SIEMENS

SANTIS ADSL 50/500

4 ETH & WLAN Router

User Manual

Rev:03_32

2003-02-24

Safety Notes

For Installation

- Use only the type of power source indicated on the marking labels.
- Use only the power adapter supplied with the product.
- Do not overload wall outlet or extension cords as this may increase the risk of electric shock or fire. If the power cord is frayed, replace it with a new one.
- Proper ventilation is necessary to prevent the product overheating. Do not block or cover the slots and openings on the device, which are intended for ventilation and proper operation. It is recommended to mount the product with a stack.
- Do not place the product near any source of heat or expose it to direct sunshine.
- Do not expose the product to moisture. Never spill any liquid on the product.
- Do not attempt to connect with any computer accessory or electronic product without instructions from qualified service personnel. This may result in risk of electronic shock or fire.
- Do not place this product on an unstable stand or table.

For Using

- Power off and unplug this product from the wall outlet when it is not in use or before cleaning. Pay attention to the temperature of the power adapter. The temperature might be high.
- After powering off the product, power on the product at least 15 seconds later.
- Do not block the ventilating openings of this product.
- When the product is expected to be not in use for a period of time, unplug the power cord of the product to prevent it from the damage of storm or sudden increases in rating.

For Service

Do not attempt to disassemble or open covers of this unit by yourself. Nor should you attempt to service the product yourself, which may void the user's authority to operate it. Contact qualified service personnel under the following conditions:

- If the power cord or plug is damaged or frayed.
- If liquid has been spilled into the product.
- If the product has been exposed to rain or water.
- If the product does not operate normally when the operating instructions are followed.
- If the product has been dropped or the cabinet has been damaged.
- If the product exhibits a distinct change in performance.

Warning

- This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Content

Before You Use

The SANTIS ADSL 50/500 is an Asymmetric Digital Subscriber Line (ADSL) Router. With the asymmetric technology, this device runs over standard copper phone lines. In addition, ADSL allows you to have both voice and data services in use simultaneously all over one phone line.

The SANTIS ADSL 50/500 is designed to offer cost-effective high-speed services for home or office users. It provides a downstream rate of up to 8 Mbps and upstream rate of up to 1 Mbps for ADSL connection, even offers auto-negotiation capability for different flavors (ANSI T1.413 Issue 2, G.lite, G.dmt for Annex A, G.dmt for Annex B or G.hs) according to central office DSLAM's settings (Digital Subscriber Line Access Multiplexer). Also the feature-rich routing functions are seamlessly integrated to ADSL service for existing corporate or home users. Now users can enjoy various bandwidth-consuming applications via the SANTIS ADSL Router.

Features

ADSL Compliance

- ANSI T1.413 Issue 2
- ITU G.992.2 Annex A (G.lite)
- ITU G.992.1 Annex A (G.dmt)
- ITU G.992.1 Annex B (G.dmt)
- ITU G.994.1 (G.hs)

Wireless LAN Features

- Fully compatible to IEEE 802.11b standard and allow operating range up to 300 meters (open space) and 100 meters (indoor).
- The Direct Sequence Spread Spectrum (DSSS) technology is exploited.
- Seamless roaming within the 802.11 and 802.11b wireless LAN infrastructure
- Low power consumption via efficient power management
- Support the Association Control function: Only registered wireless clients can be allowed to associate to wireless ADSL router.

ATM Features

- Compliant to ATM Forum UNI 3.1 / 4.0 Permanent Virtual Circuits (PVCs)
- Support up to 8 AAL5 Virtual Circuit Channels (VCCs) for UBR, CBR, VBR-rt, and VBR-nrt with traffic shaping
- TR-037 Auto PVC (auto-provisioning)
- RFC1483 (RFC2684) LLC Encapsulation and VC Multiplexing over AAL5
- RFC2364 Point-to-Point Protocol (PPP) over AAL5
- RFC2225 Classical IP and ARP over ATM
- RFC2516 PPP over Ethernet: support Relay (Transparent Forwarding) and Client functions
- OAM F4/F5 End-to-End/Segment Loopback Cells

Bridging Features

- Supports self-learning bridge specified in IEEE 802.1D Transparent Bridging
- Supports up to 4000 learning MAC addresses
- Transparent bridging among 10/100 Mb Ethernet and 802.11b Wireless LAN interfaces

Routing Features

- UPnP IGD (Internet Gateway Device) with NAT traversal capability support

- NAT (Network Address Translation) / PAT (Port Address Translation) let multiple users on the LAN to access the internet for the cost of only one IP address and enjoy various multimedia applications.
- ALGs (Application Level Gateways): such as NetMeeting, FTP, Quick Time, mIRC, Real Player, CuSeeMe, etc.
- Multiple Virtual Servers (e.g., Web, FTP, Mail servers) can be setup on user's local network.
- Static routes, RFC1058 RIPv1, RFC1723 RIPv2.
- DNS Relay and DNS Server
- ARP Proxy

Security Features

- PAP (RFC1334), CHAP (RFC1994) for PPP session
- Firewall support IP packets filtering based on IP address/Port number/Protocol type and TCP code field flags
- Intrusion Detection provides protection from a number of attacks (such as SYN/FIN/RST Flood, Smurf, WinNuke, Echo Scan, Xmas Tree Scan, etc)
- WEP (Wired Equivalent Privacy) encryption uses RC4 with 64/128 bit key length

Configuration and Management

- User-friendly embedded web configuration interface with password protection
- Remote management accesses control
- Telnet session for local or remote management
- HTTP firmware upgrades via web browser GUI directly
- Distribute IP addresses to end users via DHCP server provided by ADSL router
- SNMPv1/v2c agent with MIB-II, PPP MIB, ADSL Line MIB.

System Requirements

For using this, you have to make sure you have the following that installed on the clients:

For Wireless Clients

- Operating System must be Windows 98 SE/ME/2000/XP
- Wireless LAN PC card
- Wireless LAN PC card driver

For Ethernet Clients

- Operating System must be Windows /98 SE/ME/NT/2000/XP
- 10/100 Base-T NIC
- 10/100 Base-T (UTP) network cable

Unpacking

Check the contents of the package against the pack contents checklist below. If any of the items is missing, then contact the dealer from whom the equipment was purchased.

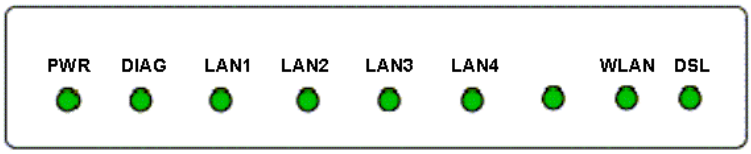
- ADSL Router
- Power Adapter and Cord
- RJ-11 ADSL Line Cable
- RJ-45 Ethernet Cable
- CDROM with Quick Start Guide / user manual

Chapter 1: Overview

Physical Outlook

Front Panel

The following illustration shows the front panel of the ADSL Router:



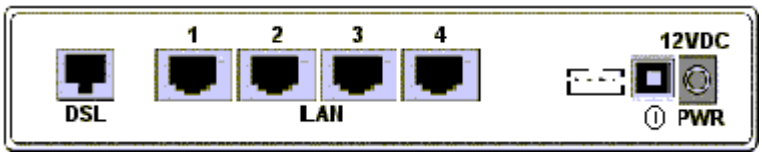
LED Indicators (Front Panel System Messages)

The ADSL Router is equipped with LEDs on the front panel as described in the table below (from left to right):

LED	Color	Status	Description
PWR	Green	OFF	Power off.
		ON	Power on.
DIAG	Green	OFF	Power off or initial self-test of the unit is OK.
		Blinking	When software downloading or updating operation parameters located in FLASH memory is in progress.
		ON	Initial self-test failure or programming FLASH memory failure.
LAN1 to LAN4	Green	OFF	Power off or no Ethernet carrier is present.
		Blinking	Ethernet carrier is present and user data is going through Ethernet port.
		ON	Ethernet carrier is present.
WLAN	Green	OFF	Power off or no radio signal (WLAN card is not present or fails to function).
		Blinking	Traffic is going through Wireless LAN interface.
		ON	Wireless LAN interface ready to work.
DSL	Green	OFF	Power off or ADSL line connection is handshaking or training is in progress.
		Blinking	User data is going through ADSL port.
		ON	ADSL line connection is OK.

Rear Panel

The following figure illustrates the rear panel of your ADSL Router.



DSL:	RJ-11 connector
LAN 1 - 4:	Ethernet RJ-45 connector
Console:	Console connector
⏻**:**	Power switch
12VDC:	Power connector

Note:
The Router incorporates a four-port switch for connection to your local Ethernet network. The Ethernet ports are marked LOCAL, and are capable of operation at either 10 Mbps (10 BASE-T) or 100 Mbps (100 BASE-Tx).

Chapter 2: Installation

Choosing a place for the ADSL Router

1. Place the ADSL Router close to ADSL wall outlet and power outlet for the cable to reach it easily.
2. Avoid placing the device in places where people may walk on the cables. Also keep it away from direct sunshine or heat sources.
3. Place the device on a flat and stable stand.

Connecting the ADSL Router

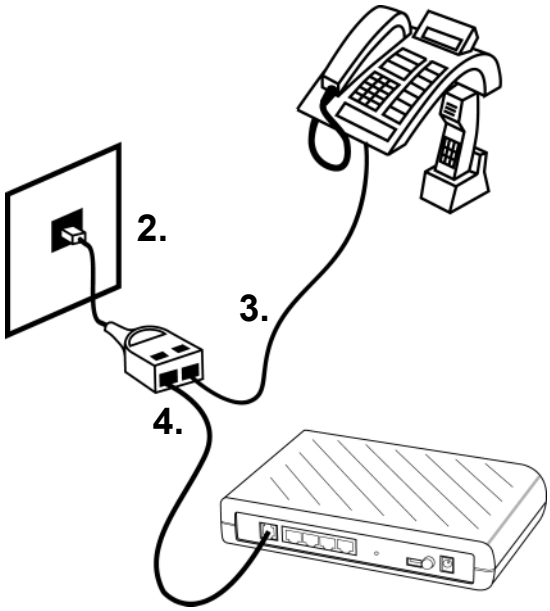
Follow the steps below to connect the related devices.

Note:
For ADSL standard, a PSTN Microfilter or an ISDN Splitter is necessary on subscriber's premise to keep the telephone and ADSL signals separated, giving them the capability to provide simultaneous Internet access and telephone service on the same line.

1a) Analog (PSTN) installation
If your telephone service is analog (SANTIS ADSL 50), proceed as follows to install your Hardware: Remove the end of the phone line from your phone connector and plug it into the "LINE" plug of the PSTN Microfilter. Use another phone line to connect your phone and Microfilter. Plug this phone line into the "PHONE" plug of the ADSL Microfilter, and plug the other end of the line onto your phone.

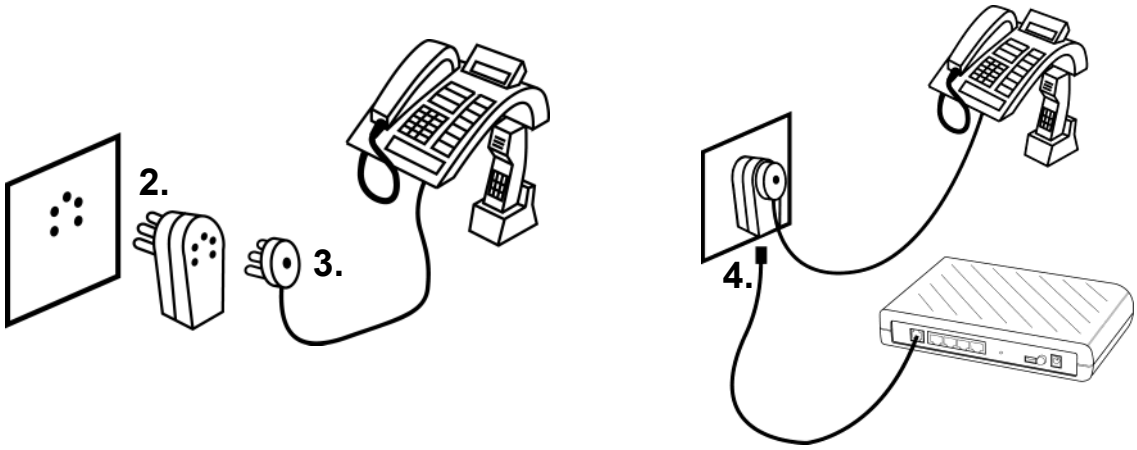
Y-Line Filters:

1. Unplug the device's cord from the phone jack.
2. Plug the Y-Line Filter into the phone jack.
3. Plug the phone cord (or other device cord) into the "PHONE" jack of your Y-Line Filter.
4. Plug the ADSL cord into the "ADSL" jack of your Y-Line Filter.



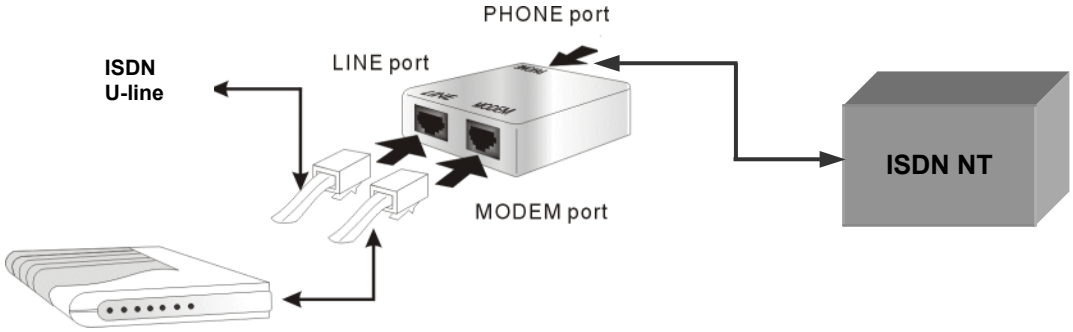
Belgium-Line Filters:

1. Unplug the device's cord from the phone jack.
2. Plug the Belgium-Line Filter into the phone jack.
3. Plug the phone cord (or other device cord) into the "PHONE" jack of your Belgium-Line Filter.
4. Plug the ADSL cord into the "ADSL" jack of your Belgium-Line Filter.



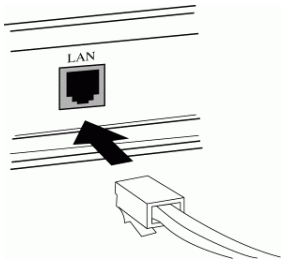
1b) ISDN installation

If your telephone service is ISDN (SANTIS ADSL 500), proceed as follows to install your Hardware:
Remove the U-Line (incoming line) form your ISDN NT and plug it into the "LINE" plug of the ISDN Splitter. Use another phone line to connect your ISDN NT with your ISDN Splitter. Plug this phone line onto the "PHONE" plug of the ADSL splitter, and plug the other end of the line into the U-Line plug of your ISDN NT.

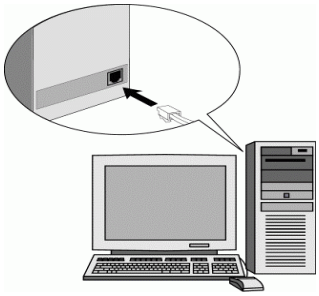


2) Use the line to connect the ADSL Microfilter or Splitter and your ADSL LAN port.

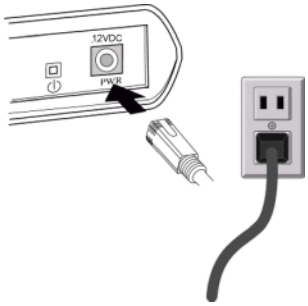
3) Please attach one end of the Ethernet cable with RJ-45 connector to the **LAN** port of your ADSL Router.



4) Connect the other end of the cable to the Ethernet port of the client PC.



5) Connect the supplied power adapter to the **PWR** port of your ADSL Router, and plug the other end to a power outlet.



6) Turn on the power switch.

Chapter 3: Configuration

In order to access the Internet through the router, you must check the TCP/IP settings before configuring the router.

Step 1: Configure TCP/IP on Client PC

To access the ADSL Router via Ethernet, the host computer must meet the following requirements:

- With Ethernet network interface.
- Must have TCP/IP protocol installed.
- Set client PC with obtain an IP address automatically.
- With a web browser installed: Internet Explorer 5.x or later.

The ADSL Router is configured with the **default IP address of 192.168.1.1** and subnet mask of **255.255.255.0. As t**he **DHCP server is Enabled by default,** the DHCP clients should be able to access the ADSL Router. **Or** you could assign an IP address to the host PC first for initial configuration.

You also can manage the ADSL Router through a web browser-based manager: **ADSL ROUTER CONTROL PANEL**. The ADSL Router manager uses the HTTP protocol via a web browser to allow you to set up and manage the device.

To configure the device via web browser, at least one properly configured PC must be connected to the network (either connected directly or through an external hub/switch to the LAN port of the device).

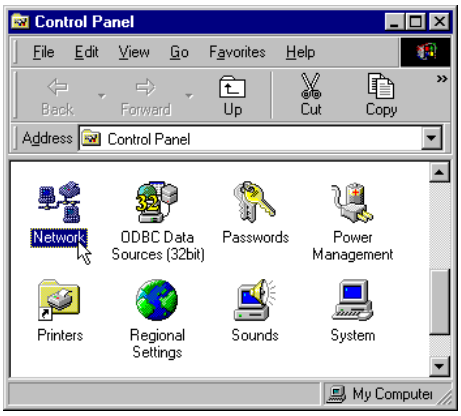
If TCP/IP is not already installed, follow the steps below for installation.

For Windows 98 SE

Note:
Windows 98 SE users need the **Windows 98 SE installation CD-ROM** to complete the installation!

1. Click on the **Start** menu, point to **Settings** and click on **Control Panel**.

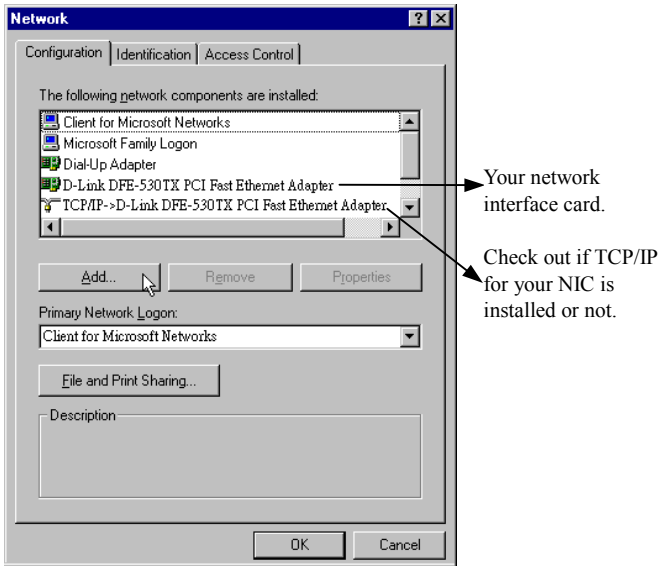
2. Double-click the **Network** icon.



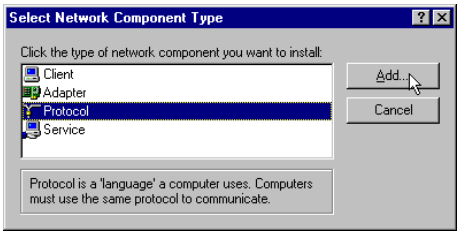
3. The **Network** window appears. On the **Configuration** tab, check out the list of installed network components.

   Option 1: If you have **no** TCP/IP protocol, click **Add**.

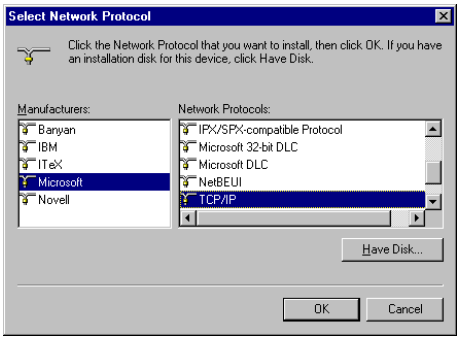
   Option 2: If you have TCP/IP protocol, go to Step 6.



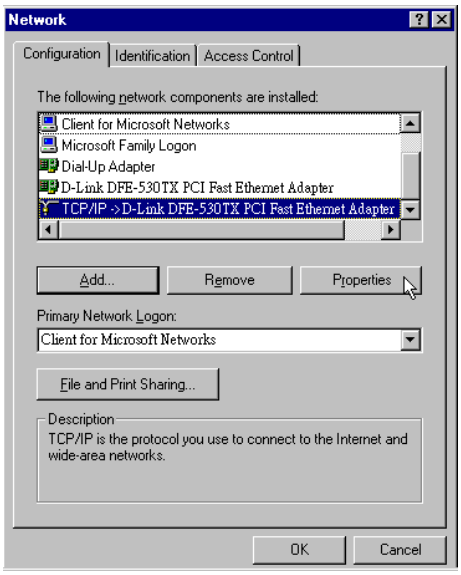
4. Highlight **Protocol** and click **Add**.



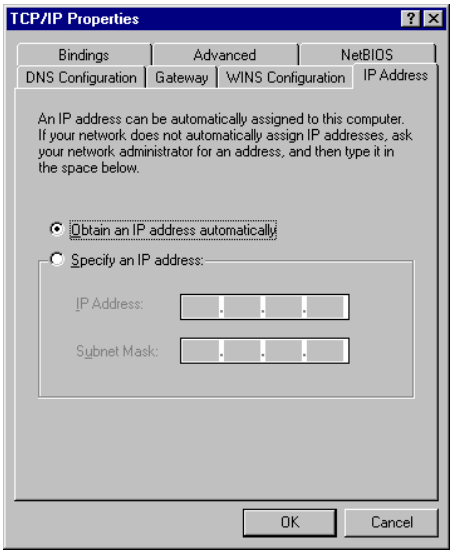
5. On the left side of the windows, highlight **Microsoft** and then select **TCP/IP** on the right side. Then click **OK**.



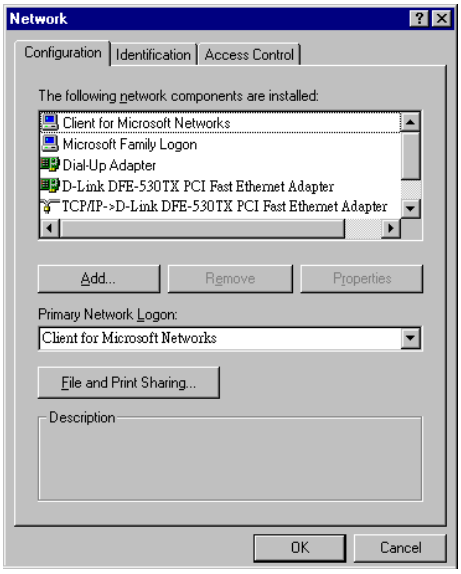
6. When returning to **Network** window, highlight **TCP/IP** protocol for your NIC and click **Properties**.



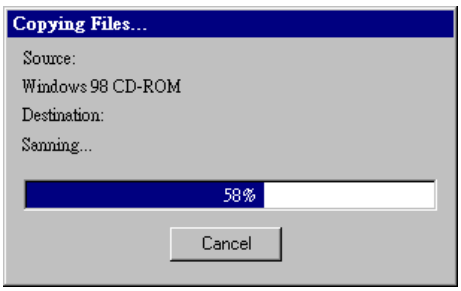
7. On **IP Address** tab:
   Select **Obtain an IP address automatically**. Then click **OK**.



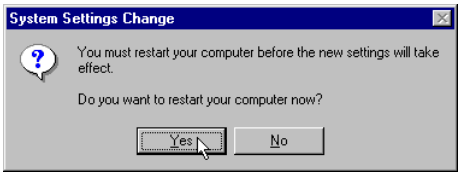
8. When returning to **Network** window, click **OK**.



9. Wait for Windows copying files.



10. When prompted with **System Settings Change** dialog box, click **Yes** to restart your computer.

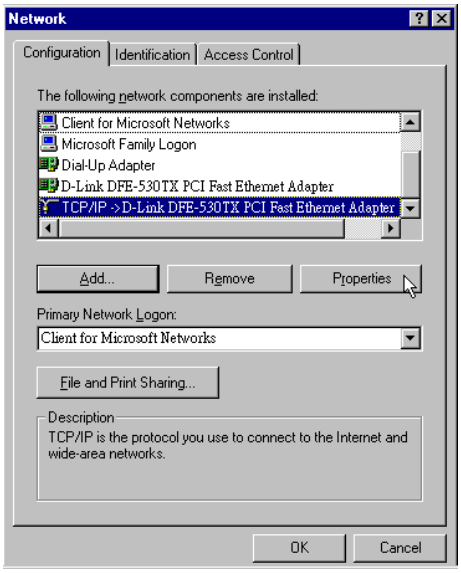


For Windows ME

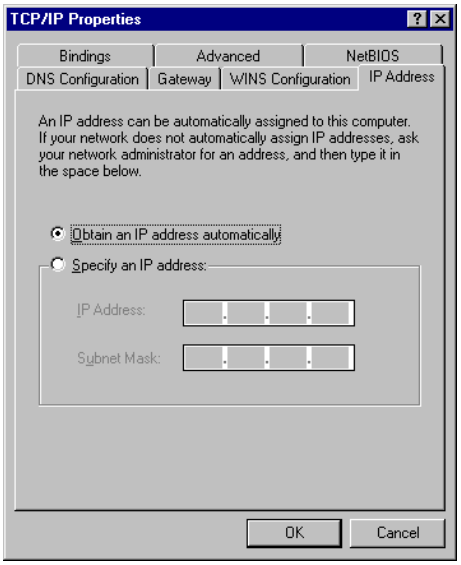
1. Click on the **Start** menu, point to **Settings** and click on **Control Panel**.
2. Double-click the Network icon.
3. Step 3 The Network window appears. On the Configuration tab, check out the list of installed network components.

   Option 1: If you have **no** TCP/IP protocol, click **Add**.

   Option 2: If you have TCP/IP protocol, go to Step 6.
4. Highlight Protocol and click **Add**.
5. On the left side of the windows, highlight Microsoft and then select TCP/IP on the right side. Then click **OK**.
6. While returning to Network window, highlight TCP/IP protocol for your NIC and click Properties.



7. On the IP Address tab, select Obtain an IP address automatically. Then click **OK**.

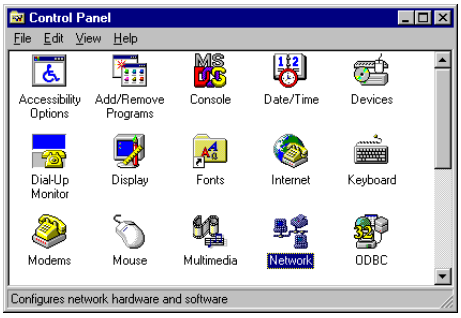


8. While returning to the Network window, click **OK**.
9. Wait for Windows copying files.
10. When prompted with the System Settings Change dialog box, click **Yes** to restart your computer.

For Windows NT

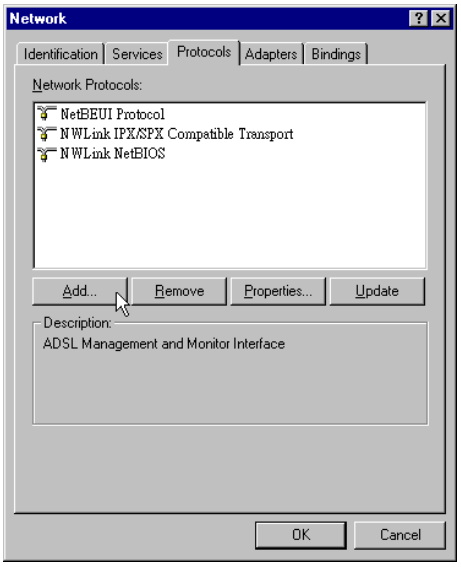
1. Click **Start**, point to **Settings**, and then click **Control Panel**.

2. Double-click the **Network** icon.

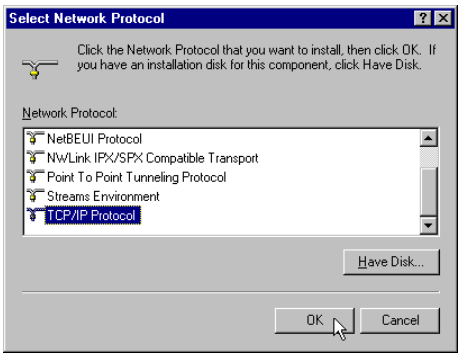


3. The **Network** window appears. On the **Protocols** tab, check out the list of installed network components.
   Option 1: If you have **no** TCP/IP Protocol, click **Add**.

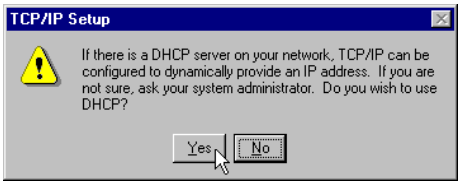
   Option 2: If you have TCP/IP Protocol installed, go to Step 7.



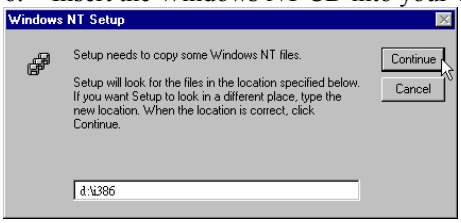
4. Highlight **TCP/IP Protocol** and click **OK**.



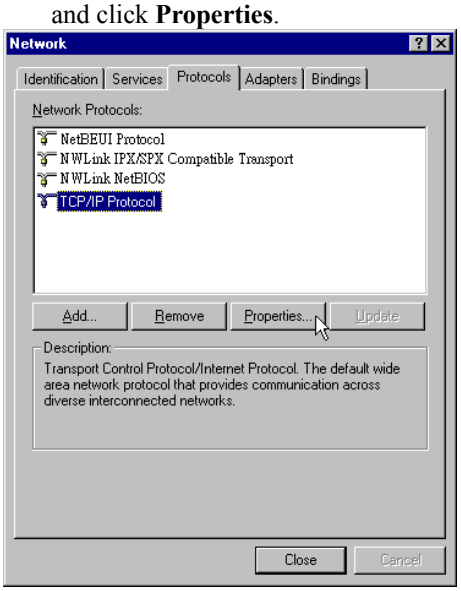
5. Click **Yes** to use DHCP.



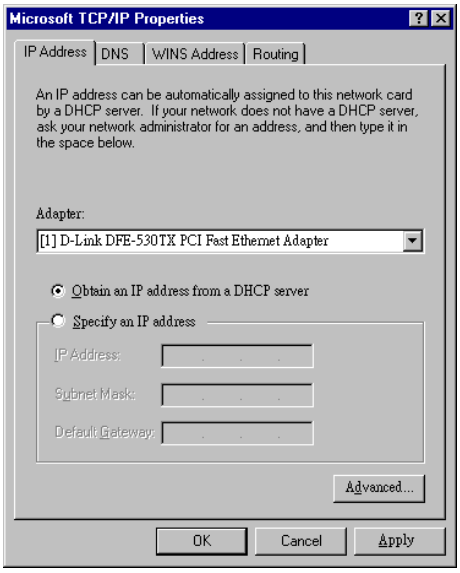
6. Insert the Windows NT CD into your CD-ROM drive and type the location of the CD. Then click **Continue**.



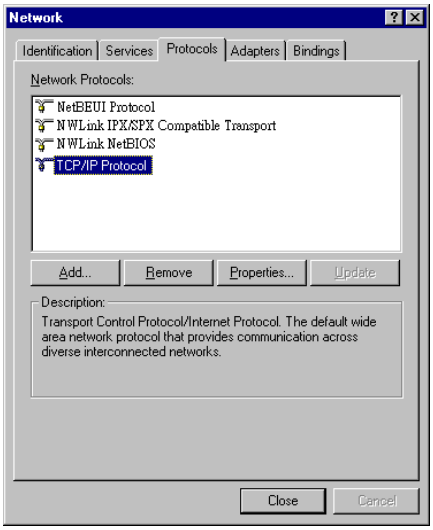
7. Returning to the **Network** window, you will find the **TCP/IP Protocol** among the list. Select **TCP/IP Protocol** and click **Properties**.



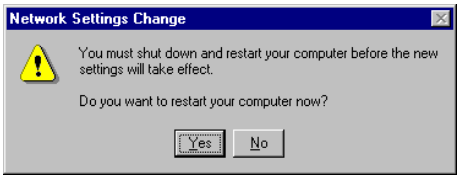
8. Select **Obtain an IP address from a DHCP server**. Then click **OK**.



9. When returning to **Network** window, click **Close**.

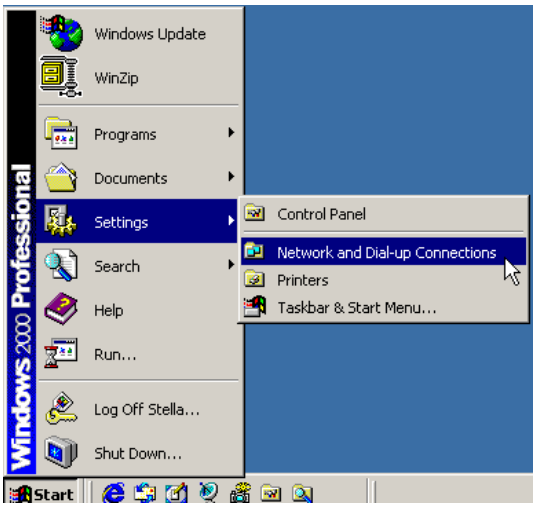


10. When prompted with **Network Settings Change** dialog box, click **Yes** to restart your computer.

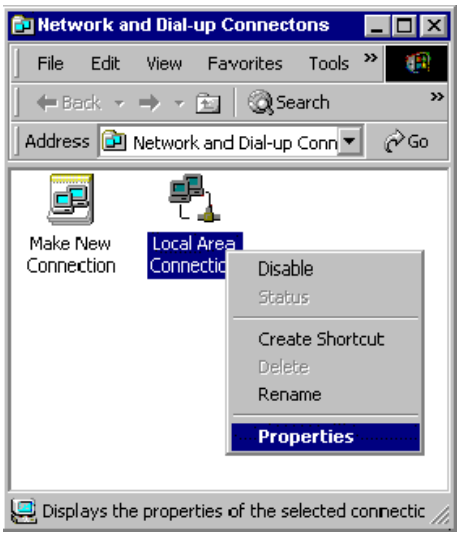


For Windows 2000

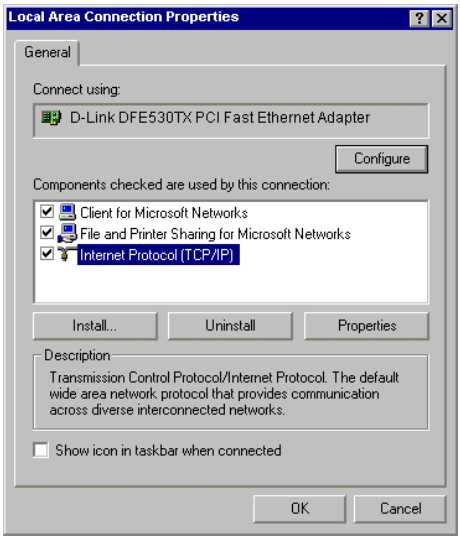
1. From the Start menu, point to Settings and then click Network and Dial-up Connections.



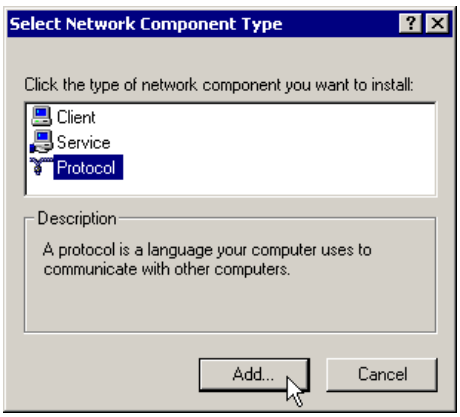
2. Right-click the **Local Area Connection** icon and then click **Properties**.



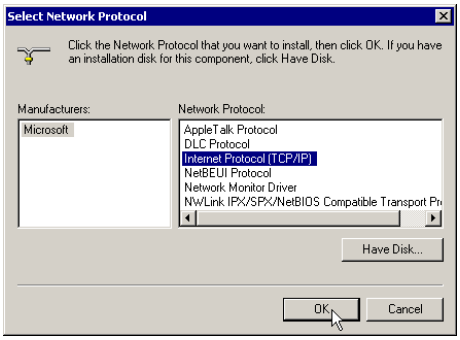
3. On the **General** tab, check out the list of installed network components.
   Option 1: If you have **no** TCP/IP Protocol, click **Install**.
   Option 2: If you have TCP/IP Protocol, go to Step 6.



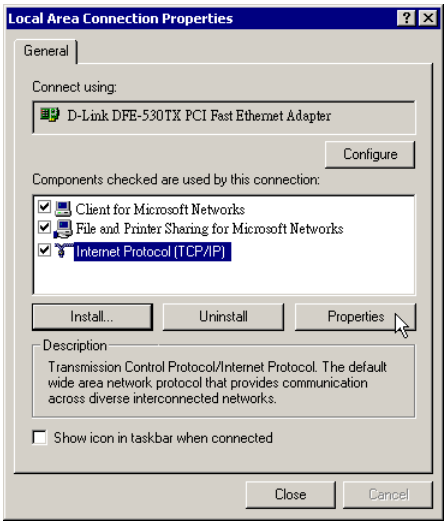
4. Highlight **Protocol** and then click **Add**.



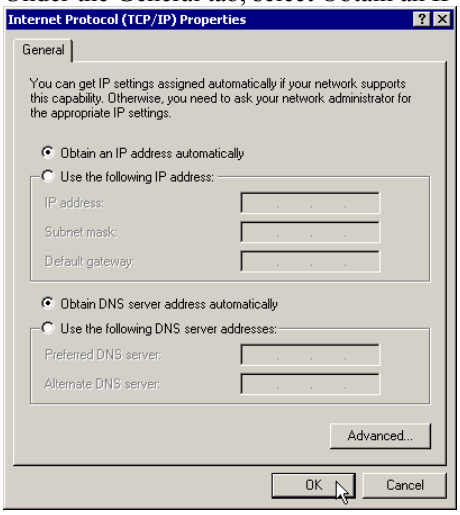
5. Click Internet Protocol(TCP/IP) and then click OK.



6. When returning to Local Area Connection Properties window, highlight Internet Protocol (TCP/IP) and then click Properties.



7. Under the General tab, select Obtain an IP address automatically. Then click OK.



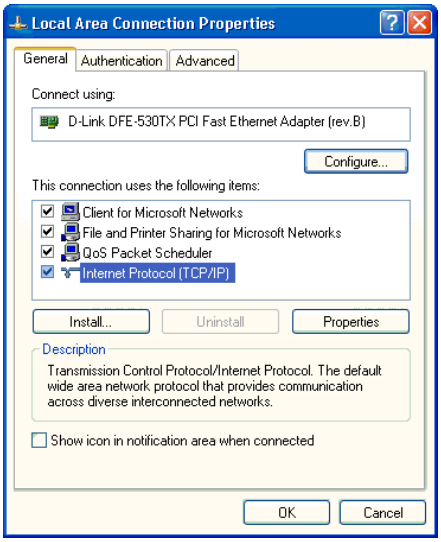
8. When prompted to restart your computer, reboot it to enable the settings.

For Windows XP

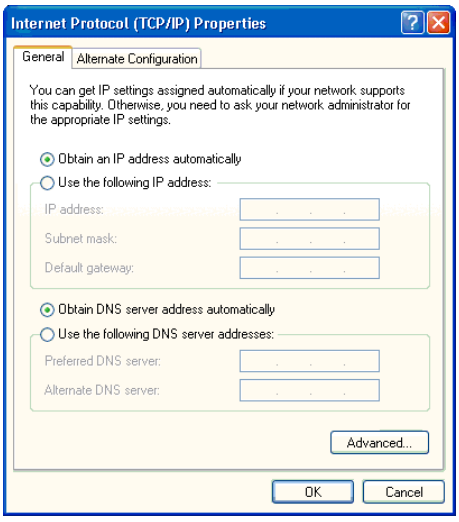
1. From the **Start** menu, point to **Control Panel** and then click **Network and Internet Connections**.
2. Click Network Connection and then click **Properties**.
3. On the General tab, check out the list of installed network components.

   Option 1: If you have **no** TCP/IP Protocol, click **Install**.

   Option 2: If you have TCP/IP Protocol, go to Step 6.
4. Highlight **Protocol** and then click **Add**.
5. Click Internet Protocol(TCP/IP) and then click **OK**.
6. On the Local Area Connection Properties window, highlight Internet Protocol (TCP/IP) and then click **Properties**.



7. Under the General tab, enable **Obtain an IP address automatically**. Then click **OK**.



8. When prompted to restart your computer, reboot it to enable the settings.

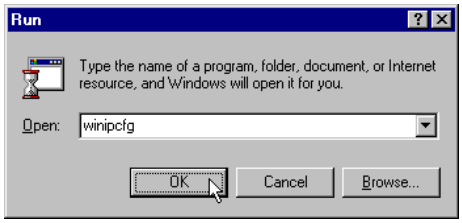
Renew IP Address on Client PC

There is a chance that your PC does not renew its IP address after the ADSL Router is on line and the PC cannot access the Internet. Please follow the procedures below to renew PC's IP address.

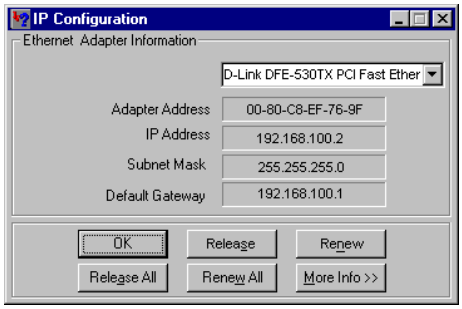
For Windows 98 SE

1. Select **Run** from the **Start** menu.

2. Type **winipcfg** in the dialog box and the click **OK**.

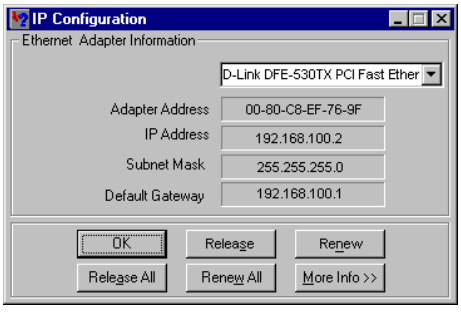


3. When the figure below appears, click **Release** and then **Renew** to get an IP address.



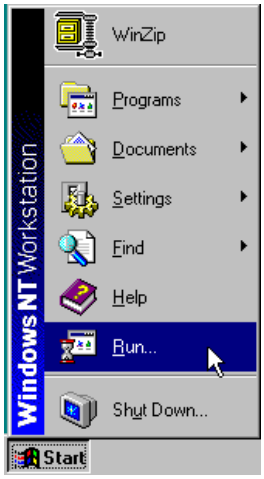
For Windows ME

1. Select **Run** from the **Start** menu.
2. Type **winipcfg** in the dialog box and the click **OK**.
3. When the figure below appears, click **Release** and then **Renew** to get an IP address.



For Windows NT

1. Select **Run** from the **Start** menu.



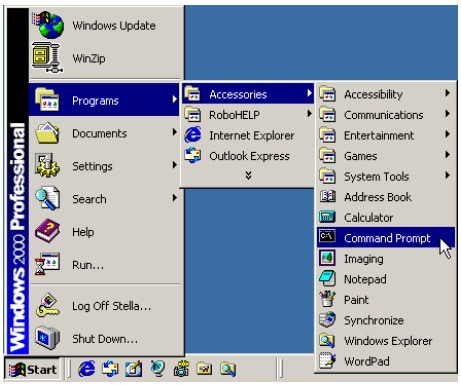
2. Type **cmd** in the dialog box and the click **OK**.

3. Type **ipconfig** at prompt. Then you will see the IP information from DHCP server.

4. If you want to get a new IP address, type **ipconfig /release** to release the previous IP address and then type **ipconfig /renew** to get a new one.

For Windows 2000

1. From the **Start** menu, point to **Programs**, **Accessories** and then click **Command Prompt**.



2. Type **`ipconfig`** at prompt. Then you will see the IP information from DHCP server.
3. If you want to get a new IP address, type **`ipconfig /release`** to release the previous IP address and then type **`ipconfig /renew`** to get a new one.

For Windows XP

1. From the **Start** menu, point to **Programs**, **Accessories** and then click **Command Prompt**.
2. Type **`ipconfig`** at prompt. Then you will see the IP information from DHCP server.
3. If you want to get a new IP address, type **`ipconfig /release`** to release the previous IP address and then type **`ipconfig /renew`** to get a new one.

Securing your wireless network

Using radio waves, a wireless network introduces some security risks which are not present in a wired network; an unauthorized third party can intercept transmitted data, gain access to your wireless network, … In order to make your wireless network as secure as a wired network you should apply, at least, the following guidelines:

Change the SSID

Your wireless network is identified on the basis of an SSID (Service Set Identifier). This parameter, which can be considered as the network name, is broadcasted periodically through a beacon. Also the SSID is, in most cases, set default to a well-known value. To improve the security you can:

1. Disable the SSID broadcast. Users who want to connect to your wireless network must know this value to become connected. Also, your wireless network becomes invisible to a third party.
2. Change the default value of the SSID. The SSID can contain maximal 32 characters and it's best to choose a value, which is not too obvious.

Activate WEP

To guarantee that your data is transmitted in a private manner, you should activate WEP (Wired Equivalent Privacy). Use of this protocol will result in your data being encrypted while traveling through the air. Choose the largest encryption key possible (in most cases this is 128 bits) and make sure that each PC on your wireless network uses the same key as the access point.

You can even improve the security by changing the WEP-key on a regular base.

Activate MAC-address control list

By means of the MAC-address list, also known as the Association Control List, you can determine which client adapters can access your wireless network. This is done by introducing the MAC-address of the client adapter in the concerned list of the access point. A MAC address consists of 12 characters (0-9,A-F) and can be found on the back of the client adapter. A client adapter whose MAC address is not included in the list will not be granted access to your wireless network.

Change / activate passwords

Configuration of the access point is done through a web browser. Secure this access, and any other access, which may exist, by a carefully chosen password. If a default password, set by the manufacturer, is used, you should replace this by your own password.

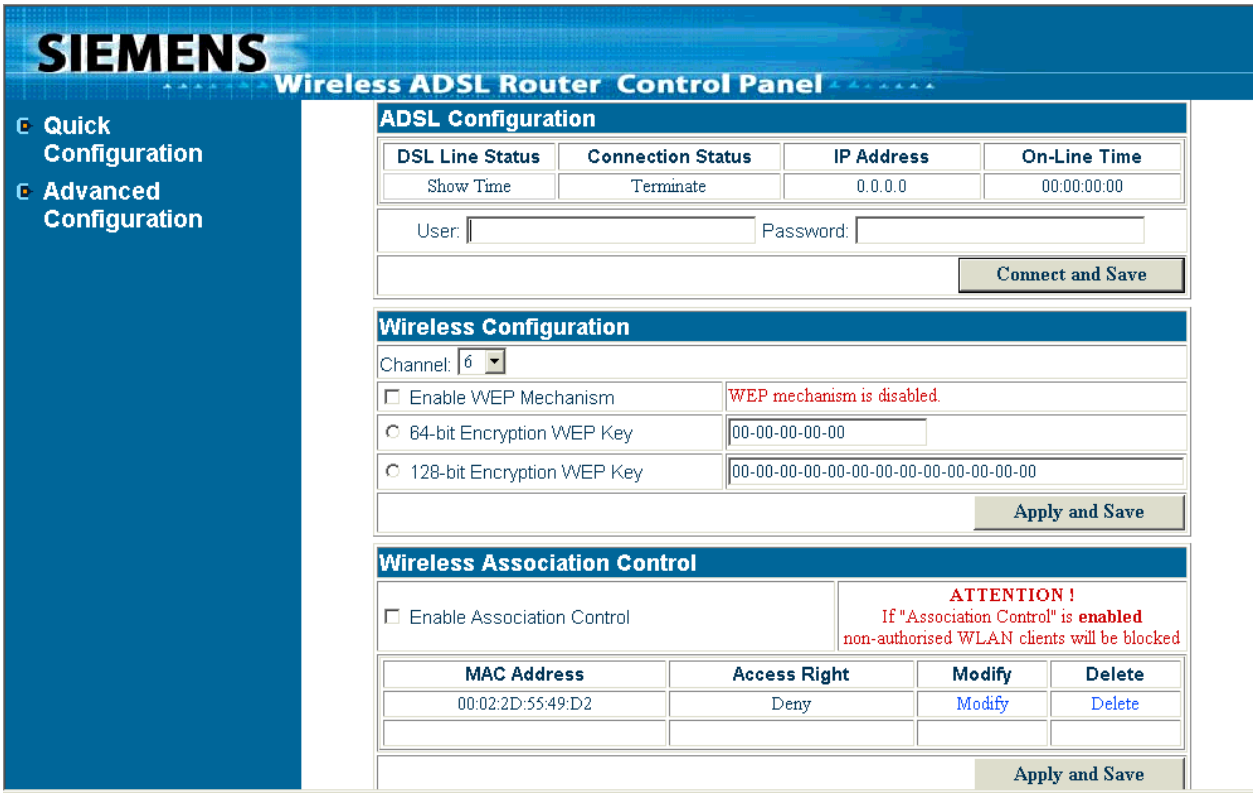
Step 2: Quick Configuration via web browser

Note:
For security reasons it is very important that you follow carefully the instructions in paragraphs **Wireless Configuration** and **Wireless Security** below!

Once your host PC is properly configured, please proceed as follows:

Start your web browser and type **192.168.1.1** in the address field of your browser. **Press Enter.**

After connecting to the device, the 'Quick Configuration' page will be displayed:



Internet Access Configuration

1. Enter 'User Name' and 'Password' of your Internet Service Provider.
2. Click to 'Connect and Save'.
3. Username and Password will automatically be saved and the status of the Internet connection will be prompted.

Wireless Configuration (WEP encryption)

Note:
For the WEP key the following digits and letters can be used: 0 – 9, a or A, b or B, c or C, d or D, e or E and f or F

1. Choose the Wireless channel (we recommend to use channel 6).
2. Choose if WEP encryption should be enabled or not. If the WEP encryption is turned on, transferred user data trough wireless LAN will be encrypted.
3. If WEP is enabled, choose if 64-bit encryption or 128-bit encryption (higher security level) should be used.
4. Type in a WEP key. Use digits from 0 – 9 and letters from a (A) to f (F) (e.g. 1a-01-d2-8c-3b).
5. Click to 'Apply and Save'.

Wireless Security (Association Control)

With 'Association control' you can decide which wireless clients have authorization to connect to your access point. This means that you can prevent that unauthorized people have access to your Internet connection.

If any wireless client is listed in the Association Control list proceed as follows:

1. Decide if the listed wireless LAN client is authorized to have access.
2. If yes, click to modify and change the status from 'Deny' to 'Allow'.
3. Click to 'Apply and Save'.
4. If more than one wireless LAN client is listed proceed with step 1
5. To enable 'Association Control' activate the checkbox and click to 'Apply and Save'

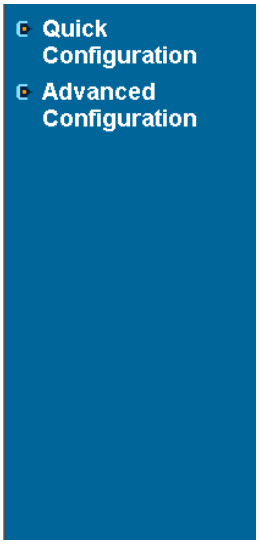
Note:
Association Control' has to be enabled in order that non-authorized wireless LAN clients are blocked!

Advanced Configuration via web browser

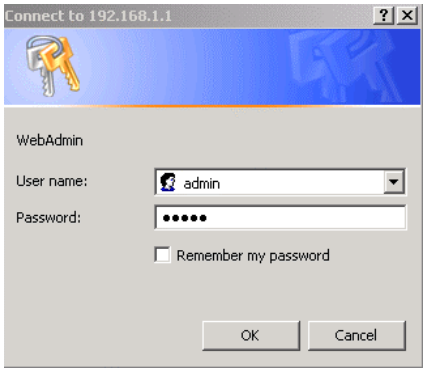
Note:
Please follow carefully the instructions in the whole chapter in order to be sure that your PC and your ADSL router are working properly.

Access to the Advanced Configuration

1. For advanced configuration click to 'Advanced Configuration'



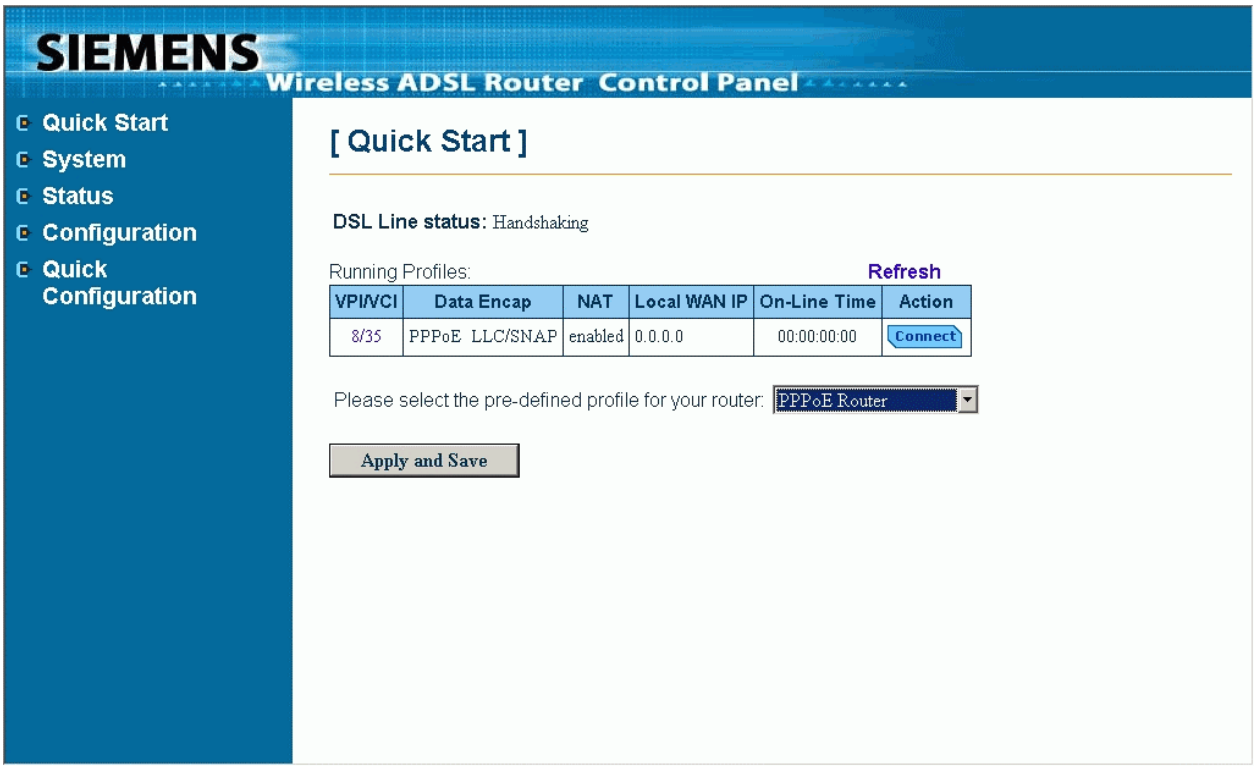
2. You will be prompted to enter username and password. By default, the username is **admin** and the password is **admin**.



If you login successfully, the main page of the **ADSL ROUTER CONTROL PANEL** appears. From now on the ADSL Router acts as a web server sending HTML pages/forms on your request. You can fill in these pages/forms and apply them to the ADSL Router.

Menus of the Advanced Configuration

The home page is composed of some areas:



- **Main Menu**: Includes Quick start, System, Status, Configuration and Home User

  Quick Start: Allows you to select some pre-defined profile to have basic configuration.

  System: The system menu includes the sub-menus of Device Info, Administration, Save Configuration, Upgrade Firmware and Reset Router.

  Status: Displays the current status of the ADSL Router, including DSL Connection, WAN Connection, Traffic Counter, Routing Table, DHCP Table and Wireless Client.

  Configuration: It displays the configuration categories of the ADSL Router, including DSL, LAN, WLAN, WAN, IP Route, DNS, Security, Virtual Server and UPnP settings.

  Quick Configuration: Allows you to go back to the 'Quick Configuration' page.

  You can move the mouse cursor over the sub-menu to display the hierarchy popup menu. Clicking on each of the item will bring out its content in main window accordingly.

- **Main Window**: It is the current workspace of the web management, containing configuration or status information.

To Have the New Settings Take Effect

The ADSL Router uses the following mechanism to enable new settings:

- **Apply** button.

  When **Apply** is clicked, your customizations will only be stored to the DRAM. If you do not execute **Save** & **Restart**, the customizations will not take effect for rebooting the ADSL Router next time.

- **Apply & Save** button.

  When **Apply & Save** is clicked, your customizations will be saved to the flash memory and immediately take effect.

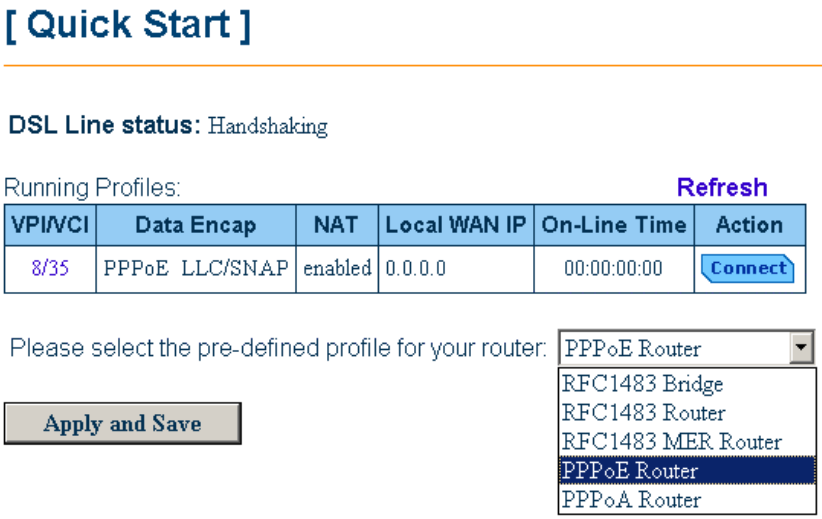
- **Save & Restart** button.

  When **Save** is clicked, your customizations will be saved to the flash memory. After clicking **Restart**, your customizations take effect.

Advanced Features

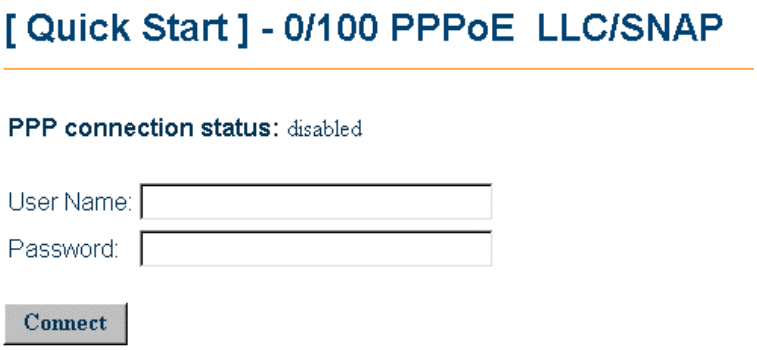
Quick start

On this page you can see some pre-defined connection services. Select that you want to be used connection mode and execute the **Apply and Save** to change and save configuration.



This application provides some pre-defined profile for you to select for the router. Please use the drop-down menu to the right side and select PPPoE for ADSL. Then click on Apply and Save to show the selected profile data.

Click on the **Connect** button to choose the one to be connected to your ISP. Enter the **Username** and **Password** provide by ISP and then click the **connect** button.

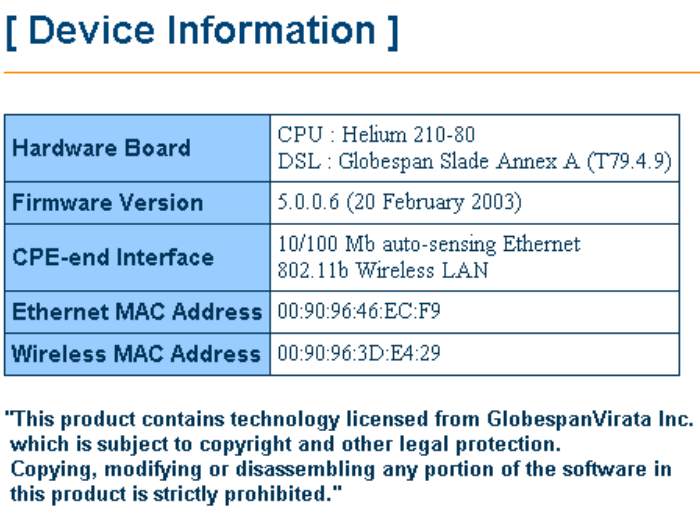


If you want block the connection, just click the **Action** mode—**Disconnect** button. If you choose any one of RFC series profiles, there is no Connect button on the Action mode. In addition, you can click on the item below **VPI/VCI** to show/modify the more detail configurations.

System

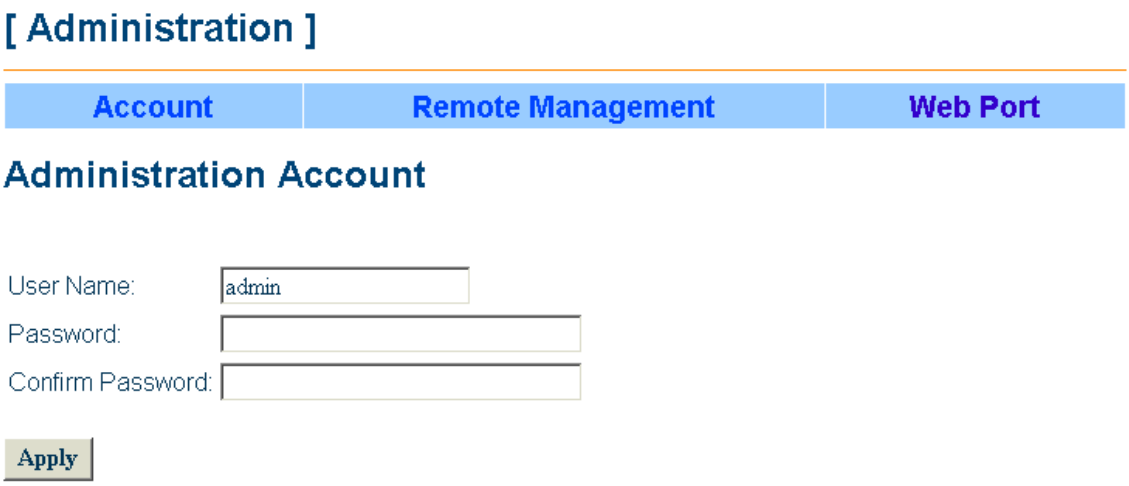
Device Information

This page shows the basic information of your ADSL Router, including the hardware board and software version, etc. It provides a general overview of your ADSL Router.



Administration

There are three types of administration, Account, Remote Access and Web Port.



Account

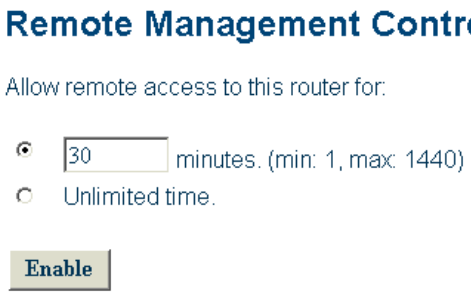
It limits this web-based manager access to users with the correct user name and password. After entering user name & password, click **Apply**. By default, both the user name and password values are **admin**.

To modify the password of the user account, just enter the new password in the **Password** and the **Confirm Password** field and click **Apply**.

Note:
After clicking **Apply** to change the use name and password, the new setting takes effect immediately. When you continue to access other pages, you will be prompted to re-login with new user name and password immediately.
To save the new settings to flash memory and take effect next time your reboot the ADSL Router, after clicking A**pply**, you should perform the task of **Save Configuration**.

Remote Access

This function allows remote client to access this router from WAN side. You can set the lease time and click **Enable** to enable this setting. To disable this function, just click **Disable**.



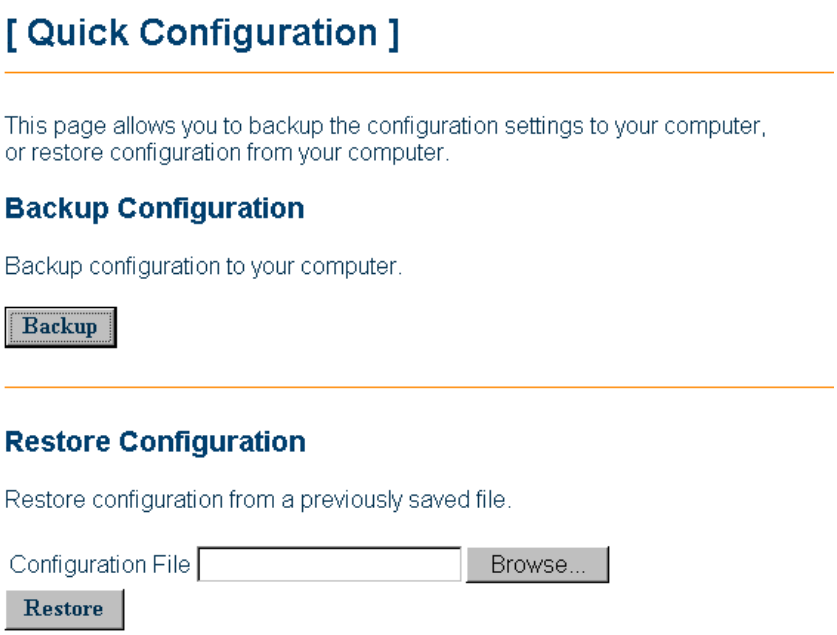
Web Port

The default web server port is 80. You can change the web server port to another one and then click **Apply** to enable this setting.

Note:
Clicking **Apply** will enable the new setting right away. When you continue to access other pages, you will need to re-login at new web port.

Quick Configuration

This page allows you to backup the configuration settings to your computer or to restore your configuration settings.



To backup your configuration proceed as follows:

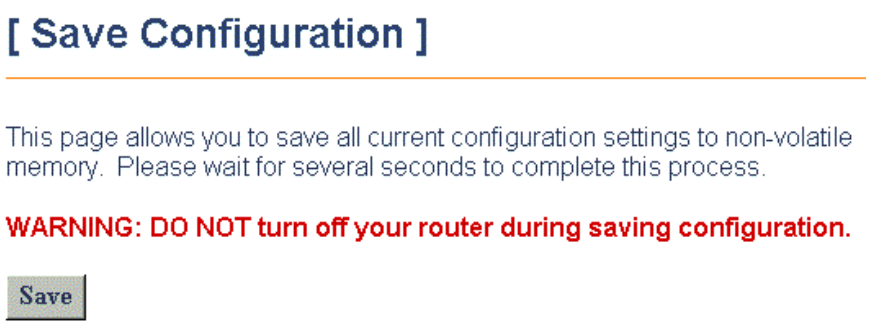
1. Click to **Backup**.
2. Read the warning message and click to **Ok**.
3. Choose **Save this file to disk** and click **Ok**.
4. Choose a filename for your configuration settings and select the directory where the configuration should be saved.
5. Your configuration settings are saved now.

To restore your configuration proceed as follows:

1. Click to **Browse**.
2. Select the file where your configuration is saved.
3. Click to **Open**.
4. Click to **Restore**.
5. Your configuration will be restored now.
6. Click to **Save** to save to your configuration

Save Configuration

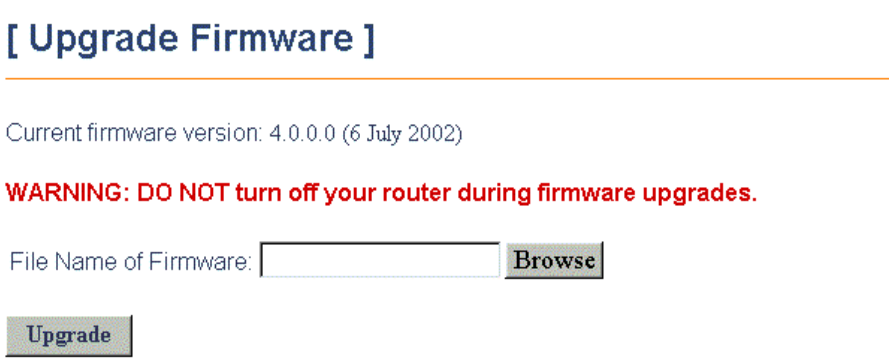
This page allows you to save all current configuration settings to non-volatile memory. Please wait for several seconds to complete this process.



Upgrade Software

The ADSL Router supports the upgrading by using HTTP. To transfer the firmware file, follow the steps below:

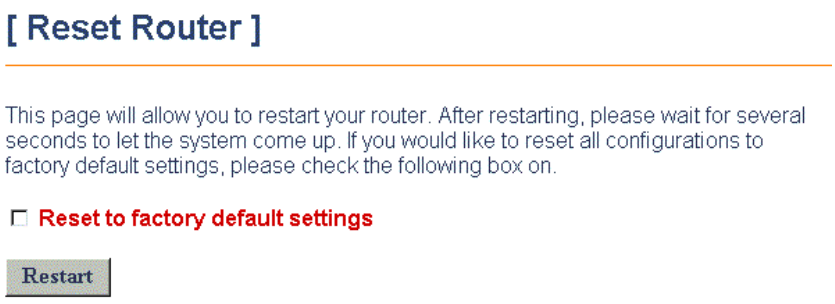
1. Download and unzip the new software file from vendor.
2. In the **File Name of Firmware** field, click **Browse** to locate the upgrade file.
3. Click the **Upgrade** button.



After upgrading, the original configuration will still exist and not reset to the factory defaults.

Reset Router

This page allows you to restart your router for invoking new configuration. After restarting, you should wait for several seconds to let the system come up. When restarting the system, your brower session will be disconnected. Please wait until the device finish restarting.



Note:
If **Reset to factory default settings** is checked, the settings will return to factory defaults, including the **Username** and **Password**.

Status

DSL Connection

This page shows the DSL line connection status as below:

Refresh

Line Mode	Inactive	Line State	Handshaking
DS Speed	0 Kbps	US Speed	0 Kbps
DS Latency		US Latency	
Trellis Coding		Loss of Signal	0
Line Attenuation		Loss of Frame	0
Noise Margin		CRC Error	0
Line Up Count	0	Error Second	0 seconds
Line Up Time		System Up Time	0:01:02:34

Line Mode: The ADSL Router supports multi-mode standard: **ANSI T1.413**, **G.lite** (ITU-T G.992.2) and **G.dmt** (ITU-T G.922.1).

DS (Downstream)/ US (Upstream) Speed: The downstream/upstream speed of the DSL line.

DS/US Latency: Displays whether a fast or interleaved latency path is specified.

Trellis coding: Indicates trellis coding is enabled or disabled. Trellis coding is a method of providing better performance in a noisy environment. It helps to transmit at faster line rates with lower error rates, thus providing a faster overall throughput in a moderately noisy environment.

Line Attenuation: Indicates the signal attenuation caused by line length. It increases with line length and frequency and decreases as wire diameter increases.

Noise Margin: Signal to noise ratio. The ratio of good data (signal) to bad (noise) on the line, expressed in decibels (dB).

Loss of Signal /Frame: Indicates the loss of signals or frames detected.

CRC Error: Cyclic Redundancy Checksum generated.

Line Up Count: The number of times that you connect to.

Line Up Time: The duration time of the line connecting.

Error Second: The accumulated seconds of the seconds during which packet error message occur.

System Up Time: The time from system startup.

WAN Connection

This page shows all the ATM PVC interfaces you defined. For each ATM PVC interface, it shows the parameter you defined for ATM PVC name, VPI/VCI values, Mode, Encapsulation Type, if NAT is enabled or not and Local WAN IP address.

[WAN Connection]

Refresh

PVC Name	VPI	VCI	Data Encap	NAT	Local WAN IP
ppp-0	8	35	PPPoE LLC/SNAP	enabled	0.0.0.0

Traffic Counter

This page shows the records of data going through the LAN and WAN interface. For each interface, cumulative totals are displayed for **Sent**/**Received Packets** and **Sent**/**Received Bytes**.

[Traffic Counter]

The statistic of user data going through your router is list below.

Refresh

Connection	Tx Packets	Rx Packets	Tx Bytes	Rx Bytes
Ethernet	121366 / 0	66705 / 0	69802681	10169605
Wireless Lan	10006 / 0	10 / 0	2673253	1320
8 / 35 (vpi/vci)	3561 / 0	3719 / 40	60994	327545

By clicking **Refresh**, all the records will be reset.

Routing Table

This page shows all the routing rules of data packets going through your ADSL Router if it runs in routing mode. By clicking **Refresh**, all the records will be reset.

[Routing Table]

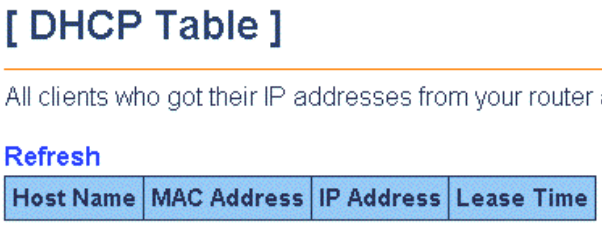
All of current routing rules in your router are listed below.

Refresh

Destination	Netmask	Gateway / Interface	Cost	Timeout	Attribute
0.0.0.0	0.0.0.0	ppp-0	1	0	static

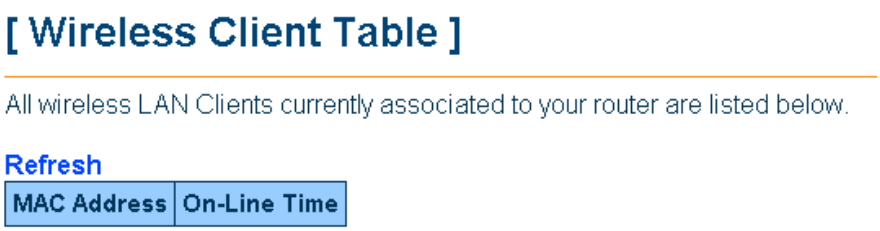
DHCP Table

This page shows all DHCP clients who get their IP addresses from your ADSL Router. For each DHCP client, it shows the **Host Name**, **MAC Address**, **IP Address** and the **Lease Time**.



Wireless Client

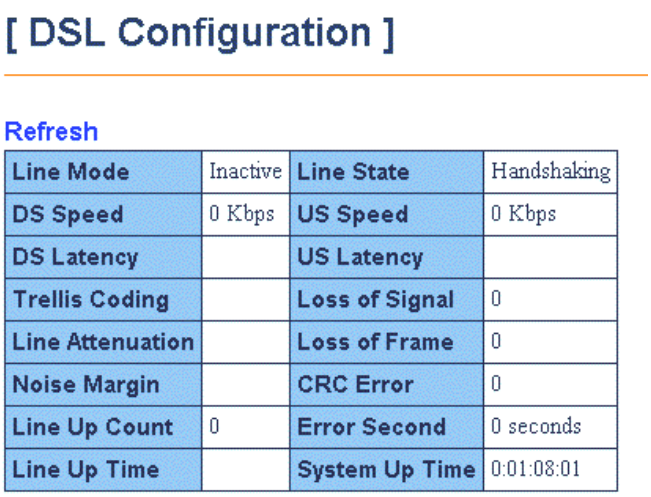
This page shows wireless clients that associated to the router. For each client, it shows the **MAC Address** and the **On-Line Time**.



Configuration

DSL Configuration

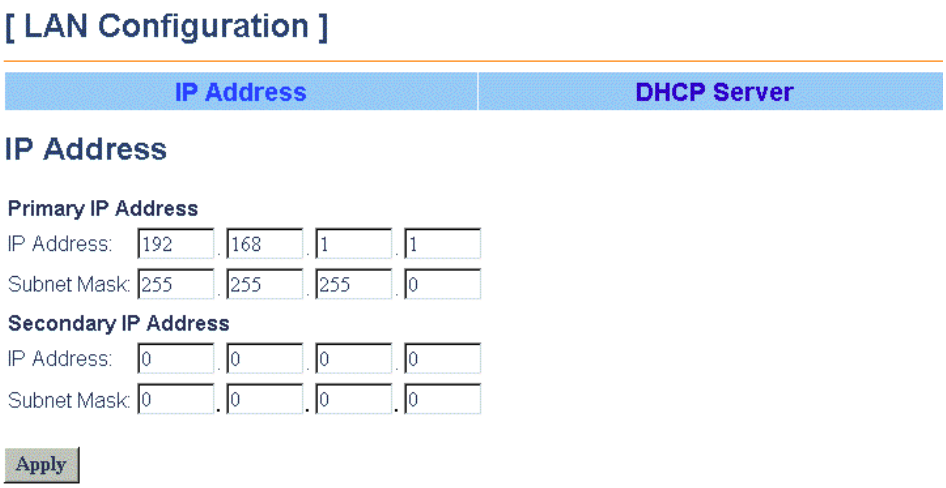
DSL Line Mode: The ADSL Router supports multi-mode standard: **Auto**, **G.dmt, G.lite** and **T1.413**. Choose an appropriate line mode according to the setting of DSLAM in central office and then click **Apply**.



The DSL line mode you specify will be applied to the entire ADSL Router unit. All ATM PVC profiles created will use the same line mode. Consult your ISP to find out which option applies to your DSL line.

LAN Configuration

For the LAN Configuration, there are two types that you have to know, IP Address and DHCP Server.



IP Address

LAN Configuration allows you to define the public/private IP address over the LAN interface.

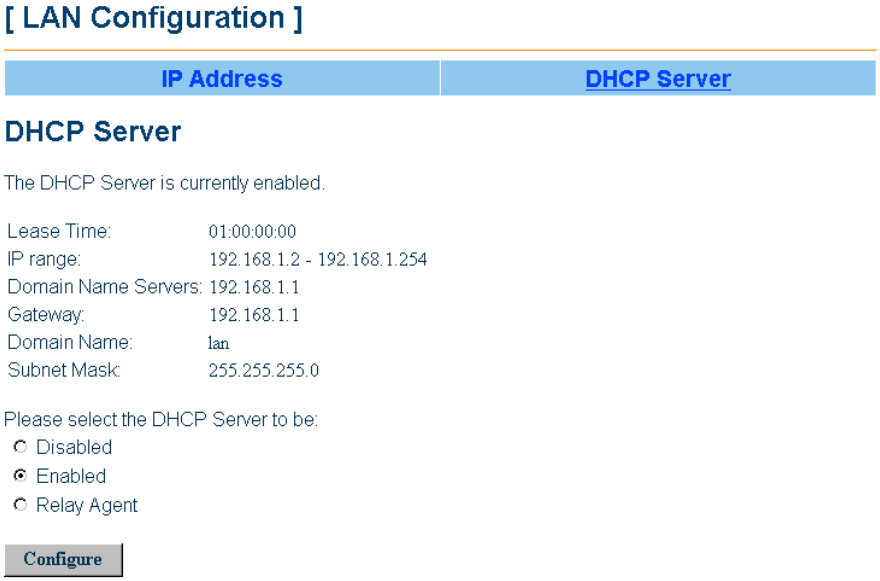
Primary IP Address: Private IP address is used for the purpose of system management. When it is assigned, PC on the LAN is able to use the specified address to access this ADSL Router through Ethernet.

By default, the IP address and subnet mask is **192.168.1.1** and **255.255.255.0** respectively. This will give you an available range of IP addresses from 192.168.1.2 to 192.168.1.254 that can be assigned to PCs on the LAN.

Secondary IP Address: If you applied for multiple IP address from your ISP, you will have a range of IP address for the ADSL Router and other network devices on the LAN. You can fill in the IP address assigned by ISP in the public IP address field.

DHCP Server

This page allows you to enable DHCP server on LAN interface and then your router can assign IP addresses to those PCs connected to your router.



The ADSL Router implements a built-in DHCP (Dynamic Host Configuration Protocol) server, which dynamically assigns IP addresses and DNS server to the PCs on the LAN. DHCP function spares you the hassle of manually assigning a fixed IP address to each PC on the LAN. It is probably you already have a DHCP server on your network and you do not enable this function. By default the DHCP Server is enabled on private LAN interface (192.168.1.1).

Start IP address: First IP address of the DHCP address range.

End IP address: Last IP address of the DHCP address range.

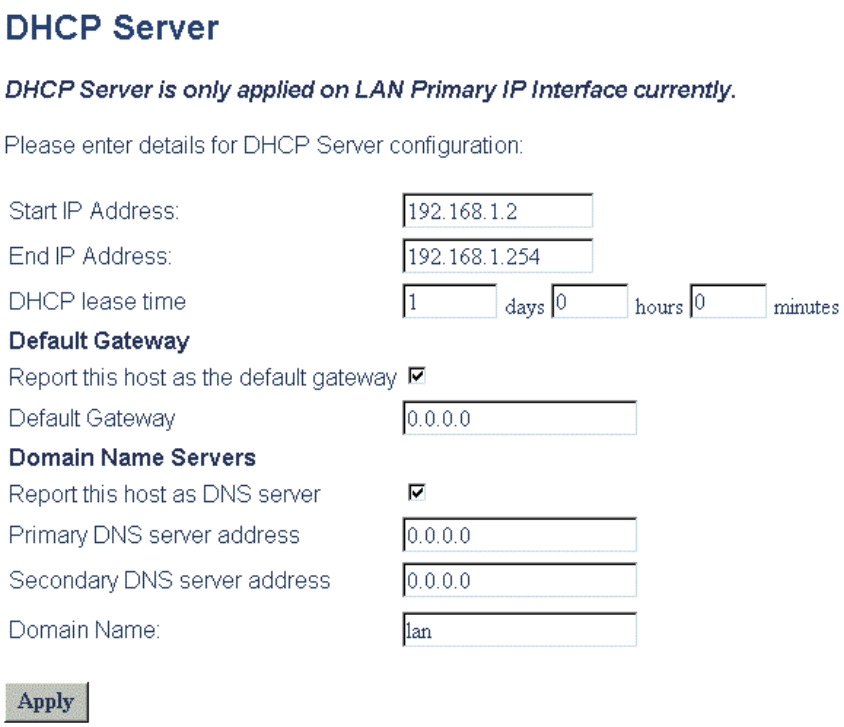
DHCP lease time: Specify the time that a network device can lease a private IP address before the ADSL Router reassigning the IP address.

Default Gateway: You check the **Report this host as the default gateway** box to use this host as the default gateway or fill in an IP address as the default gateway.

Domain Name Servers: You can check the **Report this host as the DNS server** box to use this host as the default DNS. Or you can uncheck the box and manually set up the DNS IP address in the **Primary/Secondary DNS IP address** fields. The DNS server addresses will be passed to the DHCP clients along with the IP addresses. The DHCP clients use the DNS to map a domain name to its corresponding IP address and vice versa.

DHCP Relay Agent: If the DHCP Relay Agent is activated, those DHCP Discover or Request packets coming from the end users' PCs will be relayed to a remote end DHCP server which is hosted by an Internet Service Provider (ISP). Some ISPs would like to be able to distribute IP addresses to end user PCs directly.

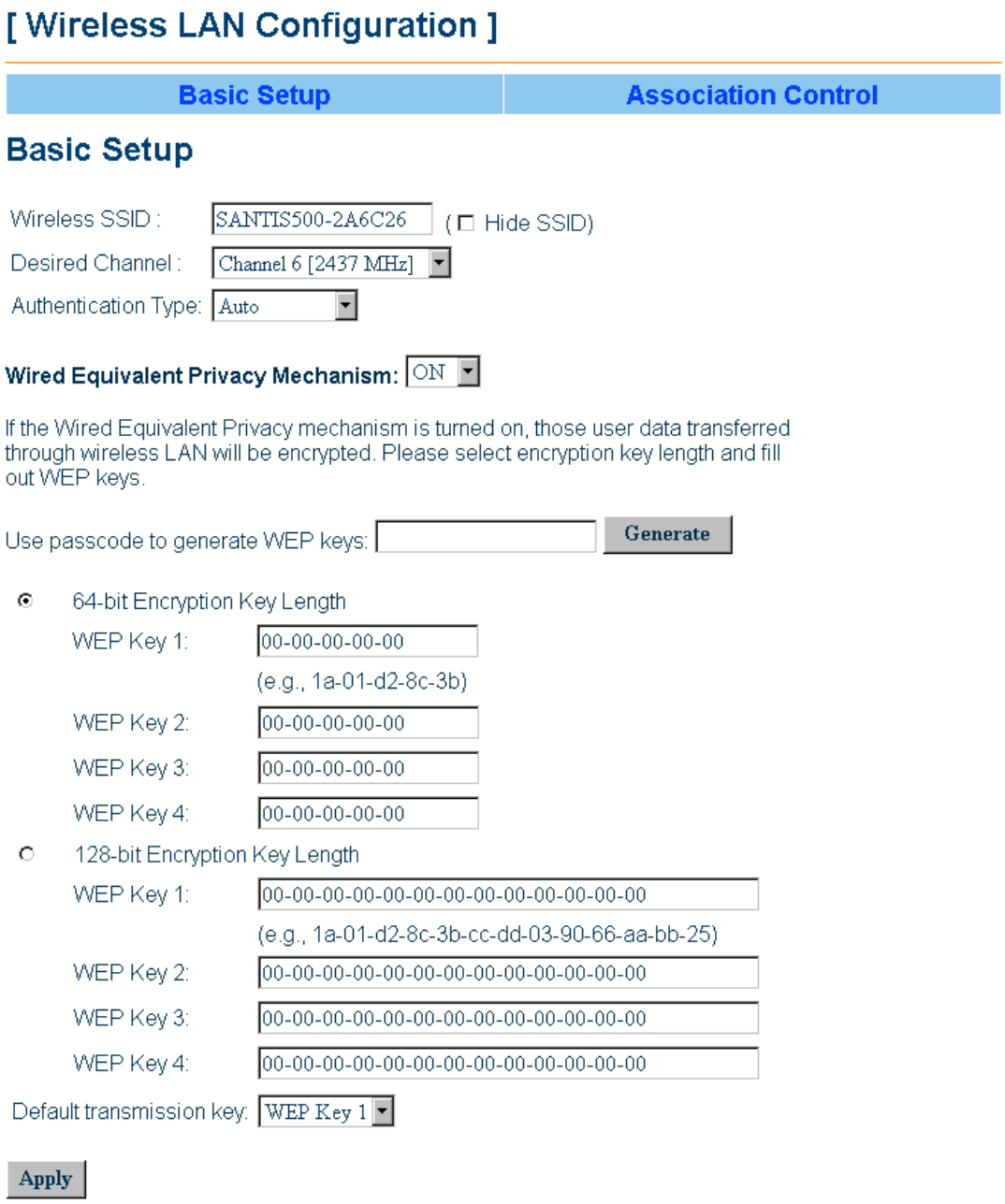
Select DHCP Server **Enabled** and click **Configure** to get advanced settings. Please enter the requiring information and click **Apply** to invoke the configurations.



WLAN Configuration

This section shows you how to configure the wireless LAN setting. To types are provided here, Basic Setup and Association Control.

Basic Setup



Note:
If you are entering the WEP key manually, make sure that you use only the following digits and letters: 0 – 9, a or A, b or B, c or C, d or D, e or E and f or F

Wireless SSID
(Service Set Identity): A name that uniquely identifies a wireless domain. All wireless clients that want to communicate with the ADSL Router must have the same SSID as it.

Note:
Click **Hide SSID** to not broadcast the SSID on the wireless network, which prevents your wireless LAN Access Point from hacker attacks. If the SSID is hidden, an unauthorized wireless LAN client is not able to connect to your wireless LAN Access Point.

Frequency Domain: The frequency in which the radio links are about to be established.

Desired Channel: The frequency in which the radio links are about to be established. Select channel that you want. Usually the wireless clients will scan the whole operable channels and then select the desired communications channel automatically.

Authentication Type: The ADSL Router supports three authentication types: **Open System, Shared key** and **Auto**. This should be considered with the WEP (Wired Equivalent Privacy) mechanism.

Wired Equivalent Privacy Mechanism

The privacy security function can enhance wireless media security by encryption technology. All wireless clients must set the same encryption key to maintain the tightened communication with the ADSL Router properly. The Authenticate Algorithm options are:

When the wired Equivalent Privacy Mechanism is Turns off. Using Open-key as authentication algorithm, you are running the risk of allowing some unauthorized wireless LAN cards that have the capability of eavesdropping your SSID to associate itself to the device.

Turns on encryption. Wired Equivalent Privacy Mechanism is Turns on. You should select the encryption key length as 64 or 128 bit keys. Then enter the encryption key in Key Entry fields.

Note:
When Wired Equivalent Privacy Mechanism is enabled, the wireless client must be configured with exactly the same encryption level (64 or 128-bit) and encryption key as identified in the ADSL Router, so that access to the unit is allowed.

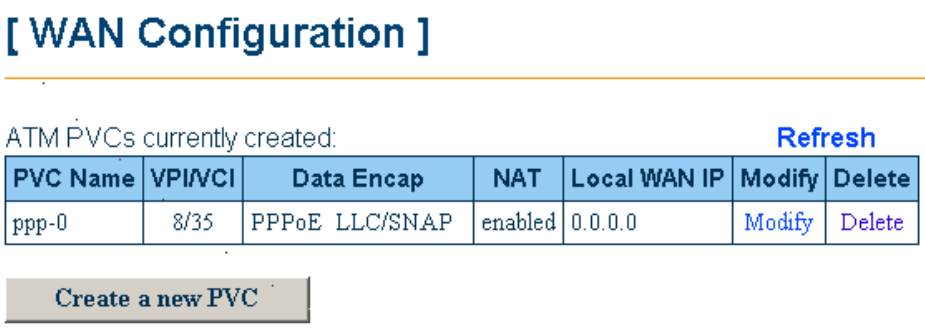
Association Control

You can enable this control to associate to your router with other wireless clients.

You can add a new client for associating to the router. Click **Add a new client** to get into another page. Enter the MAC address for the new wireless LAN client. Choose if this new wireless LAN client is an authorized (Allow) or a non-authorized client (Deny) and click **Apply**.

WAN Configuration

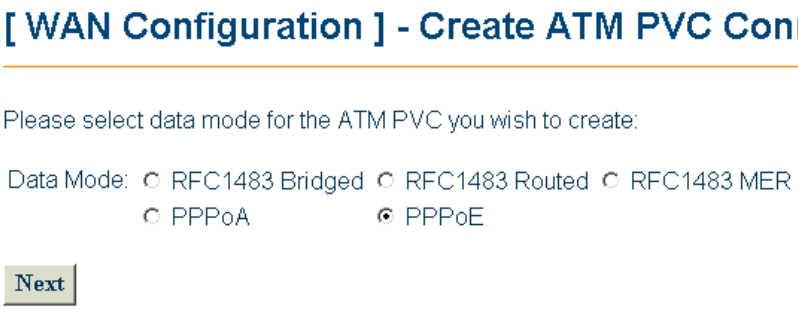
The ADSL Router supports for Asynchronous Transfer Mode (ATM) over ADSL. To set up connections over the WAN, you have to define ATM PVC interface for each remote connection. On this page, you can create, modify and delete PVC interface.



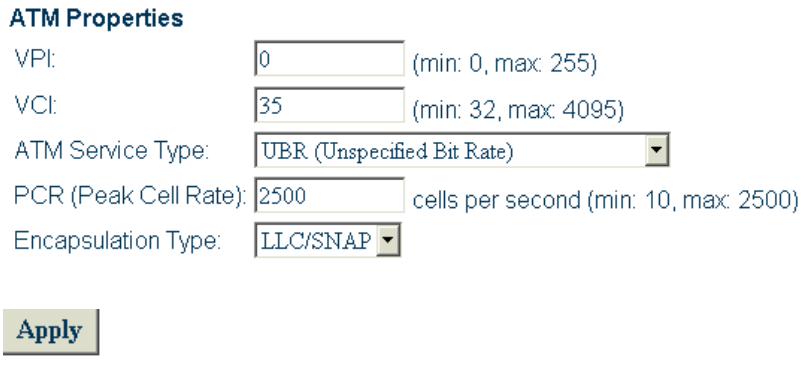
You can select an existing ATM PVC interface and click **Modify** to edit its parameters or click **Delete** if you want to delete it.

To add a new PVC interface, click **Create a new PVC** and follow these steps:

1. Select one of connection type in the Data Mode (RFC1483 Bridged, RFC1483 Routed, RFC1483 MER, PPPoA or PPPoE) and click **Next**.

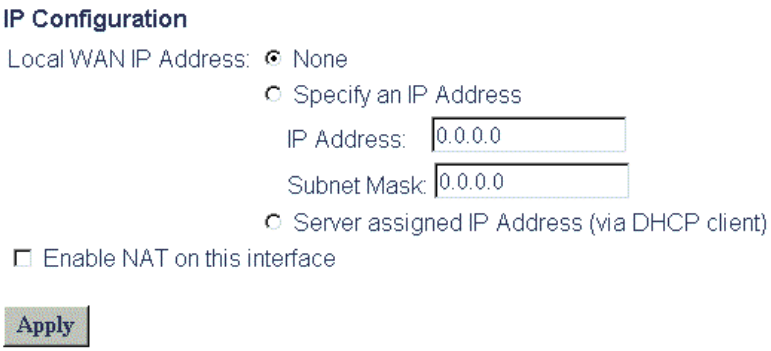


2. Fill in the VPI/VCI values and select ATM Service Type, Encapsulation Type and PCR.

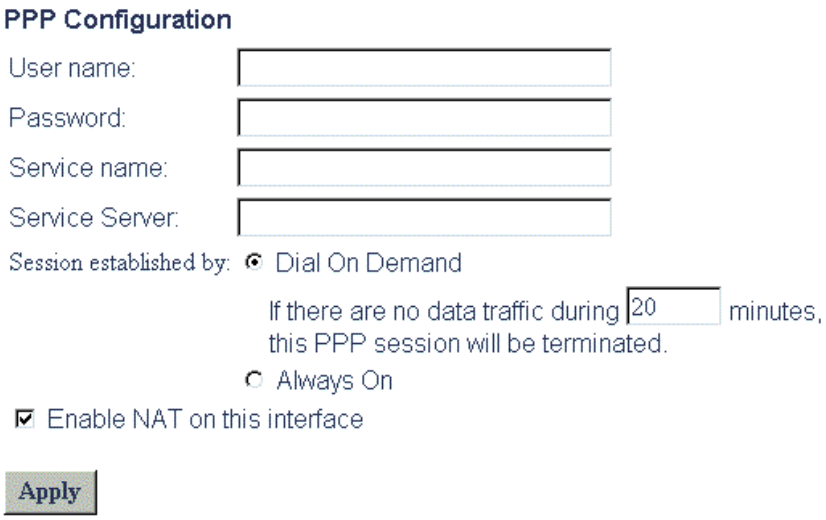


3. Click **Apply**.

4. At PPPoE, PPPoA, RFC1483 Routed and RFC1483 MER mode Configuration, you can select Specify an IP address or Server assigned IP address.



5. Unless your ATM PVC is set on RFC1483 Bridged mode, you can check NAT box to enable NAT function.
6. If you are using PPP (PPPoE or PPPoA) configuration mode, you need to fill in the user name and password and you can set the PPP session to Dial on demand or Always on mode.



The parameters are described as below:

VPI (Virtual Path Identifier):	Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255.
VCI (Virtual Channel Identifier):	Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 4095 (1 to 31 is reserved for well-known protocols).
ATM Service Type:	Currently, the ADSL Router supports the **UBR (Unspecified Bit Rate)** service type.
PCR (Peak Cell Rate):	Specify the PCR cells per second.
Encapsulation Type:	There are two types for your choosing, VC MUX or LLC/SNAP. Select the encapsulation based on the setting of the ISP. Consult your ISP for this information.
Local WAN IP Address:	On Router mode, selecting **None** means you have public LAN IP address setting. If you select **Specify an IP address**, you can specify a WAN IP provided by ISP for your router. If **Server assigned IP address** is selected, the router will get a dynamic WAN IP address whenever it connects to the remote server or ISP.

Note:
If a fixed WAN IP is entered, note that this IP address and the subnet mask could not be the same with the public LAN interface.

Enable NAT on this interface: If your LAN interface is set on primary LAN you should check the box of the Enable Network Address Translation. NAT translates a private IP within one network to a public IP address.

User Name/Password: The user name and password used to access the remote server or ISP.

Dial On Demand: If checked, under disconnected status, if any client PC sends out request for connection, the ADSL Router will dial the ISP automatically. In this case, if the system administrator wants to disconnect the PPP session, just click the **Disconnect** button at Quick Start page.

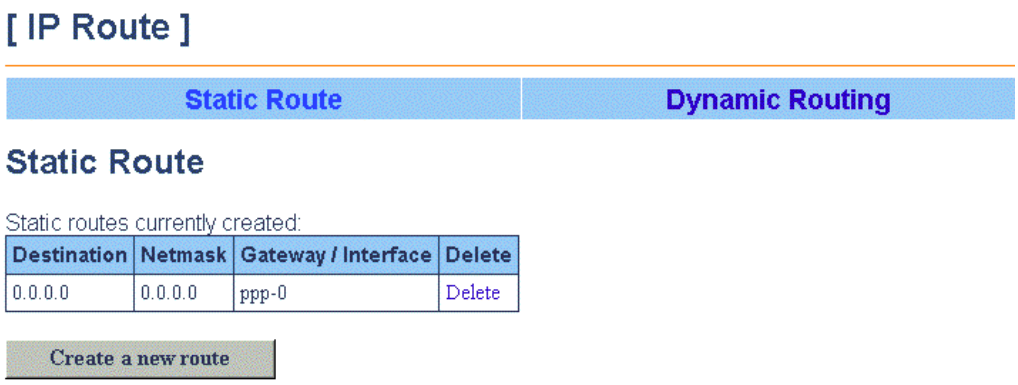
Always On: Enabling this feature will send echo request to ISP. This prevents the connection from being hung up by ISP.
The parameters for PPPoE configuration are generally the same as those of PPPoA. The additional parameters are:

Service Name: Enter the name of your PPPoE service here.

Service Server: Enter the name of your PPPoE service server here.

Note: When you initially add a PVC for the PPP connection and connect to ISP, a default routing of **0.0.0.0** is added automatically to the IP Static Routing. If you set up more than one PVC profiles and the first PVC is deleted, then you have to manually add the default routing.

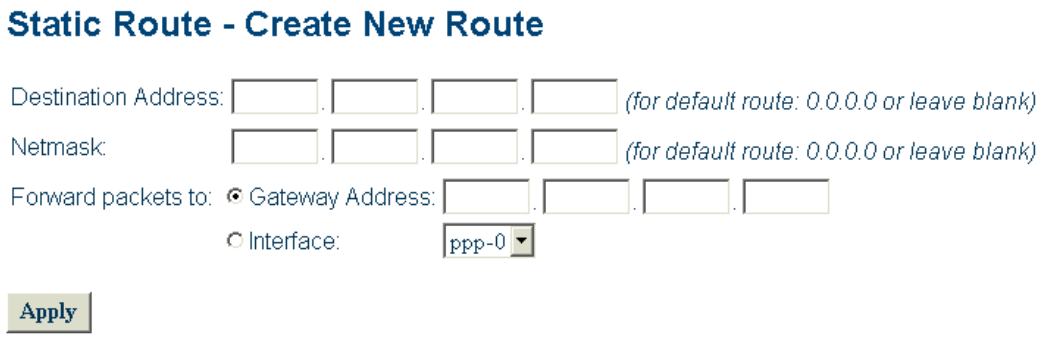
IP Route



Static Route

This page shows all static route status and allows you to add new static IP route or delete IP route. A Static IP Routing is a manually defined path, which determines the data-transmitting route. If your local network is composed of multiple subnets, you may want to specify a routing path to the routing table.

You can click **Create a new route** to add new route.



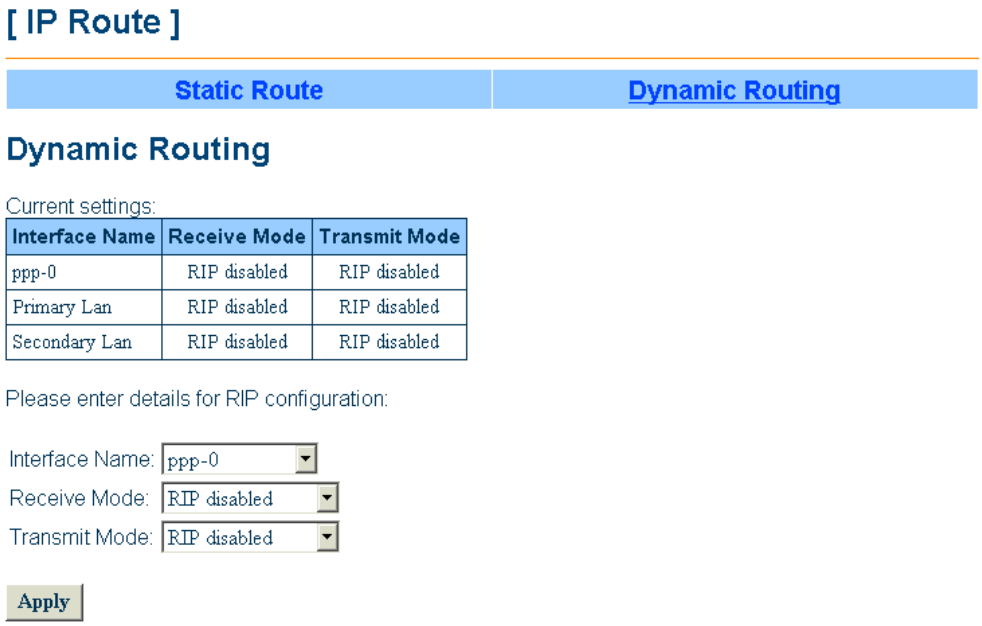
Destination Address: The destination IP address of the network where data packets are to be sent.

Netmask: The subnet mask of the destination IP address.

Forward packets to: If you want add a rout on LAN side, you should choose the **Gateway Address**. Enter the router address and then click **Apply**. If you want add a rout on WAN side, you should choose the **Interface**. Select ATM PVC interface and then click **Apply**.

Dynamic Routing

Routing Information Protocol (RIP) is utilized as a means of exchanging routing information between routers. It helps the routers to determine optimal routes. This page allows you to enable/disable this function.



By default, RIP is disabled with **Disabled** selected. You are allowed to enable RIP over the primary LAN interface. Upon each interface, you can customize the RIP on **Receive Mode** and **Transmit Mode** respectively.

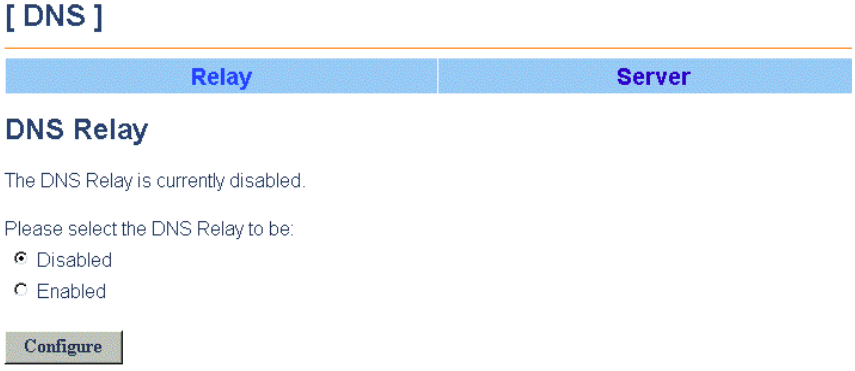
Receive Mode: It incorporates the RIP information when receiving the RIP packets. From the drop-down list select which RIP version should be accepted, RIP disabled, RIPv1, RIPv2 and both.

Transmit Mode: It broadcasts the routing table. From the drop-down list select which RIP version should be broadcasted, RIP disable, RIPv1, RIPv2 and both.

DNS

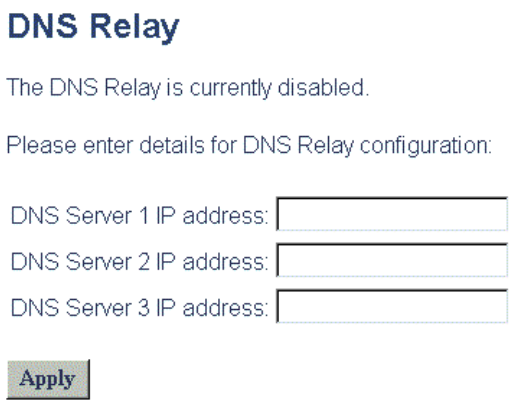
DNS Relay

On this page you can choose to disable or enable DNS Relay function. If your DNS is disabled and you choose to enable DNS relay, after selecting the **Enabled** option, please click **Configure** and then specify up to three DNS IP addresses in the **DNS server 1-3 IP address** fields. Then click **Apply** to enable the DNS relay function.

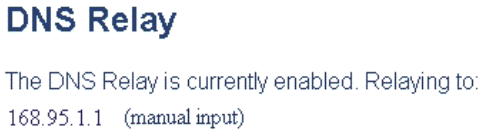


If you log in DNS Relay page for the first time: when you choose Enabled and enter this page by clicking **Configure**.

The page will show **DNS server 1-3 IP address** fields specify up to three DNS IP addresses click **Apply**.

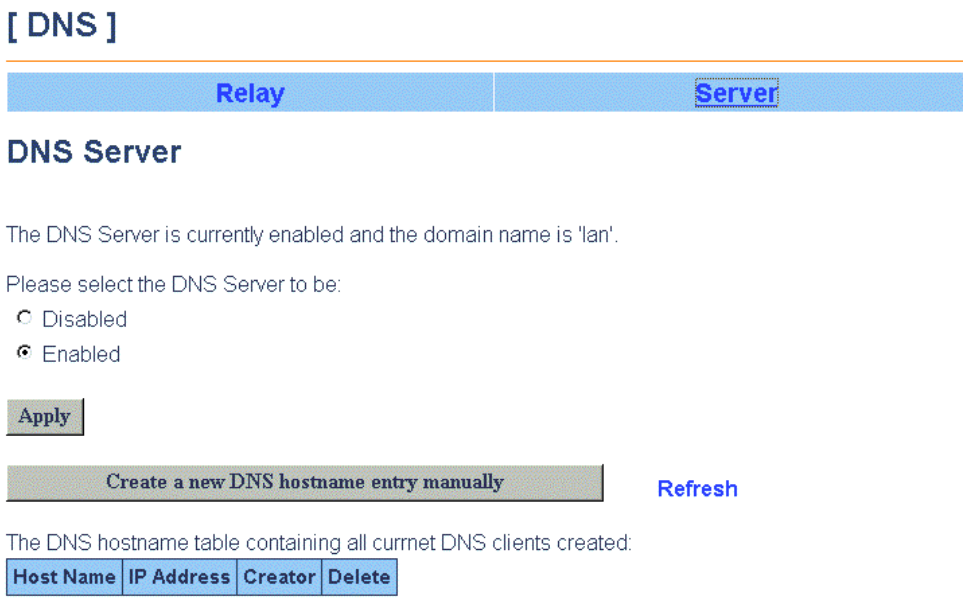


If you have been setting before, the page will show all the DNS Relay status. To disable DNS relay, just select the **Disabled** option then click **Configure.** To modify setting select enable and click **Configure** again.



DNS Server

The DNS server address will be passed to the DHCP clients along with the IP address and the DHCP clients use the DNS to map a domain name to its corresponding IP address and vice versa.



DNS Server: Select **Enabled** or **Disabled** to enable/disable the DNS server and then click **Configure**. The DNS hostname table shows all the current DNS clients, whether created by DHCP client or manually created. If it created by manual client, you can delete the hostname entry on the table.
If you want to change the domain name, please select **Enabled** and click **Configure**. Then fill in **Domain Name** and click **Apply**.

Create New DNS Hostname Entry: To add new hostname entry, please click **Create a new DNS hostname entry manually** button. Then fill in the **Hostname** and **IP address** and click **Apply**.

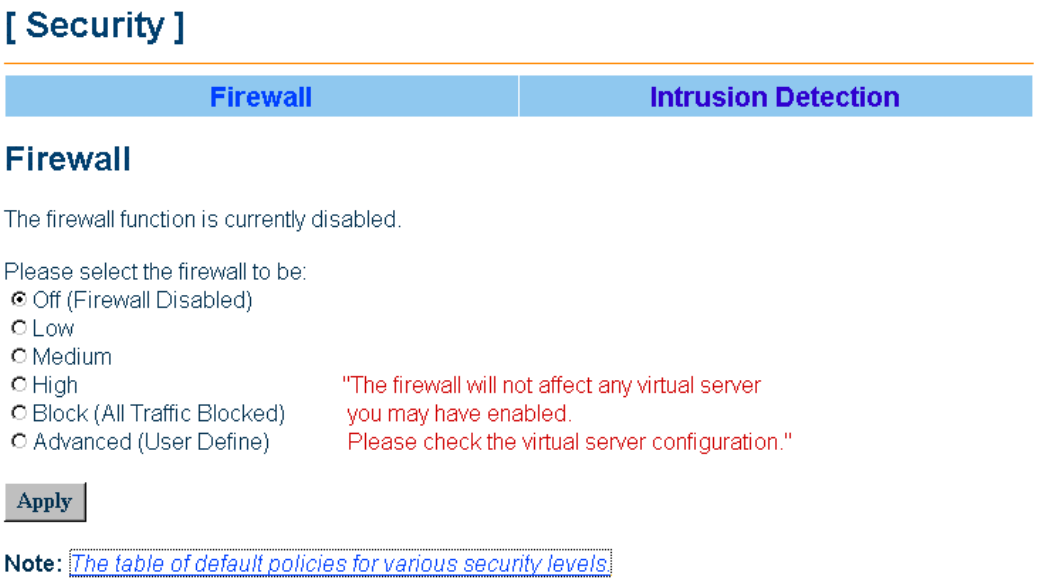
Delete Hostname Entry: To delete the hostname entry, select the required one from the DNS hostname table. After confirming the data, click **Delete**.

Note:
1. When DNS Relay is disabled, the DNS server function is invalid.
2. If DNS IP is left as 0.0.0.0, then you should specify the DNS on each client PC.

Security

Firewall

This page is used to set the firewall for your system. Please choose one from the provided items and click Apply to enable it.



Click on **The table of default policies for various security levels** to see the traffic blocked status for each setting.

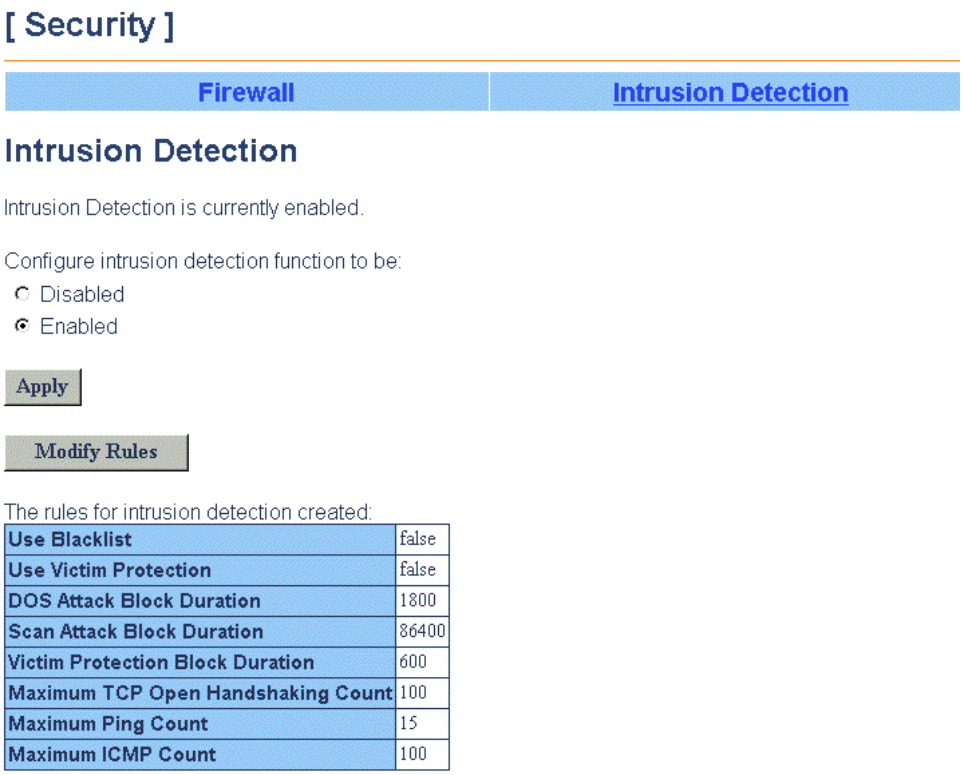
Security Level		Low		Medium		High	
Service	Port	In	Out	In	Out	In	Out
HTTP(tcp)	80	Yes	Yes	No	Yes	No	Yes
DNS(udp)	53	Yes	Yes	No	Yes	No	Yes
FTP(tcp)	21	Yes	Yes	No	Yes	No	Yes
Telnet(tcp)	23	Yes	Yes	No	Yes	No	Yes
ICMP	N/A	Yes	Yes	Yes	Yes	No	Yes
SMTP(tcp)	25	Yes	Yes	No	Yes	No	Yes
POP3(tcp)	110	Yes	Yes	No	Yes	No	Yes
HTTP-SSL(tcp)	443	Yes	Yes	No	Yes	No	Yes
News-NNTP(tcp)	119	Yes	Yes	No	Yes	No	No
Internet Locator Server(tcp)	389	Yes	Yes	Yes	Yes	No	No
User Location Server(tcp)	552	Yes	Yes	Yes	Yes	No	No
T.120(tcp)	1503	Yes	Yes	Yes	Yes	No	No
H.323 call setup(tcp)	1720	Yes	Yes	Yes	Yes	No	No
Audio call control(tcp)	1731	Yes	Yes	Yes	Yes	No	No
RTP(udp)	21-65535	Yes	Yes	Yes	Yes	No	No
MSN Messager File Transfer(tcp)	6891-6900	Yes	Yes	Yes	Yes	No	No
Remote Messenger Remote Assistance(tcp)	3389	Yes	Yes	Yes	Yes	No	No
MSN Messenger Messaging(tcp)	1863	Yes	Yes	Yes	Yes	No	No
MSN Messenger Voice Comm(tcp/udp)	6901	Yes	Yes	Yes	Yes	No	No
Yahoo! Messenger Webcam(tcp)	5100	Yes	Yes	Yes	Yes	No	No
RealAudio/Video(tcp/udp)	554	Yes	Yes	No	No	No	No
RealAudio/Video(tcp)	7070-7071	Yes	Yes	No	No	No	No
RealAudio/Video(udp)	6770-7170	Yes	Yes	No	No	No	No
MS Media Player(tcp/udp)	1755	Yes	Yes	No	No	No	No
PPTP(tcp/udp)	1723	Yes	Yes	Yes	Yes	No	No
GRE(47)	N/A	Yes	Yes	Yes	Yes	No	No
ESP(50)	N/A	Yes	Yes	No	No	No	No
AH(51)	N/A	Yes	Yes	No	No	No	No
IKE(udp)	500	Yes	Yes	No	No	No	No
ICQ(tcp)	5190	Yes	Yes	Yes	Yes	No	No
ICQ Chat(tcp)	7152	Yes	Yes	Yes	Yes	No	No
(tcp)	411-412	Yes	Yes	No	No	No	No
(tcp)	4998-4999	Yes	Yes	No	No	No	No

The higher the security level is, the more traffic blocked for the service is.

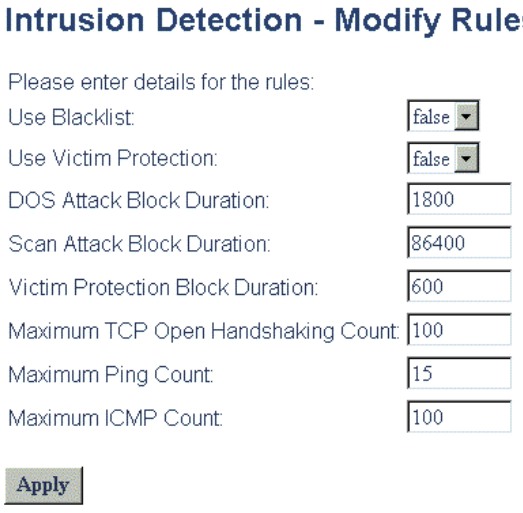
If you are not satisfied with the preset functions such as Low, Medium, High, please click **Advance (User Define)** for setting them by yourself.

Intrusion Detection

This page displays the rules for intrusion detection.



You can select **Disable** and click **Apply** to disabled intrusion detection. Select Enabled to invoke this function. In addition, click **Modify Rules** to enter or modify details for the rules if necessary. After finishing the modification, click **Apply**.



Virtual Server

This page shows all virtual server rules configured in your ADSL Router.

The Router implements NAT to let your entire local network appear as a single machine to the Internet. The typical situation is that you have local servers for different services and you want to make them publicly accessible. With NAT applied, it will translate the internal IP addresses of these servers to a single IP address that is unique on the Internet. NAT function not only eliminates the need for multiple public IP addresses but also provides a measure of security for your LAN.

When the router receives an incoming IP packet requesting for access to your local server, the router will recognize the service type according to the port number in this packet (e.g., port 80 indicates HTTP service and port 21 indicates FTP service). By specifying the port number, you tell the router which service should be forwarded to the

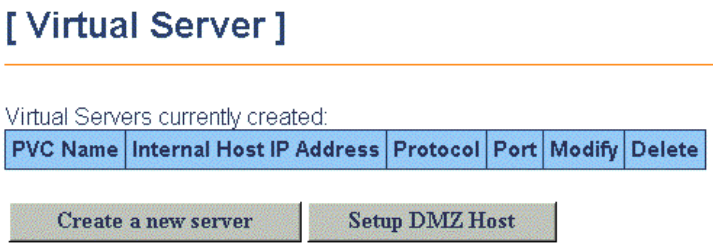
local IP address you specify.

After you setting the virtual server you should modify the filter rule whichever port and service you set on virtual server. Because the firewall has protect the route by filter rule so that you should update the filter rule after you set up virtual server.

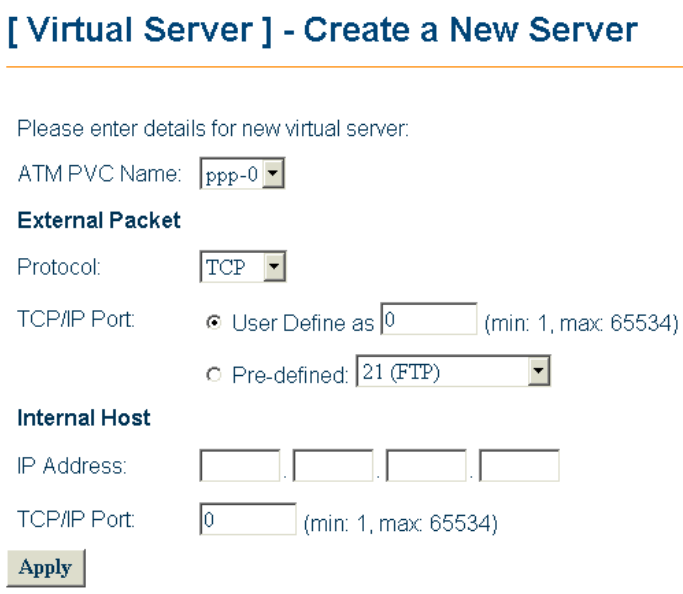
Protocol: Select a protocol type used by the service that will be forwarded.

TCP/IP Port: The Router supports port mapping function that translates a standard port number to a non-standard number. Incoming data packets sent to a specific IP port can be mapped to the port you specify. The most often used port numbers include:
21 (FTP), 80 (HTTP), 23 (Telnet) and 25(SMTP)

IP Address: Specify the internal IP address to which the packets are forwarded.

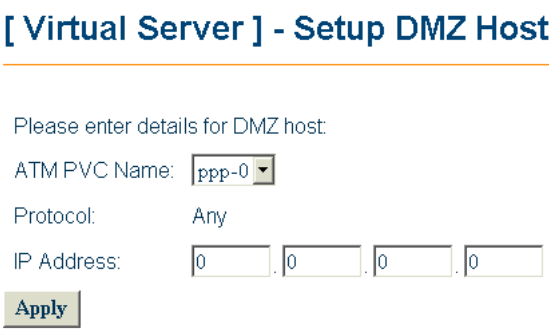


In the virtual server list table, you may select required entry to modify or delete it by clicking **Modify** or **Delete**. In order to add new virtual server service entry, click **Create a new server** button.



Then follow the steps below:

1. Select the ATM PVC interface.
2. Select the protocol type from the drop-down list.
3. Select a service in TCP /IP Port field and enter the port number you want to use.
4. Enter the IP address of the internal server in the IP Address filed.
5. Click **Apply** to commit the setting.



Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static private IP address if you want to use DMZ. The DMZ Host settings allow one local user to be exposed to the Internet to use special-purpose service such as Internet gaming or Video-conferencing. It is strongly recommended that you only define servers as DMZ host, which do not signify a security risk. To set up a DMZ host proceed as follows:

1. Enter the IP address of your DMZ host and click to **Apply**.
2. Your designated servers on the LAN are no accessible to the outside.

IGMP Proxy

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered via standard IGMP interfaces. The system acts as a **proxy** for its hosts.

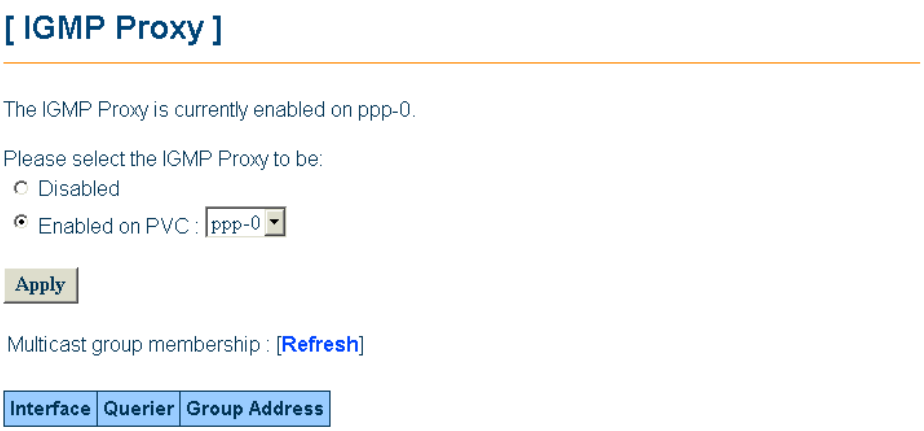
If you enable IGMP proxy on your ADSL Router, your ADSL Router is the **upstream interface**.

On the interfaces connected to your ADSL Router you have to run IGMP. These interfaces are known as **downstream interfaces**.

Downstream interfaces connected to the **upstream interface** (IGMP Proxy) can join for example the same video stream at the same time. The advantage with the IGMP Proxy is, that the bandwidth of the video stream is only used once: from the **upstream interface** to the video server in the Internet. All **downstream interfaces** will download the video stream form the IGMP Proxy and not from the Internet directly.

In IGMP operation, hosts interact with the system through the exchange of IGMP messages. Similarly, when you configure IGMP proxy, the system interacts with the router on its upstream interface through the exchange of IGMP messages. However, when acting as the proxy, the system performs the host portion of the IGMP task on the upstream interface as follows:

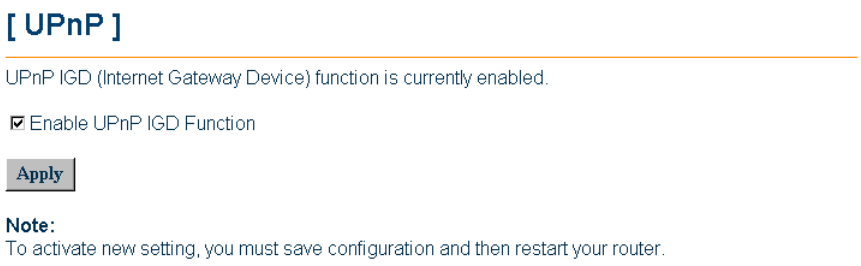
- When queried, sends group membership reports to the group
- When one of its hosts joins a multicast address group to which none of its other hosts belong, sends unsolicited group membership report to that group
- When the last of its hosts in a particular multicast group leaves the group, sends an unsolicited leave group membership report to all-routers group



UPnP

Universal plug and play (UPnP) is architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet.

To disable UPnP function, just deselect the **Enable UPnP Function** box and then click **Apply** to disable the function.



Chapter 4: Connection Mode

The ADSL Router is delivered pre-configured from the factory in Router Mode. This chapter presents some deployment examples for your reference. Each mode includes its general configure procedures. For more detailed information about web configuration, refer to "Web Configuration".

- Router Mode
- Bridge Mode
- MER Mode
- PPPoA+ NAT Mode
- PPPoE + NAT Mode
- Multiple PVCs Mode

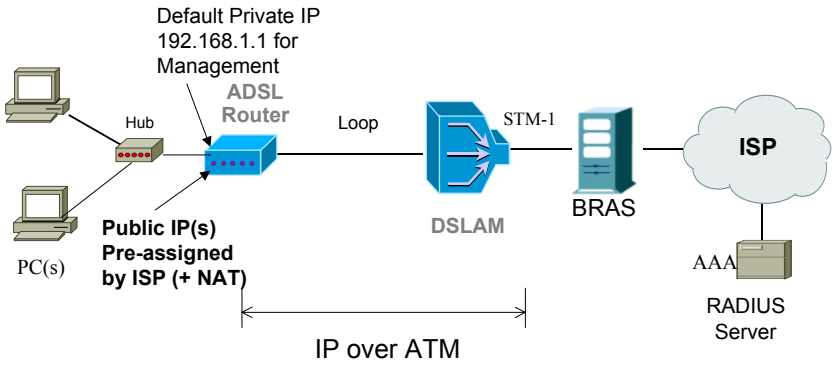
For making sure that you can connect the ADSL to your computer well and get into Internet successfully, please make sure the following first.

1. Make sure you have installed a network interface card onto your computer.
2. Make sure the connection between the ADSL and your computer is OK.
3. Check to see the TCP/IP protocol and set the IP address as “Auto Get IP Address” (See chapter 3:

When you are sure all above is Ok, you can open the Browser and type in “192.168.1.1” and start to do the web configuration with different connection modes.

This chapter is going to introduce the function of each connection mode and tell you the basic configuring steps that you have to do. If you did not follow the configuring steps for using these connection modes, you might get some connection problems and cannot connect to Internet well.

Router Mode



* BRAS：Broadband Remote Access Server

Description:

In this deployment environment, we make up a private IP network of 192.168.1.1. NAT function is enabled (on ADSL Router or use another NAT box connected to hub) to support multiple clients to access the Router and some public servers (WWW, FTP).

If you apply for multiple IP addresses from your ISP, you can assign these public IP addresses to the ADSL Router and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as router IP address and the last one is subnet broadcasting. Other remaining IP addresses can be assigned to PCs on the LAN.

For example: You are given the IP addresses 10.251.2.0 ~ 10.251.2.7. Then:

10.251.2.0 is network IP address
10.251.2.1 is assigned to router IP address.
10.251.2.7 is subnet broadcasting
10.251.2.2~10.251.2.6 can be assigned to public servers on the LAN.

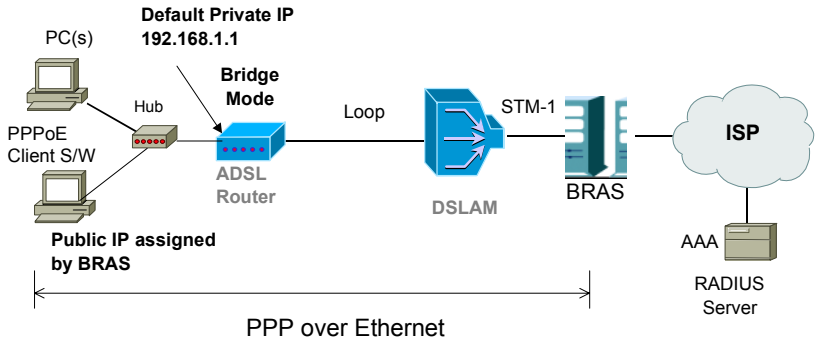
Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Advanced User > Configuration > WAN Configuration > Create a new PVC**. And select the Data Mode –**RFC1483 Routed**. Then click **Next** button.
3. Enter the VPI/VCI values provided by your ISP and select the encapsulation type as **LLC/SNAP** or **VC MUX**. Then click **Apply**.
4. Set IP configuration for Local WAN IP Address. Choose **Specify an IP Address** item. Please set as the following example,
   IP Address: **10.3.80.105** (should be the one that you get from ISP)
   Subnet Mask: **255.255.255.248**
   Check on **Enable NAT on this interface** and click **Apply.**
5. Go to **Configuration > LAN Configuration** and set as the following
   Primary IP: **192.168.1.1**, Subnet Mask: 255.255.255.0
   Secondary IP: **10.3.80.105,** Subnet Mask: 255.255.255.248
   (should be the one that you get from ISP)
   Then click **Apply**.
6. Go to **Configuration > IP Route** and click **Create a New Route** to add a new route.
   Destination Address: leave default
   Netmask: leave default
   Forward packets to: **Interface**
   Then click **Apply**.
7. Go to **Configuration > DNS** and enable **DNS Relay** setting and click **Next**. On the DNS Relay web page, enter the DNS Server IP address, for example **168.95.1.1** (you should get this value from your ISP).
8. Save the configuration from **System** >**Save Configuration** and **System** >**Restart** to restart your router for initiating these settings.

9. Then you have set the web configuration successfully. And you can surf on the Internet.

Note:
If you have multiple PCs on the LAN, you may enable DHCP function on the private or public IP address. The ADSL Router implements a built-in DHCP server, which assigns IP addresses to the clients PCs on the LAN.

Bridge Mode



BRAS Broadband Remote Access Server

Description:

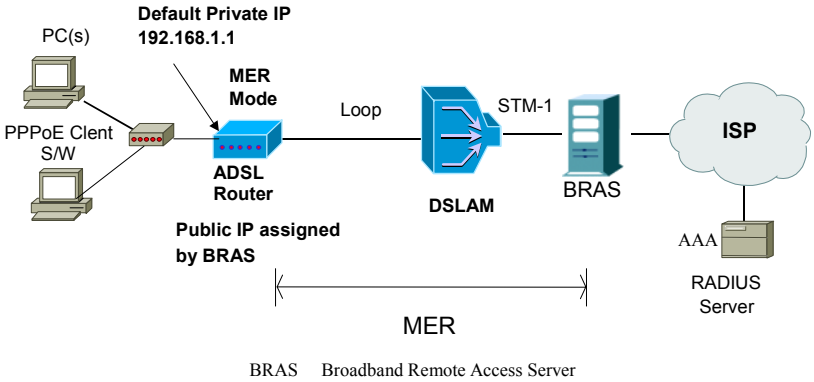
In this example, the ADSL Router acts as a bridge which bridging PC IP address from LAN to WAN. PC IP address can be a static public address that is pre-assigned by ISP or a dynamic public address that is assigned by ISP DHCP server, or can be got from PPPoE software.

Therefore, it does not require a public IP address. It only has a default private IP address (192.168.1.1) for management purpose.

Configuration:

1. Choose a client PC and set the IP as 192.168.1.x (x is between 2 and 254) and the gateway as 192.168.1.1. Or enter the IP address that came from the ISP DHCP server of the Router.
2. Start up your browser and type **192.168.1.1** as the address to enter the web-based manager.
3. Go to **Advanced User > Configuration >WAN Configuration > Create a New PVC** and select the Data Mode –**RFC1483 Bridged**. Then click **Next** button.
4. Enter the VPI/VCI values provided by your ISP and select the encapsulation type as **LLC/SNAP** or **VC MUX**. Then click **Apply**.
5. Save the configuration from **System** >**Save Configuration** and **System** >**Restart** to restart your router for initiating these settings.

MER Mode



BRAS Broadband Remote Access Server

Description:

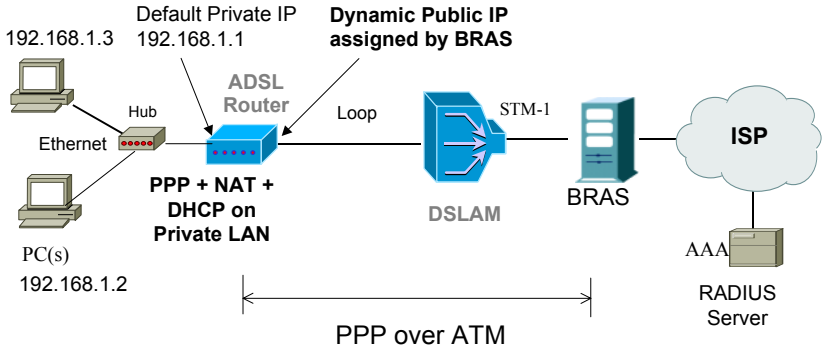
In this deployment environment, we make up a private IP network of 192.168.1.1. NAT function is enabled to support multiple clients to access Internet.

In this example, the ADSL Router acts as NAT device, which translate a private IP address into a public address. Therefore multiple users can share with one public IP address to access Internet through this router. The public address can be a static public address that is pre-assigned by ISP or a dynamic public address that is assigned by ISP DHCP server.

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Advanced User > Configuration > WAN Configuration > Create a new PVC** and select the Data Mode –**RFC1483 MER**. Then click **Next** button.
3. Enter the VPI/VCI values provided by your ISP and select the encapsulation type as **LLC/SNAP** or **VC MUX**. Then click **Apply**.
4. Set IP configuration for Local WAN IP Address. Choose **Specify an IP Address** item. Please set as the following example,
   IP Address: **10.3.86.105** (should be the one that you get from ISP)
   Subnet Mask: **255.255.255.0**
5. Go to **Configuration > IP Route** and click **Create a new route** to add a new route. Configure the settings as the following example,
   Destination Address: leave default
   Netmask: leave default
   Forward packets to: **Gateway Address: 10.3.86.1** (you should get this value from your ISP)
   Then click **Apply**.
6. Go to **Configuration > DNS** and enable **DNS Relay** setting and click **Next**. On the DNS Relay web page, enter the DNS Server IP address, for example **168.95.1.1** (you should get this value from your ISP).
7. Save the configuration from **System** >**Save Configuration** and **System** >**Restart** to restart your router for initiating these settings.
8. Then you have set the web configuration successfully. And you can surf on the Internet.

PPPoA + NAT Mode



* BRAS：Broadband Remote Access Server

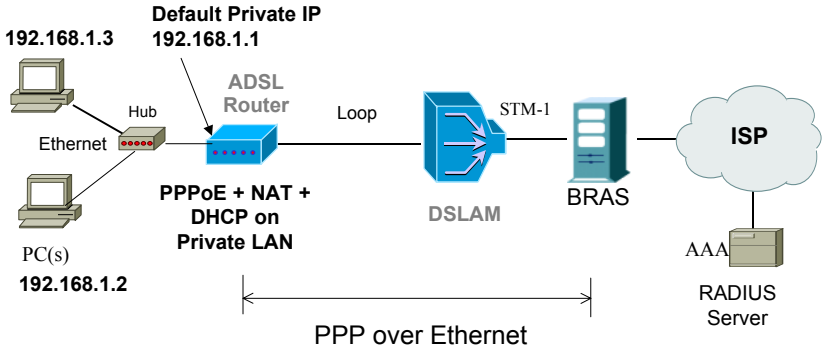
Description:

In this deployment environment, the PPPoA session is between the ADSL WAN interface and BRAS. The ADSL Router gets a public IP address from BRAS when connecting to DSLAM. The multiple client PCs will get private IP address from the DHCP server enabled on private LAN. The enabled NAT mechanism will translate the IP information for clients to access the Internet.

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Advanced User > Configuration > WAN Configuration > Create a new PVC** and select the Data Mode – **PPPoA**. Then click **Next** button.
3. Enter the VPI/VCI values provided by your ISP and select the encapsulation type as **LLC/SNAP** or **VC MUX**.
4. Fill in the **User Name** and **Password** (you should get from ISP). Check on **Enable NAT on this interface** and click **Apply.**
5. Go to **Configuration > DNS** and enable **DNS Relay** setting and click **Next**. On the DNS Relay web page, enter the DNS Server IP address, for example **168.95.1.1** (you should get this value from your ISP).
6. Save the configuration by execute **System** >**Save** and **System** >**Restart** to restart your router for initiating these settings.

PPPoE + NAT Mode



* BRAS：Broadband Remote Access Server

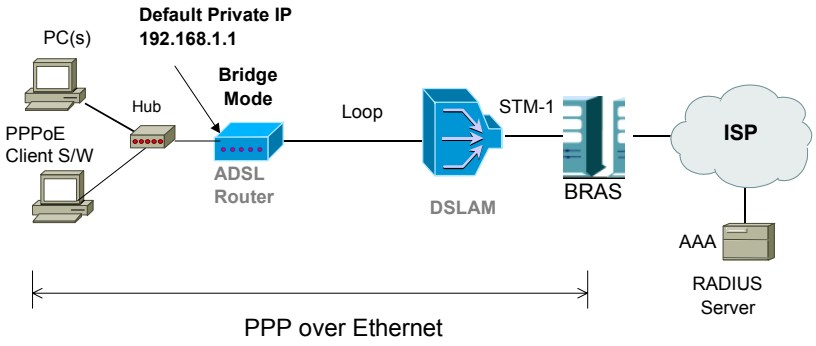
Description:

In this deployment environment, the PPPoE session is between the ADSL WAN interface and BRAS. The ADSL Router gets a public IP address from BRAS when connecting to DSLAM. The multiple client PCs will get private IP address from the DHCP server enabled on private LAN. The enabled NAT mechanism will translate the IP information for clients to access the Internet.

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Advanced User > Configuration > WAN Configuration > Create a new PVC** and select the Data Mode – **PPPoE**. Then click **Next** button.
3. Enter the VPI/VCI values provided by your ISP and select the encapsulation type as **LLC/SNAP** or **VC MUX**.
4. Fill in the **User Name** and **Password** (you should get from ISP). Check on **Enable NAT on this interface** and click **Apply.**
5. Go to **Configuration > DNS** and enable **DNS Relay** setting and click **Next**. On the DNS Relay web page, enter the DNS Server IP address, for example **168.95.1.1** (you should get this value from your ISP).
6. Save the configuration by execute **System** >**Save** and **System** >**Restart** to restart your router for initiating these settings.

PPPoE Relay



BRAS Broadband Remote Access Server

Description:

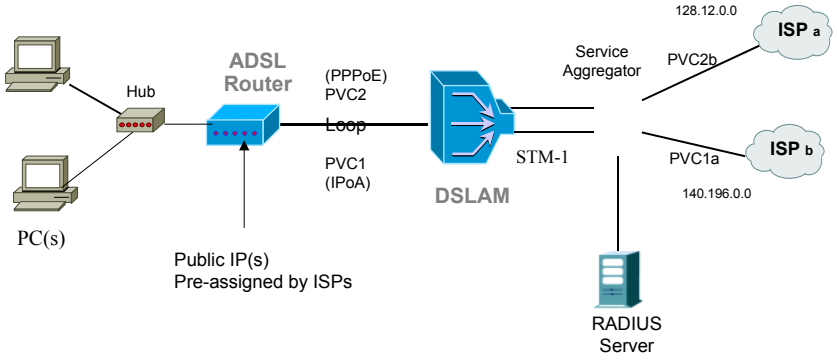
In this example, the ADSL Router acts as a bridge which bridging PC IP address from LAN to WAN. Client PCs on the LAN should be equipped with PPPoE software to get public IP address from BRAS.

That is to say, the router does not require a public IP address. It only has a default private IP address (192.168.1.1) for management purpose.

Configuration:

1. Choose a client PC and set the IP as 192.168.1.x (x is between 2 and 254) and the gateway as 192.168.1.1. Or enter the IP address that came from the ISP DHCP server of the Router.
2. Start up your browser and type **192.168.1.1** as the address to enter the web-based manager.
3. Go to **Advanced User > Configuration >WAN Configuration > Create a New PVC** and select the Data Mode –**RFC1483 Bridged**. Then click **Next** button.
4. Enter the VPI/VCI values provided by your ISP and select the encapsulation type as **LLC/SNAP** or **VC MUX**. Then click **Apply**.
5. Save the configuration from **System** >**Save Configuration** and **System** >**Restart** to restart your router for initiating these settings.
6. Download the PPPoE client from the Belgacom website: (http://slf.skynet.be/static/pc/support/solution/adsl/drivers/Enternet15b.zip)
7. Run Windows PPPoE client application. Fill in the **User Name** and **Password** (you should get from ISP).
8. Click **Connect**.

Multiple PVCs Mode



Description:

As this ADSL Router supports multiple PVCs in the ADSL loop, you are allowed to configure several logical channels in one physical loop. You can use mixed encapsulation types by applying them to different PVCs. When the system starts up, it will connect to CO site through the PVCs according to the sequence they are created. Therefore the default route will be the last PVC you created. You can also modify the default route manually from the **IP Route** page.

The traffic from CPE side will be sent to different PVCs according to the routing rules.

Configuration:

1. Start up your browser and type 192.168.1.1 as the address to enter this ADSL web-based manager.
2. Create the first PVC (e.g. PVC1) using the **RFC1483** data mode.
   Refer to the section of "Router Mode" for details.
3. Create the second PVC (e.g.PVC2) using the **PPPoE** data mode. Refer to the section of "PPPoE + NAT Mode" for details.
4. Save the configuration by execute **System** >**Save** and **System** >**Restart** to restart your router for initiating these settings.

Chapter 6: Troubleshooting

If the suggested solutions in this section do not resolve your issue, contact your system administrator or Internet service provider.

Problems with LAN

PCs on the LAN can not get IP addresses from the ADSL Router.

The chances are that the interface used as DHCP server is modified and the clients PCs do not renew IP addresses.

If your DHCP server is enabled on Private IP Address previously and you modify the interface to Public IP Address, the client PCs should renew IP addresses.

The PC on the LAN cannot access the Web page of the ADSL Router.

Check that your PC is on the same subnet with the ADSL Router.

The virtual server can't be access after setting virtual server.

Check the filter rule of the port that virtual server service setting for example, the virtual server service set FTP 21 you need update the filter rule of the ftp 21 **Direction** setting**:** Choose filter the packets that incoming action (In Bound) are **Allow** on the interface.

Problems with WAN

You cannot access the Internet.

- If your ADSL Router is set to routing mode and you use private IP addresses on the LAN, go to **WAN Configuration > ATM PVC > Setup the ATM PVC Interface** page. Make sure that **Enable network address Translation (NAT)** is checked.
- Check the IP settings:
  Go to LAN Configuration > IP Address page, ensure you specify IP address on Public IP Address field.

  Or go to WAN Configuration > ATM PVC > Setup the ATM PVC Interface page, ensure you specify IP address on Specified Local WAN IP address field
- Check the physical connection between the ADSL Router and the LAN.

  If the DSL LED on the front panel is off or keeps blinking, there may be problem on the cable connecting to the ADSL Router.

  At the DOS prompt, ping the IP address of the ADSL Router, e.g., ping 192.168.1.1. If the following response occurs:

  ```
  Relay from 192.168.1.1 bytes=32 time=100ms TTL=253
  ```

  Then the connection between the ADSL Router and the network is OK.

  If you get a failed ping with the response of:

  ```
  Request time out
  ```

  Then the connection is fail. Check the cable between the ADSL Router and the network.
- Check the DNS setting of the ADSL Router.

  At the DOS prompt, ping the IP address of the DNS provided by your ISP. For example, if your DNS IP is 168.95.1.1, then ping 168.95.1.1. If the following response occurs:

  ```
  Relay from 168.65.1.1 bytes=32 time=100ms TTL=253
  ```

  Then the connection to the DNS is OK.

  If you get a failed ping with the response of:

```
Request time out
```

Then the DNS is not reachable. Check your DNS setting on the ADSL Router.

Problems with Upgrading

The following lists the error messages that you may see during upgrading and the action to take.

- **Error Message**: invalid checksum

  Possible cause: The firmware file to be used is damaged or the file format is wrong.

  Action: Make sure that your firmware file format is valid or get a new firmware file.

- **Error Message**: invalid hardcode

  Possible cause: The firmware file is not compatible with the model of your ADSL Router.

  Action: Download a compatible firmware from the web.

- **Error Message**: unknown flags type

  Possible cause: The firmware version is not compatible.

  Action: Download a compatible firmware from the web.

- **Error Message**: internal isfs error / internal flashfs error

  Possible cause: System error occurs. It may cause by the lack of memory.

  Action: Reboot your ADSL Router and perform the upgrade task again.

- **Error Message**: invalid file format

  Possible cause: The firmware file format is invalid.

  Action: Check the file format is correct, otherwise download a firmware file with correct format.

- **Error Message**: get an error message

  Possible cause: The TFTP server responses with error message.

  Action: Make sure the file name you enter is correct. Otherwise the TFTP server may response with the error message “File not found”.

- **Error Message**: transfer time out

  Possible cause: The transfer session is interrupted.

  Action:
  a. Make sure the TFTP server is on the same subnet with the ADSL Router.
  b. Make sure you the IP address of the TFTP server you specify is correct and that your TFTP server is started.
  c. If error still occurs, reboot your ADSL Router and perform the upgrade task again.

- **Error Message**: firmware update in process

  Possible cause: The upgrade is already in process.

  Action: Do not turn off your ADSL Router otherwise you will cause damage to the device.

- **Error Message**: no remote server IP

  Possible cause: The IP address of the TFTP server is not specified.

  Action: Specify the IP address of the TFTP server is not specified.

- **Error Message**: can't allocate update buffer

  Possible cause: It may cause by the lack of memory.

  Action: Reboot your ADSL Router and perform the upgrade task again.

Chapter 7: Glossary

ARP (Address Resolution Protocol)

ARP is a TCP/IP protocol for mapping an IP address to a physical machine address that is recognized in the local network, such as an Ethernet address.

A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

Inverse ARP (In-ARP), on the other hand, is used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

DHCP (Dynamic Host Configuration Protocol)

When operates as a DHCP server, the ADSL Router assign IP addresses to the client PCs on the LAN. The client PCs "leases" these Private IP addresses for a user-defined amount of time. After the lease time expires, the private IP address is made available for assigning to other network devices.

The DHCP IP address can be a single, fixed public IP address, an ISP assigned public IP address, or a private IP address.

If you enable DHCP server on a private IP address, a public IP address will have to be assigned to the NAT IP address, and NAT has to be enabled so that the DHCP IP address can be translated into a public IP address. By this, the client PCs are able to access the Internet.

LAN (Local Area Network) & WAN (Wide Area Network)

A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN, on the other hand, is an outside connection to another network or the Internet.

The Ethernet side of the ADSL Router is called the LAN port. It is a twisted-pair Ethernet 10Base-T interface. A hub can be connected to the LAN port. More than one computers, such as server or printer, can be connected through this hub to the ADSL Router and composes a LAN.

The DSL port of the ADSL Router composes the WAN interface, which supports PPP or RFC 1483 connecting to another remote DSL device.

NAT (Network Address Translation) IP Address

NAT is an Internet standard that translates a private IP within one network to a public IP address, either a static or dynamic one. NAT provides a type of firewall by hiding internal IP addresses. It also enables a company to use more internal IP addresses.

If the IP addresses given by your ISP are not enough for each PC on the LAN and the ADSL Router, you need to use NAT. With NAT, you make up a private IP network for the LAN and assign an IP address from that network to each PC. One of some public addresses is configured and mapped to a private workstation address when accesses are made through the gateway to a public network.

For example, the ADSL Router is assigned with the public IP address of 168.111.2.1. With NAT enabled, it creates a Virtual LAN. Each PC on the Virtual LAN is assigned with a private IP address with default value of 192.168.1.2 to 192.168.2.254. These PCs are not accessible by the outside word but they can communicate with the outside world through the public IP 168.111.2.1.

Private IP Address

Private IP addresses are also LAN IP addresses, but are considered "illegal" IP addresses to the Internet. They are private to an enterprise while still permitting full network layer connectivity between all hosts inside an enterprise as well as all public hosts of different enterprises.

The ADSL Router uses private IP addresses by assigning them to the LAN that cannot be directly accessed by the Internet or remote server. To access the Internet, private network should have an agent to translate the private IP address to public IP address.

Public IP Address

Public IP addresses are LAN IP addresses that can be considered "legal" for the Internet, because they can be recognized and accessed by any device on the other side of the DSL connection. In most cases they are allocated by your ISP.

If you are given a range of fixed IP addresses, then one can be assigned to the router and the others to network devices on the LAN, such as computer workstations, ftp servers, and web servers.

PVC (Permanent Virtual Circuit)

A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.

RIP (Routing Information Protocol)

RIP is a routing protocol that uses the distance-vector routing algorithms to calculate least-hops routes to a destination. It is used on the Internet and is common in the NetWare environment. It exchanges routing information with other routers. It includes V1, V2 and V1&V2, which controls the sending and receiving of RIP packets over Ethernet.

UDP (User Datagram Protocol)

UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.

Virtual Server

You can designate virtual servers, e.g., a FTP, web, telnet or mail server, on your local network and make them accessible to the outside world. A virtual server means that it is not a dedicated server -- that is, the entire computer is not dedicated to running on the public network but in the private network.

VPI (Virtual Path Identifier) & VCI (Virtual Channel Identifier)

A VPI is a 8-bit field while VCI is a 16-bit field in the ATM cell header. A VPI identifies a link formed by a virtual path and a VCI identifies a channel within a virtual path. In this way, the cells belonging to the same connection can be distinguished. A unique and separate VPI/VCI identifier is assigned in advance to indicate which type of cell is following, unassigned cells, physical layer OAM cells, metasignalling channel or a generic broadcast signaling channel. Your ISP should supply you with the values.

Appendix: Specification

Software

ADSL Compliance

- ANSI T1.413 Issue 2
- ITU G.992.2 Annex A (G.lite)
- ITU G.992.1 Annex A (G.dmt)
- ITU G.992.1 Annex B (G.dmt)
- ITU G.994.1 (G.hs)

Wireless LAN Features

- Fully compatible to IEEE 802.11b standard and allow operating range up to 150 meters (outdoor) and 30 meters (indoor).
- The Direct Sequence Spread Spectrum (DSSS) technology is exploited.
- Seamless roaming within the 802.11 and 802.11b wireless LAN infrastructure
- Low power consumption via efficient power management

ATM Features

- Compliant to ATM Forum UNI 3.1 / 4.0 Permanent Virtual Circuits (PVCs)
- Support up to 8 AAL5 Virtual Circuit Channels (VCCs) for UBR, CBR, VBR-rt, and VBR-nrt with traffic shaping
- TR-037 Auto PVC (auto-provisioning)
- RFC1483 (RFC2684) LLC Encapsulation and VC Multiplexing over AAL5
- RFC2364 Point-to-Point Protocol (PPP) over AAL5
- RFC2225 Classical IP and ARP over ATM
- RFC2516 PPP over Ethernet: support Relay (Transparent Forwarding) and Client functions
- OAM F4/F5 End-to-End/Segment Loopback Cells

Bridging Features

Supports self-learning bridge specified in IEEE 802.1D Transparent Bridging

- Supports up to 4000 learning MAC addresses
- Transparent bridging among 10/100 Mb Ethernet and 802.11b Wireless LAN interfaces

Routing Features

- UPnP IGD (Internet Gateway Device) with NAT traversal capability support
- NAT (Network Address Translation) / PAT (Port Address Translation) let multiple users on the LAN to access the internet for the cost of only one IP address and enjoy various multimedia applications.
- ALGs (Application Level Gateways): such as NetMeeting, FTP, Quick Time, mIRC, Real Player, CuSeeMe, etc.
- Multiple Virtual Servers (e.g., Web, FTP, Mail servers) can be setup on user's local network.
- Static routes, RFC1058 RIPv1, RFC1723 RIPv2.
- DNS Relay
- ARP Proxy

Security Features

- PAP (RFC1334), CHAP (RFC1994) for PPP session
- Firewall support IP packets filtering based on IP address/Port number/Protocol type and TCP code field flags
- Intrusion Detection provides protection from a number of attacks (such as SYN/FIN/RST Flood, Smurf, WinNuke, Echo Scan, Xmas Tree Scan, etc)
- WEP (Wired Equivalent Privacy) encryption uses RC4 with 64/128 bit key length

Configuration and Management

- User-friendly embedded web configuration interface with password protection
- Remote management accesses control
- Telnet session for local or remote management
- HTTP firmware upgrades via web browser GUI directly
- Distribute IP addresses to end users via DHCP server provided by ADSL router
- SNMPv1/v2c agent with MIB-II, PPP MIB, ADSL Line MIB

Hardware

Interface

- One RJ-11 port for ADSL connection
- Four RJ-45 port for IEEE 802.3 10/100 Base-T auto-sensing Ethernet connection
- Hidden PCMCIA interface for IEEE 802.11b (2.4 GHz) wireless LAN connection
- One hidden reset button for restoring to factory default settings

Regulatory Approvals and Compliance

- EMI/Immunity: FCC part 15 and part 68 Class B
- Safety: UL, CE

Power Requirement and Operation Environment Requirement

- Power Adaptor: Input 110±10 or 230±10 VAC; Output 12 VDC, 1A
- Power Consumption: less than 10 Walt
- Ambient Temperature: 0 to 45°C (32 to 113°F)
- Relative Humidity: 20% to 90% (non-condensing)

Physical

- Dimensions: 220mm(L) x 155mm(W) x 38mm(H)
- Weight: 515g