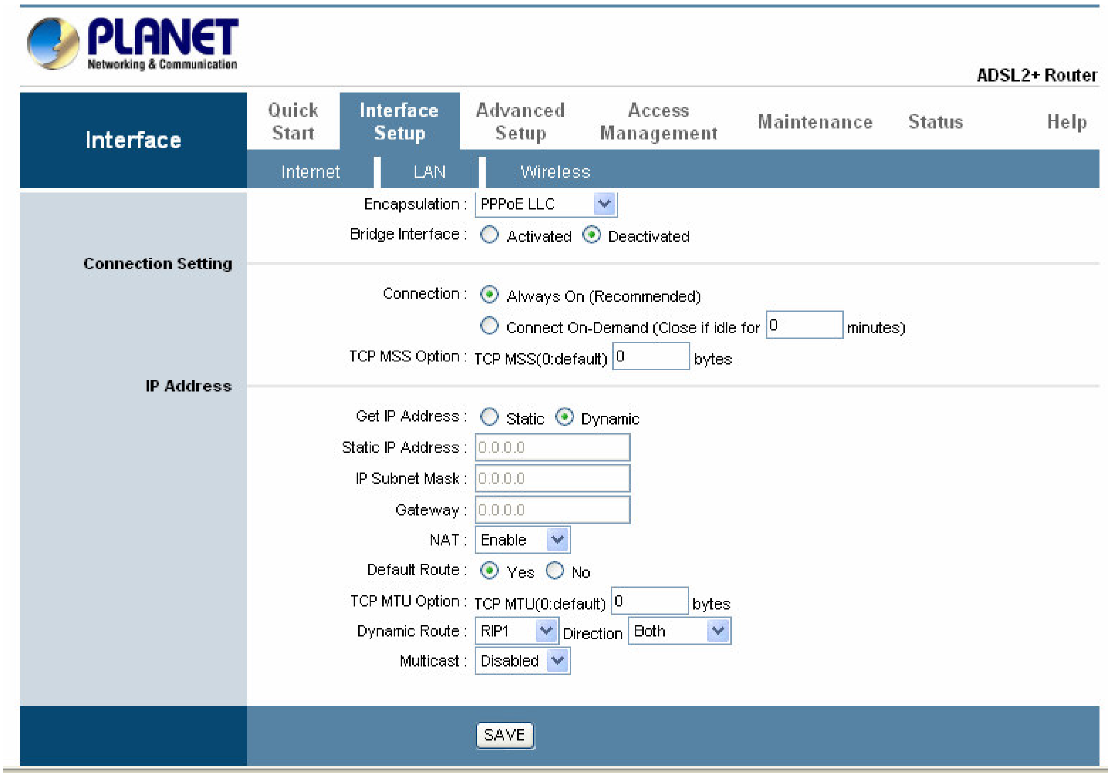
The Dynamic Route field controls the format and the broadcasting method of RIP packets that the router sends. It recognizes both formats when receiving packets.

RIP-1 is universally supported, but **RIP-2** carries more information. **RIP-1** is adequate for most networks. Only consider **RIP-2** if your network has unusual topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in **RIP-2** format. **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

Direction: Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.

Multicast: IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL router supports both **IGMP-v1** and **IGMP-v2.** Select **None** to disable it. Please refer to Internet→ Multicast. The only difference is the interface.

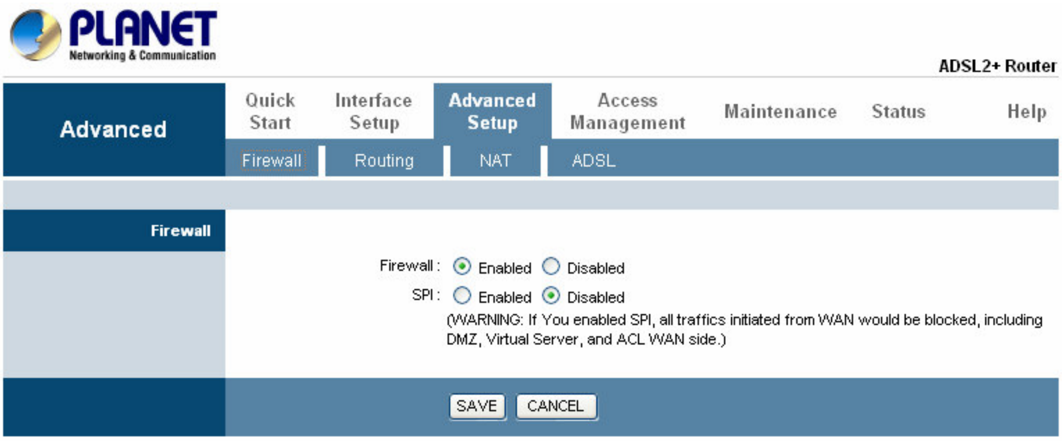


Encapsulation : PPPoE LLC
Bridge Interface : ○ Activated ● Deactivated
Connection : ● Always On (Recommended)
○ Connect On-Demand (Close if idle for 0 minutes)
TCP MSS Option : TCP MSS(0:default) 0 bytes
Get IP Address : ○ Static ● Dynamic
Static IP Address : 0.0.0.0
IP Subnet Mask : 0.0.0.0
Gateway : 0.0.0.0
NAT : Enable
Default Route : ● Yes ○ No
TCP MTU Option : TCP MTU(0:default) 0 bytes
Dynamic Route : RIP1 Direction Both
Multicast : Disabled

■ 3.10.4 Firewall

Go to **Advance Setup-> Firewall** to set firewall rule.

User can enable or disable firewall feature of the ADSL router in the page.



Firewall : ● Enabled ○ Disabled

SPI : ○ Enabled ● Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

Firewall: Select this option can automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

SPI: Select this option to Enabled or Disabled the SPI feature.

(NOTE: If you enable SPI, all traffics initiate from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side)

Appendix A: Glossary

Address mask

A bit mask select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address
and one or more bits of the local portion. Sometimes it called subnet mask.

AAL5

ATM Adaptation Layer - This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

ADSL

Asymmetric digital subscriber line

ATM

Asynchronous Transfer Mode - A cell-based data transfer technique in which channel demand determines packet allocation. ATM offers fast packet technology,
real time, and demand led switching for efficient use of network resources.

AWG

American Wire Gauge - The measurement of thickness of a wire

Bridge

A device connects two or more physical networks and forward packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are repeaters which simply forward electrical signals from one cable to the other and full-fledged routers which make routing decisions based on several criteria.

Broadband

Characteristic of any network multiplexes independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another. Broadcast a packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

CO

Central Office. Refers to equipment located at a Telco or service provider's office.

CPE

Customer Premises Equipment located in a user's premises

DHCP (Dynamic Host Configuration Protocol)

DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DHCP eliminates having to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as Routers.

DMT

Discrete Multi-Tone frequency signal modulation

Downstream rate

The line rate for return messages or data transfers from the network machine to the user's premises machine.

DSLAM

Digital Subscriber Line Access Multiplex

Dynamic IP Addresses

A dynamic IP address is an IP address that is automatically assigned to a client station (computer, printer, etc.) in a TCP/IP network. Dynamic IP addresses are typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as the Router. A dynamic IP address may change every time your computer connects to the network.

Encapsulation

The technique layer protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), and followed by the application protocol data.

Ethernet

One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps.

FTP

File Transfer Protocol. The Internet protocol (and program) transfer files between hosts.

Hop count

A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.

HTML

Hypertext Markup Language - The page-coding language for the World Wide Web.

HTML browser

A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

http

Hypertext Transfer Protocol - The protocol carry world-wide-web (www) traffic between a www browser computer and the www server being accessed.

ICMP

Internet Control Message Protocol - The protocol handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

Internet address

An IP address is assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where x is an eight- bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

Internet Protocol (IP)

The network layer protocol for the Internet protocol suite

IP address

The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

ISP

Internet service provider - A company allows home and corporate users to connect to the Internet.

MAC

Media Access Control Layer - A sub-layer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

MIB

Management Information Base - A collection of objects can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

NAT

Network Address Translation - A proposal for IP address reuse, where the local IP address is mapped to a globally unique address.

NVT

Network Virtual Terminal

PAP

Password Authentication Protocol

PORT

The abstraction used in Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

POTS

Plain Old Telephone Service - This is the term describe basic telephone service.

PPP

Point-to-Point-Protocol - The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoE

PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Remote server

A network computer allows a user to log on to the network from a distant location.

RFC

Request for Comments - Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFC can be found at www.ietf.org.

Route

The path that network traffic takes from its source to its destination. The route a datagram may follow can include many gateways and many physical networks.
In the Internet, each datagram is routed separately.

Router

A system is responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics".

Routing Table

Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

Routing Information Protocol

Routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

SNMP

Simple Network Management Protocol - The network management protocol of choice for TCP/IP-based Internet.

SOCKET

(1) The Berkeley UNIX mechanism for creating a virtual connection between processes.

(2) IBM term for software interfaces that allow two UNIX application programs to talk via TCP/IP protocols.

Spanning-Tree Bridge Protocol (STP)

Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment. When three or more LAN's segments are connected via bridges, a loop can occur. Because of a bridge forwards all packets that are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

Spoofing

A method of fooling network end stations into believing that keep alive signals have come from and returned to the host. Polls are received and returned locally at either end

Static IP Address

A static IP address is an IP address permanently assigned to computer in a TCP/IP network. Static IP addresses are usually assigned to networked devices that are consistently accessed by multiple users, such as Server PCs, or printers. If you are using your Router to share your cable or DSL Internet connection, contact your ISP to see if they have assigned your home a static IP address. You will need that address during your Router's configuration.

Subnet
For routing purposes, IP networks can be divided into logical subnets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

TCP
Transmission Control Protocol - The major transport protocol in the Internet suite of protocols provides reliable, connection-oriented full-duplex streams.

TFTP
Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often boot diskless workstations and other network devices such as routers over a network (typically a LAN).

Telnet
The virtual terminal protocol in the Internet suite of protocols - Allows users of one host to log into a remote host and act as normal terminal users of that host.

Transparent bridging
The intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses, and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

UDP
User Datagram Protocol - A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagram without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first setting up a connection would take more time than sending the data.

UNI signaling
User Network Interface signaling for ATM communications.

Virtual Connection (VC)
A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In

reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

WAN

Wide area network - A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider).