

***C54APRA for Annex A***  
***C54APRB for Annex B***  
***802.11g Wireless ADSL Router***  
***User's Guide***

---

---

(May 2004)

---

.....

## TABLE OF CONTENTS

---

About This User's Guide .....	v
Before You Start .....	v
Installation Requirements .....	v
Introduction .....	1
Router Description and Operation.....	1
Standards Compatibility and Compliance .....	3
Front Panel Display .....	4
Rear Panel Connections .....	5
Hardware Installation.....	6
Choosing an Optimal Location for Wireless Operation .....	6
Network Connections.....	7
Power on Router .....	8
Factory Reset Button .....	8
Basic Router Configuration.....	9
Configuring IP Settings on Your Computer .....	9
Access the Configuration Manager .....	15
Using the Web Manager .....	16
Using the Setup Wizard .....	16
Basic Wireless LAN Setup .....	21
Configure WAN Connection.....	22
PPPoE and PPPoA Connection for WAN .....	24
Bridged Connection for WAN .....	25
Static IP Address for WAN .....	27
LAN IP Settings .....	28
DHCP Server Settings for the LAN .....	29
Use the Router for DHCP.....	29
Disable the DHCP Server .....	30
DNS Server Settings.....	30
Save New Settings .....	31
Advanced Configuration/Network Management .....	32
UPnP .....	33
Virtual Server .....	33
Filters .....	36
Routing .....	38

---

DMZ.....	38
Firewall.....	39
RIP.....	40
PPP Settings.....	41
ADSL Modulation Settings.....	41
ATM VC.....	42
Advanced Wireless LAN Configuration.....	43
Wireless Management.....	43
Wireless Performance.....	44
Wireless Security.....	45
Tools and Utilities.....	48
Change System Password.....	48
Save Configuration File to PC.....	48
Load Saved Configuration Files.....	49
Restore Factory Default Settings.....	49
Firmware Upgrade.....	50
Save Router Configuration Settings.....	50
Router Status Information.....	52
Device Information Display.....	52
Multiple Virtual Connections.....	53
Technical Specifications.....	55
IP Address Setup.....	57
IP Concepts.....	59
Microfilters and Splitters.....	62
Licensing Information.....	64
Availability of source code.....	64
GNU GENERAL PUBLIC LICENSE.....	65



## About This User's Guide

This user's guide provides instructions on how to install the C54APRA/C54APRB Wireless ADSL Router and use it to provide Internet access for an Ethernet or 802.11g/802.11b wireless LAN.

If you are using a computer with a functioning Ethernet port, the quickest and easiest way to set up the C54APRA/C54APRB is follow the instructions provided in the **Hard Installation Guide**.

## Before You Start

Please read and make sure you understand all the prerequisites for proper installation of your new Router. Have all the necessary information and equipment on hand before beginning the installation.

### Installation Overview

The procedure to install the Router can be described in general terms in the following steps:

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment.
2. Install the hardware, connect the cables to the device and connect the power adapter.
3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based software built into the Router.
4. Use the web-based management software to configure the device to suit the requirements of your ADSL service and wireless LAN.

## Installation Requirements

In order to establish a connection to the Internet it will be necessary to provide information to the Router that will be stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required. You can print out the two pages below and use the tables to list this information. This way you have a hard copy of all the information needed to setup the Router. If it is necessary to reconfigure the device, all the necessary information can be easily accessed. Be sure to keep this information safe and private.

### Low Pass Filters

Since ADSL and telephone services share the same copper wiring to carry their respective signals, a filtering mechanism may be necessary to avoid mutual interference. A low pass filter device can be installed for each telephone that shares the line with the ADSL line. These filters are easy to install passive devices that connect to the ADSL device and/or telephone using standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

### Operating Systems

The C54APRA/C54APRB uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, and Windows XP.

### Web Browser

Any common web browser can be used to configure the Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Opera, Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

## **Ethernet Port (NIC Adapter)**

Any computer that uses the Router must be able to connect to it through the Ethernet port on the Router. This connection is an Ethernet connection and therefore requires that your computer be equipped with an Ethernet port as well. Most notebook computers are now sold with an Ethernet port already installed. Likewise, most fully assembled desktop computers come with an Ethernet NIC adapter as standard equipment. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the Router. If you must install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

## **Additional Software**

It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using the device a simple bridge. For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device, not in the Router itself.

If your ADSL service is delivered through a PPPoE or PPPoA connection, the information needed to establish and maintain the Internet connection can be stored in the Router. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

All connections to the Internet require a unique global IP address. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN side of the bridge, such as a PC, a server, a gateway device such as a router or similar firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

## Wireless LAN Configuration

All the 802.11g wireless LAN settings are configured on a single page using the web-based manager. For basic wireless communication, you need to decide what channel to use and what SSID to assign. These two settings must be the same for any wireless workstations or other wireless access points that communicate with the C54APRA/C54APRB through the wireless interface. The IEEE 802.11g wireless LAN standard is fully compatible with IEEE 802.11b devices.

Security for wireless communication can be accomplished using 64, 128 Or 256-bit WEP.

### ***Information you will need about your C54APRA/C54APRB ADSL Router:***

<b>Username</b>	This is the Username needed access the Router's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Router is <b>admin</b> . The user cannot change this.	Record info here
<b>Password</b>	This is the Password you will be prompted to enter when you access the Router's management interface. The default Password is <b>admin</b> . The user may change this.	
<b>LAN IP addresses for the C54APRA/C54APRB</b>	This is the IP address you will enter into the Address field of your web browser to access the Router's management interface using a web browser. The management interface is referred to as the web manager in the manual. The default LAN IP address 10.0.0.1 may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.	
<b>LAN Subnet Mask for the C54APRA/C54APRB</b>	This is the subnet mask used by the C54APRA/C54APRB, and will be used throughout your LAN. The default subnet mask is <b>255.0.0.0</b> . This can be changed later.	

### ***Information you will need about your LAN or computer:***

<b>Ethernet NIC</b>	If your computer has an Ethernet NIC, you can connect the C54APRA/C54APRB to the computer's Ethernet port. You can also use any Ethernet port on the C54APRA/C54APRB to connect to other Ethernet devices, such as a Wireless Access Point.	Record info here
<b>DHCP Client status</b>	Your C54APRA/C54APRB ADSL Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the C54APRA/C54APRB will assign are from 10.0.0.2 to 10.0.0.254. Your computer (or computers) needs to be configured to Obtain an IP address automatically (that is, they need to be configured as DHCP clients.)	

### ***Information you will need from your ADSL service provider:***

<b>Username</b>	This is the Username used to log on to your ADSL service provider's network. It is commonly in the form – user@isp.com. Your ADSL service provider uses this to identify your account.	Record info here
<b>Password</b>	This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network.	

	This is used to verify the identity of your account.	
<b>Connection Protocol</b>	This is the method your ADSL service provider uses to send and receive data between the Internet and your computer. Your Router supports the following connection protocols: PPPoE, PPPoA, Dynamic IP, Bridge, and Static IP.	
<b>Encapsulation Type</b>	Referred to as the Connection Type in the web manager, this is the method used to encapsulate data packets for transport across the network. The type used depends on the connection protocol you are using. The available options are: PPPoA VC-Mux, PPPoA LLC, PPPoE LLC, Bridged IP VC-Mux, Bridged IP LLC, IPoA, Routed IP VC-Mux and Routed IP LLC.	
<b>Modulation Type</b>	The default DSL modulation (MMODE) used for the Router automatically detects all types of ADSL modulation. If you are instructed to specify the modulation type used for the Router, you have three alternatives: G.LITE, G.DMT and T1.413	
<b>Security Protocol</b>	This is the method your ADSL service provider will use to verify your Username and Password when you log on to their network. Your Router supports the PAP and CHAP protocols.	
<b>VPI</b>	This is the Virtual Path Identifier (VPI). It is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your ADSL service provider's network and your computer.	
<b>VCI</b>	This is the Virtual Channel Identifier (VCI). It is used in conjunction with the VPI to identify the data path between your ADSL service provider's network and your computer.	

It is recommended that you collect and record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your C54APRA/C54APRB Wireless ADSL Router.



**Note**

*The Modem may be reset to its factory default settings by performing a Restore settings operation within the management interface, see **Error! Reference source not found.** for more information. If you cannot gain access to the management interface, you may opt to use the Reset button on the rear panel of the device (see Factory Reset Button below).*



# Introduction

This section provides a brief description of the Router, its associated technologies and a list of Router features.

## Router Description and Operation

The C54APRA/C54APRB Router is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or 802.11g/802.11b wireless network. The Router combines high-speed ADSL Internet connection, IP routing for the LAN and wireless connectivity in one package.

The Router is easy to install and use. The C54APRA/C54APRB connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary twisted-pair telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address.

The Router can be used for IP packet routing on your private LAN or over the Internet. Cost saving features of the Router such as NAT (Network Address Translator) and DHCP (Dynamic Host Configuration Protocol) improve administration efficiency and improve security for your private network. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

### ADSL

Asymmetric Digital Subscriber Line (ADSL) is an access technology that utilizes ordinary copper telephone lines to enable broadband high-speed digital data transmission and interactive multimedia applications for business and residential customers.

ADSL greatly increases the signal carrying capacity of copper telephone lines without interfering with regular telephone services. For the ADSL user, this means faster downloads and more reliable connectivity. ADSL devices make it possible to enjoy benefits such as high-speed Internet access without experiencing any loss of quality or disruption of voice/fax telephone capabilities.

ADSL provides a dedicated service over a single telephone line operating at speeds of up to 8 Mbps downstream and up to 640 Kbps upstream, depending on local telephone line conditions. A secure point-to-point connection is established between the user and the central office of the service provider.

### 802.11g Wireless

The embedded 802.11g wireless access point provides Internet access and connectivity to the Ethernet. IEEE 802.11g is fully compatible with IEEE 802.11b wireless devices. The 802.11g standard supports data transfer rates of up to 54 Mbps. The Router supports common security protocols used for wireless LAN including WEP (Wireless Encryption Protocol or Wired Equivalent Privacy) encryption, 802.1x and WPA.

## Router Features

The C54APRA/C54APRB ADSL Router utilizes the latest ADSL enhancements to provide a reliable Internet portal suitable for most small to medium sized offices. C54APRA/C54APRB advantages include:

- **802.11g Wireless Access Point** - The built-in 802.11g wireless access point connects 802.11g and 802.11b wireless devices to the Internet and the Ethernet.
- **PPP (Point-to-Point Protocol) Security** - The C54APRA/C54APRB ADSL Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections.
- **DHCP Support** - Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT)** - For small office environments, the C54APRA/C54APRB allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user.  
  
NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.
- **TCP/IP (Transfer Control Protocol/Internet Protocol)** - The C54APRA/C54APRB supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.
- **RIP-1/RIP-2** - The C54APRA/C54APRB supports both RIP-1 and RIP-2 exchanges with other routers. Using both versions lets the Router to communicate with all RIP enabled devices.
- **Static Routing** - This allows you to select a data path to a particular network destination that will remain in the routing table and never "age out". If you wish to define a specific route that will always be used for data traffic from your LAN to a specific destination within your LAN (for example to another router or a server) or outside your network (to a ISP defined default gateway for instance).
- **Default Routing** - This allows you to choose a default path for incoming data packets for which the destination address is unknown. This is particularly useful when if the Router functions as the sole connection to the Internet.
- **ATM (Asynchronous Transfer Mode)** - The C54APRA/C54APRB supports Bridged Ethernet over ATM (RFC1483), IP over ATM (RFC1577) and PPP over ATM (RFC 2364).
- **Precise ATM Traffic Shaping** - Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.
- **G.hs (Auto-handshake)** - This allows the Router to automatically choose either the G.lite or G.dmt ADSL connection standards.
- **High Performance** - Very high rates of data transfer are possible with the Router. Up to eight Mbps downstream bit rate using the G.dmt.
- **Full Network Management** - The C54APRA/C54APRB incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via an RS-232 or Telnet connection.
- **Telnet Connection** - The Telnet enables a network manager to access the Router's management software remotely.
- **Easy Installation** - The C54APRA/C54APRB uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router.

## Standards Compatibility and Compliance

The C54APRA/C54APRB complies with or is compatible with the following standards as recognized by their respective agencies.

- ITU G.992.2 (G.lite "Splitterless ADSL") compliant
- ITU-T Rec. I.361 compliant
- RFC 791 Internet Protocol compliant
- RFC 792 UDP compliant
- RFC 826 Address Resolution Protocol compliant (ARP) compliant
- RFC 1058 Routing Information Protocol (RIP) compliant
- RFC 1213 MIB II for IP compliant
- RFC 1334 PPP Authentication Protocol compliant
- RFC 1389 Routing Information Protocol 2 (RIP2) compliant
- RFC 1483 IP over AAL5/ Bridged Ethernet over AAL5 compliant
- RFC 1557 Classical IP over ATM (IPoA) compliant
- RFC 1661 Point to Point Protocol (PPP) compliant
- RFC 1877 Automatic IP assignment compliant
- RFC 1994 Challenge Handshake Authentication Protocol compliant
- Supports RFC 2131 and RFC 2132 DHCP functions including: automatic assignment of IP address, use of subnet mask and default gateway and provision of DNS server address for all hosts
- RFC 2364 PPP over ATM compliant (PPPoA) compliant
- RFC 2516 PPP over Ethernet compliant (PPPoE) compliant
- RFC 2684 Bridged/Routed Ethernet over ATM compliant
- IEEE 802.3 compliant
- IEEE 802.3u compliant
- IEEE 802.1d compliant
- IEEE 802.11g compliant
- IEEE 802.3x compliant
- Embedded web server support
- Supports Dynamic Learning
- Supports Static Routing
- Supports NAT for up to 4096 connections
- Supports DHCP for up to 253 hot connections
- Supports IGMP
- Supports ATM Forum UNI 3.1/4.0
- Supports ATM VCC (Virtual Channel Circuit) for up to eight sessions
- Supports TELNET and TFTP
- Supports back pressure for half-duplex

## Packing List

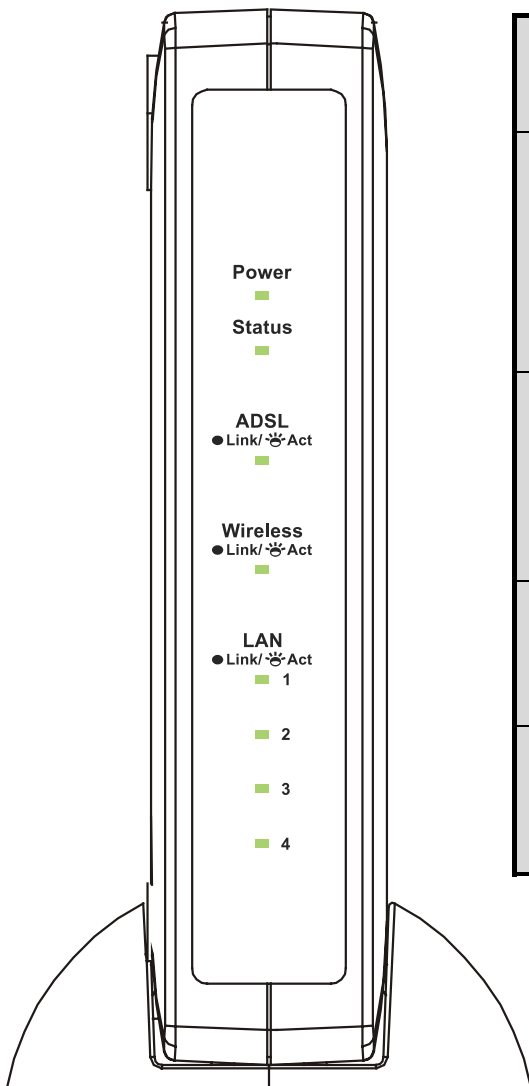
Open the shipping carton and carefully remove all items. In addition to this User's Guide, ascertain that you have:

- One C54APRA/C54APRB ADSL Router
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- One AC power adapter suitable for your electric service
- An Installation CD-ROM containing the USB drivers and this User's Guide
- One Quick Installation Guide

## Front Panel Display

Place the Router in a location that permits an easy view of the LED indicators on the front panel.

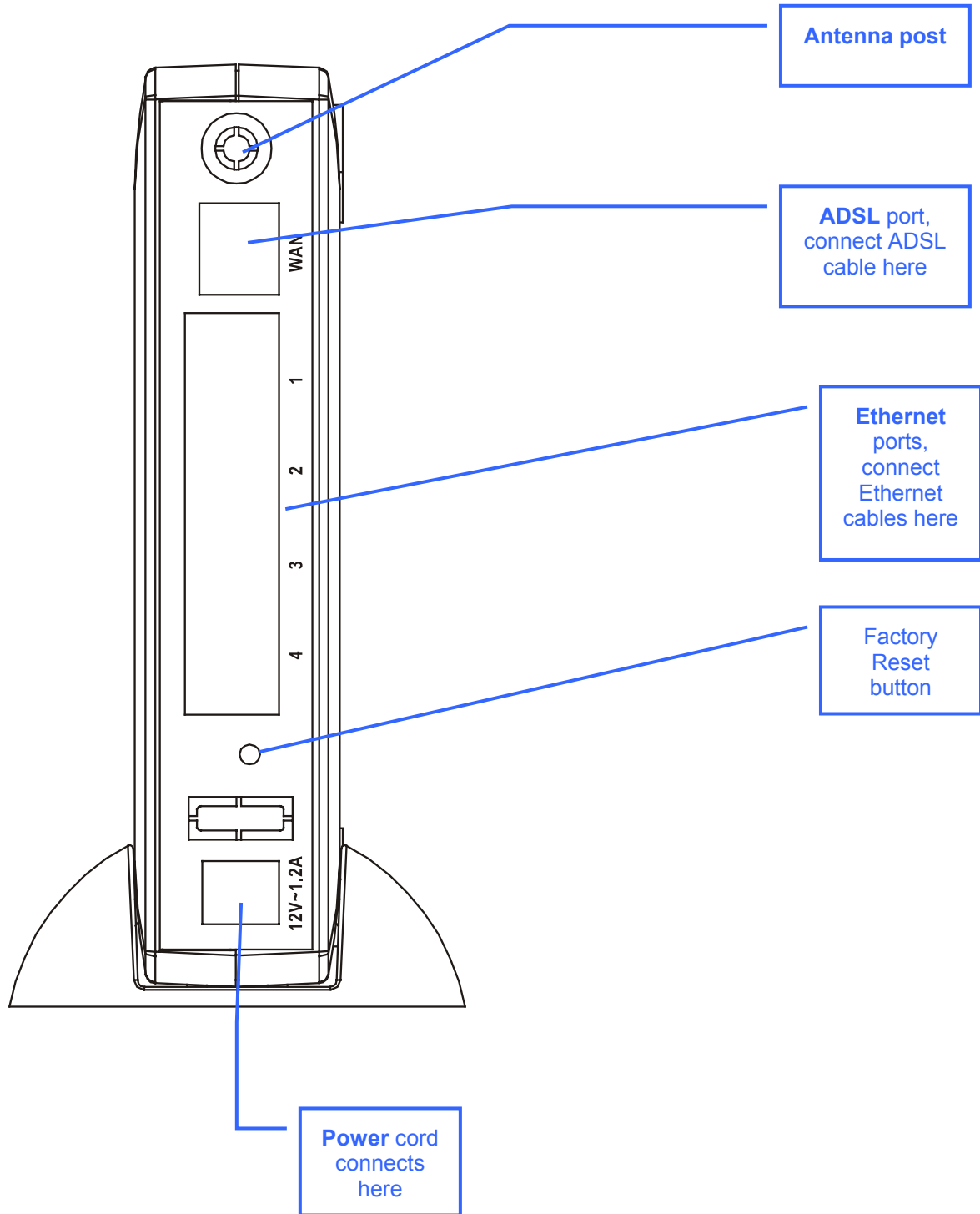
The LED indicators on the front panel include the **Power**, **Status**, **ADSL Link/Act**, **Ethernet Link/Act**, and **WLAN Link/Act** indicators. The ADSL, Ethernet, and WLAN indicators monitor link status and activity (Link/Act).



<b>Power</b>	Steady green light indicates the unit is powered on. When the device is powered off this remains dark.
<b>Status</b>	Lights steady green during power on self-test (POST). Once the connection status has been settled, the light will blink green. If the indicator lights steady green after the POST, the system has failed and the device should be rebooted.
<b>ADSL: Link/Act</b>	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking green light indicates activity on the WAN (ADSL) interface.
<b>Ethernet: Link/Act</b>	A solid green light indicates a valid link on startup. This light will blink when there is activity currently passing through the Ethernet port.
<b>Wireless: Link/Act</b>	Steady green light indicates a wireless connection. A blinking green light indicates activity on the WLAN interface.

## Rear Panel Connections

All cable connections to the Router are made at the rear panel. Connect the power adapter here to power on the Router. Use the Reset button to restore the settings to the factory default values (see Factory Reset Button in the next chapter for instructions on using the reset button).



## Hardware Installation

The C54APRA/C54APRB maintains three separate interfaces, an Ethernet, a wireless and an ADSL interface. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

## Choosing an Optimal Location for Wireless Operation

Many environmental factors can affect the effective wireless function of the C54APRA/C54APRB. If this is your first time setting up a wireless network device, read and consider the points listed below.

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Wireless LAN lets you access your network from anywhere you want. However, the number of walls, ceilings, or other objects that the wireless signals must pass through can limit signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. To range and signal strength, use these basic guidelines:

- 1. Keep the number of walls and ceilings to a minimum:**  
The signal emitted from Wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range Wireless LAN devices from 1 to 30M. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.
- 2. Consider the direct line between access points and workstations:** A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it is over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90° angle) a wall or ceiling for better reception.
- 3. Building Materials make a difference:** Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signal can pass through drywall or open doorways, avoid positioning them so that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.
- 4. Position the antennas for best reception.** Play around with the antenna position to see if signal strength improves. Some adapters or access points allow the user to judge the strength of the signal.
- 5. Keep your product away (at least 1-2 meters) from electrical devices:**  
Position wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

## Network Connections

Wired network connections are provided through the ADSL port and Ethernet ports on the back of the Router. See the Rear Panel diagram above and the illustrations below for examples.

### Connect ADSL Line

Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

### Connect Router to Ethernet

The Router may be connected to a single computer or Ethernet device through the 10BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port.

Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch.

The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

### Hub or Switch to Router Connection

Connect the Router to an uplink port (MDI-II) on an Ethernet hub or switch with a straight-through cable. If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.

### Computer to Router Connection

You can connect the Router directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a PC using the Ethernet cable provided.

## Power on Router



**CAUTION:** The Router must be used with the power adapter included with the device.

To power on the Router:

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a suitable nearby power source.
2. You should see the Power LED indicator light up and remain lit. The Status LED should light solid green and begin to blink after a few seconds.
3. If the Ethernet port is connected to a working device, check the Ethernet Link/Act LED indicators to make sure the connection is valid. The Router will attempt to establish the ADSL connection, if the ADSL line is connected and the Router is properly configured this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the Router can establish a connection.

## Factory Reset Button

The Router may be reset to the original factory default settings by depressing the reset button for a few seconds while the device is powered on. Use a ballpoint or paperclip to gently push down the reset button. Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The factory default IP address of the Router is 10.0.0.1 and the subnet mask is 255.0.0.0, the default management Username is **admin** and the default Password is **admin**.



## Basic Router Configuration

The first time you setup the Router it is recommended that you configure the WAN connection using a single computer making sure that both the computer and the Router are not connected to the LAN. Once the WAN connection is functioning properly, you may continue to make changes to Router configuration including IP settings and DHCP setup. This chapter is concerned with using your computer to configure the WAN connection. The following chapter describes the various menus used to configure and monitor the Router including how to change IP settings and DHCP server setup.

### Wan Configuration Summary

1. **Connect to the Router** To configure the WAN connection used by the Router it is first necessary to communicate with the Router through its management interface, which is HTML-based and can be accessed using a web browser. To access the management software your computer must be able to “see” the Router. Your computer can see the Router if it is in the same “neighborhood” or subnet as the Router. This is accomplished by making sure your computer has IP settings that place it in the same subnet as the Router. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the Router. The next section describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client.
2. **Configure the WAN Connection** Once you are able to access the configuration software you can proceed to change the settings required to establish the ADSL connection and connect to the service provider’s network. There are different methods used to establish the connection to the service provider’s network and ultimately to the Internet. You should know what Encapsulation and connection type you are required to use for your ADSL service. It is also possible that you must change the PVC settings used for the ADSL connection. Your service provider should provide all the information you need to configure the WAN connection.

## Configuring IP Settings on Your Computer

In order to configure your system to receive IP settings from the Router it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. If you are using Windows XP the TCP/IP is enabled by default for standard installations. Below is an illustrated example of how to configure a Windows XP system to automatically obtain IP settings from the Router. Following this example is a step-by-step description of the procedures used on the other Windows operating systems to first check if the TCP/IP protocol has been installed; if it is not, instructions are provided for installing it. Once the protocol has been installed you can configure the system to receive IP settings from the Router.

For computers running non-Windows operating systems, follow the instructions for your OS that configure the system to receive an IP address from the Router, that is, configure the system to be a DHCP client.

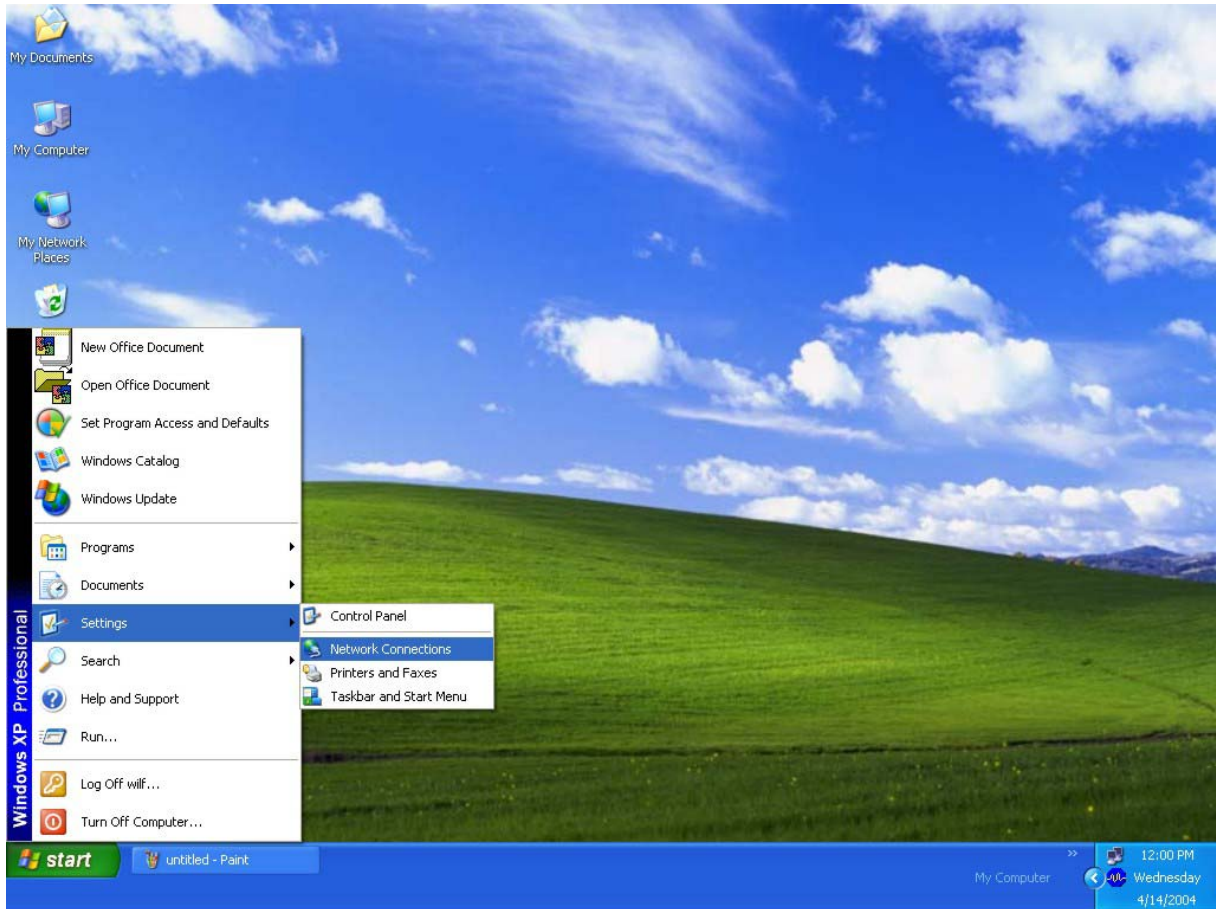


*If you are using this Router to provide Internet access for more than one computer, you can use these instructions later to change the IP settings for the other computers. However, you cannot use the same IP address since every computer must have its own IP address that is unique on the local network.*

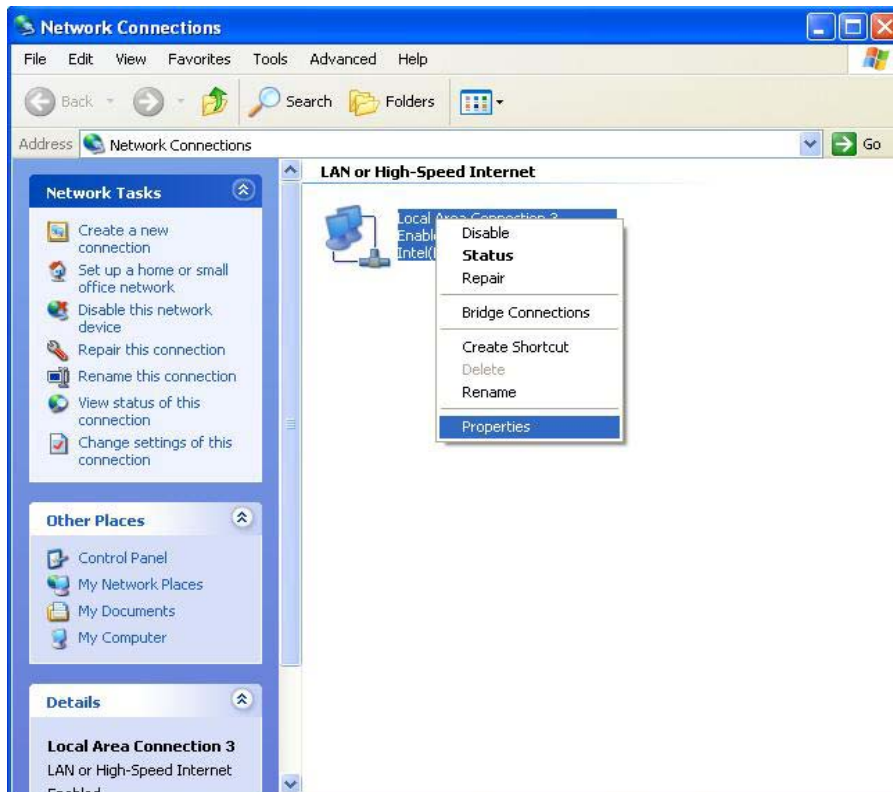
## Configure Windows XP for DHCP

Use the following steps to configure a computer running Windows XP to be a DHCP client.

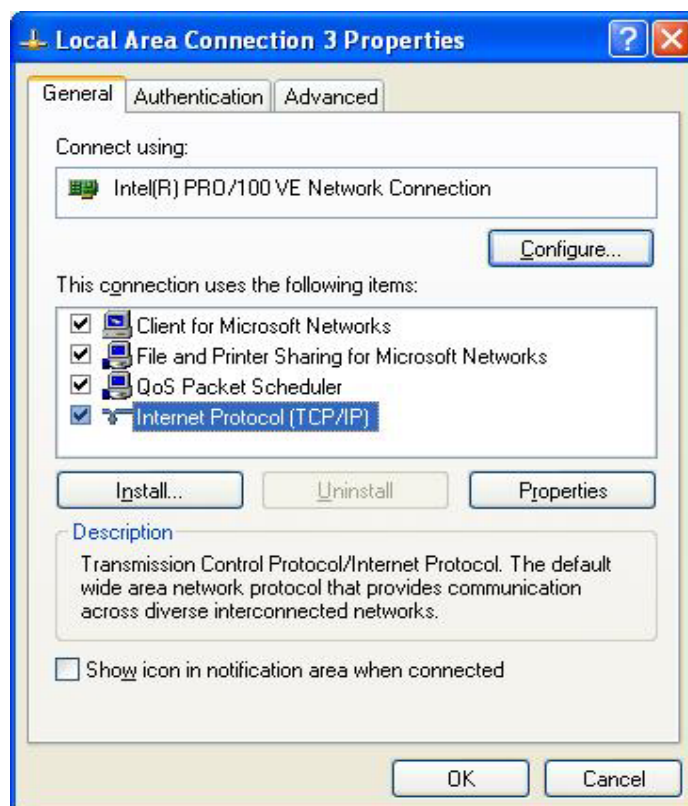
1. From the **Start** menu on your desktop, go to **Settings**, then click on **Network Connections**.



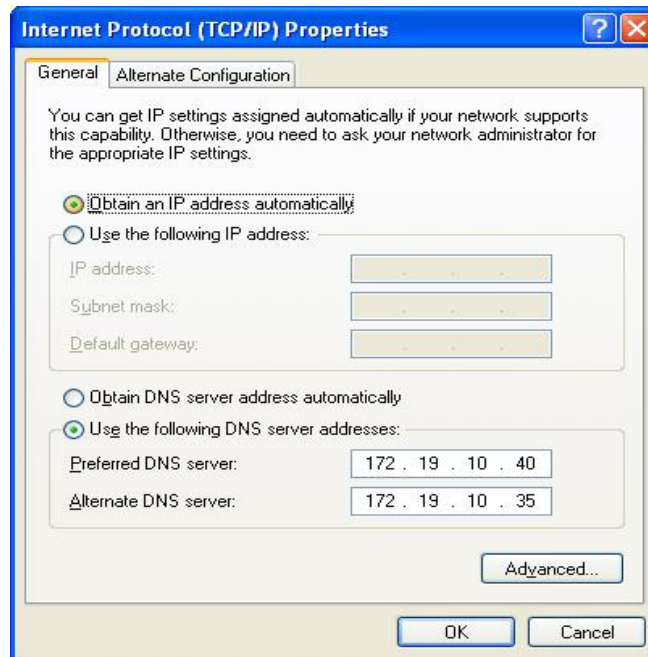
2. In the **Network Connections** window, right-click on **LAN (Local Area Connection)**, then click **Properties**.



3. In the **General** tab of the **Local Area Connection Properties** menu, highlight **Internet Protocol (TCP/IP)** under “This connection uses the following items:” by clicking on it once. Click on the **Properties** button.



4. Select “Obtain an IP address automatically” by clicking once in the circle. Click the **OK** button.



Your computer is now ready to use the Router's DHCP server.

## Windows 2000

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
4. The **Local Area Connection Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, skip ahead to *Configure Windows 2000 for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Install**.
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
8. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
9. If prompted, click **OK** to restart your computer with the new settings.

## Configure Windows 2000 for DHCP

1. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
2. In **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
3. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the button labeled **Obtain an IP address automatically**.
5. Double-click **OK** to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

## Windows ME

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
4. The **Network Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip ahead to *Configure Windows ME for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add**.
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
7. Select **Microsoft** in the Manufacturers box.
8. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
9. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
10. If prompted, click **OK** to restart your computer with the new settings.

## Configure Windows ME for DHCP

1. In the **Control Panel**, double-click the **Network and Dial-up Connections** icon.
2. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
3. In the **Network Properties** dialog box, select **TCP/IP**, and then click **Properties**.
4. In the **TCP/IP Settings** dialog box, click the **Obtain an IP address automatically** option.
5. Double-click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

## Windows 95 and Windows 98

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**. Double-click the **Network** icon.
2. The **Network** dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled, skip to *Configure IP Information Windows 95, 98*.
3. If TCP/IP does not display as an installed component, click **Add**. The **Select Network Component Type** dialog box displays.
4. Select **Protocol**, and then click **Add**. The **Select Network Protocol** dialog box displays.
5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
6. Click **OK** to return to the Network dialog box, and then click **OK** again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
7. Click **OK** to restart the PC and complete the TCP/IP installation.

## Configure Windows 95 and Windows 98 for DHCP

1. Open the **Control Panel** window, and then click the **Network** icon.
2. Select the network component labeled TCP/IP, and then click **Properties**.
3. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
4. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.
5. Click the **Obtain an IP address automatically** option.
6. Double-click **OK** to confirm and save your changes. You will be prompted to restart Windows.
7. Click **Yes**.

When it has restarted, your computer is ready to use the Router's DHCP server.

## Windows NT 4.0 Workstations

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows NT** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. In the **Control Panel** window, double-click the **Network** icon.
3. In the **Network** dialog box, click the **Protocols** tab.
4. The **Protocols** tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to "Configure IP Information"
5. If TCP/IP does not display as an installed component, click **Add**.
6. In the **Select Network Protocol** dialog box, select **TCP/IP**, and then click **OK**. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
7. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
8. Click **Yes** to continue, and then click **OK** if prompted to restart your computer.

## Configure Windows NT 4.0 for DHCP

1. Open the **Control Panel** window, and then double-click the **Network** icon.
2. In the **Network** dialog box, click the **Protocols** tab.
3. In the **Protocols** tab, select **TCP/IP**, and then click **Properties**.
4. In the **Microsoft TCP/IP Properties** dialog box, click the **Obtain an IP address automatically** option.
5. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

## Access the Configuration Manager

Now that your computer's IP settings allow it to communicate with the Router, you can access the configuration software.



Note

*Be sure that the web browser on your computer is not configured to use a proxy server in the Internet settings. In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:*

- 1. In Windows, click on the **Start** button, go to **Settings** and choose **Control Panel**.*
- 2. In the **Control Panel** window, double-click on the **Internet Options** icon.*
- 3. Click the **Connections** tab and click on the **LAN Settings** button.*
- 4. Verify that the "Use proxy server" option is **NOT** checked. If it is checked, click in the checked box to deselect the option and click **OK**.*

*Alternatively, you can access this **Internet Options** menu using the **Tools** pull-down menu in Internet Explorer.*

To use the web-based management software, launch your web browser software and use the LAN IP address of the Router to access the management software. The default LAN IP address of the Router is used in the Address bar of your web browser window. Type in **http://** followed by the default IP address, **10.0.0.1** in the address bar of the browser. The URL in the address bar should read: **http://10.0.0.1**

When you successfully connect to the web manager, the **Home** directory tab will display the **Setup Wizard** menu. You can launch the Setup Wizard from this page or use the menu buttons located in the left panel of the web page to view other menus used for basic configuration. You may use the Setup Wizard if your Internet connection is a PPPoE connection. If you are using a PPPoE and connection and want to use the Setup Wizard, follow the instructions below. If your Internet connection is a PPPoA, Bridge, Static IP, or Dynamic IP type connection, you should follow the instructions below in the section **Configure WAN Connection**.

Click on a directory tab to view the menus available in that directory

Click here to Run the Setup Wizard

Click on a menu button to use or view the menu

Web Manager - First Time Log On

## Using the Web Manager

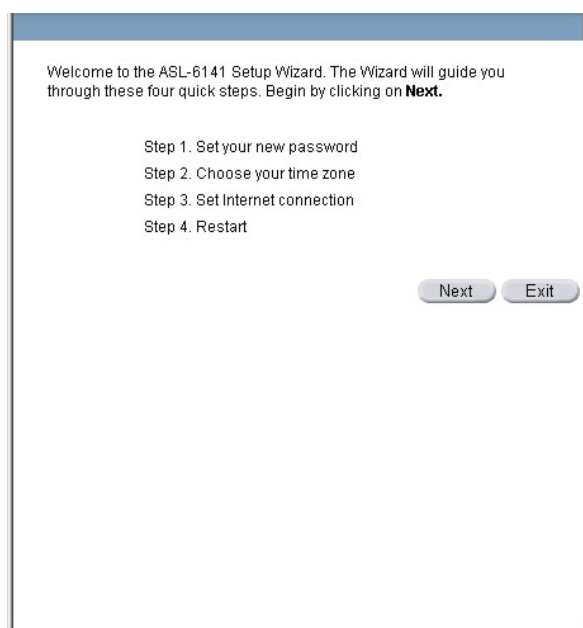
All configuration and management of the Router is done using the web-based management interface pictured in the above example. The various menus accessed by clicking on one of the directory tabs, Home, Advanced, Tools, Status and Help. Each tab displays menu buttons located in the left hand panel of the web interface. The table below lists the menus for each directory in the web manager.

Directory	Configuration and Read-only Menus
Home	Click the Home tab to access the Setup Wizard, Wireless LAN setup, WAN Configuration, LAN IP Configuration, DHCP for the LAN Setup and DNS IP Configuration menus.
Advanced	Click the Advanced tab to access the UPnP, Virtual Server, IP Filters, IP Routing, DMZ, Firewall, RIP, PPP, ADSL, ATM VCC, Wireless Performance and Wireless Management menus.
Tools	Click the Tools tab to access the Administrator Settings (used to set the system user name and password), System Time Configuration, System Settings (load and save configuration files), Firmware Upgrade, Miscellaneous Configuration (Save & Reboot, Ping test, enable IGMP) and Diagnostic Test menus.
Status	Click the Status tab to view the Device Information, Event Log, Traffic Statistics and ADSL Status information windows.
Help	The Help menu presents links to pages that explain various functions and services provided by the Router.

## Using the Setup Wizard

To use the Setup Wizard, click the **Run Wizard** button in the first browser window and follow the instructions in the pop-up window that appears.

The first window summarizes the setup process. Click the **Next** button to proceed. You may stop using the Setup Wizard at any time by clicking the **Exit** button. If you exit the wizard you will return to the first page without saving any of the settings changed during the process.

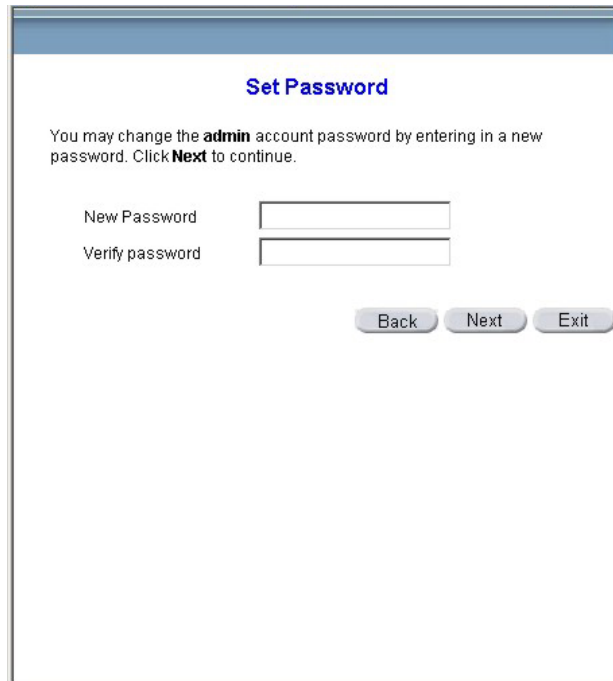


The first window of the Setup Wizard lists the basic steps in the process. These steps are as follows:

1. Set your new system password.
2. Set the system time.
3. Configure the connection to the Internet.
4. Save the new configuration settings and reboot the system.

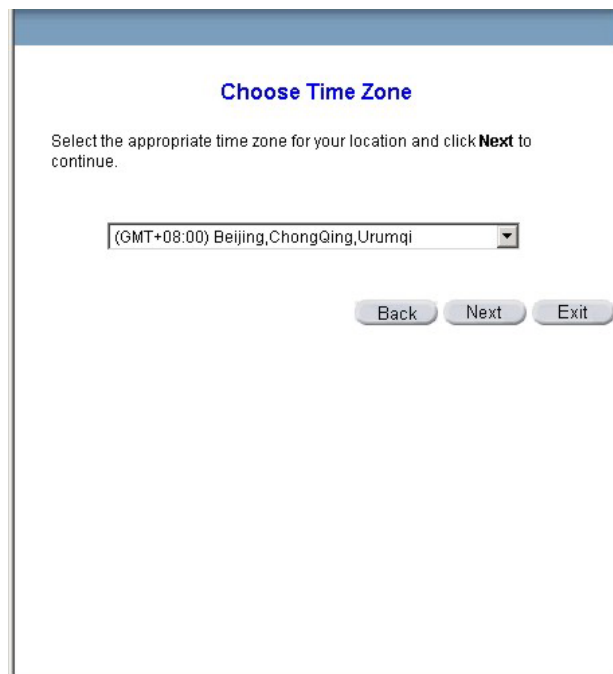


**Step 1** asks you to set a password that is required to make changes to the configuration settings of the Router in the Advanced Configurations menus. Type in a password and verify it by typing a second time. Click **Next** to continue.



The screenshot shows a web-based configuration page titled "Set Password". The page has a blue header bar. Below the header, the title "Set Password" is centered in blue. The main content area contains the following text: "You may change the **admin** account password by entering in a new password. Click **Next** to continue." Below this text are two input fields: "New Password" and "Verify password". At the bottom right of the page are three buttons: "Back", "Next", and "Exit".

Set the system time of the Router in **Step 2**. Choose the time zone you are in from the pull-down menu and click **Next**. If you wish to return to the previous menu during the setup process, click the **Back** button.



The screenshot shows a web-based configuration page titled "Choose Time Zone". The page has a blue header bar. Below the header, the title "Choose Time Zone" is centered in blue. The main content area contains the following text: "Select the appropriate time zone for your location and click **Next** to continue." Below this text is a pull-down menu with the text "(GMT+08:00) Beijing,ChongQing,Urumqi" and a downward arrow. At the bottom right of the page are three buttons: "Back", "Next", and "Exit".

In **Step 3** you **Select the Internet Connection Type** for the WAN interface. Your ISP has given this information to you. If you do not know what type of connection to use, exit the Setup Wizard and contact your ISP for the information. The Setup wizard menu that appears when you click the **Next** button depends on what connection type you select. The connection types available in the Setup Wizard menu are Dynamic IP Address, Static IP Address, PPPoE/PPPoA and Bridge Mode. Follow the instructions below for the type of connection you are using.

### Select Internet Connection Type (WAN)

Select the 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.**

Back   Next   Exit

### Dynamic IP Address Connections

If you selected the Dynamic IP Address connection type, select the **Connection Type** used for encapsulation. If you have been instructed to change the **VPI** number and **VCI** number, type in the new values. Click **Next** when you are ready to continue the Setup Completed menu.

**Note:** An option for Dynamic IP Address connections is to use the MAC address from your computer in place of the Router's actual MAC address for the purpose of Address Resolution by the ISP's DHCP server. To implement this feature click on the Clone MAC Address button before continuing to the next window.

### Set Dynamic IP Address

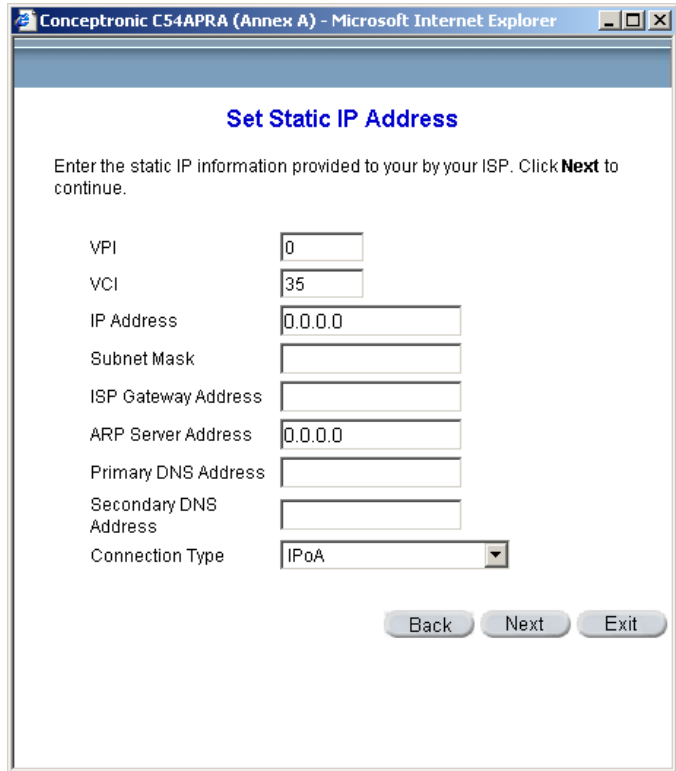
The **Clone MAC Address** is used to copy the MAC address of your Ethernet adapter to the Conceptronic C54APRA (Annex A). Click **Next** to continue.

VPI        
VCI        
Connection Type        
Cloned MAC Address     

Back   Next   Exit

## Static IP Address Connections

If you selected the Static IP Address connection type, change the WAN **IP Address**, **Subnet Mask**, **ISP Gateway Address** and (if available) **Secondary DNS Server IP address** as instructed by your ISP. Select the **Connection Type** used for encapsulation. If you have been instructed to change the **VPI** number and **VCI** number, type in the new values. Click **Next** when you are ready to continue the Setup Completed menu.

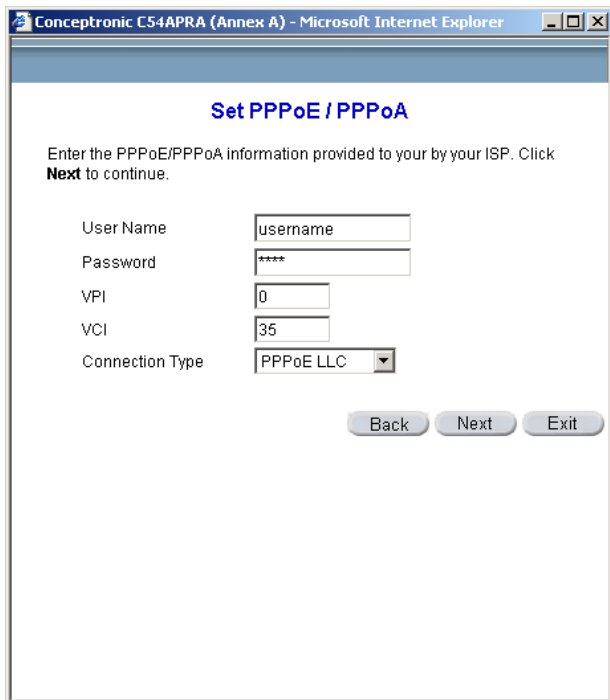


The screenshot shows a web browser window titled "Conceptronic C54APRA (Annex A) - Microsoft Internet Explorer". The page content is titled "Set Static IP Address" and includes the following fields and controls:

- Instruction: "Enter the static IP information provided to you by your ISP. Click **Next** to continue."
- VPI: Input field with value "0"
- VCI: Input field with value "35"
- IP Address: Input field with value "0.0.0.0"
- Subnet Mask: Empty input field
- ISP Gateway Address: Empty input field
- ARP Server Address: Input field with value "0.0.0.0"
- Primary DNS Address: Empty input field
- Secondary DNS Address: Empty input field
- Connection Type: Dropdown menu with "IPoA" selected
- Navigation buttons: "Back", "Next", and "Exit"

## PPPoE/PPPoA Connections

If you selected the PPPoE/PPPoA connection type in the previous menu, you will see the Setup Wizard menu pictured here. Type in the **Username** and **Password** used to identify and verify your account to the ISP. If you have been instructed to change the **VPI** number and **VCI** number, type in the new values. Select the **Connection Type** used for encapsulation specific to your service. Click **Next** when you are ready to continue the Setup Completed menu.



The screenshot shows a web browser window titled "Conceptronic C54APRA (Annex A) - Microsoft Internet Explorer". The page content is titled "Set PPPoE / PPPoA" and includes the following fields and controls:

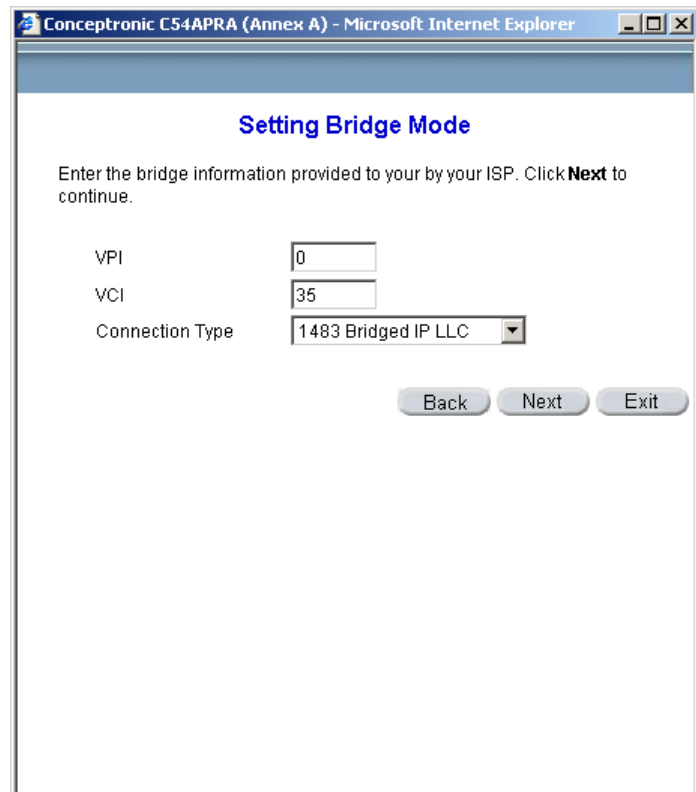
- Instruction: "Enter the PPPoE/PPPoA information provided to you by your ISP. Click **Next** to continue."
- User Name: Input field with value "username"
- Password: Input field with value "\*\*\*\*"
- VPI: Input field with value "0"
- VCI: Input field with value "35"
- Connection Type: Dropdown menu with "PPPoE LLC" selected
- Navigation buttons: "Back", "Next", and "Exit"



*Do not confuse the user name and password used to access the web-based manager with the ADSL account user name and password needed for PPPoE connections to access the ISP's network.*

## Bridge Connections

If you selected the Bridge connection type, select the **Connection Type** used for encapsulation. If you have been instructed to change the **VPI** number and **VCI** number, type in the new values. Click **Next** when you are ready to continue the Setup Completed menu.



The screenshot shows a web browser window titled "Conceptronic C54APRA (Annex A) - Microsoft Internet Explorer". The page content is as follows:

### Setting Bridge Mode

Enter the bridge information provided to you by your ISP. Click **Next** to continue.

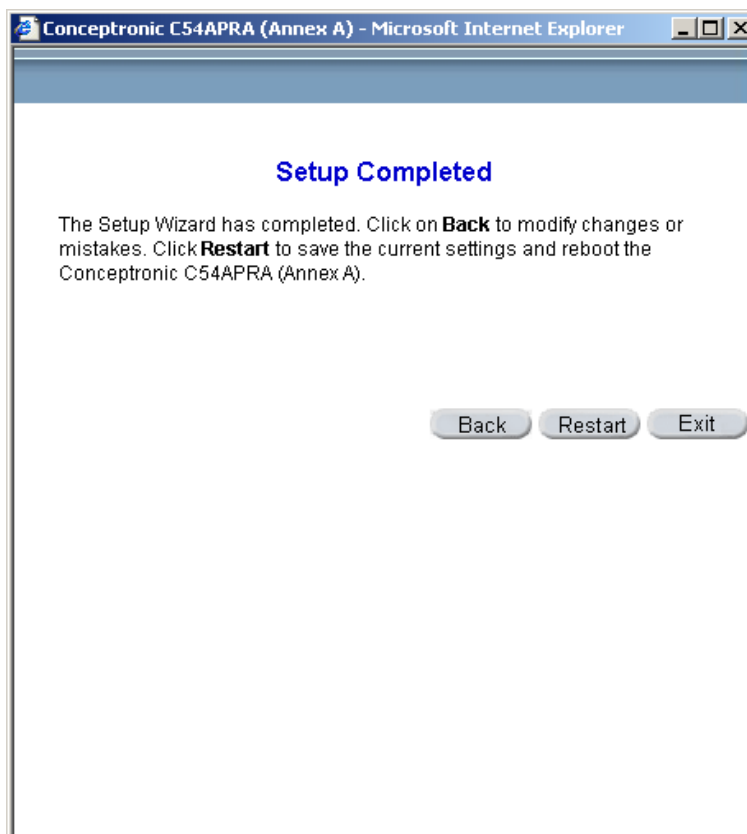
VPI:

VCI:

Connection Type:

Buttons: Back, Next, Exit

Finally you can confirm that the setup process is completed. If you are satisfied that you have entered all the necessary information correctly, click the **Restart** button to save the new configuration settings and restart the Router. If you need to change settings from a previous menu, click the **Back** button.



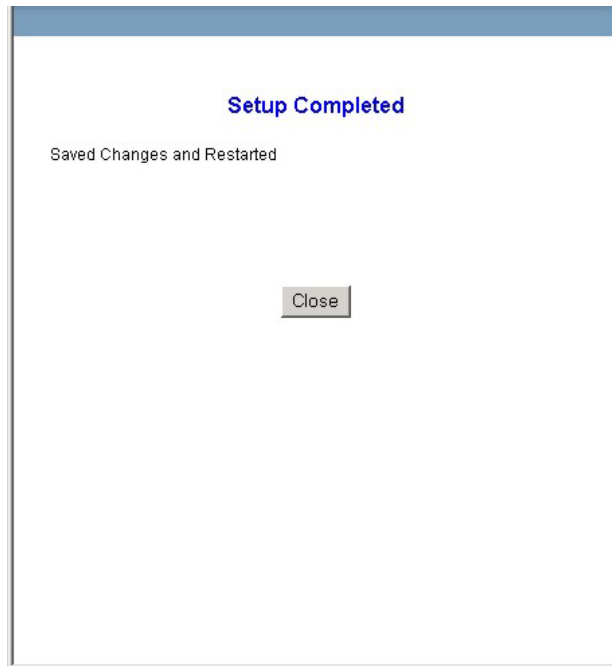
The screenshot shows a web browser window titled "Conceptronic C54APRA (Annex A) - Microsoft Internet Explorer". The page content is as follows:

### Setup Completed

The Setup Wizard has completed. Click on **Back** to modify changes or mistakes. Click **Restart** to save the current settings and reboot the Conceptronic C54APRA (Annex A).

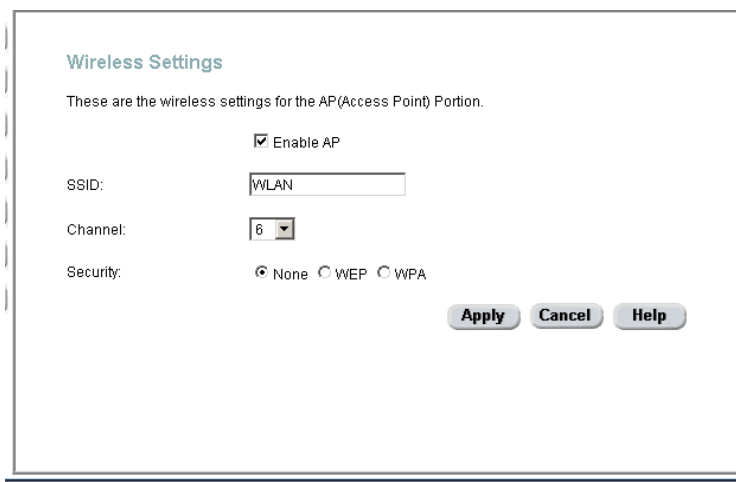
Buttons: Back, Restart, Exit

Do not turn the Router off while it is restarting. When it is finished restarting the dialog box below appears. Click **Close** to close the box and continue to configure the Router as desired.



## Basic Wireless LAN Setup

The two essential settings for wireless LAN operation are the SSID and Channel Number. The SSID (Service Set Identifier) is used to identify a group of wireless LAN components. To enable or disable the wireless interface, configure a new SSID or change the broadcast channel, click on the **Wireless Setup** link to view the menu displayed below. For instructions on setting up wireless security, please read the next chapter.



**Configure Basic Wireless LAN settings**



*Any changes to the Channel or SSID configuration will go into effect upon restarting the access point. After applying the new wireless settings, click the **Restart Access***

## Configure Basic Wireless Settings

Follow the instructions below to change basic wireless settings.

1. **To disable the wireless interface:** click in the **Enable AP** check box to remove the check mark and click the **Apply** button. This will immediately disable the wireless access point, it is not necessary to restart the access point to make this change.
2. **If the wireless interface has been disabled:** click the **Enable AP** check box to place a check mark in it. Click the **Apply** button. It is not necessary to restart the access point unless you have also changed the channel or SSID.
3. The **SSID** can be changed to suit your wireless network. Remember that any wireless device using the access point must have the same SSID and use the same channel. The SSID can be a continuous character string (i.e. no spaces) of up to 16 characters in length. To disable SSID sharing, use the Advanced Wireless Setup menu (see next chapter). Click the **Apply** button to save any change to the SSID, and click the **Restart Access Point** link to restart it.

The **Channel:** may be changed to channels that are available in your region. Channels available for wireless LAN communication are subject to regional and national regulation. Click the **Apply** button to save any change to the Channel, and click the **Restart Access Point** link to restart it.

## Configure WAN Connection

To configure the Router's basic configuration settings without running the Setup Wizard, you can access the menus used to configure WAN, LAN, DHCP and DNS settings directly from the **Home** directory. To access the WAN Settings menu, click on the **WAN** link button on the left side of the first window that appears when you successfully access the web manager.

The WAN Settings menu is also used to configure the Router for multiple virtual connections (Multiple PVCs). The next chapter contains a section describing how to set up multiple PVCs on the Router.

### ATM VC Setting

PVC Pvc0 ▾

VPI 0

VCI 35

Virtual Circuit Enabled ▾

### WAN Settings

Please select the appropriate options to connect to your ISP.

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.**

### PPPoE/PPPoA

User Name username

Password \*\*\*\*

Connection Type PPPoE LLC ▾

MRU 1492 bytes

Default Route Enabled ▾

NAT Enabled ▾

△ ATM

### WAN Settings Menu - PPPoE / PPPoA

Select the connection type used for your account. The menu will display settings that are appropriate for the connection type you select. Follow the instruction below according to the type of connection you select in the WAN Settings menu.

## PPPoE and PPPoA Connection for WAN

Follow the instructions below to configure the Router to use a PPPoE or PPPoA for the Internet connection. Make sure you have all the necessary information before you configure the WAN connection.

1. Click to select the **PPPoE/PPPoA** radio button in the **WAN Settings** options list. This is selected by default if you are configuring the Router for the first time. If it is not selected, click the **PPPoE/PPPoA** radio button located under the **WAN Settings** heading.
2. The **ATM VC Settings** at the top of the menu should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** settings at their default (*Pcv0* and *Enabled*) values for now. These can be used later if you are configuring multiple virtual circuits for your ADSL service.
3. Under the **PPPoE/PPPoA** heading, type the **User Name** and **Password** used for your ADSL account. A typical User Name will be in the form user@isp.com.th, the Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP.
4. Choose the **Connection Type** from the pull-down menu located under the User Name and Password entry fields. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *PPPoA VC-MUX*, *PPPoA LLC* and *PPPoE LLC*. If have not been provided specific information for the Connection Type setting, leave the default setting.
5. Leave the **MRU** value at the default setting (default = 1492) unless you have been instructed to change this.
6. If you are instructed to use enable **Default Route**, this setting specifies that the Router be used to define the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer.
7. Set **NAT** to *Enabled* unless you have been told to NAT must be *Disabled* for your account.
8. If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the **Service Category** and type in the values for **PCR** and **VCI** in Kbps.
9. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
10. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** (Miscellaneous) menu button. In the Miscellaneous menu, click he **Save & Reboot** button. The Router will save the new settings and restart. Upon restarting the Router will automatically establish a connection to the Internet.



## Bridged Connection for WAN

For Bridged connections it will be necessary for most users to install additional software on any computer that will the Router for Internet access. The additional software is used for the purpose of identifying and verifying your account, and then granting Internet access to the computer requesting the connection. The connection software requires the user to enter the User Name and Password for the ISP account. This information is stored on the computer, not in the Router.

Follow the instructions below to configure a Bridged connection for the WAN interface.

The screenshot shows a configuration window titled "WAN Settings Menu - Bridge Mode". It is divided into several sections:

- ATM VC Setting:** Contains fields for PVC (set to Pvc0), VPI (set to 0), VCI (set to 35), and Virtual Circuit (set to Enabled).
- WAN Settings:** Includes a note: "Please select the appropriate options to connect to your ISP." Below this are four radio buttons: Dynamic IP Address, Static IP Address, PPPoE/PPPoA, and Bridge Mode (which is selected). To the right of these buttons are instructions: "Choose this option to obtain a IP address automatically from your ISP.", "Choose this option to set static IP information provided to you by your ISP.", "Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)", and "Choose this option if your ISP uses Bridge Mode."
- Bridge Mode:** Contains a "Connection Type" dropdown menu set to "1483 Bridged IP LLC".
- ATM:** Contains a "Service Category" dropdown menu set to "UBR", and two input fields for PCR and SCR, both with "kbps" units.

At the bottom right of the window are three buttons: "Apply", "Cancel", and "Help".

### WAN Settings Menu - Bridge Mode

1. Click to select the **Bridge Mode** radio button in the **WAN Settings** options list. The menu will change to offer a different set of configuration options.
2. Under the **ATM VC Setting** heading, do not change the **PVC (Pvc0)** index for the initial connection.
3. Also under the **ATM VC Setting**, you see two numbers, the **VCI** and **VPI** values. Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.
4. Set the **Virtual Circuit** setting to *Enabled* in the pull-down menu if it is not already enabled.
5. Under **Bridge Mode**, choose the **Connection Type** from the pull-down menu. For bridge mode connections the available encapsulation methods are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*.
6. If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the **Service Category** and type in the values for **PCR** and **VCI** in Kbps.
7. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
8. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc (Miscellaneous)** menu button. In the Miscellaneous menu, click the **Save & Reboot**

button. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

## Dynamic IP Address for WAN

When the Router is configured to use Dynamic IP Address assignment for the WAN connection, a server on the ISP's network assigns the global IP address settings used for the WAN connection. This is method is simply Dynamic Host Control Protocol (DHCP) for the WAN. The Router is configured to be a DHCP client and obtain its IP settings automatically for the DHCP server owned by the ISP. Follow the instruction below to configure the Router to use Dynamic IP Address assignment for the WAN connection.

1. Click to select the **Dynamic IP Address** radio button listed in the **WAN Settings** options list. The menu will change to offer a different set of configuration options.
2. Select the **Connection Type** from the pull-down menu under the **Dynamic IP** heading. Your ISP should provide this information to you. The available option are *1483 Routed VC-Mux*, *1483 Routerd LLC*, *IpoA VC-Mux*, *IpoA LLC* and *IpoA (1577)*. If have not been provided specific information for the Connection Type setting, leave the default setting.

**ATM VC Setting**

PVC: Pvc0  
VPI: 0  
VCI: 35  
Virtual Circuit: Enabled

**WAN Settings**

Please select the appropriate options to connect to your ISP.

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.

**Dynamic IP**

Connection Type: 1483 Bridged IP LLC  
Cloned MAC Address: 0:0:0:0:0:0  
Clone MAC Address  
NAT: Enabled

**ATM**

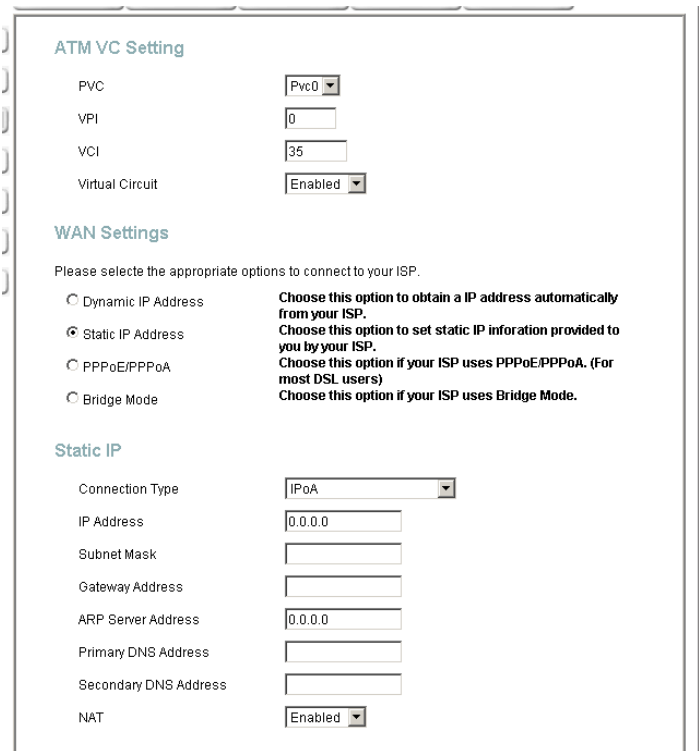
Service Category: UBR  
PCR: kbps  
SCR: kbps

### WAN Settings - Dynamic IP

3. Under the **ATM VC Setting** heading, do not change the **PVC (Pvc0)** index for the initial connection.
4. Also under the **ATM VC Setting**, you see two numbers, the **VCI** and **VPI** values. Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.
5. Set the **Virtual Circuit** setting to *Enabled* in the pull-down menu if it is not already enabled.
6. Under **Dynamic IP**, choose the **Connection Type** from the pull-down menu. The available encapsulation methods are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*.
7. Set **NAT** to *Enabled* unless you have been told to NAT must be *Disabled* for your account
8. If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the **Service Category** and type in the values for **PCR** and **VCI** in Kbps.
9. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
10. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** (Miscellaneous) menu button. In the Miscellaneous menu, click the **Save & Reboot** button. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

## Static IP Address for WAN

When the Router is configured to use Static IP Address assignment for the WAN connection, you must manually assign a global IP Address, Subnet Mask and Gateway IP Address used for the WAN connection. Most users will also to configure DNS server IP settings in the DNS Settings configuration menu (see below). Follow the instruction below to configure the Router to use Static IP Address assignment for the WAN connection.



**ATM VC Setting**

PVC

VPI

VCI

Virtual Circuit

**WAN Settings**

Please select the appropriate options to connect to your ISP.

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.**

**Static IP**

Connection Type

IP Address

Subnet Mask

Gateway Address

ARP Server Address

Primary DNS Address

Secondary DNS Address

NAT

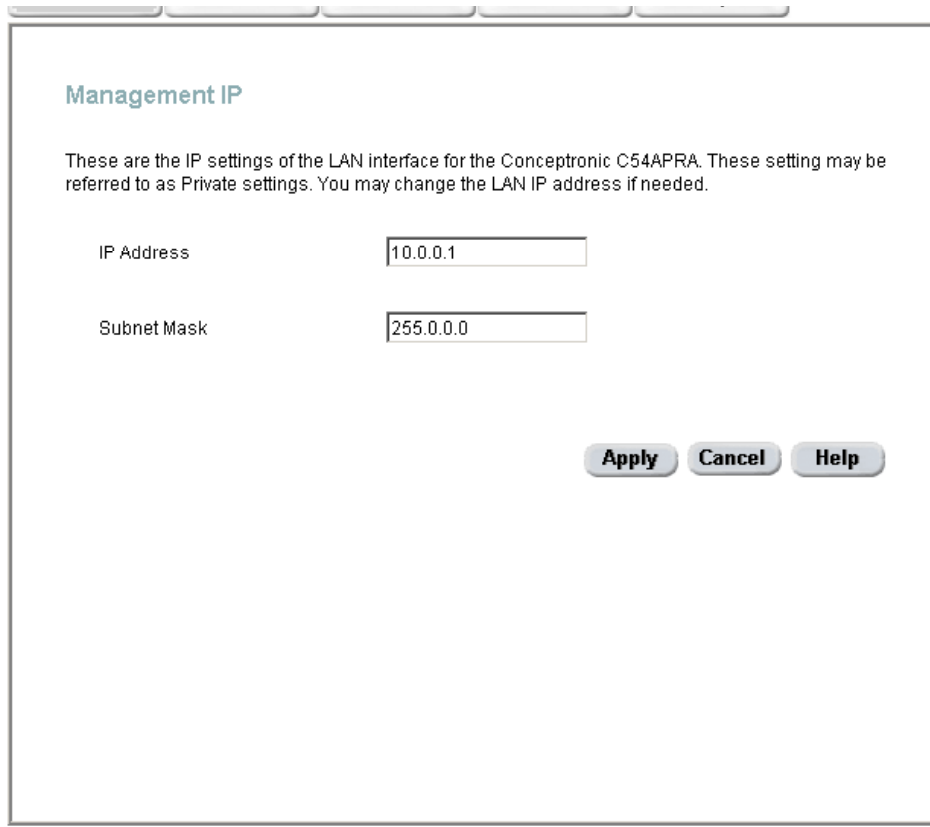
### WAN Settings - Static IP

1. Click to select the **Static IP Address** radio button listed in the **WAN Settings** options list. The menu will change to offer a different set of configuration options.
2. Under the **ATM VC Setting** heading, do not change the **PVC (Pvc0)** index for the initial connection.
3. Also under the **ATM VC Setting**, you see two numbers, the **VCI** and **VPI** values. Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.
4. Set the **Virtual Circuit** setting to *Enabled* in the pull-down menu if it is not already enabled.
5. Select the **Connection Type** from the pull-down menu under the **Static IP** heading. Your ISP should provide this information to you. The available options are *IPOA*, *1483 Bridged VC-Mux*, *1483 Bridged LLC*, and *1483 Routed VC-Mux*. If have not been provided specific information for the Connection Type setting, leave the default setting.
6. Change the **IP Address**, **Subnet Mask**, **Gateway Address** and (if available) **Secondary DNS** Server IP address as instructed by your ISP. Your ISP should have provided these IP settings to you.
7. Set **NAT** to *Enabled* unless you have been told to NAT must be *Disabled* for your account
8. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
9. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** (Miscellaneous) menu button. In the Miscellaneous menu, click he **Save & Reboot** button. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

## LAN IP Settings

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

To access the **LAN Settings** menu, click the **LAN** button in the **Home** directory.



**Management IP**

These are the IP settings of the LAN interface for the Conceptronic C54APRA. These setting may be referred to as Private settings. You may change the LAN IP address if needed.

IP Address

Subnet Mask

**Apply** **Cancel** **Help**

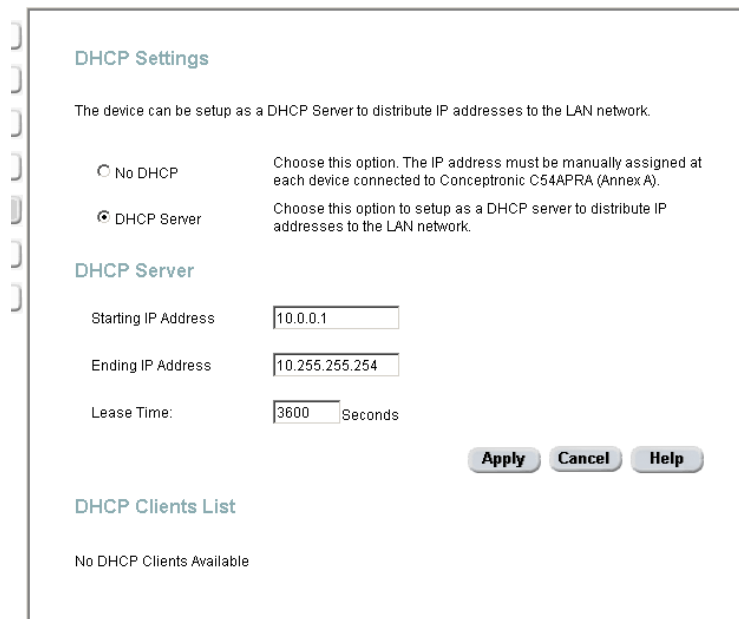
### Configure LAN IP settings

To change the **LAN IP Address** or **LAN Network Mask**, type in the desired values and click the **Apply** button. The new IP settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** (Miscellaneous) menu button. In the Miscellaneous menu, click he **Save & Reboot** button. The Router will save the new IP settings and restart. Your web browser should automatically be redirected to the new IP address. The new IP settings will be applied upon restarting.

## DHCP Server Settings for the LAN

The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the Router through the Ethernet port. When the Router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router, you must change the range of IP addresses in the pool used for DHCP on the LAN.

To display the **DHCP Server** menu, click the **DHCP** button in the **Home** directory. Active DHCP Clients appear listed in the **DHCP Client List** below the configuration menu. Information about DHCP clients includes the IP address, MAC address, host name and lease time are displayed in the list.



**DHCP Settings**

The device can be setup as a DHCP Server to distribute IP addresses to the LAN network.

No DHCP      Choose this option. The IP address must be manually assigned at each device connected to Conceptronic C54APRA (Annex A).

DHCP Server      Choose this option to setup as a DHCP server to distribute IP addresses to the LAN network.

**DHCP Server**

Starting IP Address:

Ending IP Address:

Lease Time:  Seconds

**DHCP Clients List**

No DHCP Clients Available

### Configure DHCP server settings for the LAN

The three options for DHCP service are as follows:

- You may use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for workstations.
- You use DHCP service provided by your ISP.

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured the DHCP Settings as you want them, click the **Apply** button to commit the new settings. The new DHCP settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** (Miscellaneous) menu button. In the Miscellaneous menu, click the **Save & Reboot** button.

## Use the Router for DHCP

To use the built-in DHCP server, click to select the **DHCP Server** option if it is not already selected. The IP Address Pool settings can be adjusted. The **Starting IP Address** is the lowest available IP address (default = 10.0.0.2). If you change the IP address of the Router this will change automatically to be 1 more than the IP address of the Router. The **Ending IP Address** is the highest IP address number in the pool. Type in the **Lease Time** in the entry field provided. This is the

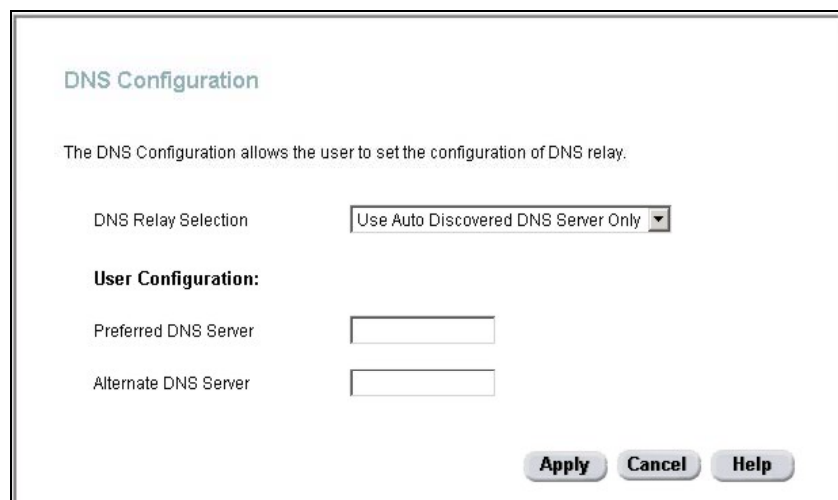
amount of time in seconds that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off. Be sure to save the new settings.

## Disable the DHCP Server

To disable DHCP, click to select the **No DHCP** option and click on the **Apply** button. Be sure to save the new settings.

## DNS Server Settings

The Router can be configured to relay DNS from your ISP or another available service to workstations on your LAN. When using DNS relay, the Router will accept DNS requests from hosts on the LAN and forward them to the ISP (or alternative) DNS servers. DNS relay can use auto discovery or the DNS IP address can be manually entered by the user. Alternatively, you may also disable the DNS relay and configure hosts on your LAN to use DNS servers directly. Most users who are using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network, will leave DNS relay enabled (either auto discovery or user configured).



**DNS Configuration**

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

DNS Relay Selection: Use Auto Discovered DNS Server Only

**User Configuration:**

Preferred DNS Server:

Alternate DNS Server:

Apply Cancel Help

### Configure DNS Settings

In the DNS Relay Selection pull-down menu, choose to *Use Auto Discovery*, *Use User Configured* or *Disable* DNS relay.

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

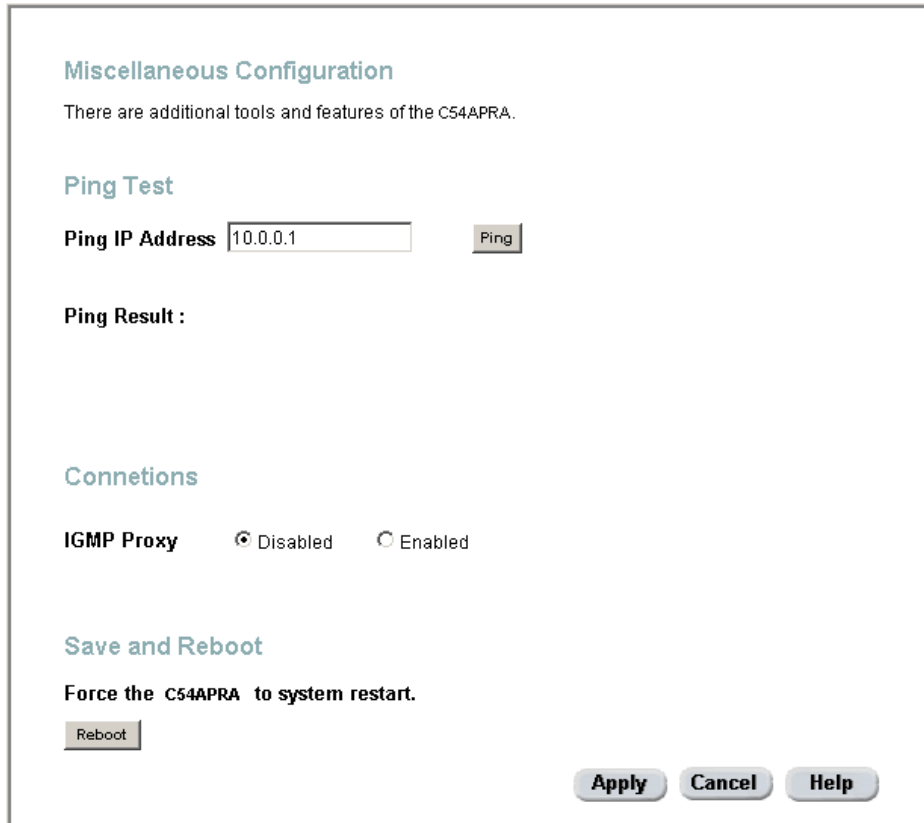
If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the **Preferred DNS Server** and the **Alternative DNS Server**.

If you choose to disable DNS relay, it will be necessary to configure DNS settings for hosts on the LAN since they will not be depending on the Router to forward the DNS requests.

When you have configured the DNS settings as desired, click the **Apply** button. Be sure to save the settings.

## Save New Settings

Any changes you have made to the must be saved to the Router's memory and the device must be restarted for the settings to take effect. To save settings you need to access the **Miscellaneous Configuration** menu. Click on the **Tools** directory tab then click the **Misc** menu button to view the menu pictured below.



The screenshot shows the 'Miscellaneous Configuration' page. At the top, it says 'Miscellaneous Configuration' and 'There are additional tools and features of the C54APRA.' Below this is a 'Ping Test' section with a 'Ping IP Address' field containing '10.0.0.1' and a 'Ping' button. Underneath is a 'Ping Result :' label. The 'Connections' section has an 'IGMP Proxy' option with 'Disabled' selected. At the bottom, there is a 'Save and Reboot' section with the text 'Force the C54APRA to system restart.' and a 'Reboot' button. At the very bottom right, there are three buttons: 'Apply', 'Cancel', and 'Help'.

### Save Settings and Restart the Router

To save the new settings, click the **Reboot** button near the bottom of the menu. It will take about two minutes for the whole process to be completed. Do not turn off the power while the Router is saving and restarting.

## Advanced Configuration/Network Management

This chapter introduces and describes the management features that have not been presented in the previous chapter. These include the more advanced features used for network management and security as well as administrative tools to manage the Router, view statistics and other information used to examine performance and for troubleshooting.

Use your mouse to click the directory tabs and menu buttons in order to display the various configuration and read-only menus discussed below. The table below summarizes again the directories and menus available in the management web interface. In this chapter you will find descriptions for the menus located in the Advanced, Tools and Status directories.

ID	Private IP	Protocol	Port Start	Port End	Port Map
----	------------	----------	------------	----------	----------

Figure 4- 1. Advanced configuration menus

Directory	Configuration and Read-only Menus
Home	Click the Home tab to access the Setup Wizard, Wireless LAN Configuration, WAN Configuration, LAN IP Configuration, DHCP for the LAN Setup and DNS IP Configuration menus. These menus are discussed in the previous Chapter on Basic Router Configuration.
Advanced	Click the Advanced tab to access the UPnP, Virtual Server, IP Filters, IP Routing, DMZ, Firewall, RIP, PPP, ADSL, ATM VCC, Wireless Performance and Wireless Management menus.
Tools	Click the Tools tab to access the Administrator Settings (used to set the system user name and password), System Time Configuration, System Settings (load and save configuration files), Firmware Upgrade, Miscellaneous Configuration (Save & Reboot, Ping test, enable IGMP) and Diagnostic Test menus.
Status	Click the Status tab to view the Device Information, Event Log, Traffic Statistics and ADSL Status information windows.
Help	The Help menu presents links to pages that explain various functions and services provided by the Router.



## UPnP

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network.

UPnP can be supported by diverse networking media including Ethernet, 802.11b wireless, Firewire, phoneline and powerline networking.

Select	Available Connections
<input type="radio"/>	pppoe123
<input type="radio"/>	connection1
<input type="radio"/>	connection2
<input type="radio"/>	connection3
<input type="radio"/>	connection4
<input type="radio"/>	connection5
<input type="radio"/>	connection6
<input type="radio"/>	connection7

Figure 4- 2. Universal Plug and Play setup

To enable UPnP for any available connection, click to check the **Enable UPnP** selection box, select the connection or connections on which you will enable UPnP listed under **Available Connections** and click the **Apply** button.

## Virtual Server

A Virtual Server can allow remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The C54APRA/C54APRB will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the Private IP address you specify. Remember that the Private IP Address must be within the range specified for your LAN.

The Virtual Server feature employs UDP/TCP port redirection to direct traffic through the WAN port to specified servers on your private network. Port redirection can also be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, you can configure the Router to direct HTTP packets to a designated HTTP server in the DMZ. You can define a set of instructions for a specific incoming port or for a range of incoming ports. Each instruction set or rule is indexed and can be modified or deleted later as needed.

Virtual server configuration sets can be used together with complimentary features such as Firewall Rules, DMZ devices and IP Filters to improve efficiency and security. Consider how these other functions will effect the virtual server sets you have configured and enabled.

The table below describes the configuration settings presented in the Virtual Server menu.

### Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

Rule Name

Private IP

Protocol

Port Start  Port End

Port Map

ID	Rule Name	Private IP	Protocol	Port Start	Port End	Port Map
1	smtp	10.0.0.1	TCP	25	25	25

**Figure 4- 3. Virtual Server Menu and List**

To modify virtual server settings for any previously created virtual server set listed, click on the note pad icon in the right hand column of the **Virtual Servers List** for the set you want to configure. The set will appear highlighted in the list and the parameters that have been configured appear in the settings fields above the list. Adjust the settings as desired and click the **Apply** button to put them into effect.

To configure a virtual server set, define the following settings in the Virtual Server configuration menu located in the top half of the browser window.

<b>Rule Name</b>	Provide a name for the rule. This name will not appear in the list below, however it may be useful if you later need to edit the settings for the rule. Rule names are optional.
<b>Private IP</b>	This is the IP address of the server on your LAN that will provide the service to remote users. The Private IP address is used to direct the service to a specific computer on your private network such as an FTP, Email or public web server. Type in the IP address of the server used for the service being configured here.
<b>Protocol</b>	You can select the transport protocol (TCP or UDP) that the application on the virtual server will use for its connections. Select one of the following options from the pull-down menu to define a <i>TCP</i> , <i>UDP</i> or <i>Both</i> . The choice of this protocol is dependent on the application that is providing the service. If you do not know which protocol to choose, check your application's documentation.
<b>Port Start/Port End</b>	Configure a range of ports for forwarding. Type the lowest numbered port in the range in the Port Start space. Type the highest numbered port in the Port End space. For a single port, just enter the same number in both spaces.  Virtual server port redirection must be used with a specified server or computer on the LAN (identified by the Private IP address).
<b>Port Map</b>	This is the local port being forwarded to from the Port Start/Port End port(s). Keep in mind that if you use a non-standard port number for an application with a reserved UDP/TCP port, some additional configuration may be required for the servers or workstations using the application on the LAN side.

Click the **Apply** button to put the new virtual server configuration set or modification into effect. Any server sets configured in the menu will appear in the Virtual Server List with the new settings. The Router must save the new settings and reboot before the new virtual server configurations are applied.

To remove any configuration set from the Virtual Server List, click on the trashcan icon for set you want to delete.



**Note**

*Some applications require multiple TCP or UDP ports to function properly. Applications such as Internet gaming, video conferencing, and Internet telephony are some examples of applications that often require multiple connections. These applications often conflict with NAT, and therefore require special handling. See the discussion of DMZ configuration below.*

# Filters

Filter rules in the Router are put in place to allow or block specified traffic. The Filter Rules however can be used in a single direction to examine and then Allow or Deny traffic for Inbound (WAN to LAN) or Outbound (LAN to WAN) routed data. The rules based on IP address and TCP/UDP port.

Configure the filter rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the Outbound Filter List at the bottom of the menu. The table below describes the various parameters that are configured for the filter rules.

The screenshot shows the 'Filters' configuration interface. At the top, there are radio buttons for 'Outbound Filter' (selected) and 'Inbound Filter'. Below this is the 'IP Outbound Filter' section, which includes a description: 'Filters are used to allow or deny LAN users from accessing the internet.' The configuration fields are: Source IP (two input boxes with a tilde separator and a dropdown set to 'Any IP'), Destination IP (two input boxes with a tilde separator and a dropdown set to 'Any IP'), Source Port (two input boxes with a tilde separator and a dropdown set to 'Any Port'), Destination Port (two input boxes with a tilde separator and a dropdown set to 'Any Port'), Protocol (a dropdown set to 'TCP'), and Action (a dropdown set to 'Allow'). At the bottom right are 'Apply', 'Cancel', and 'Help' buttons. At the bottom of the window is a table header with columns: ID, Source IP, Destination IP, Prot., Act., and Enable.

**Figure 4- 4. Filters Configuration Menu**

To modify any previously created filter rule, click on the note pad icon in the right hand column of the Filter List for the set you want to configure. Adjust the settings as desired and click the **Apply** button to put the new settings into effect.

First determine the direction of the traffic you want the rule to filter. To filter WAN to LAN traffic, select the **Inbound Filter** option. Any new Inbound Filter rules created will appear in the list. Likewise, should you to filter LAN to WAN traffic, create an **Outbound Filter** rule.

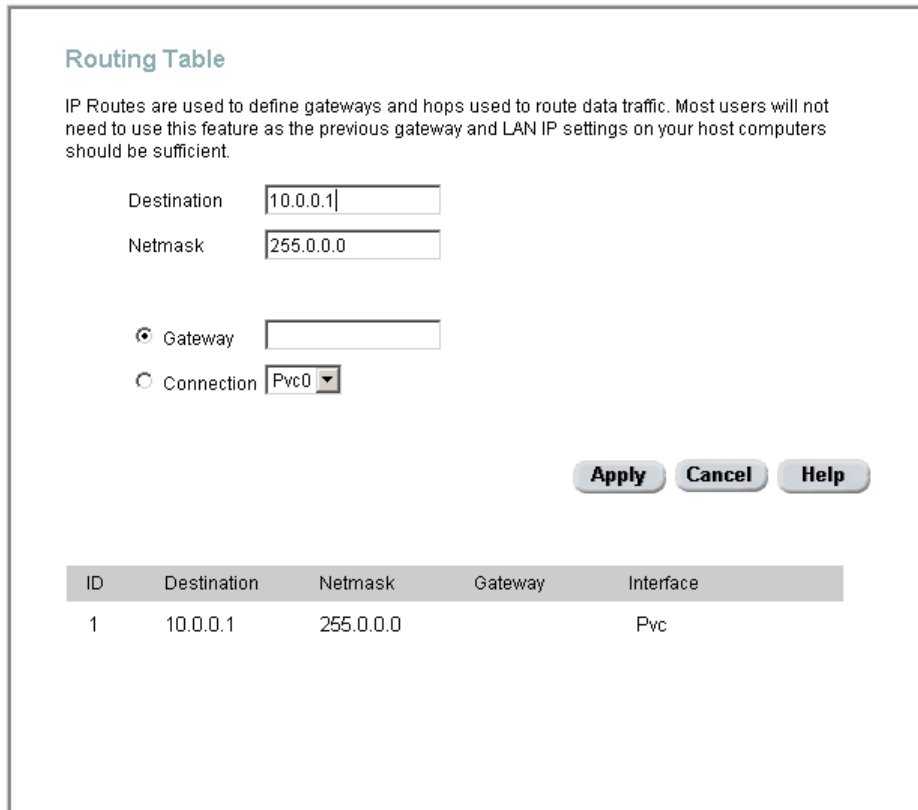
The parameters described below are used to set up filter rules.

<b>Source IP</b>	For an Outbound Filter, this is the IP address or IP addresses on your LAN for which you are creating the filter rule. For an Inbound Filter, this is the IP address or IP addresses for which you are creating the filter rule. You can opt to indicate a <i>Mask Range</i> , a <i>Single IP</i> , an <i>IP Range</i> or <i>Any IP</i> from the pull-down menu. Choosing Any IP will apply the rule to all WAN or all LAN IP addresses depending on which type of rule (Inbound or Outbound) is being configured.
<b>Destination IP</b>	Where the Destination IP address resides also depends on if you are configuring an Inbound or Outbound filter rule. You can opt to indicate a <i>Mask Range</i> , a <i>Single IP</i> , an <i>IP Range</i> or <i>Any IP</i> from the pull-down menu.
<b>Source Port</b>	The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. Select one of the following options from the pull-down menu to define a <i>Any Port</i> , <i>Single Port</i> , <i>Port Range</i> or <i>Safe Range</i> (ports above 1024).
<b>Destination Port</b>	The Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. Select one of the following options from the pull-down menu to define a <i>Any Port</i> , <i>Single Port</i> , <i>Port Range</i> or <i>Safe Range</i> (ports above 1024).
<b>Protocol</b>	Select the transport protocol ( <i>TCP</i> , <i>UDP</i> or <i>All</i> ) that will be used for the filter rule.
<b>Action</b>	Select to <i>Allow</i> or <i>Deny</i> transport of the data packets according to the criteria defined in the rule. Packets that are allowed are routed to their destination; packets that are denied are blocked.

Click the **Apply** button to put the new rule into effect. Any filter rule configured in the menu will appear in the Filters List with the new settings. The Router must save the new settings and reboot before the new rules are applied.

## Routing

Use Static Routing to specify a route used for data traffic within your Ethernet LAN or to route data on the WAN. This is used to specify that all packets destined for a particular network or subnet use a predetermined gateway.



**Routing Table**

IP Routes are used to define gateways and hops used to route data traffic. Most users will not need to use this feature as the previous gateway and LAN IP settings on your host computers should be sufficient.

Destination:

Netmask:

Gateway

Connection

ID	Destination	Netmask	Gateway	Interface
1	10.0.0.1	255.0.0.0		Pvc

Figure 4-5. Static Routing menu

To add a static route to a specific destination IP on the local network, enter a **Destination** IP address, **Netmask**, click the **Gateway** radio button and type in the Gateway's IP address. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation.

To add a static route to a specific destination IP on the WAN, click the **Connection** radio button and choose a connection from the pull-down menu, then enter a **Destination** IP address and **Netmask**. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation.

To remove a static route from the table in the bottom half of the window, choose to **Delete** it from the table and click the **Apply** button. Remember to save the configuration changes.

## DMZ

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

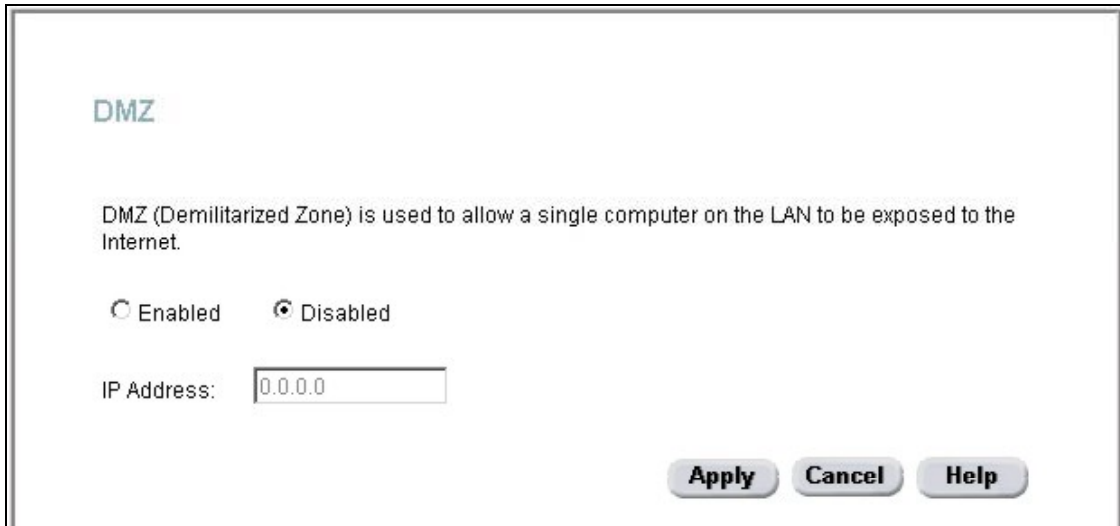


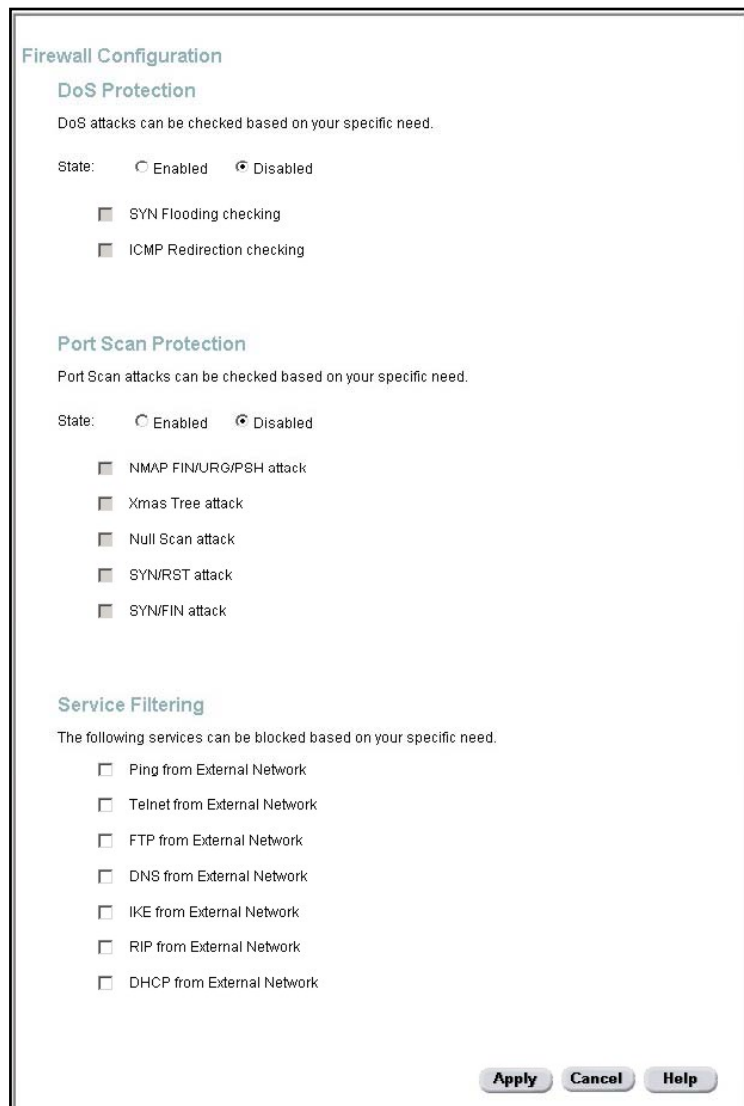
Figure 4- 6. DMZ IP address configuration

To designate a DMZ IP address, type in the **IP Address** of the server or device on your LAN, select the **Enabled** radio button and click the **Apply** button. To remove DMZ status from the designated IP address, select the **Disabled** radio button and click **Apply**. It will be necessary to save the settings and reboot the Router before the DMZ is activated.

## Firewall

The Firewall Configuration menu allows the Router to enforce specific predefined policies intended to protect against certain common types of attacks. There are two general types of protection (DoS, Port Scan) that can be enabled on the Router, as well as filtering for specific packet types sometimes used by hackers.

You can choose to **Enable** or **Disable** protection against a customized basket of attack and scan types. To enable **DoS Protection** or **Port Scan Protection**, select the **Enable** radio button for the protection type and click in the selection boxes for the various types of protection listed under each.



**Figure 4- 7. Firewall Configuration Menu**

When DoS, Port Scan, or Service Filtering Protection is enabled, it will create a firewall policy to protect your network against the following:

<b>Dos Protection</b>	<b>Port Scan Protection</b>	<b>Service Filtering</b>
SYN Flood check	Nmap/FIN attack	Ping from WAN
ICMP Redirection check	URG/PSH attack	Telnet from WAN
	Xmas Tree Scan	FTP from WAN
	Null Scan attack	DNS from WAN
	SYN/RST attack	IKE from WAN
	SYN/FIN Scan	RIP from WAN
		DHCP from WAN

A DoS "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person.

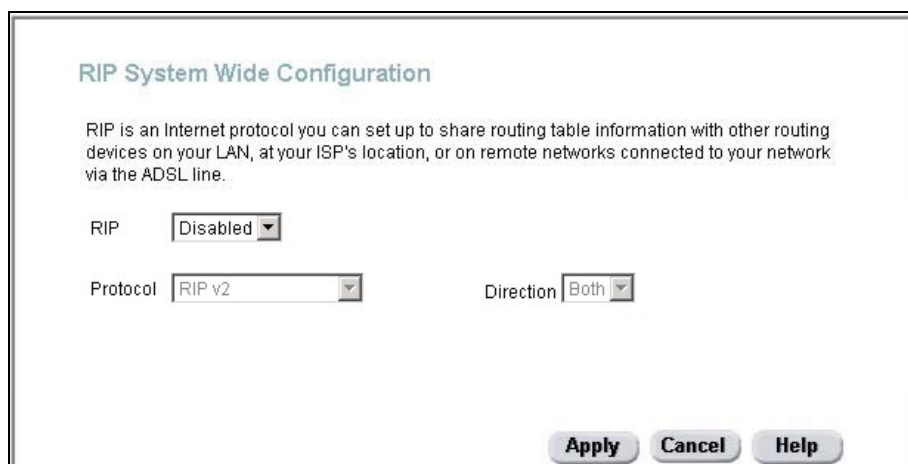
Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

The Service Filtering options allow you to block FTP, Telnet response, Pings, etc, from the external network. Check the category you want to block to enable filtering of that type of packet.

When you have selected the desired Firewall policies, click the **Apply** button to enforce the policies. Remember to save any configuration changes.

## RIP

The Router supports RIP v1 and RIP v2 used to share routing tables with other Layer 3 routing devices on your local network or remote LAN.



**Figure 4- 8. RIP menu**



To enable RIP, select *Enabled* from the **RIP** pull-down menu, select the **Protocol** (*RIPv1*, *RIPv2* and *RIPv1 Compatible*) and **Direction** (*In*, *Out*, or *Both*), and click **Apply**.

The RIPv1 Compatible option will respond to or send RIP requests compatible with both RIP v1 and RIP v2.

The direction configuration refers to the RIP request. Select *In* to allow RIP requests from other devices. Select *Out* to instruct the Router to make RIP requests for routing tables from other devices. Select *Both* to share routing tables in both directions.

## PPP Settings

When the WAN connection is configured for either PPPoA or PPPoE, you can configure the Router's PPP session to remain on all the time, or to disconnect after some period of no activity. You may also choose to instruct the Router to connect each time you want to access the WAN or the Internet.

**ATM VC Setting**

This page is used to view and PPP connection status and setting.

PVC PVC0

**Connection State** Disconnected

**Connection Setting**

Always ON

Connection On Demand

Manual

**Recommended**

Connection will close if idle for 1 minutes

Use Connect/Disconnect button only

**ATM VCs List**

ID	PVC	VPI	VCI	Connection Type
1	PVC0	8	35	PPPoA

**Figure 4- 9. PPP Connection settings menu**

If you want the Internet or WAN connection to be available any time a host on your LAN requests access, select the **Always On** option.

If your ISP account is billed according to the amount of time the Router is connected, choose the **Connection On Demand** option. You can configure an idle time in minutes to disconnect the PPP connection after a period of inactivity. This will discontinue the PPP session and require a few seconds to reconnect when a host requests access to the WAN. Alternatively you can choose the **Manual** option and use the **Connect** button to initiate a PPP connection each time you want to use the Router to access the WAN. If you use the Manual option, you must return to this menu and click the **Disconnect** button to terminate the PPP session.

## ADSL Modulation Settings

The default modulation technique used by the Router will automatically detect what ADSL protocol is used for your account. However it can be changed to any of the recognized standard modulations used for ADSL. Select the **Modulation Type** from the pull-down menu and click the **Apply** button to change the modulation.

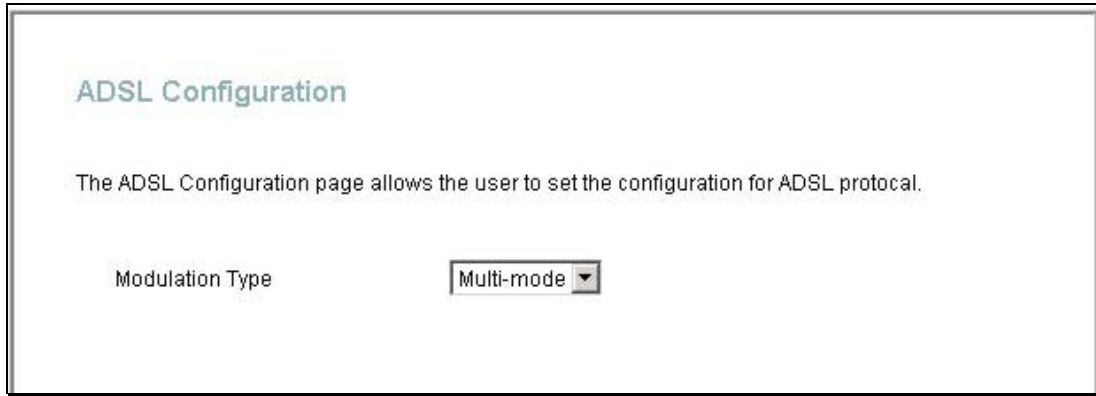


Figure 4- 10. ADSL Modulation Configuration menu

## ATM VC

The ATM Virtual Circuit connection menu is used to configure the WAN connection. If you are using multiple PVCs, you can change the configuration of any PVC in this menu. To create new or additional PVCs, read the section below on Multiple PVCs.

This menu can be used as an alternative menu to configure the same settings found on the WAN menu in the Home directory.

Figure 4- 11. ATM Virtual Circuit configuration menu

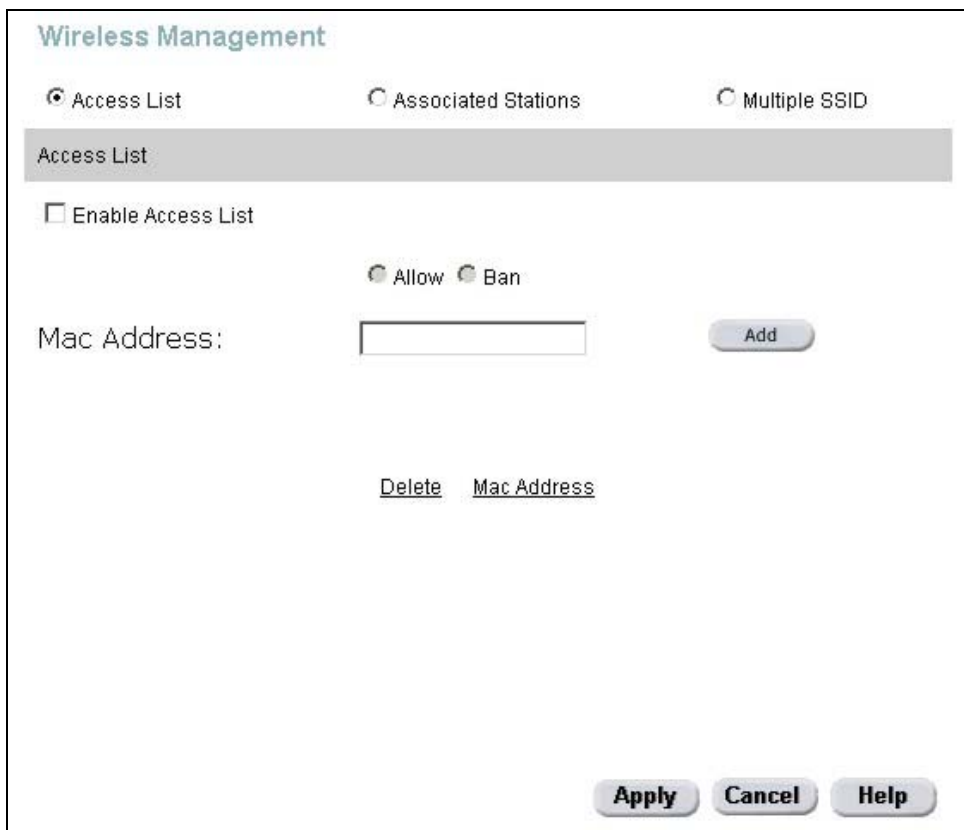
To configure an existing PVC configuration set, click the corresponding notepad icon in the right-hand column of the ATM VCs List. The PVCs current settings appear above in the entry fields of the ATM VC Settings menu. Configure the appropriate settings and click the **Apply** button to put the new settings into effect.

## Advanced Wireless LAN Configuration

The menus used to configure Wireless LAN settings available in the Advanced directory included the Wireless Performance and Wireless Management menus. Wireless security settings are configured using the WirelessSettings menu located in the Home directory. The wireless performance, management and security features are described below.

### Wireless Management

The **Wireless Management** menu located in the **Advanced** directory is used to control MAC address access to the wireless access point and to view a list of MAC addresses that are currently associated with the access point. This menu is also used to enable and configure use of multiple SSIDs. To use more than one SSID, WEP and WPA security must first be disabled (see below).



The screenshot shows the 'Wireless Management' configuration interface. At the top, there are three radio buttons: 'Access List' (selected), 'Associated Stations', and 'Multiple SSID'. Below this, the 'Access List' section is highlighted. It contains a checkbox for 'Enable Access List' which is currently unchecked. There are two radio buttons for 'Allow' and 'Ban', with 'Allow' selected. Below these is a text input field for 'Mac Address:' and an 'Add' button. At the bottom of the list area, there are links for 'Delete' and 'Mac Address'. At the very bottom of the page are three buttons: 'Apply', 'Cancel', and 'Help'.

Figure 4- 12. Wireless LAN Management - Access Control

To view a list of stations currently associated with the access point, click the **Associated Stations** radio button.

#### Configure Wireless Access Control

To create a list of MAC addresses that are banned or allowed association with the wireless access point:

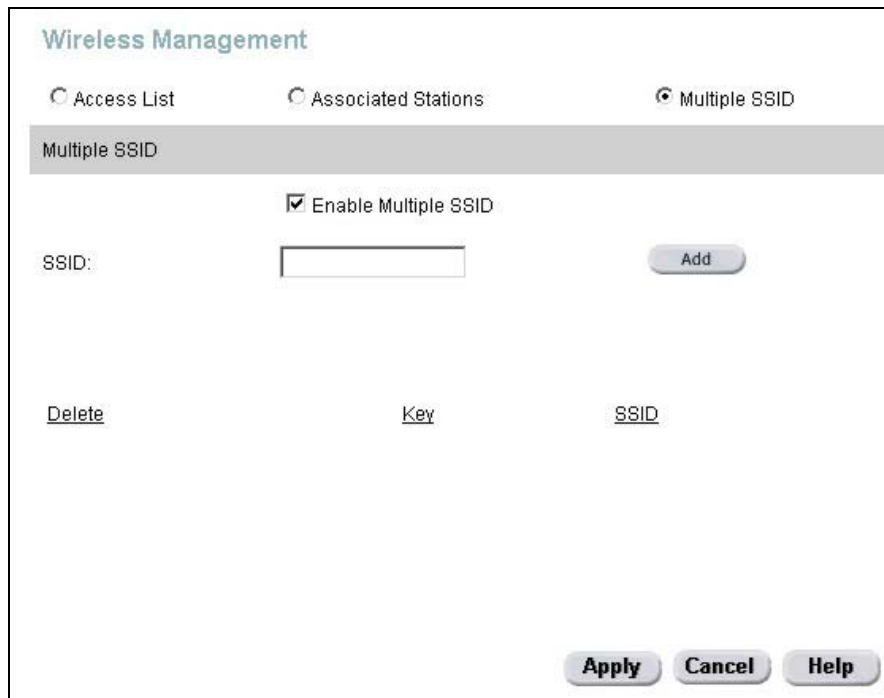
1. Click in the **Enable Access List** option box to select it.
2. Select the action to perform on the MAC address to be specified. Choose to **Allow** or **Ban** association.
3. Type in the **MAC Address** in the entry field provided.
4. Click the **Add** button to add the MAC address to the list. The MAC address will appear listed in the table below.

5. After compiling the list of MAC addresses as desired, click the **Apply** button to enforce access control for the MAC addresses in the list.

To remove any MAC address from the list, click the radio button in the left column of the list for the MAC address to be removed and click the **Apply** button.

### Configure Multiple SSID

Multiple SSID cannot be used if the access point has either WPE or WPA enabled. This must first be disabled in the Wireless menu located in the Home directory.



The screenshot shows the 'Wireless Management' interface. At the top, there are three radio buttons: 'Access List', 'Associated Stations', and 'Multiple SSID'. The 'Multiple SSID' option is selected. Below this, the 'Multiple SSID' section is highlighted. There is a checkbox labeled 'Enable Multiple SSID' which is checked. Below the checkbox is a text input field labeled 'SSID:' and an 'Add' button. At the bottom of the interface, there are three buttons: 'Apply', 'Cancel', and 'Help'. Below the 'Add' button, there is a table with three columns: 'Delete', 'Key', and 'SSID'. The 'Delete' column contains a radio button, and the 'Key' and 'SSID' columns are currently empty.

Figure 4- 13. Wireless Management - Multiple SSID

To configure multiple SSID:

1. Disable WEP or WPA in the **Wireless** menu of the **Home** directory.
2. Click in the **Enable Multiple SSID** option box to select it.
3. Enter the **SSID** you want to add.
4. Click the **Add** button to add the SSID to the list.
5. Click the **Apply** button to enable the listed SSIDs.

To remove an SSID from the list, click the radio button in the left column of the list for the SSID to be removed and click the **Apply** button.

## Wireless Performance

If you want to disable broadcast of the SSID or tweak wireless settings, click the **Wireless Performance** menu button in the **Advanced** directory.

**Wireless Performance**

These are the Wireless Performance feature for the AP(Access Point) portion.

Beacon interval:  (msec, range:1~1000,default:200)

DTIM:  (range:1~25,default:2)

Hidden SSID:  Enabled

Antenna transmit power:

Domain: ETSI

RTS Threshold:

Frag Threshold:

b/g Mode:

**Apply** **Cancel** **Help**

Figure 4- 14. Wireless LAN Performance settings

To disable SSID information sharing (SSID broadcast), click the **Hidden SSID** check box to enable it and click the **Apply** button.

## Wireless Security

The wireless access point has various security features used to limit access to the device or to encrypt data and shared information. The available standardized security for wireless LAN includes WEP, 802.1x and WPA. Wireless security is configured with the **Wireless Settings** menu located in the **Home** directory.



Note

*Before enabling any security function for wireless operation, make sure the access point is working. Test the wireless interface to be sure stations are able to associate with the C54APRA/C54APRB before configure security.*

### Configure Security Protocols

In the Wireless Settings menu, select the type of security you want to configure. A new menu will appear that is specific to the method being configured.

**Virtual Server**

Virtual Server is used to allow Internet users access to LAN services.

Rule Name

Private IP

Protocol

Port Start  Port End

Port Map

ID	Rule Name	Private IP	Protocol	Port Start	Port End	Port Map
1	smtp	10.0.0.1	TCP	25	25	25

Figure 4- 15. Configure WEP Wireless Security

## WEP Encryption

WEP (Wireless Encryption Protocol or Wired Equivalent Privacy) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. WEP keys used for the C54APRA/C54APRB are shared keys which means that it will allow only wireless devices that have the shared key to associate with it. Decryption of the data contained in each packet can only be done if the both the receiver and transmitter have the correct key.

WEP can use different methods of Authentication. Use the **Authentication Type:** drop-down menu to choose **Open**, **Shared** or **Both**.

- Select **Open** to allow any wireless station to associate with the access point.
- Select **Shared** to only allow stations using a shared key encryption to associate with it.
- Select **Both** to allow stations to associate with or without data encryption.

WEP is disabled by default. To enable WEP, click the **Enable WEP Wireless Security** option to place a check mark in the box. Configure the Encryption Keys as desired and click the **Apply** button. The Encryption key setup is described below.

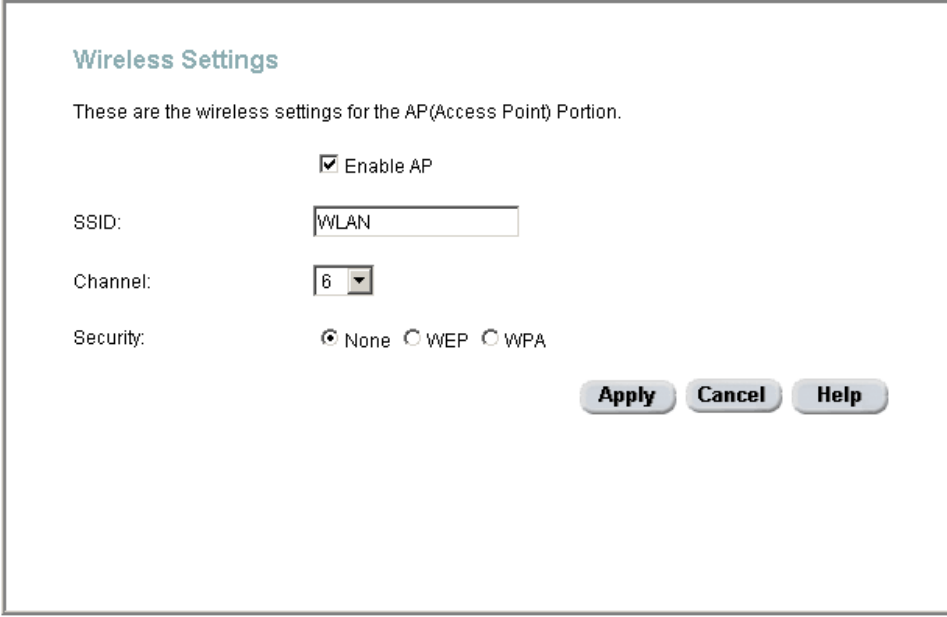
## Setup Encryption Keys

Configure the available Encryption Keys as 64, 128 or 256-bit keys. Only one key can be active. The active key is selected by clicking the **Select** radio button for the key you want to use. Type in a hexadecimal key according to the level of encryption used. For 64-bit cipher, use 10 digit keys, for 128-bit cipher, use 26 digit keys and for 256-bit cipher, use 58 digit keys. Hexadecimal digits are defined as the numerical digits 0 - 9 and the letters A - F (upper and lower case are recognized as the same digit).

Click the **Apply** button when you have configured WEP as desired to put the changes into effect.

## Configure WPA Settings

WPA security for wireless communication has been developed to overcome some of the shortcomings of WEP. WPA combines the key generation of WEP with the authentication services of a RADIUS server.



**Wireless Settings**

These are the wireless settings for the AP(Access Point) Portion.

Enable AP

SSID:

Channel:

Security:  None  WEP  WPA

**Apply** **Cancel** **Help**

**Figure 4- 16. Configure WPA Security for WLAN**

To configure WPA settings, select the options available on your network. If RADIUS services are available, click the 802.1x radio button to select authentication services. For RADIUS authentication, type in the IP address of the Radius server used in the **Server IP Address** field. Change the **Port:** if necessary, type in the password in the **Secret** field and change the **Group Key Interval** as desired. Click the **Apply** button and activate the **Restart Access Point** option to put the changes into effect.

Likewise for **PSK Hex** and **PSK String** parameters, select the option that is available and type in the desired values.

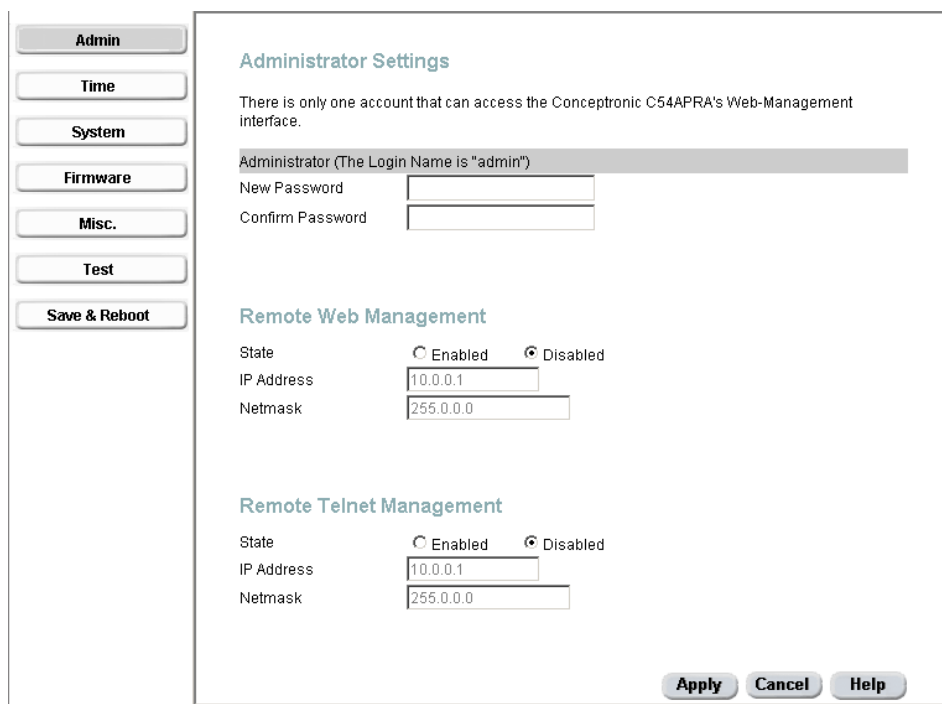
Click the **Apply** button to put the changes into effect.

## Tools and Utilities

Click the **Tools** tab to reveal the menu buttons for various functions located in this directory. These menus are used to change the system password used to access the web manager, to save or load Router configuration settings, upgrade the device firmware, save current configuration settings, restore default settings, and to perform miscellaneous actions such as performing Ping tests. These menus are described below.

### Change System Password

To change the password used to access the Router web manager, click the **Admin** button in the **Tools** directory to display the Administrator Settings menu. Under the Administrator heading, type the **New Password** and **Confirm Password** to be certain you have typed it correctly. Click the **Apply** button to activate the new password. The System User Name (Login Name) remains "admin", this cannot be changed using the web manager interface. Be sure to save the new setting (see below).



The screenshot shows the 'Administrator Settings' menu. On the left is a vertical sidebar with buttons for 'Admin', 'Time', 'System', 'Firmware', 'Misc.', 'Test', and 'Save & Reboot'. The main content area is titled 'Administrator Settings' and contains the following sections:

- Administrator (The Login Name is "admin")**: A section with two input fields for 'New Password' and 'Confirm Password'.
- Remote Web Management**: A section with a 'State' field containing radio buttons for 'Enabled' and 'Disabled' (with 'Disabled' selected). Below are input fields for 'IP Address' (10.0.0.1) and 'Netmask' (255.0.0.0).
- Remote Telnet Management**: A section with a 'State' field containing radio buttons for 'Enabled' and 'Disabled' (with 'Disabled' selected). Below are input fields for 'IP Address' (10.0.0.1) and 'Netmask' (255.0.0.0).

At the bottom right of the main content area are three buttons: 'Apply', 'Cancel', and 'Help'.

Figure 4- 17. Administrator Settings Menu

### Enable Remote Web Management and Telnet Access

The Administrator Settings menu (see above) is also used to enable remote Telnet management and remote web management access to the Router. To enable remote management of the Router, select the **Enabled** radio button for either Remote Web or Remote Telnet Management and type the IP Address and Netmask of the remote network or system used for management. Click the **Apply** button to activate remote management from the chosen IP address. Be sure to save the new setting (see below).

### Save Configuration File to PC

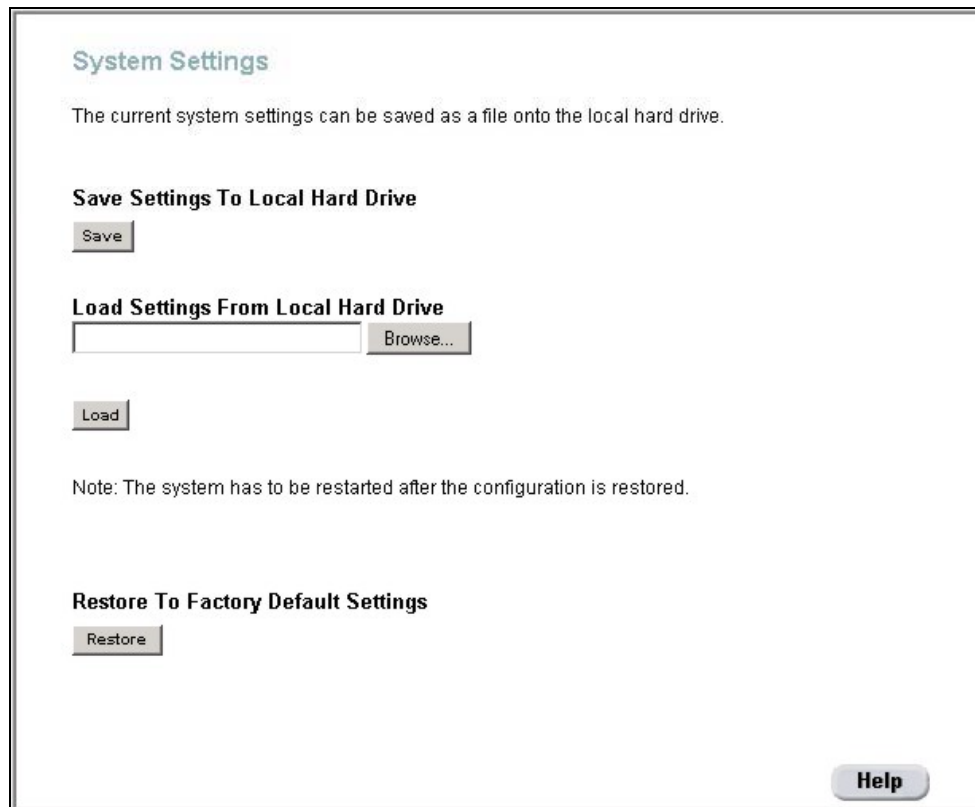
Once you have configured the Router to your satisfaction, it is a good idea to back up the configuration file to your computer. Use the System Setting menu to save the existing configuration file to the hard drive of the system you are using to access the web manager. To save the system configuration file to your computer, click the **Save** button. You will be prompted to select a



location on your computer to put the file. The file type is .cfg and may be named anything you wish.

## Load Saved Configuration Files

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Or type the full path and file name of the .cfg file in the space provided. Click the **Load** button to begin transferring and loading the .cfg file to the Router. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.



**System Settings**

The current system settings can be saved as a file onto the local hard drive.

**Save Settings To Local Hard Drive**

**Load Settings From Local Hard Drive**

Note: The system has to be restarted after the configuration is restored.

**Restore To Factory Default Settings**

Figure 4- 18. System Settings

## Restore Factory Default Settings

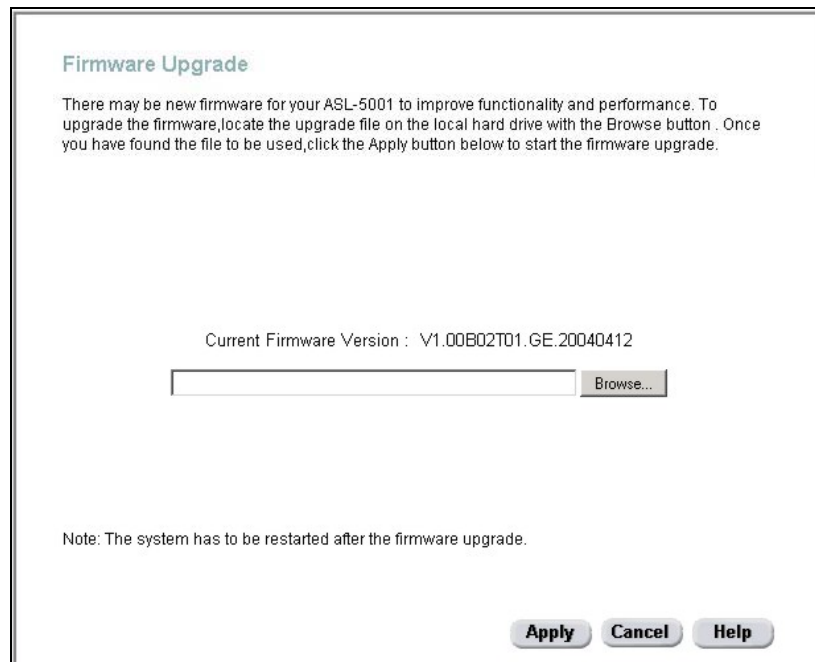
To reset the Router to its factory default settings, click the **Restore** button. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings.

## Firmware Upgrade



*Performing a Firmware Upgrade can sometimes change the configuration settings. Be sure to back-up the Router's configuration settings before upgrading the firmware.*

Use the Firmware Upgrade menu to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the System Settings menu described above.



The screenshot shows a web interface titled "Firmware Upgrade". The text reads: "There may be new firmware for your ASL-5001 to improve functionality and performance. To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Apply button below to start the firmware upgrade." Below this text, it displays "Current Firmware Version : V1.00B02T01.GE.20040412". There is a text input field followed by a "Browse..." button. At the bottom, there are three buttons: "Apply", "Cancel", and "Help". A note at the bottom states: "Note: The system has to be restarted after the firmware upgrade."

Figure 4- 19. Firmware Upgrade

To upgrade firmware, type in the name and path of the file or click on the **Browse** button to search for the file. Click the **Apply** button to begin copying the file. The file will load and restart the Router automatically.

## Save Router Configuration Settings

When you have completed configuration of the Router, make sure you save the current configuration settings to flash memory or risk losing the settings. To save the current configuration settings, click the **Misc.** menu button to view the **Miscellaneous Configuration** menu and click the **Save and Reboot** button. The current settings will be saved to NV-RAM and the system will restart. Do not turn off the Router during this process. It should take about two minutes to complete. After restarting, it is a good idea to backup the Router configuration file to your computer. See the instructions below to save configuration files to your PC.

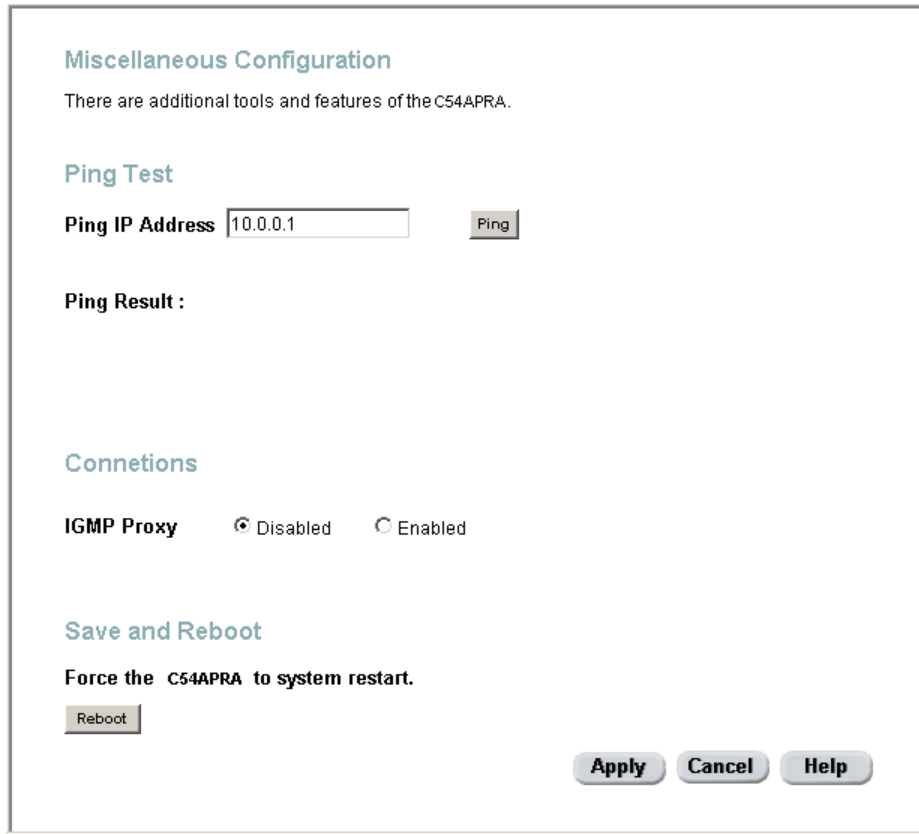


Figure 4- 20. Miscellaneous Configuration menu

Other functions available in Miscellaneous Configuration menu are a Ping test and IGMP enable/disable.

## Ping Test

The Ping test functions on the WAN and LAN interfaces. Type the IP address you want to check in the space provided and click the **Ping** button. Read the Ping test result in the space immediately below.

## IGMP

This is **Disabled** by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded to the LAN. IGMP is used to manage multicasting on TCP/IP networks, most users will not need to enable this. Some ISPs use IGMP to perform remote configuration for client devices, such as the Router. If you are unsure, check with your ISP. To enable IGMP service to the LAN interface, select **Enabled** and click the **Apply** button.

## Router Status Information

Use the various read-only menus to view system information and monitor performance.

## Device Information Display

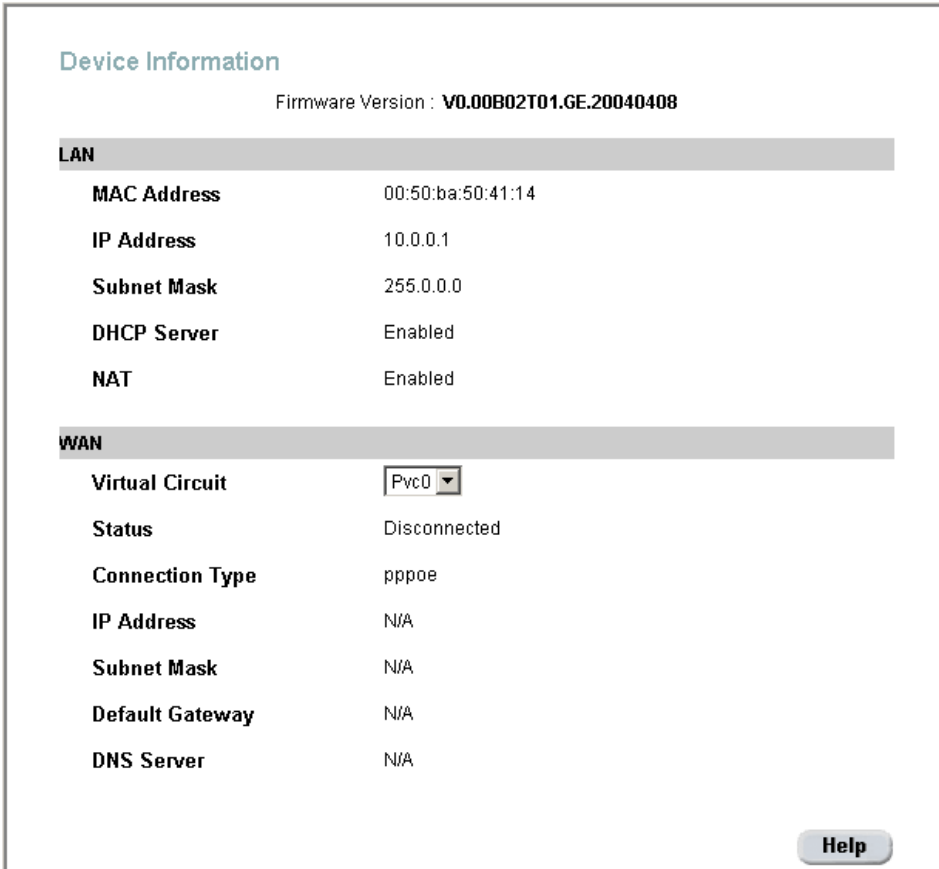
Use the Device Information window to quickly view basic current information about the LAN, WAN and Wireless interfaces. The basic information available in this window is summarized below.

### LAN

The MAC Address of the Ethernet LAN connection, IP Address, and Subnet Mask information will be displayed, as well as the setting (Enabled/Disabled) for the DHCP Server.

### WAN (ADSL)

The MAC Address of the Ethernet WAN connection, IP Address, Subnet Mask, Default Gateway, and DNS (Domain Name Server) information will be listed. The connection type includes Dynamic, Static, and PPPoE. You may click the DHCP Release or Renew the IP address assigned by the ISP for the WAN port for the Dynamic Setting Option. For PPPoE setting, you may click the button to Connect and Disconnect the DSL connection.



The screenshot shows a web interface titled "Device Information" with a firmware version of "V0.00B02T01.GE.20040408". It is divided into two sections: LAN and WAN. The LAN section lists MAC Address (00:50:ba:50:41:14), IP Address (10.0.0.1), Subnet Mask (255.0.0.0), DHCP Server (Enabled), and NAT (Enabled). The WAN section lists Virtual Circuit (Pvc0), Status (Disconnected), Connection Type (pppoe), IP Address (N/A), Subnet Mask (N/A), Default Gateway (N/A), and DNS Server (N/A). A "Help" button is located at the bottom right.

Device Information	
Firmware Version : V0.00B02T01.GE.20040408	
LAN	
MAC Address	00:50:ba:50:41:14
IP Address	10.0.0.1
Subnet Mask	255.0.0.0
DHCP Server	Enabled
NAT	Enabled
WAN	
Virtual Circuit	Pvc0
Status	Disconnected
Connection Type	pppoe
IP Address	N/A
Subnet Mask	N/A
Default Gateway	N/A
DNS Server	N/A

Figure 4- 21. Display Information window

## Multiple Virtual Connections

The Router supports multiple virtual connections. Up to eight PVCs to eight separate destinations can be created and operated simultaneously utilizing the same bandwidth. Additional PVC connections can be added for various purposes. For example, you may want to establish a private connection to remote office in order to create an extended LAN, or setup a server on a separate connection. Provisioning for additional PVC profiles must be done through your telecommunications services provider. Extended LAN operations employing multiple virtual connections require ADSL routers or modems at the remote site for a successful connection. Contact your ISP or telecommunications service provider if you are interested in setting up multiple virtual connections.

After the necessary arrangements have been made to use the Router with multiple virtual connections, follow the instructions below to setup the Router using the VPI/VCI settings given to you by your server provider.

### Configure Multiple PVCs

Additional PVCs can be configured by first accessing the WAN configuration menu in the Home directory.

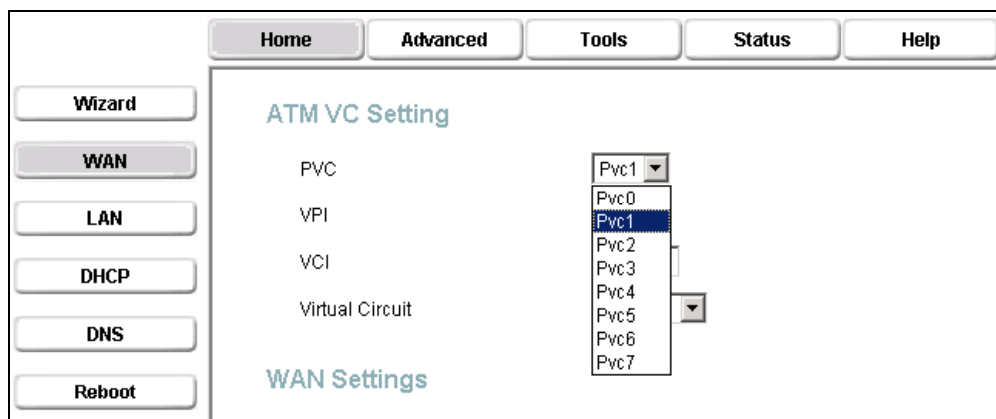


Figure 4- 22. Select new PVC to configure in the WAN menu

The PVC pull-down menu offers 8 virtual connections available for configuration. The default VC used by the Router is labeled Pvc0. Any additional connections that are configured must have a VPI/VCI combination that is unique to the Router. These numbers will have been already been established by your service provider on their network.

To add a new virtual connection:

1. Select the new **PVC** to configure from the pull-down menu.
2. Enter the values for the **VPI** and **VCI** given to you by your service provider.
3. To activate the VC, select *Enabled* from the **Virtual Circuit** pull-down menu.
4. Configure the WAN Settings and Connection Type as desired.

In the example below, a new VC (Pvc1) has been added using the WAN Settings menu. The connection is setup as a bridged connection.

**ATM VC Setting**

PVC: Pvc1  
 VPI: 3  
 VCI: 36  
 Virtual Circuit: Enabled

**WAN Settings**

Please select the appropriate options to connect to your ISP.

Dynamic IP Address  
 Static IP Address  
 PPPoE/PPPoA  
 Bridge Mode

Choose this option to obtain a IP address automatically from your ISP.  
 Choose this option to set static IP information provided to you by your ISP.  
 Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)  
 Choose this option if your ISP uses Bridge Mode.

**Bridge Mode**

Connection Type: 1483 Bridged IP VC-Mux

**ATM**

Service Category: UBR  
 PCR: kbps  
 VCI: kbps

Apply Cancel Help

Figure 4- 23. Configure new VC

The new VC appears listed in the ATM VC Setting menu located in the Advanced directory.

**ATM VC Setting**

PVC: PVC1  
 VPI: 3  
 VCI: 36  
 Virtual Circuit: Enabled  
 WAN Setting: Bridge Mode

**Bridge Mode**

Connection Type: 1483 Bridged IP VC-Mux

Apply Cancel Help

**ATM VCs List**

ID	PVC	VPI	VCI	Connection Type	Virtual Circuit
1	PVC0	8	35	PPPoE/PPPoA	Enabled
2	PVC1	3	36	Bridge Mode	Enabled

Figure 4- 24. New VC listed in ATM VC Settings menu

Any VC may be configured in the ATM VC menu by clicking the notepad icon for the PVC you want to configure. VCs configured with PPP connection types can be further configured in the PPP menu.



## Technical Specifications

General		
Standards	IEEE 802.11b/ 802.11g IEEE 802.3/ 802.3u IEEE 802.1d RFC 791 (IP Routing) RFC 792 (UDP) RFC 826 (ARP) RFC 1058 (RIP 1) RFC 1389 (RIP 2) RFC 1483 (Bridged Ethernet) RFC 1577 (IP over ATM) RFC 1661 (PPP) RFC 1994 (CHAP)	RFC 1334 (PAP) RFC 2364 (PPP over ATM) RFC 1631 (NAT) RFC 1877 (Automatic IP assignment) RFC 2516 (PPP over Ethernet) RFC 2131 (DHCP) ANSI T1.413 issue 2 ITU G.992.1 (G.dmt) ITU G.992.2 (G.lite) ITU G.994.1 (G.Hs) ITU-T Rec. I.361 Supports ATM Forum UNI V3.1/4.0 PVC
	<b>Wireless</b>	
Modulation	IEEE 802.11b: DQPSK, DBPSK, DSSS, and CCK IEEE 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM	
Frequency	2400 ~ 2484.5MHz ISM band	
Channels	11 channels for United States 13 channels for European Countries 13 channels for Japan	
Wireless Data Rates	IEEE 802.11b: 11, 5.5, 2, and 1Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps	
Media Access Protocol	CSMA/CA with ACK	
WEP	64/128/256 bits	
Wireless Certification	Wi-Fi WPA	
ADSL Data Rates	G.dmt full rate: Downstream up to 8 Mbps Upstream up to 640 Kbps G.lite: Downstream up to 1.5 Mbps Upstream up to 512 Kbps	
Media Interface	RJ-11 port ADSL telephone line connection 4 x RJ-45 ports for 10/100BASET Ethernet connection	

Physical and Environmental	
<b>DC Inputs:</b>	Input: 230V AC 50 - 60Hz (per region)
<b>Power Adapter</b>	Output: 12V AC, 1.2A
<b>Power Consumption</b>	12 Watts (max)
<b>Operating Temperature</b>	5° to 40° C (41° - 104° F)
<b>Humidity</b>	5 to 95% (non-condensing)
<b>Dimensions</b>	198 x 155 x 34 mm
<b>Weight</b>	450 g
<b>EMI</b>	FCC Class B, CE EN301489 SMA
<b>Safety:</b>	CSA International





## IP Address Setup

The C54APRA/C54APRB is designed to provide network administrators maximum flexibility for IP addressing on the Ethernet LAN. The easiest IP setup choice in most cases is to let the Router do it using DHCP, which is enabled by default. This appendix briefly describes various options including DHCP, used for IP setup on a LAN. If you are new to IP networking, the next appendix provides some background information on basic IP concepts.

### Assigning Network IP Addresses

The IP address settings, which include the IP address, subnet mask and gateway IP address are the first and most important internal network settings that need to be configured. The Router is assigned a default LAN IP address and subnet mask. If you do not have a preexisting IP network and are setting one up now, using the factory default IP address settings can greatly ease the setup process. If you already have a preexisting IP network, you can adjust the IP settings for the Router to fit within your existing scheme.

### Using the Default IP Address

The Router is shipped with a preset default IP address setting of 10.0.0.1 for the LAN port. There are two ways to use this default IP address, you can manually assign an IP address and subnet mask for each PC on the LAN or you can instruct the Router to automatically assign them using DHCP. The simplest method is to use DHCP. The DHCP function is active by default.

### Manual IP Address Assignment

Manually configuring IP settings for the LAN means you must manually set an IP address, subnet mask and IP address of the default gateway (the Router's IP address) on each networked computer. The example listed below describes IP configuration for computers running Windows 95 or Windows 98. Regardless of what operating system is used on each workstation, the three network IP settings must be defined so the network interface used by each workstation can be identified by the Router, and vice versa. For detailed information about configuring your workstations IP settings, consult the user's guide included with the operating system or the network interface card (NIC).

1. In Windows 95/98, click on the **Start** button, go to **Settings** and choose **Control Panel**.
2. In the window that opens, double-click on the **Network** icon.
3. Under the Configuration tab, select the **TCP/IP** component and click *Properties*.
4. Choose the *Specify an IP address* option and edit the address settings accordingly. Consult the table below for IP settings on a Class C network.

Using Default IP without DHCP			
Host	IP Address	Subnet Mask	Gateway IP
Router	10.0.0.1	255.0.0.0	
Computer #1	10.0.0.2	255.0.0.0	
Computer #2	10.0.0.3	255.0.0.0	10.0.0.1
Computer #3	10.0.0.4	255.0.0.0	10.0.0.1

IP Setup - Example #1

Please note that when using the default IP address as in the above example, the first three numbers in the IP address must always be the same with only the fourth number changing. The first three numbers define the network IP address (all machines must belong to the same IP network), while

the last number denotes the host IP address (each computer must have a unique address to distinguish it on the network). The IP address scheme used in Example #1 can be used for any LAN that requires up to 253 separate IP addresses (excluding the Router). Notice that the subnet mask is the same for all machines and the default gateway address is the LAN IP address of the Router.

It is a good idea to make a note of each device's IP address for reference during troubleshooting or when adding new stations or devices.

## Using DHCP

The second way to use the default settings is to allow the Router to automatically assign IP settings for workstation using DHCP. To do this, simply make sure your computers' IP addresses are set to 0.0.0.0 (under Windows, choose the option Obtain an IP address automatically in the TCP/IP network component described above). When the computers are restarted, their IP settings will automatically be assigned by the Router. The Router is set by default to use DHCP. See the discussion in Chapter 5 for information on how to use configure the Router for DHCP.

## Changing the IP Address of the Router

When planning your LAN IP address setup, you may use any scheme allowed by rules that govern IP assignment. It may be more convenient or easier to remember an IP scheme that use a different address for the Router. Or you may be installing the Router on a network that has already established the IP settings. Changing the IP address is a simple matter and can be done using the web manager (see *LAN IP Address* in Chapter 5). If you are incorporating the Router into a LAN with an existing IP structure, be sure to disable the DHCP function. Also, consider the effects of the NAT function which is enable by default.

An IP addressing scheme commonly used for Ethernet LANs establishes 10.0.0.1 as the base address for the network. Using Example #2 below, the Router is assigned the base address 10.0.0.1 and the remaining addresses are assigned manually or using DHCP.

Alternative IP Assignment			
Host	IP Address	Subnet Mask	Gateway IP
Router	10.0.0.1	255.0.0.0	
Computer #1	10.0.0.2	255.0.0.0	10.0.0.1
Computer #2	10.0.0.3	255.0.0.0	10.0.0.1
Computer #3	10.0.0.4	255.0.0.0	10.0.0.1

**IP Setup - Example #2**

These two examples are only examples you can use to help you get started. If you are interested in more advanced information on how to use IP addressing on a LAN there are numerous resources freely available on the Internet. There are also many books and chapters of books on the subject of IP address assignment, IP networking and the TCP/IP protocol suite.



## IP Concepts

This appendix describes some basic IP concepts, the TCP/IP addressing scheme and show how to assign IP Addresses.

When setting up the Router, you must make sure it has a valid IP address. Even if you will not use the WAN port (ADSL port), you should, at the very least, make sure the Ethernet LAN port is assigned a valid IP address. This is required for telnet, in-band SNMP management, and related functions such as “trap” handling and TFTP firmware download.

### IP Addresses

The Internet Protocol (IP) was designed for routing data between network sites all over the world, and was later adapted for routing data between networks within any site (often referred to as “subnetworks” or “subnets”). IP includes a system by which a unique number can be assigned to each of the millions of networks and each of the computers on those networks. Such a number is called an IP address.

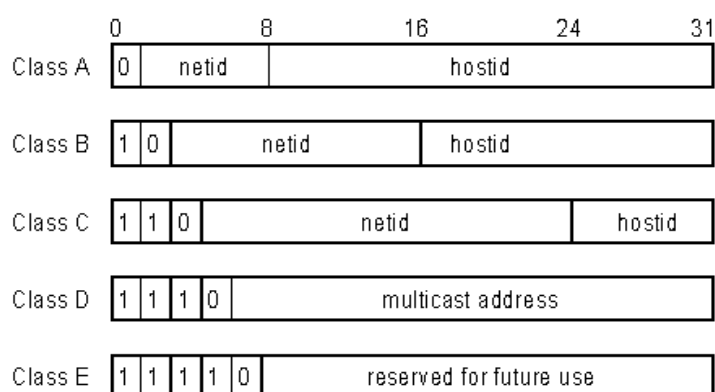
To make IP addresses easy to understand, the originators of IP adopted a system of representation called “dotted decimal” or “dotted quad” notation. Below are examples of IP addresses written in this format:

201.202.203.204      189.21.241.56      125.87.0.1

Each of the four values in an IP address is the ordinary decimal (base 10) representation of a value that a computer can handle using eight “bits” (binary digits – 1s and 0s). The dots are simply convenient visual separators.

Zeros are often used as placeholders in dotted decimal notation; 189.21.241.56 can therefore also appear as 189.021.241.056.

IP networks are divided into three classes on the basis of size. A full IP address contains a network portion and a “host” (device) portion. The network and host portions of the address are different lengths for different classes of networks, as shown in the table below.



Networks attached to the Internet are assigned class types that determine the maximum number of possible hosts per network. The previous figure illustrates how the net and host portions of the IP address differ among the three classes. Class A is assigned to networks that have more than 65,535 hosts; Class B is for networks that have 256 to 65534 hosts; Class C is for networks with less than 256 hosts.

IP Network Classes			
Class	Maximum Number of Networks in Class	Network Addresses (Host Portion in Parenthesis)	Maximum Number of Hosts per Network
A	126	1(.0.0.0) to 126(.0.0.0)	16,777,214
B	16,382	128.1(.0.0) to 191.254(.0.0)	65,534
C	2,097,150	192.0.1(.0) to 223.255.254(.0)	254

**Note:** All network addresses outside of these ranges (Class D and E) are either reserved or set aside for experimental networks or multicasting.

When an IP address's host portion contains only zero(s), the address identifies a network and not a host. No physical device may be given such an address.

The network portion must start with a value from 1 to 126 or from 128 to 223. Any other value(s) in the network portion may be from 0 to 255, except that in class B the network addresses 128.0.0.0 and 191.255.0.0 are reserved, and in class C the network addresses 192.0.0.0 and 223.255.255.0 are reserved.

The value(s) in the host portion of a physical device's IP address can be in the range of 0 through 255 as long as this portion is not all-0 or all-255. Values outside the range of 0 to 255 can never appear in an IP address (0 to 255 is the full range of integer values that can be expressed with eight bits).

The network portion must be the same for all the IP devices on a discrete physical network (a single Ethernet LAN, for example, or a WAN link). The host portion must be different for each IP device – or, to be more precise, each IP-capable port or interface – connected directly to that network.

The network portion of an IP address will be referred to in this manual as a **network number**; the host portion will be referred to as a **host number**.

To connect to the Internet or to any private IP network that uses an Internet-assigned network number, you must obtain a registered IP network number from an Internet-authorized network information center. In many countries you must apply through a government agency, however they can usually be obtained from your Internet Service Provider (ISP).

If your organization's networks are, and will always remain, a closed system with no connection to the Internet or to any other IP network, you can choose your own network numbers as long as they conform to the above rules.

If your networks are isolated from the Internet, e.g. only between your two branch offices, you can assign any IP Addresses to hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP Addresses specifically for private (stub) networks:

Class	Beginning Address	Ending Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

It is recommended that you choose private network IP Addresses from the above list. For more information on address assignment, refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

## Subnet Mask

In the absence of subnetworks, standard TCP/IP addressing may be used by specifying subnet masks as shown below.

IP Class	Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Subnet mask settings other than those listed above add significance to the interpretation of bits in the IP address. The bits of the subnet mask correspond directly to the bits of the IP address. Any bit in a subnet mask that is to correspond to a net ID bit in the IP address must be set to 1.

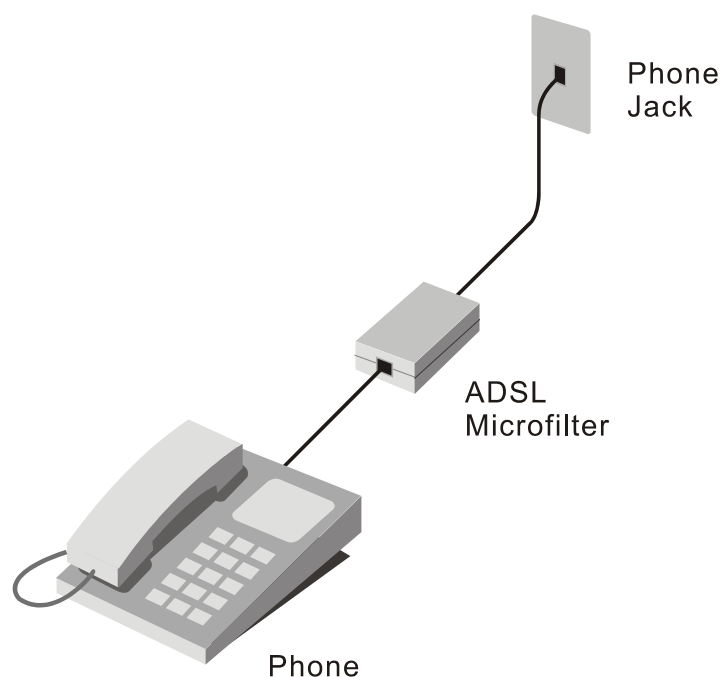
## Microfilters and Splitters

Most ADSL clients will be required to install a simple device that prevents the ADSL line from interfering with regular telephone services. These devices are commonly referred to as microfilters or sometimes called (inaccurately) line splitters. They are easy to install and use standard telephone connectors and cable.

Some ADSL service providers will send a telecommunications technician to modify the telephone line, usually at the point where the telephone line enters the building. If a technician has divided or split your telephone line into two separate lines - one for regular telephone service and the other for ADSL - then you do not need to use any type of filter device. Follow the instructions given to you by your ADSL service provider about where and how you should connect the Modem to the ADSL line.

### Microfilters

Unless you are instructed to use a "line splitter" (see below), it will be necessary to install a microfilter (low pass filter) device for each telephone or telephone device (answering machines, Faxes etc.) that share the line with the ADSL service. Microfilters are easy-to-install, in-line devices, which attach to the telephone cable between the telephone and wall jack. Microfilters that install behind the wall plate are also available. A typical in-line microfilter installation is shown in the diagram below.



Microfilter Installation

**Important:** Do not install the microfilter between the Modem and the telephone jack. Microfilters are only intended for use with regular telephones, Fax machines and other regular telephone devices.

## Line Splitter

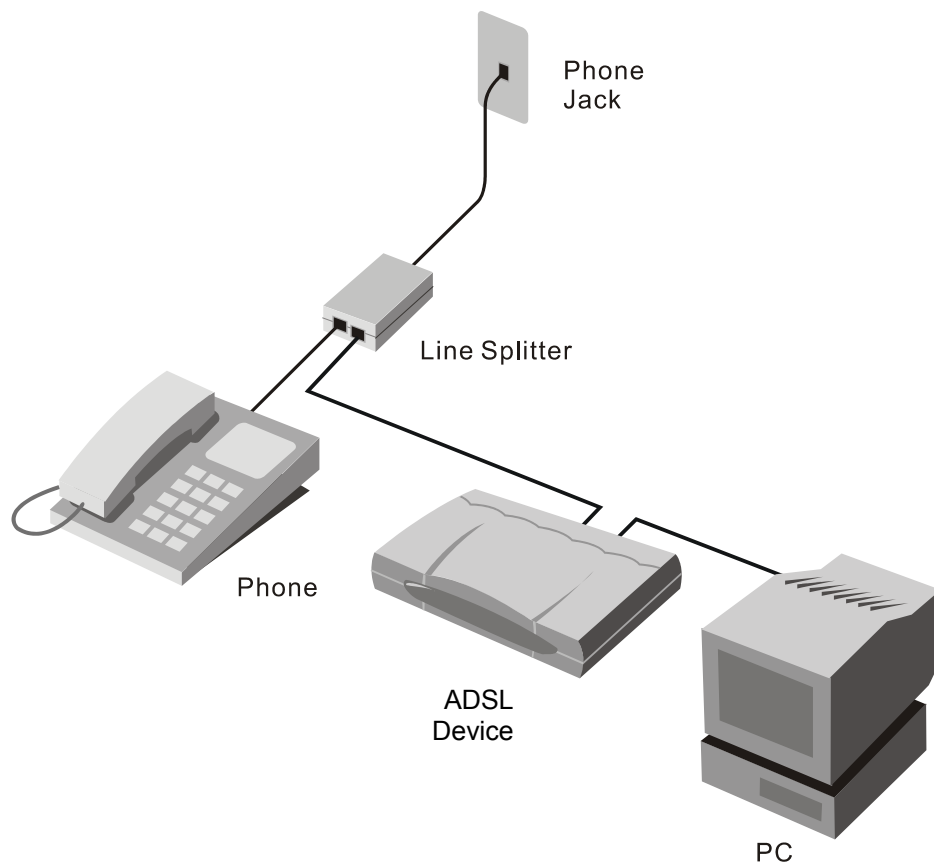
If you are instructed to use a “line splitter”, you must install the device between the Modem and the phone jack. Use standard telephone cable with standard RJ-11 connectors. The splitter has three RJ-11 ports used to connect to the wall jack, the Modem and if desired, a telephone or telephone device. The connection ports are typically labeled as follows:

**Line** - This port connects to the wall jack.

**ADSL** - This port connects to the Modem.

**Phone** - This port connects to a telephone or other telephone device.

The diagram below illustrates the proper use of the splitter.



**Line Splitter Installation**



## Licensing Information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License.

Please see The GNU General Public License for the exact terms and conditions of this license.

Specially, the following parts of this product are subject to the GNU GPL:

- The Linux operating system kernel
- The iptables packet filter and NAT software
- The udhcpd DHCP client/server implementation
- The pppd PPPoE/PPPoA client package
- The dproxy-nexgen DNS proxy package
- The bridge-utils Ethernet bridge package
- The mtd memory technology device for flash access
- The squashfs compressed read-only flash file system
- The utelnetd tiny telnet daemon
- The zlib compression library
- The libatm ATM access library
- The libopt utility library
- The uclibc C library
- The dhcp-forwarder DHCP relay package
- The net-tools network utilities package
- The thttpd HTTP server package
- The upnp uPNP device package

All listed software packages are copyright by their respective authors. Please see the source code for detailed information.

## Availability of source code

Conceptronic. has posed the full source code of the GPL licensed software, including any scripts to control compilation and installation of the object code. All future firmware updates will also be accompanied with their respective source code. For more information on how you can obtain our open source code, please visit our web site.



# GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
Temple Place, Suite 330, Boston, MA 02111-1307 USA  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-

readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### END OF TERMS AND CONDITIONS

#### How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

, 1 April 1989  
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.