Broadband Wireless Router

User's Manual

2003/04/02

Rev:01

000026-rtw

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 file. 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 file.
- 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.
- Please choose a flat place surface to locate this device in level. If you put the device vertically, it might be unsteady and might fall down. We are not responsible for such happening.

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.

FCC Information

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

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

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

Contents

Before you use

The Wireless Broadband Router is a long-range, high performance wireless LAN product, which provides Access Point services to a 2.4 GHz RF network and bridges to an Ethernet backbone and routes to an Ethernet WAN port. The Wireless Broadband Router performs all the necessary inter-networking, bridging and routing functions. It receives data from both networks, stores them locally for further processing, installs and maintains connections, and transmits the packets to the proper destination.

The Wireless Broadband Router connects computers and laptops to your local network through wireless connection. The Radio Frequency (RF) waves link the wireless clients to the Access Point, and the Access Point works as a bridge between the wireless clients and the wired LAN or Ethernet clients.

The Wireless Broadband Router is compliant with the IEEE 802.11 / IEEE 802.11b DSSS specification and is Wi-Fi certified. Thus all wireless clients, even from different vendors, that meet the 802.11b standard can access your Ethernet network through this Wireless Access Point. Also, with throughput performance of up to 11 Mbps, the wireless connection is as efficient as the wired connection. The wireless LAN security is provided through its WEP (Wireless Equivalent Privacy) support.

Wireless Broadband Router has 4 10/100 Mbps switch ports. This switching automatically detects the speed of the device that you plug into it and routes it to the appropriate port.

Features

Router Features

◆ NAT let multiple users on LAN to access the Internet for the cost of only one IP address and enjoy various multimedia applications.

◆ ALGs(Application Level Gateways) support. (NetMeeting, MSN Messenger, MSN Game Zone, Battle.net and else)

◆ Trigger port mechanism support that can allow new application through NAT

◆ UPnP support (include NAT traversal)

◆ DMZ hosting, Multiple Virtual Servers (e.g., Web, FTP, Mail servers) can be setup in local network.

◆ Static Route, RIP v1, v2

◆ Multiple kind of WAN connection: PPPoE, DHCP Client, Fixed IP, PPTP

◆ DHCP Server, DNS Relay, SNTP (Time Zone) setup, DDNS support

◆ Mac cloning (for WAN connection is DHCP client)

◆ Support VPN PPTP pass through, IPSec Pass through

◆ IGMP support Router mode and Proxy mode

Bridging Features

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

◆ Transparent Bridging between 4-port 10/100 MB Ethernet switch and 802.11b Wireless LAN interface.

Security Features

◆ PAP(RFC1334), CHAP(RFC1994) for PPPoE session

◆ Wireless support WEP (Wired Equivalent Privacy) uses RC4 with 40/64 and 128 bit key length. Passphrase key generation support.

◆ 802.1x support (also include WEP key distribution support)

◆ Mac address Filter

◆ Schedule and Group base content filtering, URL filtering and IP filtering

Wireless LAN Features

◆ Fully compatible to 802.1lb standard, allowing up to 11Mbps wireless rate with distance up to 300 feet/90 meters.

◆ The 2.4 GHz Direct Sequence Spread Spectrum (DSSS) technology is exploited.

◆ Seamless roaming within wireless LAN infrastructure.

◆ Wireless clients association list

◆ Wireless clients Mac address filter

◆ Support disable the broadcast of SSID

Configuration and Management

◆ Enable/disable Remote Management (ping and web browse)

◆ Login / Logout of web management

◆ Configurable through Web Browser

◆ HTTP firmware upgrades via Web browser directly

◆ Support DHCP Server function for IP distribution to local network users

◆ E-mail Alert and Event Logging. Also provide different level of event alert and log

System Requirements

For using Wireless Broadband Router, you have to make sure you have the following that installed on the clients:

For Wireless Clients

◆ Operating System must be Windows98/2000/NT/ME/XP

◆ Wireless card installed

◆ Wireless card driver

For Ethernet Clients

◆ Operating System must be Windows98/2000/NT/ME/XP

◆ 10/100 Base-T NIC

◆ 10/100 Base-T(UTP) network cable

◆ A Hub

Note: Be aware that Cable/DSL Modem service registered from your Internet service provider is required for Internet access.

Unpacking

After unpack the Broadband Cable/DSL Wireless Router package, please check the contents of the package with the checklist stated below. If you find any item is missing, please contact the dealer directly.

■ Broadband Cable/DSL Wireless Router

■ Power Adapter

■ Power Cord

■ RJ-45 Ethernet Cable

■ Quick Start Guide

■ Driver & Utility Software CD

Subscription for Router Service

To use the Cable/DSL Wireless Router, you have to subscribe for ADSL service from your broadband service

provider. According to the service type you subscribe, you will get various IP addresses:

Dynamic IP: If you apply for dial-up connection, you will be given an Internet account with username and password. You will get a dynamic IP by dialing up to your service provider.

Static IP address: If you apply for full-time connectivity, you may get either one static IP address or a range of IP addresses from your service provider. The number of IP addresses varies according to different ADSL service provider.

Chapter 1: Overview

Before installing the Router, please take a look at the front panel and rear panel of the router. Getting acquainted with both panels will be helpful for installation later.

Physical Outlook

Front Panel

The figure below illustrates the front panel of the Broadband Cable/DSL Wireless Router. It indicates the status of the router in.

After powering on the router, the PWR LED will be on till powering off. These LEDs will not be on simultaneously. When this device is transferring data, the LED will be blinking to indicate that which port that you are using.

PWR	DIAG	LAN1	LAN2	LAN3	LAN4	WLAN	WAN
●	●	●	●	●	●	●	●
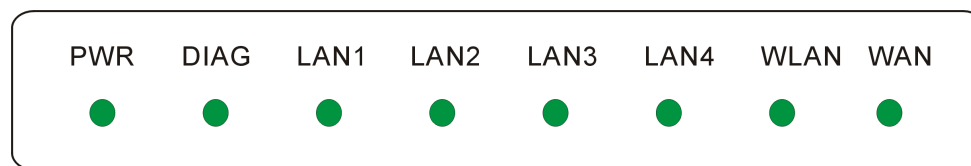
LED Indicators

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

LED	Color	Status	Description
PWR	Green	Unlit	Power off.
		Solid	Power on.
DIAG	Green	Unlit	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.
		Solid	Initial self-test failure or programming FLASH memory failure.
LAN 1 – LAN 4	Green	Unlit	Power off or no Ethernet carrier is present.
		Blinking	Ethernet carrier is present and user data is going through Ethernet port.
		Solid	Ethernet carrier is present.
WLAN	Green	Unlit	Power off or no radio signal (WLAN card is not present or fails to function).
		Blinking	Traffic is going through Wireless LAN interface.
		Solid	Wireless LAN interface ready to work.
WAN	Green	Unlit	Power off or line connection is handshaking or training is in progress.
		Blinking	User data is going through WAN port.
		Solid	Line connection is OK.

Rear Panel

Take a look at the rear panel of this wireless router.
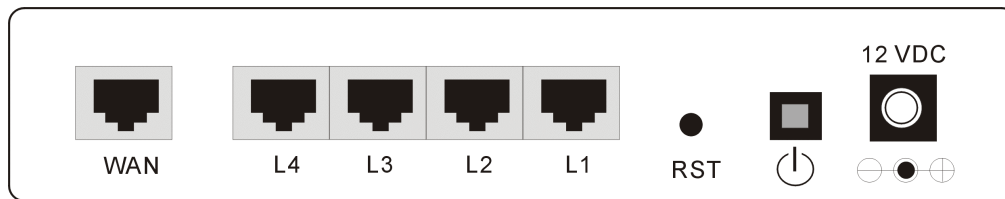
WAN - It is used to connect to an Ethernet port of Cable/DSL modem broadband device.

L1 ~ L4 - LAN port. 10/100 Base-TX

RST - A switch to reset to the default settings.

PWR - Power switch.

12VDC - Power connector.

Chapter 2: Installation

The Broadband Wireless Router incorporates a four-port switch for connection to your local Ethernet network. The Ethernet ports are capable of operation at either 10Mbps (10Base-T) or 100Mbps (100Base-Tx), depending on the Ethernet interface of the attached PC, hub or switch. For any connection which will operate at 100 Mbps, you must use a Category 5 rated cable, such as the Ethernet cable included with the Broadband Wireless Router. Please follow the steps below to connect the router to your computer.

To configure the device via web browser, at least one properly-configured PC must be connected to the **LAN** port (connected directly or through an external hub/switch to the LAN port of the device). The configuration can also be performed on a wireless client station.

On Ethernet Client

To access the Broadband Wireless Router (AP) via the **Ethernet** interface, the host computer must install TCP/IP protocol:

1. Connect the LAN cable to the LAN port of your router. And connect the other end of the cable to the Ethernet port of your client's PC. If you want to connect to a hub or switch, then connect the other end of the cable to the uplink port of the hub.
2. Connect the supplied power adapter to the PWR port on the rear of the router and plug the other end into a power outlet.
3. Press the power button on the rear of the routerj to power on the device.
4. Configure the client PC to get a dynamic IP from the Broadband Wireless Router (AP).
5. Start up your browser and type 192.168.1.1 as the address to enter the web-based manager.
6. Enter the default password - **admin**.
7. Go to **Wizard** to finish basic configuration. Select your WAN connection type. Available options include: **Dynamic IP(Cable Modem),Static IP, PPPoE** and **PPTP**. Follow the onscreen instructions to finish the basic setting procedure. Finally, click Finish to exit basic setting web page.

Note: You should contact your ISP for the correct connection type and its corresponding configuration information.

8. When the connection is established, the client PCs can access the Internet or remote network through the Broadband Wireless Router.

On Wireless Client

1. Connect the supplied power adapter to the PWR port on the rear of the router and plug the other end into a power outlet.

2. Press the power button on the rear of the routerj to power on the device.

3. Install the wireless card driver and verify the wireless setting is as below:
   The default SSID: **IEEE 802.11b LAN**
   WEP encryption is **disabled**. Authentication Type is **Open Key** (or **Open System** according to your Wireless LAN Card).
   Use **Infrastructure** connection mode.

4. Check that the TCP/IP protocol is installed on your wireless client PC. Configure it to get a dynamic IP from the Broadband Wireless Router.

5. Enter the default password - **admin**.

6. Go to **Setup Wizard** to finish basic configuration. Select your WAN connection type. Available options include: **Dynamic IP(Cable Modem),Static IP, PPPoE** and **PPTP**. Follow the onscreen instructions to finish the basic setting procedure. Finally, click Finish to exit basic setting web page.

> **Note:** You should contact your ISP for the correct connection type and its corresponding configuration information.

7. When the connection is established, the client PCs can access the Internet or remote network through the Broadband Wireless Router.

For the wireless-interfaced station, you need to set its SSID to the Broadband Wireless Router (AP)'s default SSID value and disable the WEP encryption.
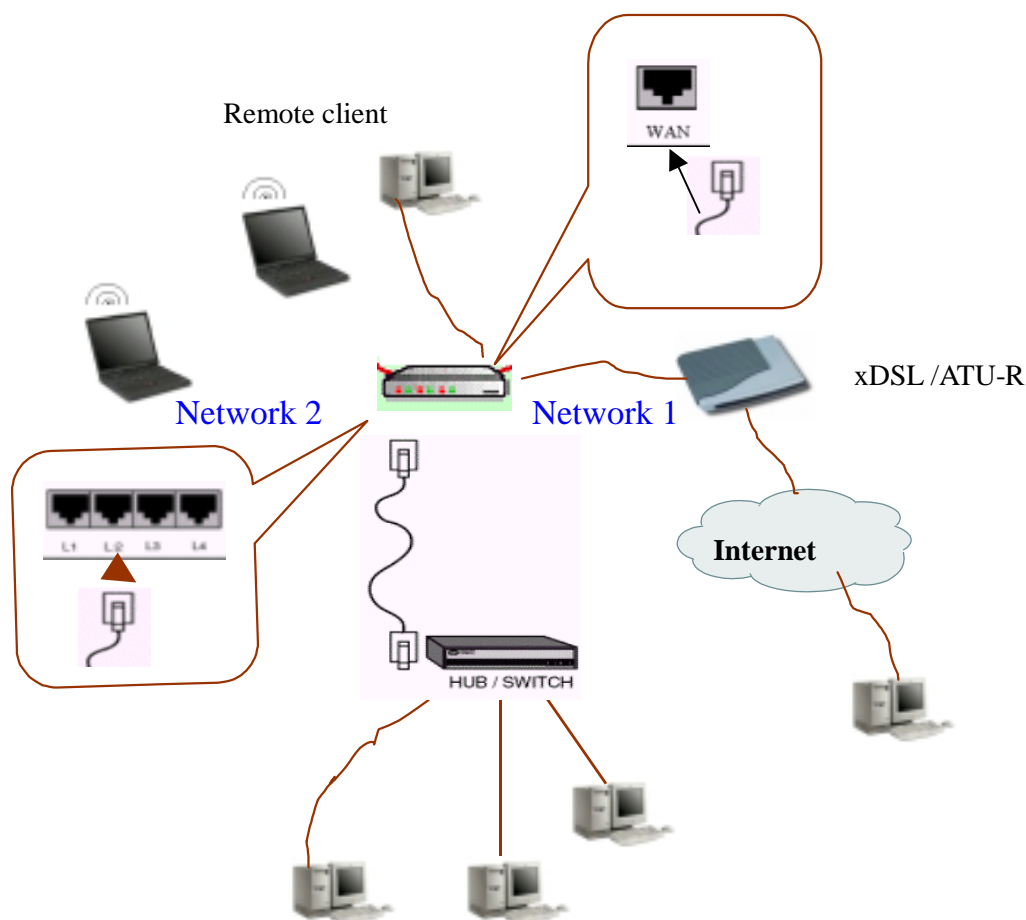
xDSL/ATU-R Modem Connection

The Broadband Wireless Router provides continuous and high-speed access between your wireless and Ethernet devices. In addition, it can connect your entire network to the Internet through an external broadband access device.

Note:
The attached xDSL/ATU-R must provide a standard 10/100Base-T Ethernet connection. Please use the Ethernet cable comes with your broadband device or any other standard 10/100Base-T Ethernet cable.

The Ethernet cable supplied by your ISP for connecting to your xDSL/ATU-R may be an Ethernet crossover cable or a straight-through cable. It is important to use the cable provided by your ISP to connect the modem to your Broadband Wireless Router.

Connecting to Your xDSL Modem

If you are going to connect the WAN port to a DSL modem, follow the steps below:

1. Use the Ethernet cable comes with your DSL modem. Plug one end to the 10/100Base-T Ethernet port of the modem, and the other end to the WAN port on your Broadband Wireless Router.

2. Attach one end of the Ethernet cable with RJ-45 connector to the LAN port of your Broadband Wireless Router, and the other end to a hub or a client PC.

3. At the LAN side, you also can use wireless client at the same time.

4. Set the xDSL Modem's connection mode as bridge mode.

5. Enter the web-based Configuration Manager to configure the WAN setting. Choose the connection type that you registered from your ISP.
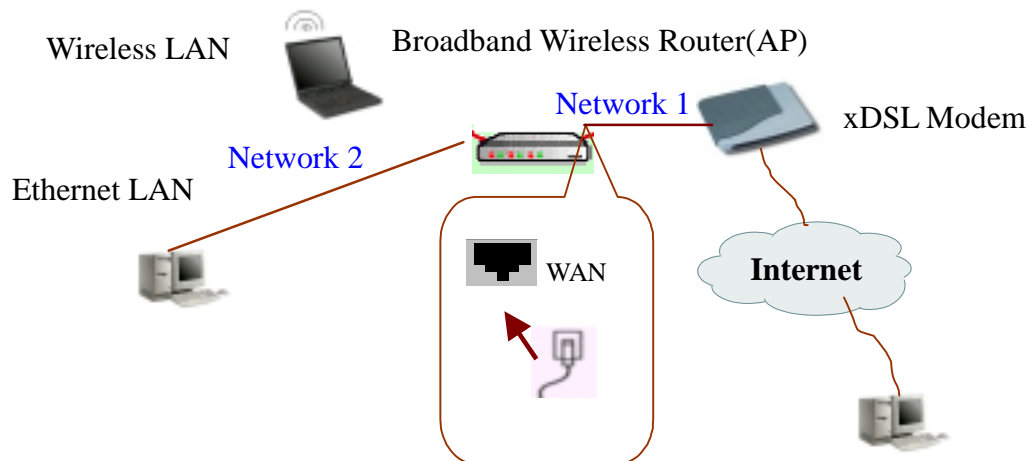
Chapter 3: Configuration

In order to access the Internet through the router, each host on your network must install/setup TCP/IP. Please follow the steps below for select a network adapter.

Setting TCP/IP on Client PC

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

- With Ethernet network interface.

- Must have TCP/IP installed.

- Set client PC with obtain an IP address automatically or set fix IP address.

- With a web browser installed: Internet Explorer 5.x or later.

The Router is configured with the **default IP address of 192.168.1.1** and subnet mask of **255.255.255.0.** As the DHCP server is **Enable** by default, the DHCP clients should be able to access the Router. Or you could assign an IP address to the host PC first for initial configuration.
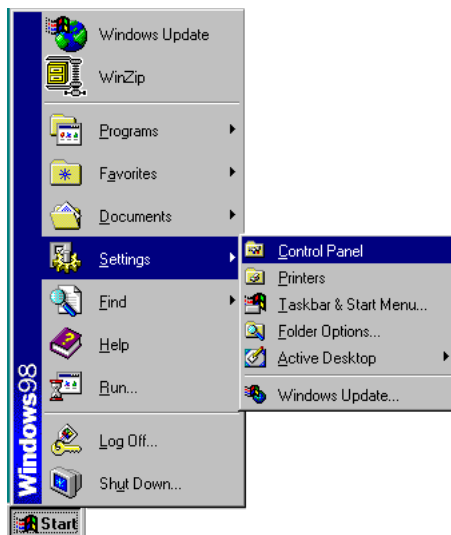
You also can manage the Router through a web browser-based manager. The Router manager uses the HTTP protocol via a web browser to allow you to set up and manage the device.

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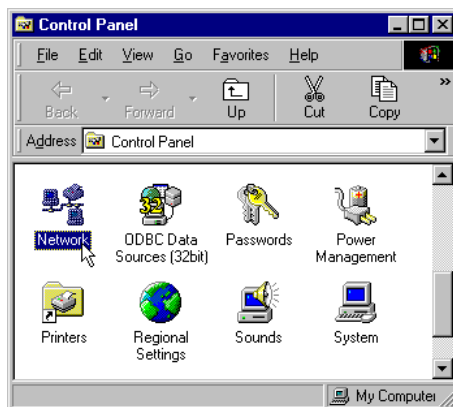
If TCP/IP is not already installed, follow the steps below for installation.

For Windows 98

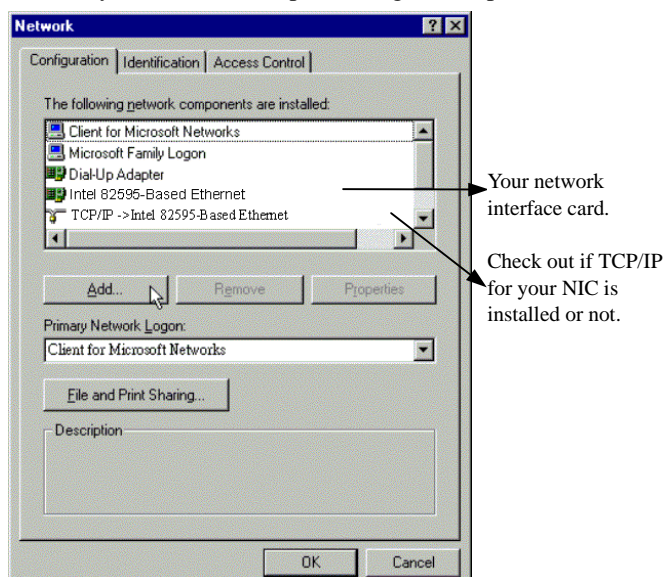1. Click on the **Start** menu, point to **Settings** and click on **Control Panel**.

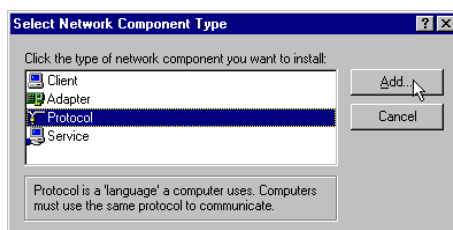2. Double-click the **Network** icon.

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

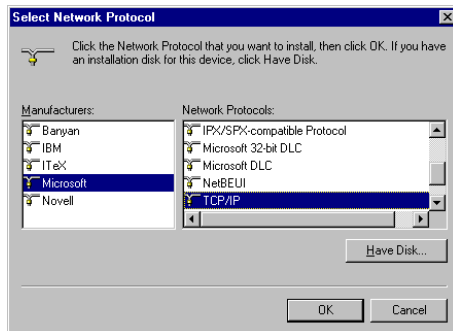   **Option 1:** If you have **no** TCP/IP protocol, click **Add**.

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

Your network interface card.

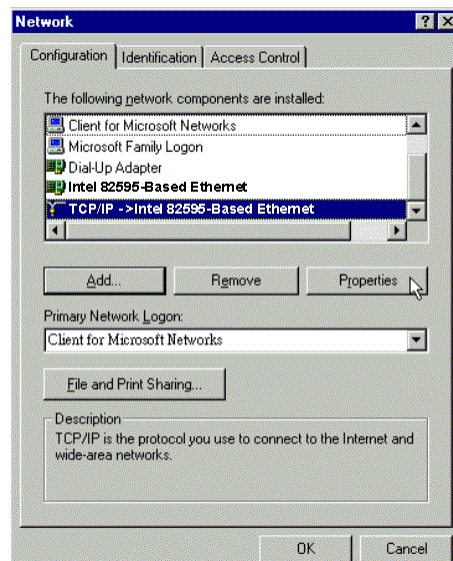Check out if TCP/IP for your NIC is installed or not.

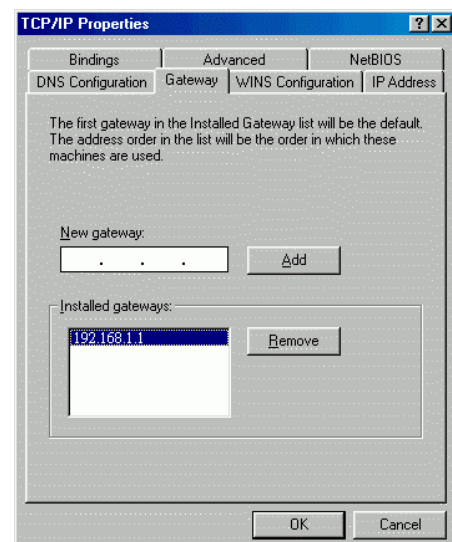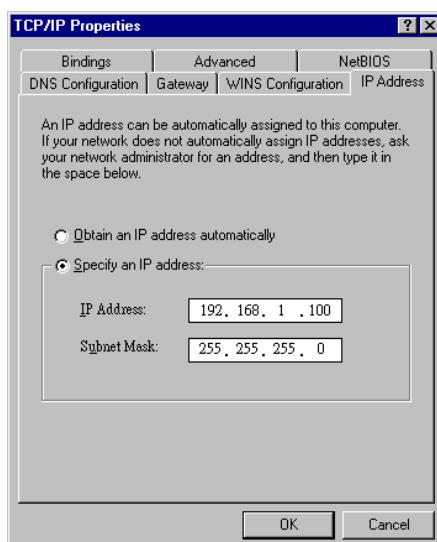4. Highlight **Protocol** and click **Add**.

8

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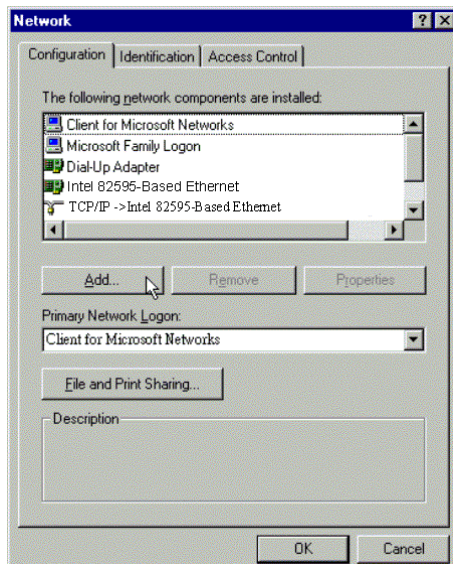

6. When returning to **Network** window, highlight **TCP/IP** protocol for your NIC and click **Properties**.

7. On **IP Address** tab:
   Enable **Specify an IP address** option. Enter the **IP Address**: 192.168.1.x (x is between 2 and 254) and **Subnet Mask**: 255.255.255.0 as in figure below. On **Gateway** tab: Add a gateway IP address: 192.168.1.1. And click **OK**.

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

9. Wait for Windows copying files.
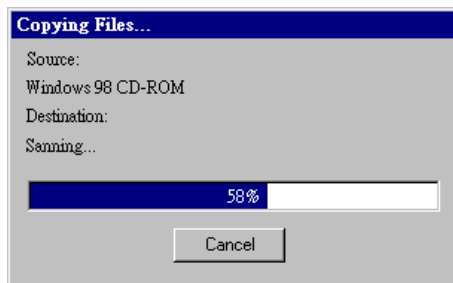
10. When prompted with **System Settings Change** dialog box, click **Yes** to restart your computer.
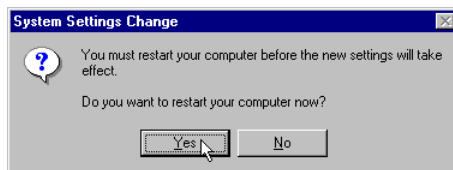
For Windows ME

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

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

3.   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**.
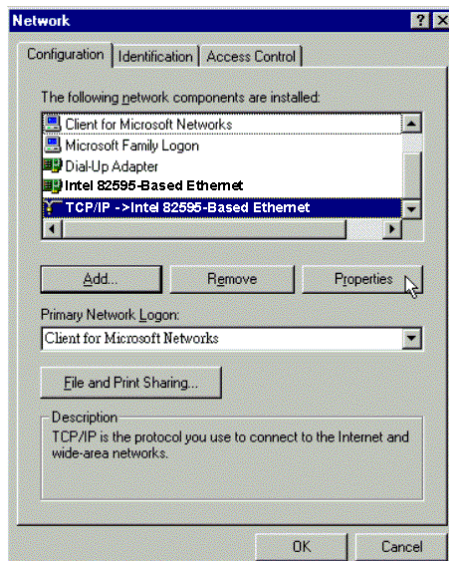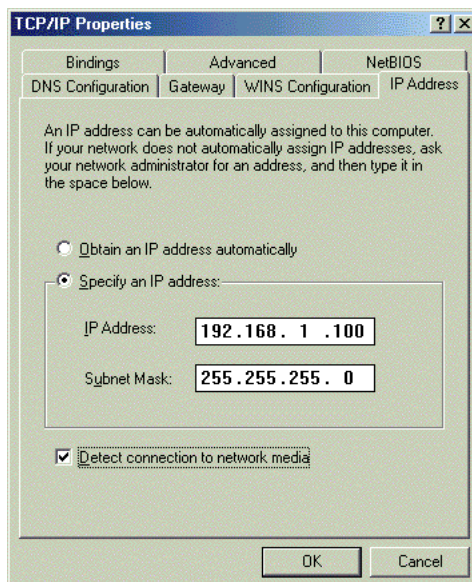
7.   On the **IP Address** tab, select **Specify an IP address**. Enter the **IP address**: **192.168.1.x** (x is between 2 and 254), **Subnet Mask**: **255.255.255.0** and **Default gateway**: **192.168.1.1**. Then click **OK**.

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**.
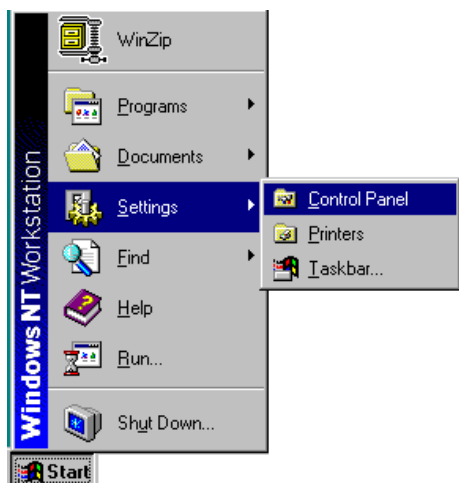
2.   Double-click the **Network** icon.
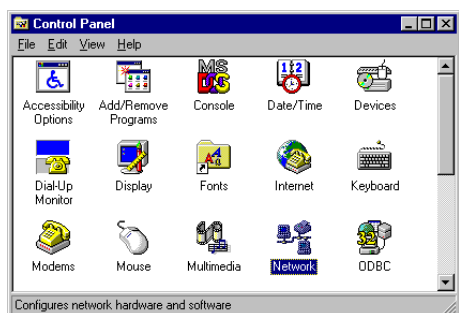
3.   The **Network** window appears. On the **Protocols** tab, check out the list of installed network components.

> **Option 1:** If you have **no** TCP/IP Protocol, click **Add**.
>
> **Option 2:** If you have TCP/IP Protocol installed, go to Step 7.
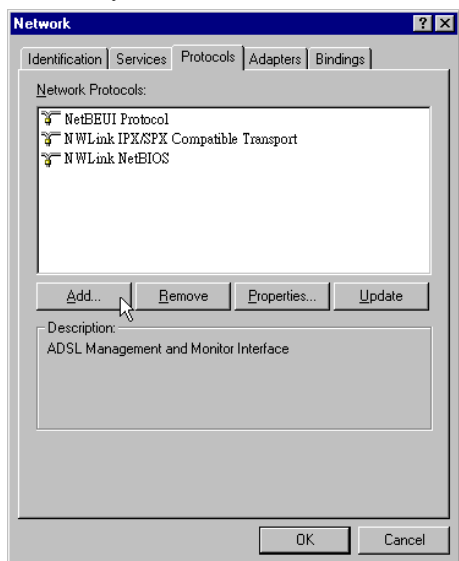
4.   Highlight **TCP/IP Protocol** and click **OK**.
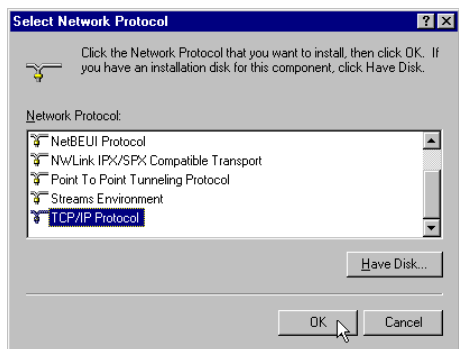
5. Click **Yes** to use DHCP.
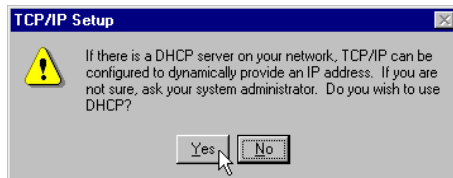
6. Insert the Windows NT CD into your CD-ROM drive and type the location of the CD. Then click **Continue**.
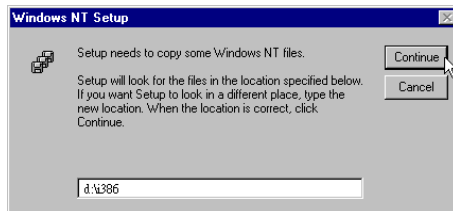
7. Returning to the **Network** window, you will find the **TCP/IP Protocol** among the list. Select **TCP/IP Protocol** and click **Properties**.
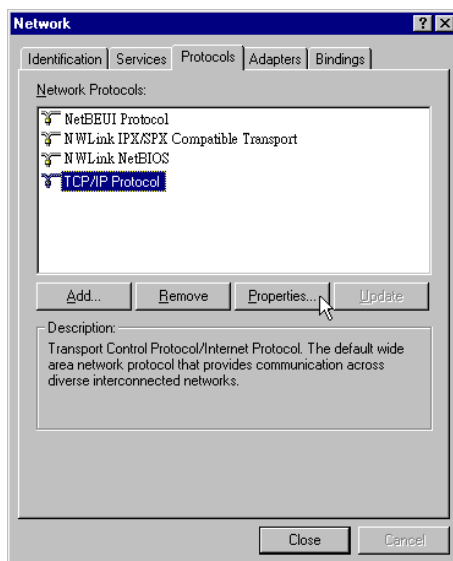
8. Enable **Specify an IP address** option. Enter the **IP Address**: 192.168.1.x (x is between 2 and 254) and **Subnet Mask**: 255.255.255.0 and **Default Gateway**: 192.168.1.1 as in figure below.
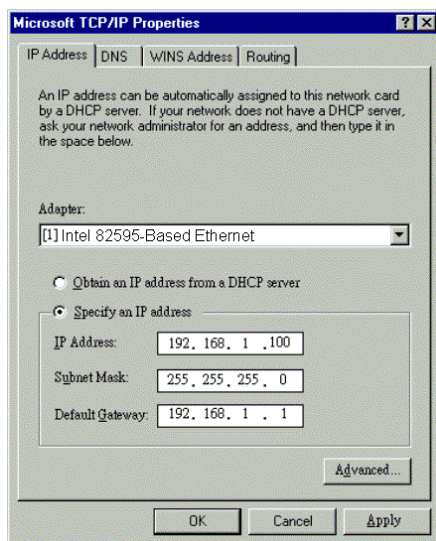

9. When returning to **Network** window, click **Close**.
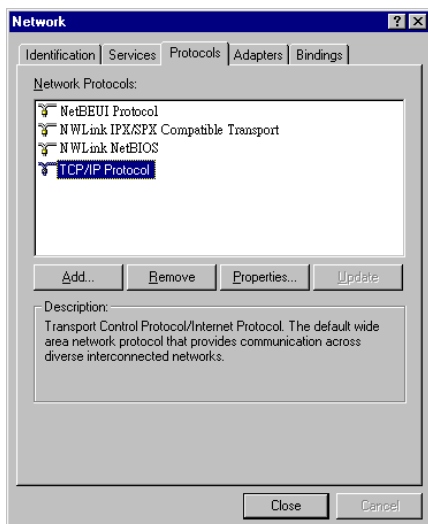
10. When prompted with **Network Settings Change** dialog box, click **Yes** to restart your computer.
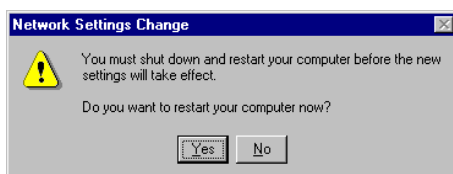
For Windows 2000

1. From the Start menu, point to Settings and then click Network and Dial-up Connections.
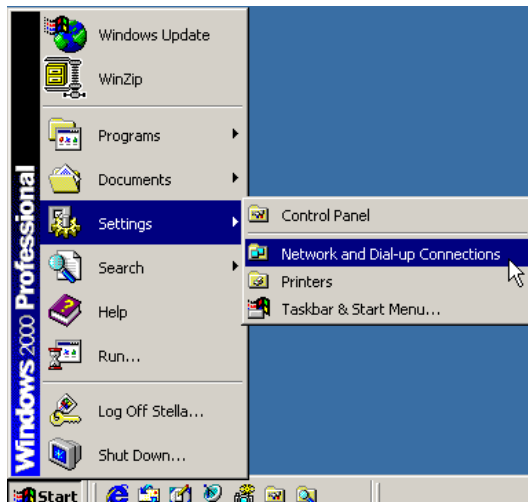
2. Right-click the **Local Area Connection** icon and then click **Properties**.
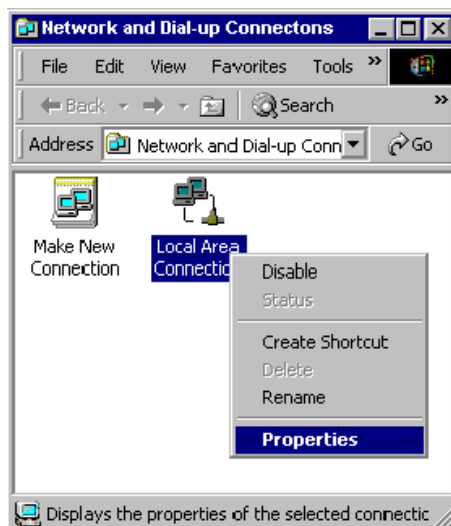
3. On the **General** tab, check out the list of installed network components.

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

    Option 2: If you have TCP/IP Protocol, go to Step 6.
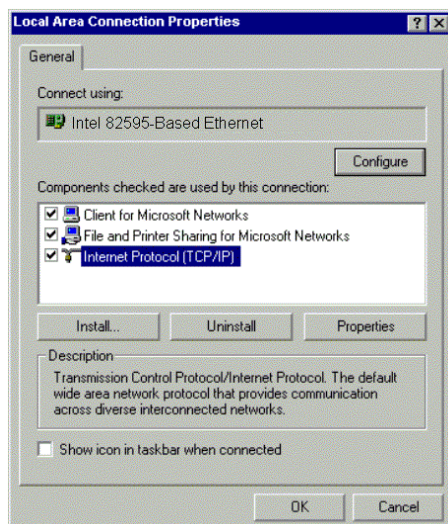
4. Highlight **Protocol** and then click **Add**.
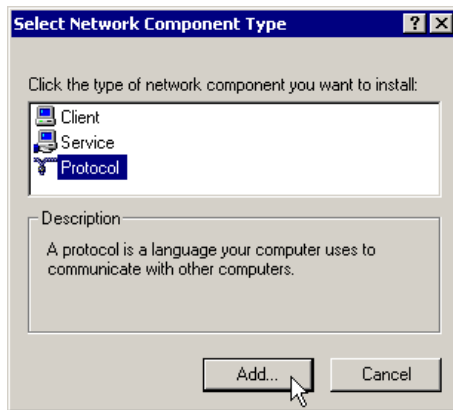
5.   Click Internet Protocol (TCP/IP) and then click OK.
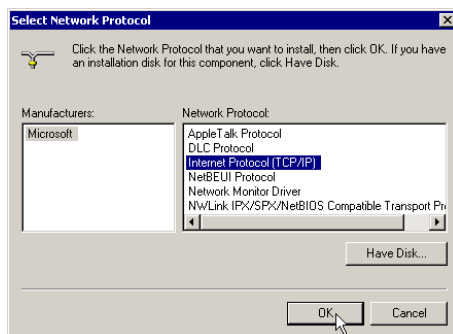
6.   When returning to Local Area Connection Properties window, highlight Internet Protocol (TCP/IP) and then click Properties.
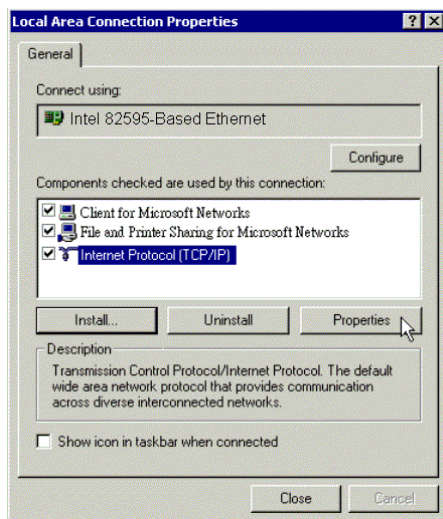
7.   Under the **General** tab, enable **Use the following IP Address**. Enter the **IP address**: **192.168.1.x** (x is between 2 and 254), **Subnet Mask**: **255.255.255.0** and **Default gateway**: **192.168.1.1**. Then click **OK**. When prompted to restart your computer, reboot it to enable the settings.
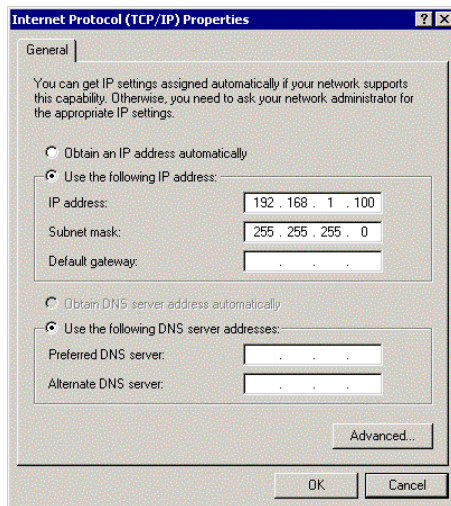
For Windows XP

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**.
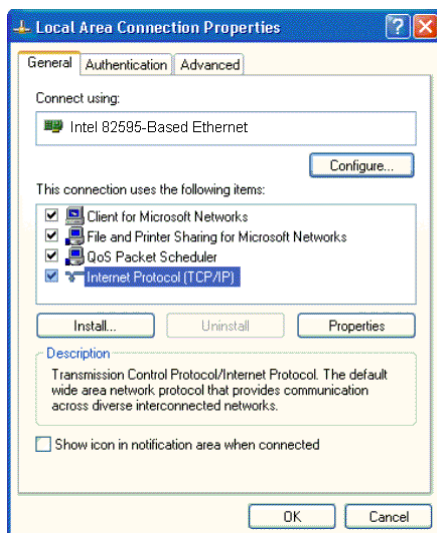

7. Under the **General** tab, enable **Use the following IP address**. Enter the **IP address**: **192.168.1.x** (x is between 2 and 254), **Subnet Mask**: **255.255.255.0** and **Default gateway**: **192.168.1.1**. Then click Ok
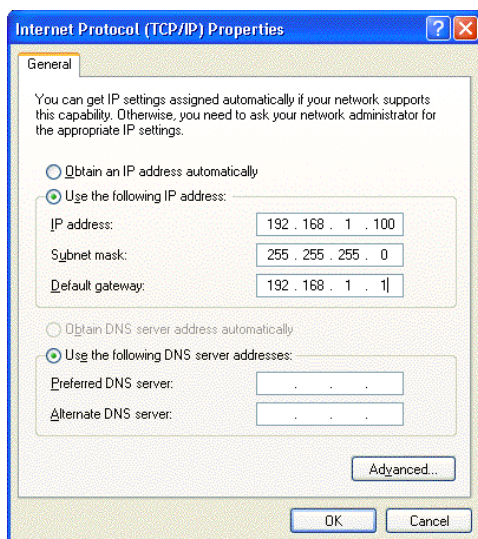
Configure PC to get IP address from DHCP

If your ADSL Router operates as a DHCP server for the client PCs on the LAN, you should configure the client PCs to obtain a dynamic IP address. Please follow the previous section to install TCP/IP component. Only that you do not need to specify an IP address when configuring TCP/IP properties.

The following section describe the procedures for CPEs to get IP address:

For Windows 98

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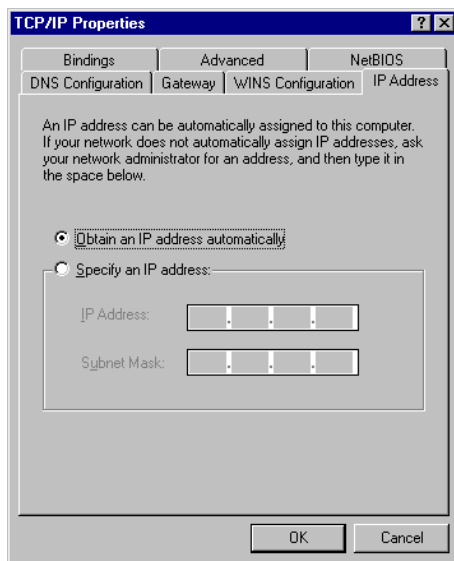
For Windows ME

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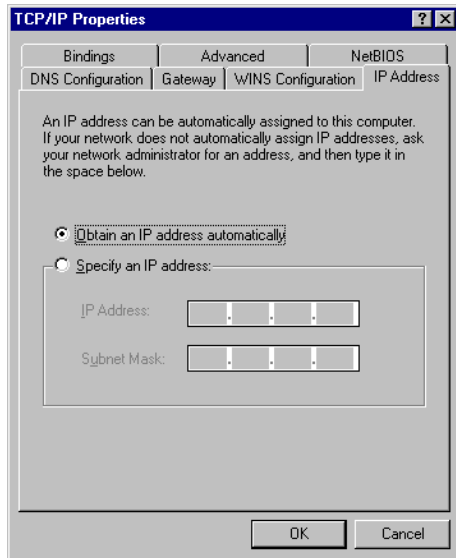
For Windows NT

On the **IP Address** tab, click on the drop-down arrow of **Adapter** to select required adapter. Enable **Obtain an IP address from a DHCP server** and then click **OK**.
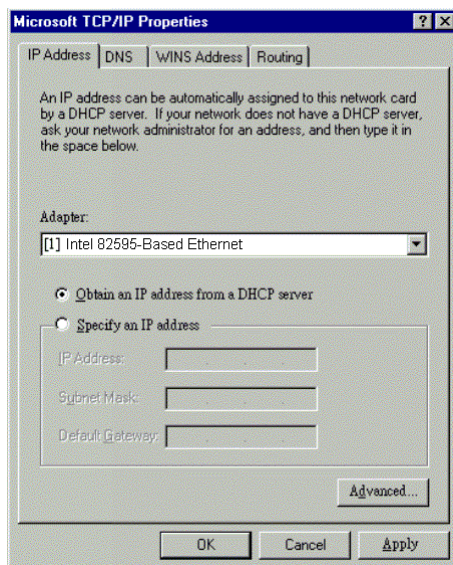
When prompted with the message below, click **Yes** to continue.
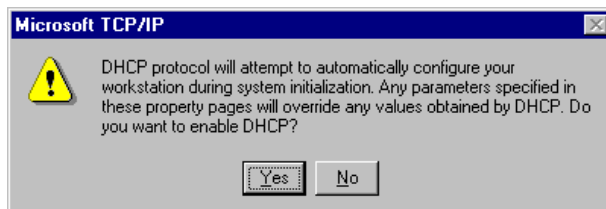
For Windows 2000

Enable **Obtain an IP address automatically** and then click OK.
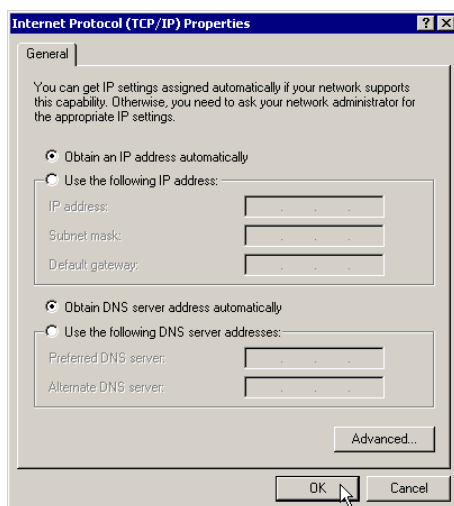
For Windows XP

On the **IP Address** tab, select **Obtain an IP address automatically**. Then click **OK**.
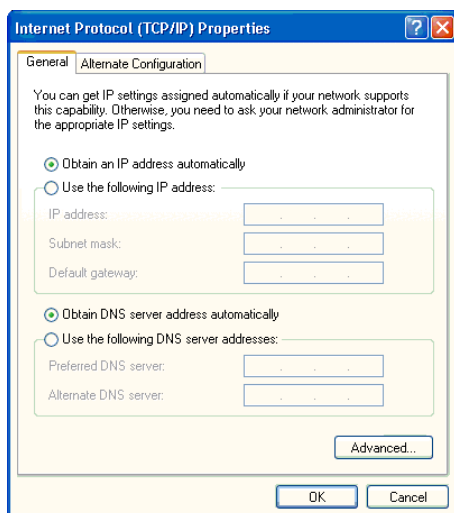
Renew IP Address on Client PC

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

For Windows 98

1.   Select **Run** from the **Start** menu.
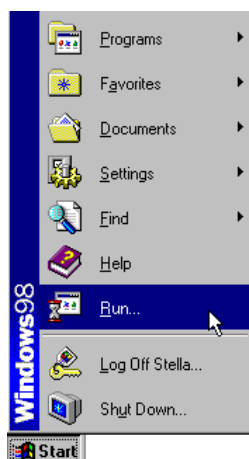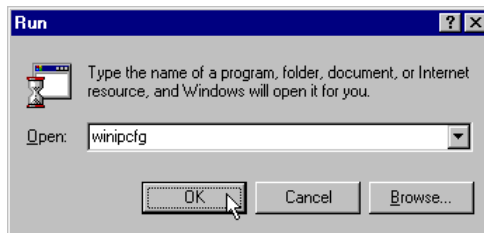
2.   Type **winipcfg** in the dialog box and the click **OK**.

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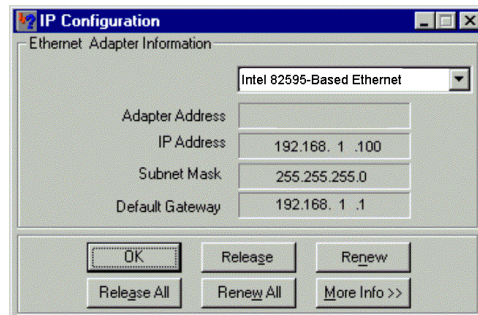
For Windows ME

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.
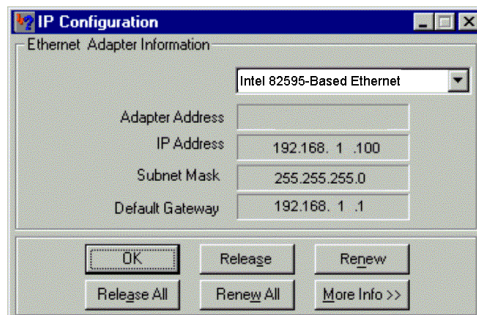
For Windows NT

1.   Select **Run** from the **Start** menu.
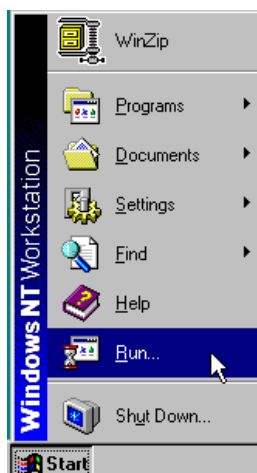
2.   Type **cmd** in the dialog box and the click **OK**.
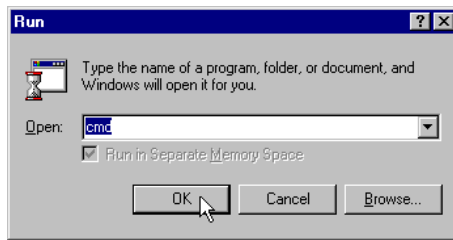
3. Type **ipconfig** at prompt. Then you will see the IP information from DHCP server.

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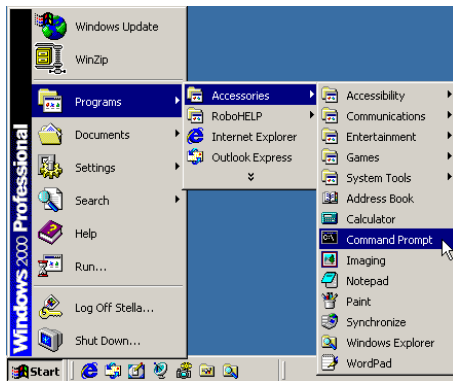
2. Type **ipconfig** at prompt. Then you will see the IP information from DHCP server.

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.

Chapter 4: Web Configuration

Using the Web-Based Manager
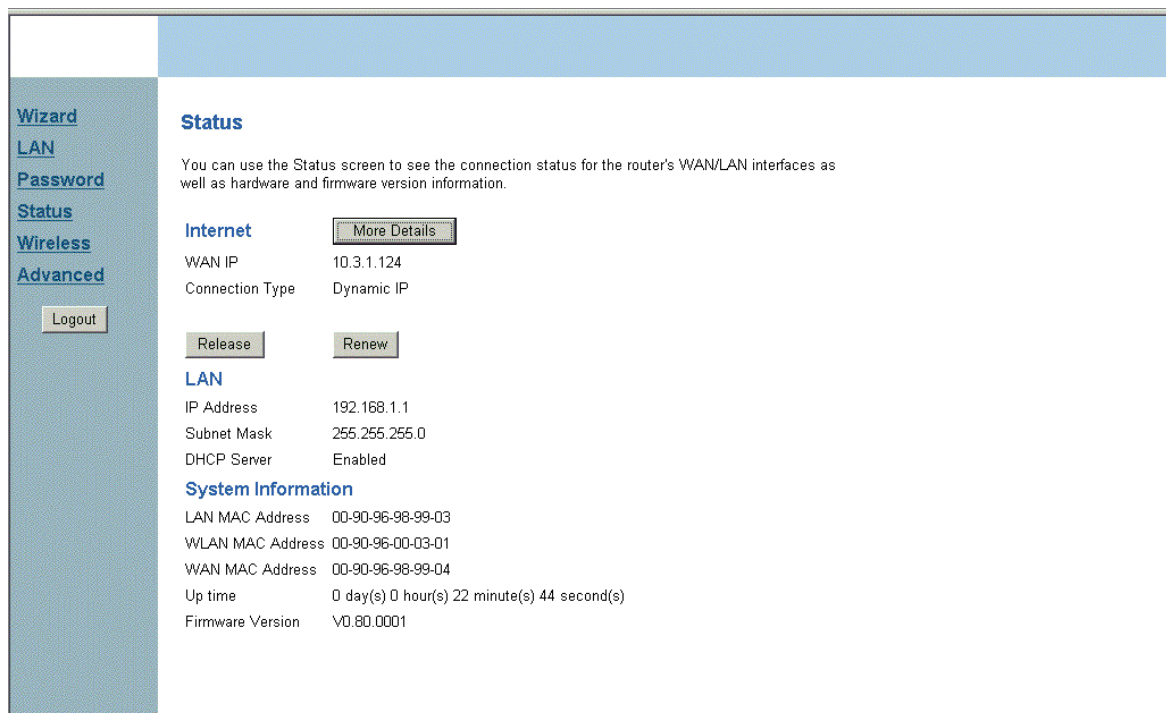
Once your host PC is properly configured as described in previous chapters, please proceed as follows:

1. Start your web browser and type the private IP address of the Wireless Broadband Router in the URL field: **192.168.1.1.**

2. After connecting to the device, you will be prompted to enter password. By default, it is **admin**.

If the login is successfully, the home screen appears. From now on the Router acts as a web server sending HTML pages/forms on your request. Enter the information requested on these pages to configure the Router for Internet access.

Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.

- Changing to another screen without clicking "Save" or "Apply" does NOT save any changes you may have made. You must "Save" or "Apply" before changing screens or your data will be ignored.

- When finished, you should use the "Logout" button, rather than just close your Browser.

Note: On each screen, clicking the "Help" button will display help for that screen. From any help screen, you can access the list of all help files (help index.)

LAN Screen

Use the LAN link on the main menu to reach the LAN screen. An example screen is shown below:

LAN Settings

You can enable DHCP to dynamically allocate IP addresses to your client PCs.

IP Address	192 . 168 . 1 . 1
Subnet Mask	255.255.255.0
DHCP Server	☑ Enable
IP Pool Start Address	192. 168. 1. 2
IP Pool End Address	192. 168. 1. 254
Lease Time	One day ▾
Local Domain Name	(optional)

[Help] [Apply] [Cancel]

IP Address:	IP address for the Router, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask:	The default values 255.255.255.0 is standard for small (class 'C') networks. For other networks, use the Subnet Mask for the LAN segment to which the Router is attached (the same value as the PCs on that LAN segment).
DHCP Server:	If enabled, the Router will allocated IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled.

- If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the Router as the Gateway. See the following section for further details.

- The Start IP Address and Finish IP Address fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported.

See the following section for further details on using DHCP.

IP Pool Start Address:	It decides the start point of an IP range for the DHCP server, usually from 2 to 253.
IP Pool End Address:	It decides the end point of an IP range for the DHCP server, usually from 3 to 254.
Lease Time:	Specify the time that a network device can lease a private IP address before the router reassigning the IP address.
Local Domain Name:	This is an optional setting.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the

Router.

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) server allocates a valid IP address to a DHCP client (PC or device) upon request.

- The client request is made when the client device starts up (boots).

- The DHCP Server provides the Gateway and DNS addresses to the client, as well as allocating an IP Address.

- The Router can act as a DHCP server.

- Windows 95/98/ME and other non-Server versions of Windows will act as a DHCP client. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term Obtain an IP Address automatically instead of "DHCP Client".

- You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

Using the Router's DHCP Server

This is the default setting. The DHCP Server settings are on the LAN screen. On this screen, you can Enable or Disable the Router's DHCP Server function or set the range of IP Address allocated to PCs by the DHCP Server function.

Note: You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you with to use another DHCP Server, rather than the Router's, the following procedure is required.

Disable the DHCP Server feature in the Router's IP Address as the Default Gateway.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 95/98/ME. Refer to Client Configuration for the procedure to check these settings.

Password Screen

The password screen allows you to assign a password to the Router.

Password Settings

Set a password to restrict management access to the router.

Current Password	
New Password	
Confirm New Password	
Idle Time Out	10 Minutes (1 - 99)

[Help] [Apply] [Cancel]

Current Password:	This box allows you to type in current password.
New Password:	If you want to change current password into another new one, you have to type a new password in this box.

Confirm New Password: Retype the new password that you entered in the New Password box to make a confirmation.

Idle Time Out: Type the idle minutes that elapse before the device disconnected automatically.

Apply: Save the data on the screen and apply the data after restarting the router.

Cancel: The "Cancel" button will discard any data you have entered and reload the file from the Router.

Once you have assigned a password to the Router (on the Password screen above) you will be prompted for the pass

Setup

Now you are getting onto the web page for proceeding setting up for your router. To configure your Wireless Broadband Router in easy way, please press **Setup**.

WAN Type

Some types for WAN connection are provided here. Specify a Dynamic IP(Cable Modem), Static IP, PPPoE and PPTP as the WAN connection type. Next pages will be changed slightly according to the connection type you choose here. It allows you to specify how the WAN port of the router connects to your service provider's server. Please choose your connection mode by clicking on the radio button as required by your service provider.

PPPoE: PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection. With PPPoE the client does not set a static IP address, instead an IP address is assigned dynamically whenever the client access to the Internet.

WAN Type

Specify the WAN connection type required by your Internet Service Provider.

- ⦿ **Dynamic IP(Cable Modem)**
- ○ **Static IP**
- ○ **PPPoE**
- ○ **PPTP**

[Help]

For Dynamic IP (Cable Modem), the settings will be:

Dynamic IP (Cable Modem)

Host Name	[ ]

MAC Clone Address   [00] - [90] - [96] - [98] - [99] - [04]   ☐ Enable

[Clone MAC Address]
(This copies the IP address of your PC into the MAC address fields.)

[< Back]   [Help]   [Finish]

Host Name:	Type in your host name.
MAC Clone Address:	Type in the MAC address.
Enable:	Check this box to enable the MAC Clone address for your router.
Clone MAC Address:	Copies the MAC address of your PC to this field.
Back:	If you don't want to adapt this setting, please press the Back button to return to WAN type screen for choosing another setting.
Finish:	Click this button to finish the wizard.

For Static IP, the settings will be:

IP address assigned by your ISP:	Type in the fixed IP address if your service provider has assigned a fixed permanent IP address.
Subnet Mask:	Type in the Subnet Mask address that your service provider assigned for you.
ISP Gateway Address:	Type in the gateway address that your service provider assigned for you.
Back:	If you don't want to adapt this setting, please press the Back button to return to WAN type screen for choosing another setting.
Finish:	Click this button to finish the wizard.

For PPPoE, the settings will be:

User Name:	Type in the user name to access the remote server or your service provider.
Password:	Type in the password to access the remote server or your service provider.
Please retype your password:	Type your password again for confirmation.
Service Name:	Enter the name of your PPPoE service.
MTU (1400-1492):	Enter the maximum transmission rate for the data transferring. The default setting is 1492.
Dial on Demand:	Check on this item to make the system reconnect automatically after disconnected by unknown reason.
Maximum Idle Time:	This value specifies the idle minutes that elapse before the Home Route automatically disconnects the PPP session. If no traffic is passing through during the span of time your specified, the PPP session is terminated.
Back:	If you don't want to adapt this setting, please press the Back button to return to WAN type screen for choosing another setting.
Finish:	Click this button to finish the wizard.

For PPTP, the settings will be:

PPTP

Enter the Account Name, Account Password, Host Name, Remote IP Address, Your IP Address, Your Subnet Mask required by your ISP in the appropriate fields. If your ISP has provided you with a connection ID, enter it in the Connection ID field, otherwise, leave it as zero.

PPTP Account	pptp
PPTP Password	****
Confirm password	****
Host Name	
Remote IP Address	10.3.1.253
My IP Address	10.3.1.2
My Subnet Mask	255.255.255.0
Gateway	10.3.1.254 (Optional)
Connection ID	0 (Optional)
MTU (1400-1460)	1460
Maximum Idle Time	0 minutes ☐ Auto-reconnect

< Back   Help   Finish

PPTP Account:	Type in the user name to access the remote server or your service provider.
PPTP Password:	Type in the password to access the remote server or your service provider.
Confirm password:	Type your password again for confirmation.
Host Name:	Enter the name of your host.
Remote IP Address:	You can assign a remote computer to access into this router for controlling. Please type in the remote IP address in this field.
My IP Address:	Type in your IP address that you get from ISP for connection.
My Subnet Mask:	You have to specify the subnet mask for the router in order to let remote user access into the router that your computer connected.
Gateway:	This is an optional setting. Please enter the Gateway if necessary.
Connection ID:	This is an optional setting. Please enter the connection ID that your ISP provided you if necessary. If not, leave this box as zero.
MTU (1400-1460):	Enter the maximum transmission rate for the data transferring. The default setting is 1460.
Maximum Idle Time:	This value specifies the idle minutes that elapse before the Home Route automatically disconnects the PPTP session. If no traffic is passing through during the span of time your specified, the PPTP session is terminated.
Auto-reconnect:	Check this box if you want the router to be connecting Internet automatically after the Idle time that you set here.
Back:	If you don't want to adapt this setting, please press the Back button to return to WAN type screen for choosing another setting.
Finish:	Click this button to finish the wizard.

Wireless

The Wireless setting must match the other Wireless stations. To change the DSL/Cable router's default settings for the Wireless feature, use the Wireless link on the main menu to reach the Wireless LAN Settings screen.

Wireless LAN

Status

SSID	RTW026
Channel	Channel 11 [2464 MHZ]
WEP Encryption	Disable
WEP Authentication	Open Key

Settings

Wireless SSID	[ ]
Channel	Channel 11 [2464 MHZ] ▼ [Configure WEP]

[Advanced Wireless Settings]   [Advanced Wireless Security]

[Help]   [Apply]   [Cancel]

Wireless SSID: If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).

To communicate, all Wireless stations should use the same SSID/ESSID.

Channel: Select the Channel you wish to use on your Wireless LAN.

If you experience interface (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which is the best.

If using multiple Access Points, adjacent Access Points should us different Channels to reduce interference.

Configure WEP: Click this button will use the passcode for generating WEP keys.

Advanced Wireless Settings: Click this button will pop up another dialog for you to set more detailed settings for the wireless setting.

Advanced Wireless Security: Click this button will pop up another dialog for you to set more detailed settings for the security of the wireless connection.

Apply: Save the data on the screen and apply the data after restarting the router.

Cancel: The "Cancel" button will discard any data you have entered and reload the file from the Router.

Configure WEP

802.1x:	**IEEE 802.1x** is a port based authentication protocol. It can be used in *any* scenario where one can abstract out the notion of a port. It requires entitie(s) to play three roles in the authentication process: that of an supplicant, an authenticator and an authentication server. The diagram below shows the basic scenario.
	Choose Used to indicate that the system will use this function.
	Choose Not Used if this function has not been opened.
WEP Key Distribution:	Choose Enable to activate the WEP key's function.
WEP Mode:	**Disable**
	If choose Disable, data is NOT encrypted before being transmitted.
	64 Bit Encryption
	If selected, data is encrypted, using the default key, before being transmitted. The receiving station must be set to use 64 Bit Encryption, and have the same Key value in the same position in its key table. Otherwise, it will not be able to decrypt the data.
	Default key – select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other keys are for decryption only.
	Key Table:
	This table is used when Encrypting and Decrypting data. All stations, including this Access Point, always transmit data encrypted using their default key. The key number (1,2,3,4) is also transmitted. The receiving station will use the key number (1,2,3,4) to determine which key value to use for decryption. If the key value does not match the transmitting station, decryption will fail.
	The easiest way to ensure there are no problems is to have every Station, including the Access Point, use the same key table (all entries identical)

31

128 Bit Encryption

If selected, data is encrypted using the key before being transmitted. The receiving station must be set to use 128 Bit Encryption, and have the same Key value. Otherwise, it will not be able to decrypt the data.

Keys – Enter the key values you wish to use. Other stations must have the same key values.

Authentication Mode:	Select the appropriate value: "Open System" or "Shared Key". Check your Wireless card's documentation to see what method to use. Some Wireless Cards do not support both methods.
WEP Key Type:	Select ASCII or HEX as the WEP Key display method.
Passphrase:	To generate a set of keys from a word or phrase: 1. Select the type of key required (64-Bit or 128-Bit) 2. Enter the word or phrase in the "Passphrase" field. 3. Click the "Generate Keys" button. 4. The screen will refresh with the key values inserted.
WEP Key #1 - #4:	Please select encryption key length and fill out WEP keys. The system allows you to type in 4 kinds of the WEP key.
Radius Server:	It is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. Choose Enable to activate this function. Type in the necessary settings on to the lines of IP Address, Port, Shared Secret, and Time-out.
Generate Key:	Click this button will use the passcode for generating WEP keys.
Advance Setting:	Click this button will pop up another dialog for you to set more detailed settings for the wireless setting.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

Advance Wireless Settings

SSID Broadcast:	Check this box will disable the function of SSID broadcast. The default setting is unchecked.
Transfer Rate:	It decides the transmission speed for data. Select Auto, the system will choose the proper rate for your data transmission. Otherwise, choose the other specific one such as 1, 2, 5.5, 11Mbps as you desired.
Beacon Interval:	Set the period of beacon transmissions to allow mobile stations to locate and identify a BSS. The measure unit is "time units"(TU) of 1024 microseconds.
RTS/CTS Threshold:	Set the value for sending a request to the destination. All the frames of a length greater than the threshold that you set here will be sent with the four-way frame exchange. And, a length less than or equal to the value that you set will not be preceded by RTS and CTS.
Fragmentation Threshold:	Set the number of the fragmenting frames to make the data be delivered without errors induced by the interference. Frames longer than the value you set here are fragmented prior to the initial transmission into fragments no longer than the value of the threshold.
DTIM Interval:	The value you set here is used to inform mobile stations when multicast frames that have been buffered at the router will be delivered and how often that delivery will happen.
Preamble Type:	This allows you to set the beginning length of a frame. Please set it by choosing Long or Short.
Apply:	Save the data on the screen and apply the data after restarting the router.
Close:	The "Close" button will discard any data you have entered and reload the file from the Router.

Advanced Wireless Security

This feature filters Internet access for local clients based on IP addresses, application types, (i.e., HTTP port), and time of day.

Wireless Association Control: Click Enable to invoke the wireless association control.

Unspecified Wireless MAC address: Click Allow to make any wireless MAC address can be linked to.

Add: It allows you to add in a new MAC address for your router.

Apply: Save the data on the screen and apply the data after restarting the router.

Close: The "Close" button will discard any data you have entered and reload the file from the Router.

For some users might want to set advanced settings for the router, please continue to see the followings sections for more detailed information.

Advanced

Click on Advanced Setup link in the menu to get Advanced configuration options such as: Security, Access Security

Security

Intrusion Detection	☑ Enable
Discard WAN Ping	☐ Enable
Remote Management	☐ Enable 0 . 0 . 0 . 0
Remote Management Port	8080 (1 - 65535)
MAC Address Filtering	☐ Enable [Configuration]

[Help] [Apply] [Cancel]

Intrusion Detect:	It can detect any attacks that penetrate and destroy the firewall & standard detection systems.
	Enable this item to enable the function.
	Disable this item to disable the function.
Discard WAN Ping:	Enable this item will block other computers try to ping your router. Disable this item will allows other computers ping your router.
Remote Management:	Enable this item to activate the remote control from other computers. You have to type in the IP address of the remote computer in this field. If you check this item and do not type any IP address in this field, then all the other computers have the opportunity to control your router.
	Disable this item to close the remote management by other computers.
	Remote Management PortType in the port for the remote control.
MAC Control:	Enable this item to enable the MAC control configuration.
	Disable this item to close the setting.
Configuration:	Allow you to add a new MAC address. See below for more detailed information.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

To have MAC control enable and adding a new one, click MAC Address Filtering check box and press Configuration button. It allows user can access to Internet from LAN to WAN.

Unspecified MAC address: Check Allow box means the one that did not list below can access Internet as well.

Allow Connect to Internet: Check this button to allow connecting to Internet.

MAC Address: Display the MAC Address that you allow it to connect to Internet or not by adding from clicking Add button.

Add: Use this button to new MAC address

Apply: Save the data on the screen and apply the data after restarting the router.

Close: The "Close" button will discard any data you have entered and reload the file from the Router.

Access Control

The Access Control allows you to restrict Internet Access by individual PCs. With the default settings, everyone has unrestricted Internet access.

To use this feature:

1.   Set the desired restrictions on the other groups ("Group 1", "Group 2", "Group 3" and "Group 4") as needed.

2.   Assign PCs to the groups are required.

Restrictions are imposed by blocking "Services", or types of connections. All common services are predefined. If required, you can also define your own services.

To view the Access Control screen, please select Access Control link on the Advanced menu.

Group:	**Select Group:** Select the desired Group. The screen will update to display the settings for the selected Group. Groups are named "Group 1", "Group 2", "Group 3" and "Group 4", and cannot be renamed. **"Members" Button:** Click this button to add or remove members from the current Group. See the following section for details of the Group Members screen.
Access Rights:	**Internet Access for this Group:** Select the desired options for the current group, as detailed below. **No Restriction:** Nothing is blocked. Use this to create the least restrictive group. **Always Block:** All traffic via the WAN port is blocked. Use this to create the most restrictive group. **Block by Schedule:** Block current group during the time that you set here.
Services for Block:	**Define Services:** Select the applications you wish to block. Multiple Services can be selected by holding the CTRL key (on the Macintosh, the SHIFT key) while selecting. **Services button:** Click this button to open the Service window, which allows you to define your own Services.
URL Filter:	**Current URL Filter:** Defined URLs lists any existing entries. If you have not entered any values, this list will be empty.
Content Filter:	**Current Content Filter:** Defined Contents lists any existing contents. If you have not entered any values, this list will be empty.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

Group Members Screen

This screen is displayed when the Members button on the Access Control screen is clicked.

Use this screen to add or remove members (PCs) from the current group.

- The Delete button will remove the selected PC in the Members (PCs) list from the current group.

- The <<Add button will add the new PC that you enter on the box to the right to the current group.

Member (PCs):	List the total members (PCs) that you have set. You can add up to 32 members for a group.
Host:	For single host setting, choose this radio button and type in the specific IP address on the box below.
Subnet:	Allow you to define an IP range for this group.
IP Address:	Type in the IP address that you need it to be included in this group.
Net Mask:	By choosing Subnet radio button, you can enter the value here.
Delete:	Delete the selected member (PC).
Close:	Close this window.

Services

This page allows you to define your own service.
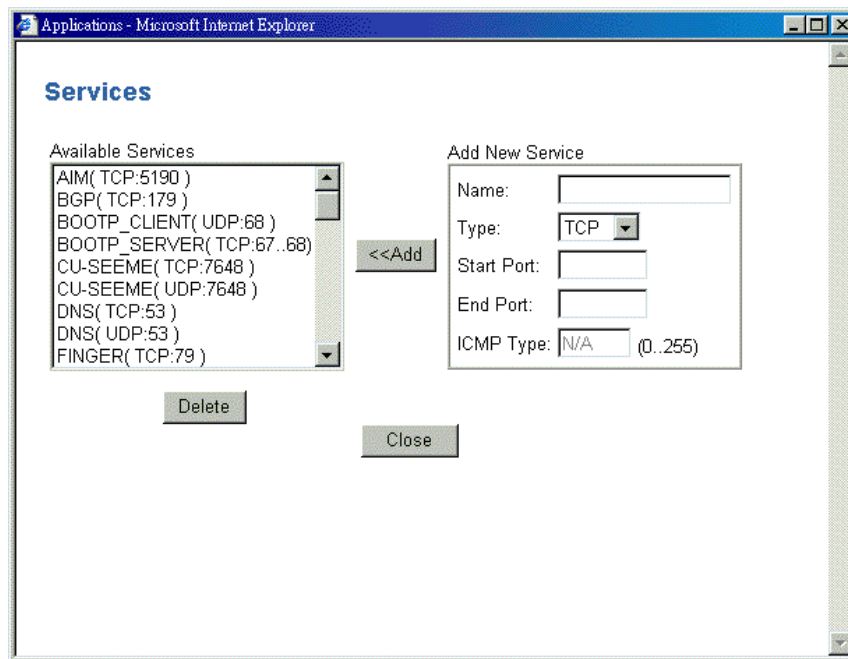
Available Services:	This lists all the available services.
Name:	Type the name that you want to add for a new service.
Type:	Choose the type for the new service.
Start Port:	For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the "Start" and "Finish" fields.
End Port:	For TCP an UDP Services, enter the end of the range of port numbers used by the service. If the service uses a single port number, enter it in both the "Start" and "Finish" fields.
ICMP Type:	For ICMP Services, enter the type number of the required service.
Delete:	Use this to delete any Service you have added.
Close:	Close this window.

Type in the necessary information and click Add. A new one will be displayed on the box of Available Services. Then, click Close to return to the previous web page.

URL Filter

The URL Filter allows you to block access to undesirable Web Sites.

To use this feature, you must define "filter strings". If the "filter strings" appears in a requested URL, the request is blocked.

Content Filter

The Content Filter allows you to block the receiving undesirable web pages with text you type in this field.

To use this feature, you must define the "content".   If the content appears in a web page, that page is not allowed to display on your computer.

NAT

NAT(Network Address Translation) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

NAT Settings

Click the Help button for in-depth descriptions and directions for use of each feature below.

Games & Utilities   Select an Application: | Half life, CounterStrike ▼ |
Send incoming calls to: 192. 168. 1. [ ]

NAT   ☑ Enable (Network Address Translation)

UPnP   ☑ Enable (Universal Plug and Play)

DMZ   ☐ Enable on 192. 168. 1. [ ]

Special Application   [Configuration]

Applications such as Internet gaming, video conferencing, and Internet telephony require multiple connections. The Special Application feature allows these applications to work properly.

Virtual Server   [Configuration]

The "Virtual Servers" feature allows Internet Users to access services such as the Web or FTP on your LAN via public IP address.

[Help]   [Apply]   [Cancel]

Games & Utilities:	Choose the games that you want to run for specific computer which is specified on the line of "Send incoming calls to".
NAT:	Check Enable to activate NAT function.
UPnP:	UPnP allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported by Windows ME, XP or later.
	If Enabled, this router will be visible via UPnP.
	If Disabled, the router will not be visible via UPnP.
DMZ:	If Enabled, it allows one (1) computer on your LAN to be exposed to all users on the Internet, allowing unrestricted 2-way communication between the DMZ PC and other Internet users or Servers.
Special Application:	Set for special applications to let them work properly. Click Configuration to get into another window.
Virtual Server:	Allow users to access services ex. Web on their LAN via public IP address. Click Configuration to get into another window.
Configuration:	Click this button to open another window for configuring special application and virtual server.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

UPnP

Only **Windows XP** supports UPnP function. Before checking this function for proper using, you have to install UPnP component to your computer first. Otherwise, the function will not take effect even click on "Enable (Universal Plug and Play)" check box.

Please follow the steps below for installing UPnP components.

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

2. Select **Add or Remove Programs > Add/Remove Windows Components** to open **Windows Components Wizard** dialog box**.**
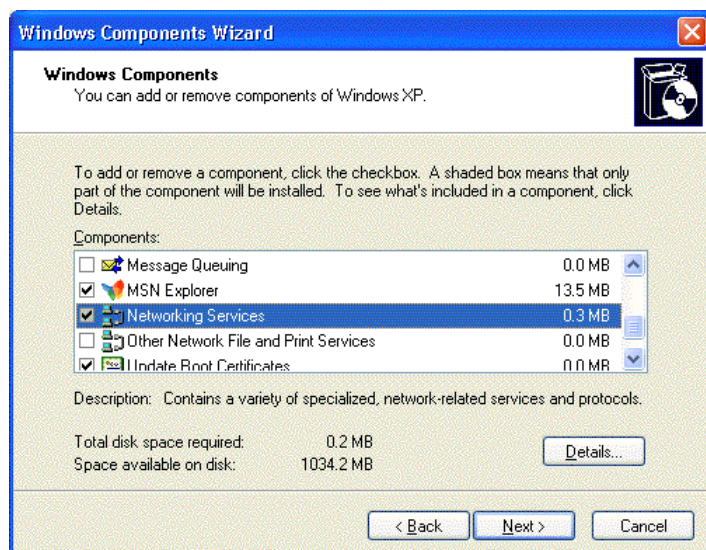
3. Select **Network Services** and click **Details.** Click the **Universal Plug and Play** check box.
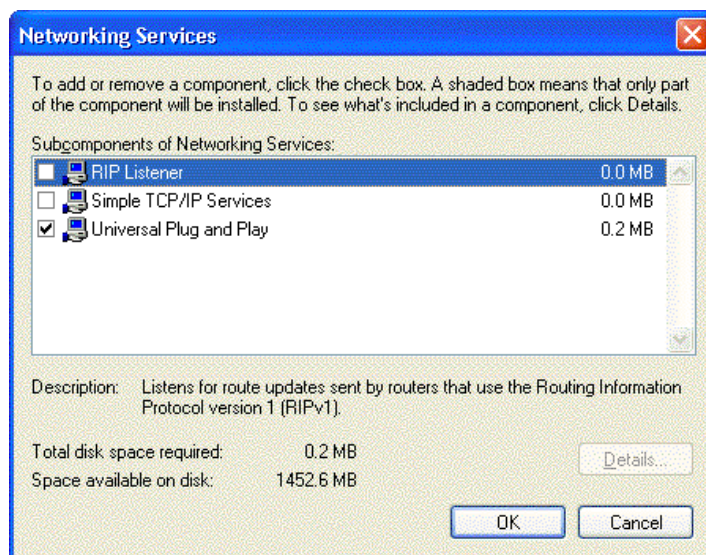
4. Click Ok. The system will install UPnP components automatically.

5. After finishing the installation, go to **My Network Places**. You will find an icon (ex: IEEE802.11b LAN) for UPnP function.
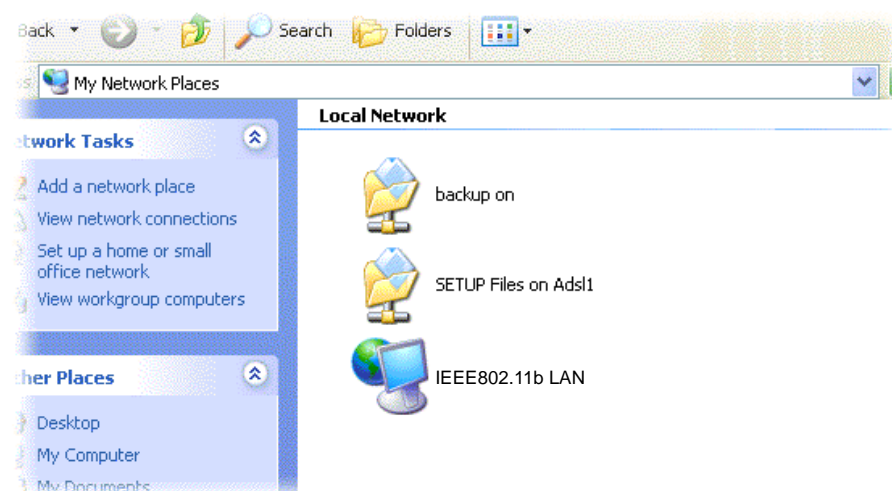
6. Double click the icon, the ADSL router will open another web page for UPnP function. The IE address will be changed as shown as the following graphic.
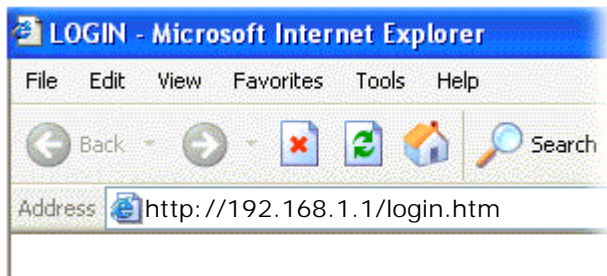
7. Now, the NAT traversal function will be provided. The ADSL router will create virtual server automatically for mapping while the router detecting the computer running some Internet applications.

DMZ

This feature, if enabled, allow one computer on your LAN to be exposed to all users on the Internet, allowing unrestricted 2-way communication between the specified IP address and other Internet users or Servers.

■ This allows almost any application to be used on the specified IP address.

■ The specified IP address will receive all "Unknown" connections and data.

■ If the DMZ feature is enabled, you must type in numbers to specify an IP address.

■ The DMZ feature can be Enabled and Disabled on the NAT setting screen.

Special Application Configuration

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by router's firewall. In this case, you can define the application as a "Special Application".

This screen can be reached by clicking the Configuration button on the Special Application item from NAT web page.

You can define your special applications. Before doing this, you will need some information about the application; this is normally available from the supplier of the application.

Also, please note that the terms "Trigger Port" and "Public Port" on this screen by referring to the traffic from client viewpoint.

Name:	Type the description for the application.
Trigger Port:	It defines the channel that is used to input data from applications. Enter the port number that is used by the application server for the data that you receive from.
Public Port:	It defines the channel that is used to output data to the applications. Enter the port number that is used by the application server for the data that you want to send to it.
Enabled:	Use this check box to enable or disable this Special Application as required.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

Using A Special Application

Please configure the Special Application screen as required.

On your PC, use the application normally. Remember that only one PC can use each Special Application at any time. Also, when one PC is finished using a particular Special Application, it might be need a "Time-Out" before another PC can use the same Special Application. The "Time Out" period may be up to 3 minutes.

Note: If any application still cannot function correctly, try to use the DMZ feature.

Virtual Server Configuration

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 protected the route by filter rule so that you should update the filter rule after you set up virtual server.

Virtual Server allows you to make servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

■   You server does not have a valid external IP Address.

■   Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The Virtual Server feature solves these problems and allows Internet users to connect to your servers, as illustrated below:
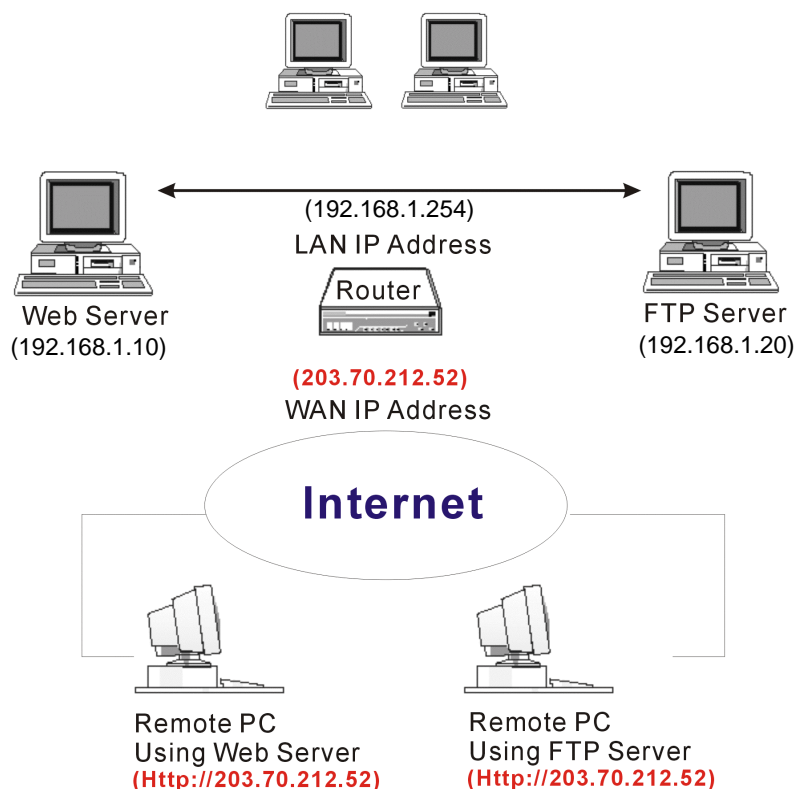
IP Address seen by Internet Users

Please note that, in the above picture, both Internet users are connecting to the same IP address, but using different protocols.

To Internet users, all virtual servers on your LAN have the same IP Address. This IP Address is allocated by your ISP. This address should be static, rather then dynamic, to make it easier for Internet users to connect to your Servers. However, you can use Dynamic DNS feature to allow users to connect to your virtual servers by using a URL, instead of an IP address.

Virtual Server Screen

This screen can be reached by clicking the Configuration button on the Virtual Server item from NAT web page.

Mapping Port:	Enter the port number which the server software is configured to use.
Server IP:	Enter the IP address for the server.
Enabled:	Use this check box to enable or disable this Virtual Server as required.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

Note: For each entry, the computer must be running the appropriate server software.

Defining your own Virtual Servers

If the type of server that you wish to use is not listed on the Virtual Server screen, you can define and manage your own servers:

1. Type in the required data as described above.

2. Click Apply.

3. The new server will now appear on the list.

IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server (located at another internal IP address).

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP.) For example,

    Http://203.70.212.52
    Ftp://203.70.212.52

It is more convenient if you are using a Static IP Address from your ISP, rather than Dynamic. However, you can use the Dynamic DNS feature to allow users to connect to your Virtual Server through a URL, rather than an IP Address.

Routing

Overview

■ If you don't have other routers or gateways on your LAN, you can ignore this Routing page.

■ If the Router is the only acting as a Gateway for the local LAN segment, ignore this Routing page.

■ If your LAN has a standard router on your LAN, and the Router is to act as a gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.

■ If your LAN has other gateways and routers, and you wish to control which LAN segments use each Gateway, do not enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers)

■ If you want to use Windows 2000 Data center server as a software Router, enable RIP on the Router, and ensure the following Windows 2000 settings are correct:

◆ Open Routing and Remote Access

◆ In the console tree, select Routing and Remote Access, IP Routing, RIP

◆ In the "Detail" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".

◆ On the "General" tab, set Outgoing packet protocol to "RIP version 2 broadcast", and Incoming packet protocol to "RIP version 1 and 2".

Routing Screen

This screen is accessed by using Routing link from the Advanced menu. Generally you will use either RIP or the Static Route as explained above. It is impossible to use both methods simultaneously.

For multiple routers that installed on your network, please configure each unit's routing functions for proper using. This setting allows different IP domain users to access the Internet through this device.

Static Route

If RIP is not used, you have to type entries in the Static Route field for each LAN segment on your network, other than the segment to which this device is attached.

The other Routers must also be configured. Refer to Configuring other Routers on your LAN later in this section for further details and an example.

Routing

Routing Infomation Protocol (RIP)

| Receive Mode | Disabled |
| Transmit Mode | Disabled |

Default Gateway

Gateway : 0 . 0 . 0 . 0 .

Static Routing

Destination : __ . __ . __ . __
Subnet Mask : __ . __ . __ . __
Gateway : __ . __ . __ . __   << Add

| Destination | Subnet Mask | Gateway | |

View Routing Table   Help   Apply   Cancel

Routing Information Protocol (RIP)

Receive Mode:
It incorporates the RIP information when receiving the RIP packets. From the drop-down list select which RIP version should be accepted, Disable, RIP1, RIP2 and both.

RIP2 supports broadcasting and multi-cast function.

Transmit Mode:
It broadcasts the routing table. From the drop-down list select which RIP version should be broadcasted, Disabled, RIP1, RIP2 and both.

RIP2 supports broadcasting and multi-cast function.

Default Gateway:	**Gateway:** Type in the value as a default gateway. Keep it in blank as a default gateway if you don't want to change it.
Static Route:	**Destination:** The destination address of the remote LAN segment. For standard class C LANs, the destination address is the first 3 fields. The 4th field can be left at 0. **Subnet Mask:** The subnet mask for the remote LAN segment. For class C networks, the default mask is 255.255.255.0. **Gateway:** The IP address of the Gateway or Router which the Router must use to communicate with the destination above (NOT the router attached to the remote segment).
Add:	Click this button to add in a new static route to your router. The information you created here will be shown on the Routing Table.
View Routing Table:	Click this button to view the routing table.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

Viewing Routing Table

This screen shows a table about routing information, such as Destination LAN IP, Subnet Mask, Gateway, Metric, Interface and so on. The router provides several default routing information. And the one that you added will be added in a proper place.

Destination:	Display the IP address of the destination that you set on Routing screen.
Subnet Mask:	Display the Subnet Mask.

Gateway:	Display the IP address of gateway.
Metric:	The number of hops (routers) to pass through to reach the remote LAN segment. The shortest path will be used. The default value is 0.
Interface:	Displays the interface that your router is using for network connection.
Refresh	Click this button to display the table again.
Close	Click this button to return to main web page.

Configuring Other Routers on Your LAN

It is essential that all IP packets for devices that are not on the local LAN can be passed to the Router, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the Router as the default route or default gateway.

Local Router

The local router is the Router installed on the same LAN segment as the Router. This router requires that the default route is the Router itself. Typically, routers have a special entry for the default route. It should be configured as follows.

Destination-->	Normally 0.0.0.0 but check your router documentation.
Subnet Mask-->	Normally 0.0.0.0 but check your router documentation.
Gateway-->	The IP Address of the Router.

Other Routers on the Local LAN

Other routers on the local LAN must use the Router's Local Router as the Default Route. The entries will be the same as the Router's local router, with the exception of the Gateway IP Address.

For a router with a direct connection to the Router's local Router, the Gateway IP Address is the address of the Router's local router.

For routers which must forward packets to another router before reaching the Router's local router, the Gateway IP Address is the address of the intermediate router.

Example – Static Route

Here provides you an example of Static Route.
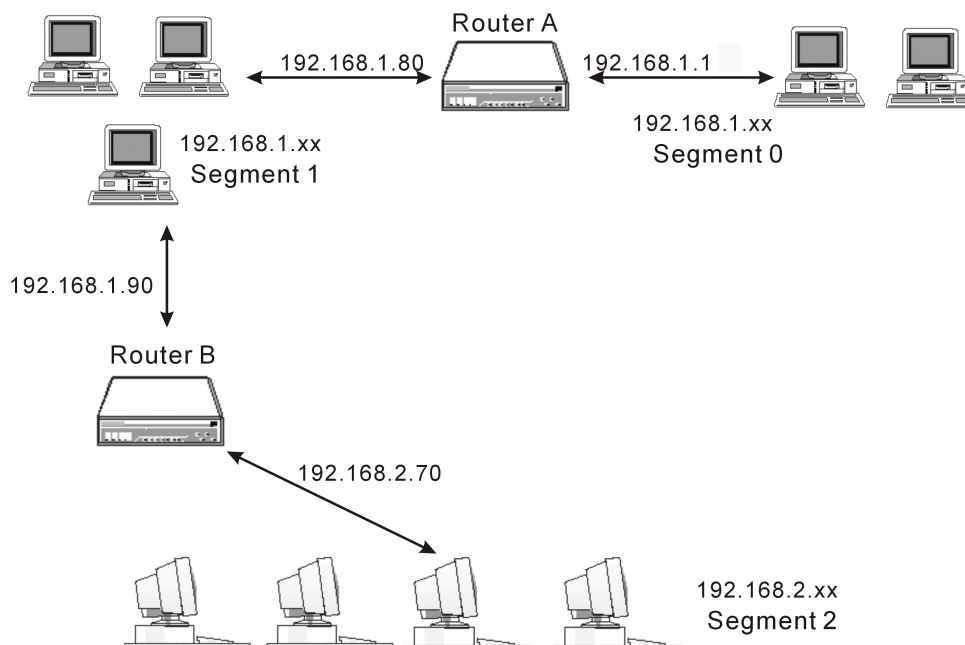
For the Router's Routing Table

49

For the LAN shown above, with 2 routers and 3 LAN segments, the Router requires to add 2 static route as follows:

For segment 1

Destination	192.168.1.0
Subnet Mask	255.255.255.0 (Standard Class C)
Gateway	192.168.1.1 (Router's local router)

For segment 2

Destination	192.168.2.0
Subnet Mask	255.255.255.0 (Standard Class C)
Gateway	192.168.1.1 (Router's local router)

Default Route for Router A

Destination	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	192.168.1.254 (Router's IP Address)

Default Route for Router B

Destination	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	192.168.1.1 (Router's local router)

IGMP

The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers.

Enable:	Check Enable to invoke the IGMP settings. Choose Router Mode or Proxy Mode as the routing method.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

Time Zone

The router's clock must synchronize with global Internet's time. The time you set in the screen will be adapted to system log.

System Time

Connecting to a Simple Network Time Protocol (SNTP) server allows the router to synchronize the system clock to the global Internet. The synchronized clock in the router is used to recored the security log and control client filtering.

Set Time Zone   (GMT-06:00) Central Time (US & Canada)

Daylight Saving   ☑

   Start from

   End by

JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT

Help   Apply   Cancel

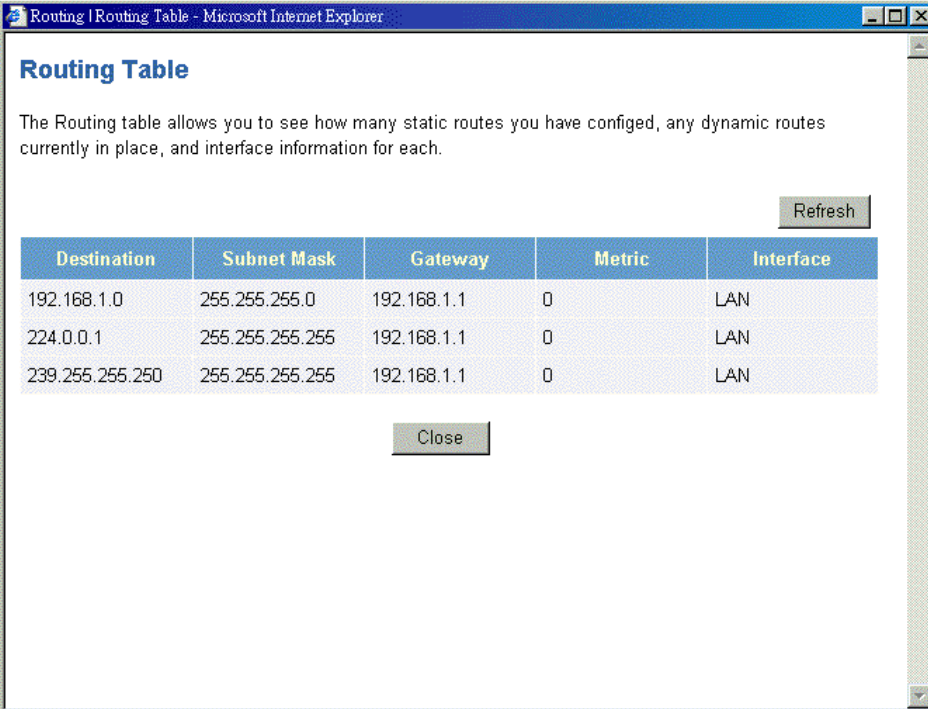|	
Set Time Zone:	Choose the time zone of your country where you are going to use the router.
Daylight Saving:	Check this button to invoke the daylight saving function.
Start from:	Set the start time by choosing the month and date to help the router perform tasks.
End by:	Set the end time by choosing the month and date to let the router know when to stop the task performing.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

DNS

On this page you can choose to disable or enable DNS function. To enable DNS, simply enter the value for Primary and Secondary DNS address and click **Apply**.

A Domain Name system (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into you browser, a DNS server will find that name in its index and find the matching IP address.

Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP addresses are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address below.

Dynamic DNS:	**Dynamic DNS:**
	Click Enable to initiate this setting.
	User Name:
	Enter the User Name specified at the www.dyndns.org Web site when you registered.
	Password:
	Enter your current password for www.dyndns.org
	Domain Name:
	Enter your domain name, as allocated at www.dyndns.org
	The name should consist only of letters and the hyphen (dash). Using any other characters may cause problems.
DNS Relay:	**Primary DNS Server:**
	Type in the DNS address that you get from your service provider.
	Secondary DNS Server:
	Type in the secondary DNS address that you get from your service provider.
Apply:	Save the data on the screen and apply the data after restarting the router.
Cancel:	The "Cancel" button will discard any data you have entered and reload the file from the Router.

Dynamic DNS

This feature is very useful when combined with the Virtual Server feature. It allows Internet users to connect to your Virtual Servers by using a URL, rather than an IP address.

It also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

The service works as follows:

1. You must register for the service at http://www.dyndns.org(Registration is free). Your password will be sent to you by e-mail.

2. After registration, use the "Create New Host" option (at www.dyndns.org) to request your desired Domain name.

3. Enter your data from www.dyndns.org in the Router's Dynamic DNS screen.

4. The Router will then automatically ensure that your current IP Address is recorded at http:// www.dyndns.org.

5. From the Internet, users will be able to connect to your Virtual Server (or DMZ PC) using your domain name, as shown in the screen.

Note: For Dynamic DNS free servcie, please note of the following:

1. You must sign up first to create a new account before using the service. The service is free.

2. Click the link www.dyndns.org for connecting to this web site.

3. Your initial password will be sent to you by e-mail. You can change it later if you wish.

4. After registration, use the "Create New Host" link (on the www.dyndns.org Web site) to request a domain name.

Network Clients

DHCP Client List shows the IP address, host name and MAC address of the clients which connected to the router.

DHCP Client List

The DHCP client list allows you to see which clients are connected to the router via IP address, host name, and MAC address.

Host Name	IP Address	MAC Address	Static
CARRIENI	192.168.1.2	00-C1-26-0A-69-2B	☐

Help | Apply | Cancel

Upgrade

The firmware (software) in the Router can be upgraded using your Web Browser.

You must first download the upgrade file, then select Upgrade on the Advanced menu. You will see a screen like this:

Firmware Upgrade

Enter the path and name of the upgrade file then click the APPLY button below. You will be prompted to confirm the upgrade.

Current Firmware Version: V 0.80.0001
Firmware Date: 2003.03.25

[_____] [Browse.]

[Apply]

To perform the firmware upgrade:

1. Click the Browse button and navigate to the location of the upgrade file.

2. Select the upgrade file. Its name will appear on the box in the center of the web page.

3. Click on the Apply button to commence the firmware upgrade.

Note: Do not interrupt the upgrade process otherwise it might cause damage to your Router. The Router is unavailabled during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Router will be lost.

Backup/Restore

To restore factory settings or backup customers settings, select Config Tool from the Advanced menu.

Backup/Restore

You can backup the router's current configuration to a file on your PC and restore it to the router as needed.

You can also reset the router to the original factory default configuration or just reset the router without erasing the configuration.

○ Backup Settings / Restore settings
◉ Restore Factory Default Configuration
○ Reset Router

[Help] [Apply] [Cancel]

Backup Settings/Restore settings: Allows you to backup settings or restored saved settings.

Restore Factory Default Configuration: Force the router performing reset and restore the original factory settings.

Reset Router: Reset your router onscreen.

Apply: Save the data on the screen and apply the data after restarting the router.

Cancel: The "Cancel" button will discard any data you have entered and reload the file from the Router.

Statistics

This screen displays the statistic for your router.

Statistics

	TCP	UDP
TX Total Packets	459	57
RX Total Packets	385	141
TX Total Bytes	229239	6455
RX Total Bytes	15894	5576

	LAN1	LAN2	LAN3	LAN4	WAN	WLAN
TX Packets	0	0	0	526	0	266
RX Packets	0	0	0	806	0	0
TX Bytes	0	0	0	271073	0	37814
RX Bytes	0	0	0	86014	0	0
Collisions	0	0	0	0	0	0
Speed (bits)	10M	10M	10M	100M	10M	--
Duplex	HALF	HALF	HALF	FULL	HALF	--
MTU	1500	1500	1500	1500	1500	1500

System Log

To view the events or send warning e-mail to somebody while certain events occur, you have to open System Log from Advanced menu and type in all the necessary information.

System Log

View the events that have been recorded by the router. If enabled, events will be logged to Flash memory and Log Server. You may also choose to have e-mail alerts generated when certain types of events are detected by the router.

[E-Mail Alert] [View Logs]

Log Status   ☑ Enable

Log Server   [_____] (IP Address or Domain Name)

Event Level   [Information ▾]

Interested Events   ☑ System   ☑ HTTP   ☑ DNS   ☑ DHCP
[Select All]   ☑ Firewall   ☑ NAT   ☑ UPnP   ☑ SNTP
   ☑ PPPoE   ☑ PPTP   ☑ Routing   ☑ WLAN

[Help] [Apply] [Cancel]

Log Status:	If Enabled, the function will be activated.
	If not Enabled, no one will receive any message about the router.
Log Server:	Type in the IP address or Domain Name for your system
Event Level:	Choose the essence of the event.
Interested Event:	Check the ones that you need.
E-Mail Alert:	Click this button to get into E-Mail Alert window for setting e-mail configuration.
View Logs:	Click this button to view system logs.
Select All:	Click this button to check all the events listed on the Interested Events.

Apply: Save the data on the screen and apply the data after restarting the router.

Cancel: The "Cancel" button will discard any data you have entered and reload the file from the Router.

E-Mail Alert

This mechanism will send e-mails to specific users automatically according to the settings that you configure in the following window.

Alert Status: If Enabled, the function will be activated.

                          If not Enabled, no one will receive any message about the router.

From: Type in the name of the mail sender, such as string, host name, or a pronoun.

To: Type in the e-mail address that you want to send to. Usually, the ones put here is the most important persons that you want to inform.

Copy to: Type in the e-mail address that you want to send to. Usually, the ones put here is less important then "To" entry.

Subject: Type in the subject of the mail that you want to let the receiver know.

SMTP Server: Type in IP address or Domain Name

Mail Priority: Decide the importance of the mail.

Event Level: Choose the essence of the event.

Interval: Tell the system the time to wait to send e-mail while events listed on the Interested Events occur.

Interested Events: Check the ones that you need.

Select All   Click this button to check all the events listed on the Interested Events.

Apply   Save the data on the screen and apply the data after restarting the router.

Close   The "Close" button will discard any data you have entered and reload the file from the Router.

Viewing System Log

System Log your service provider lays a running record of your router, including information, warning and error log. The information provided here is useful in working with your service provider or system administrators when troubleshooting.
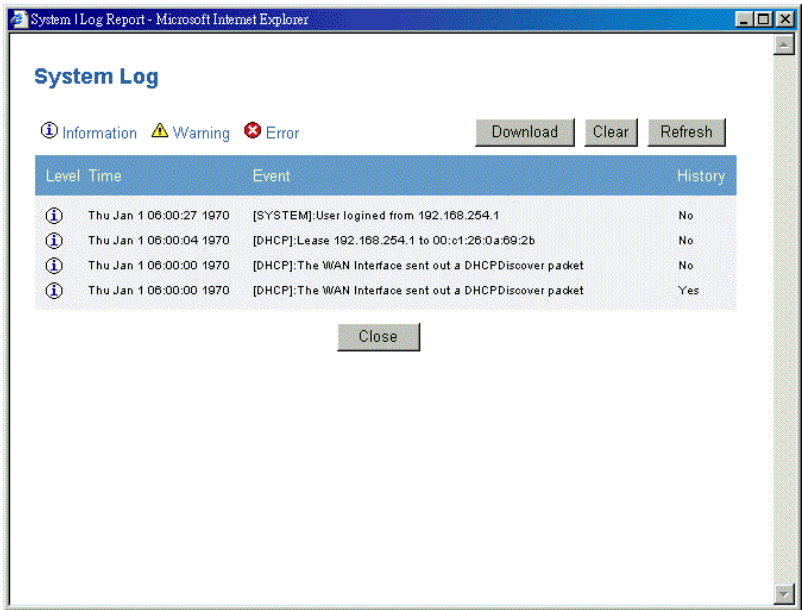
Download:	Download the log file information.
Clear:	Erase current log files information.
Refresh:	Renew current log files information.
Close:	The "Close" button will discard any data you have entered and reload the file from the Router.

Status

This page shows the basic information of your Router including the software version, WAN MAC address, LAN MAC address, etc. It provides a general overview of your Router. According to the WAN type that you choose, the status will differ slightly.

Dynamic IP (Cable Modem)

If your access method is Dynamic IP, the Status page will be shown as follows:

Status

You can use the Status screen to see the connection status for the router's WAN/LAN interfaces as well as hardware and firmware version information.

Internet   [More Details]

WAN IP   0.0.0.0

Connection Type   Dynamic IP

[Release]   [Renew]

LAN

IP Address   192.168.1.1

Subnet Mask   255.255.255.0

DHCP Server   Enabled

System Information

LAN MAC Address   00-90-96-98-65-15

WLAN MAC Address   00-90-96-00-03-00

WAN MAC Address   00-90-96-98-65-16

Up time   0 day(s) 0 hour(s) 0 minute(s) 31 second(s)

Firmware Version   V0.80.0001

More Details	Click this button to see more detailed information.
Release	If an IP address has been allocated to the Router (by ISP's DHCP Server), click on this button. It will break the connection and release the IP address.
Renew	This button is only useful if the IP address shown above is allocated automatically on connection. Otherwise, it has no effect.

If ISP's DHCP Server has not allocated an IP Address for the Router, click on this button. It will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.

Status | Internet Status - Microsoft Internet Explorer

Internet Status   [Refresh]

WAN IP   10.3.1.124

Subnet Mask   255.255.255.0

Gateway   10.3.1.234

DNS Server 1   192.168.1 .1 (Static)

DNS Server 2   0.0.0.0 (Static)

DNS Server 3   10.1.1.12 (Dynamic)

DNS Server 4   168.95.1.1 (Dynamic)

Connection Type   Dynamic IP

Lease Obtained   Thu Mar 20 00:43:09 2003

Lease Expires   Fri Mar 28 00:43:09 2003

[Close]

PPPoE

If your access method is PPPoE, the Status page will be shown as follows:

Status

You can use the Status screen to see the connection status for the router's WAN/LAN interfaces as well as hardware and firmware version information.

Internet [More Details]

WAN IP	10.2.5.111
Connection Type	PPPoE
Connection Status	CONNECTED

[Disconnect] [Connect]

LAN

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

System Information

LAN MAC Address	00-00-00-00-00-00
WLAN MAC Address	00-00-00-00-00-01
WAN MAC Address	00-00-00-00-00-02
Up time	1 days 2 hours 3 minutes 4 seconds

More Details: Click this button to see more detailed information.

Disconnect: If you find the connection is not established, please click this button to establish a connection to your ISP.

Connect: If the connection is OK, you can hang up the connection by clicking this button.

Status | Internet Status - Microsoft Internet Explorer

Internet Status [Refresh]

WAN IP	10.3.79.147
Subnet Mask	255.255.224.0
Gateway	10.3.95.210
DNS Server 1	10.3.1.1 (Static)
DNS Server 2	0.0.0.0 (Static)
DNS Server 3	168.95.1.1 (Dynamic)
DNS Server 4	168.95.192.1 (Dynamic)
Connection Type	PPPoE
Connection Status	CONNECTED

[Close]

PPTP

If your access method is PPTP, the Status page will be shown as follows:

More Details:	Click this button to see more detailed information.
Disconnect:	If you find the connection is not established, please click this button to establish a connection to your ISP.
Connect:	If the connection is OK, you can hang up the connection by clicking this button.

Static IP

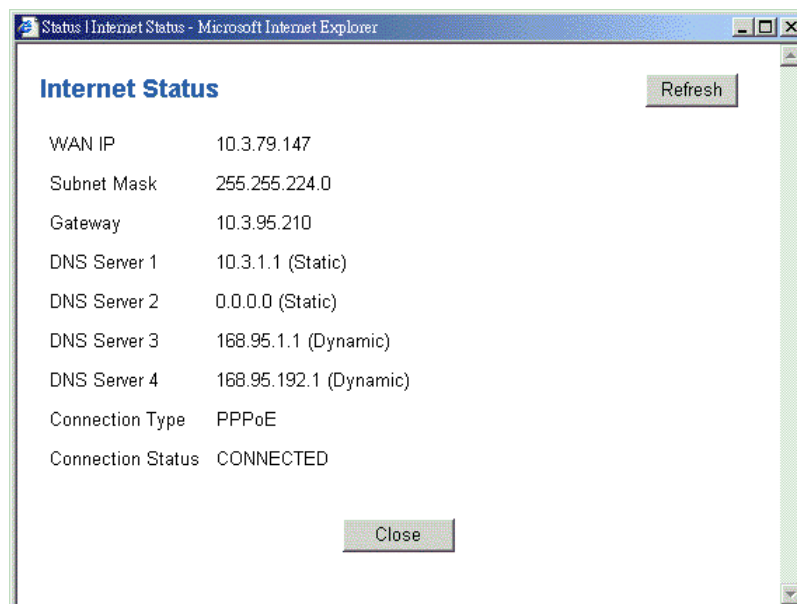If your access method is Static IP, the Status page will be shown as follows:

Status

You can use the Status screen to see the connection status for the router's WAN/LAN interfaces as well as hardware and firmware version information.

Internet [More Details]

WAN IP	10.3.1.32
Connection Type	Static IP
Connection Status	CONNECTED

LAN

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

System Information

LAN MAC Address	00-90-96-98-65-15
WLAN MAC Address	00-90-96-00-01-A7
WAN MAC Address	00-90-96-98-65-16
Up time	0 day(s) 0 hour(s) 3 minute(s) 16 second(s)

More Details   Click this button to see more detailed information.

Status | Internet Status - Microsoft Internet Explorer

Internet Status   [Refresh]

WAN IP	10.3.1.124
Subnet Mask	255.255.255.0
Gateway	10.3.1.234
DNS Server 1	10.3.1.1 (Static)
DNS Server 2	0.0.0.0 (Static)
Connection Type	Static IP
Connection Status	CONNECTED

[Close]
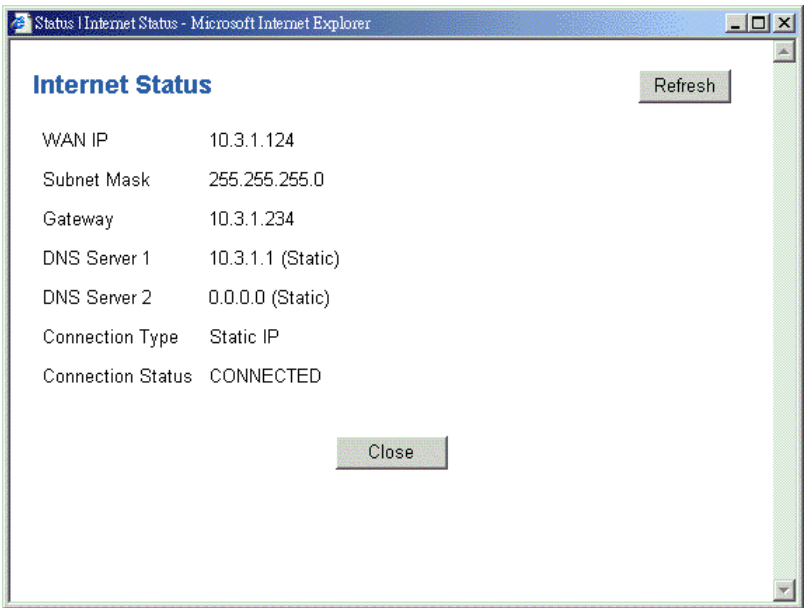
Chapter 5: Troubleshooting

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

Problems with LAN

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

The chances are that the interface used as DHCP server is modified and the client 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 Wireless Broadband Router.

Check that your PC is on the same subnet with the Wireless Broadband 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.

Can't access the Router's Web Configuration interface from a PC on your local network.

Make sure you are using the correct login information, the default password is **admin** (small letters).
Make sure your PC's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.1.2 to 192.168.1.254.

Note:

1. If you use DHCP server and your PC's IP address is shown as 169.254.x.x: please renew the IP address and check the connection from the PC to the router.
2. If you are using a wireless LAN card equipped PC, check that the SSID and WEP settings are the same for the router and PC.
3. If your router's IP address has been changed and you don't know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.1.1.

Problems with WAN

If you router can't access the Internet.

- You should first determine whether the router is able to obtain a WAN IP address from the ISP. Or you have been assigned a static IP address.

- Check the IP address for the WAN port.

- If your ISP requires a login program as PPP over Ethernet (PPPoE), ensure the user name and password you enter are correctable.

- If your Broadband Wireless Router is set to routing mode and you use private IP addresses on the LAN, make sure Network Address Translation (NAT) is enabled.

- Your PC may not recognize any DNS server address. Check your DNS setting on the Broadband Wireless Router.

- Check the physical connection between the Wireless Broadband Router and the LAN.

At the DOS prompt, ping the IP address of the Wireless Broadband 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 Wireless Broadband 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 Wireless Broadband Router and the network.

- Check the DNS setting of the Wireless Broadband 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 168.95.1.1 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 Wireless Broadband Router.

Problems with Upgrading

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

- **Error Message**: Upload Data Error！Please make sure your file is correct!

   Possible cause: The firmware file format is invalid.

   Action: Check the file format is correct, otherwise download a firmware file with correct format.
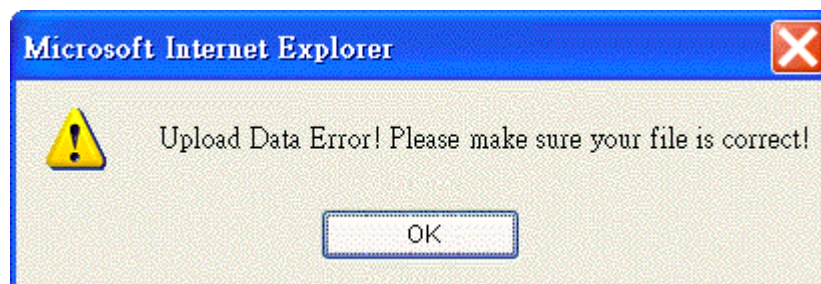
- **Error**: The router shut down for some unknown reason and the web page got problem

   Possible cause: The firmware might be damaged.

   Action: Execute recovery firmware update. Simply type 192.168.1.1 on URL line to open the page. Choose the proper file and click Apply to execute the recovery process.

When the file is copied, a successful web page appears as follows. Now the router's firmware is upgraded. It can be used again.

Upgrade Firmware Successfully

Your router has successfully been upgraded.

Please wait until the power light stops blinking.

Chapter 6: Glossary

Authentication and WEP Encryption

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security , the IEEE 802.11 standard has defined two types of authentication methods, open system and shared key. With open system authentication a wireless PC can join any network and receive any messages that are not encrypted. With shared key authentication, only those PCs that possess the correct authentication key can join the network. By default IEEE 802.11 wireless devices operate in an Open system network.

DHCP (Dynamic Host Configuration Protocol)

When operates as a DHCP server, the Wireless Broadband 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 your service provider 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.

Infrastructure mode

A backbone to extend the service provided by network. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

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 Wireless Broadband Router is called the LAN port. It is a twisted-pair Ethernet 10/100Base-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 Wireless Broadband Router and composes a LAN.

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

MAC Address

Media Access Code Address. A unique, 48-bit number assigned to every network interface card by the manufacturer.

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 your service provider are not enough for each PC on the LAN and the Wireless Broadband 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 Wireless Broadband Router is assigned with the public IP address of 168.111.1.1. 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 192.168.1.254. These PCs are not accessible by the outside word but they can communicate with the outside world through the public IP 168.111.1.1.

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 Wireless Broadband 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.

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.

SSID

SSID is a thirty-two character(maximum) alphanumeric key identifying the wireless local area network.

Service Set Identity. A group name shared by all members of an IEEE 802.11b network. Only devices with the same SSID are allowed to establish connections. For the wireless devices in a network to communicate with each other, all device must be configured with the same SSID.

UDP (User Data gram Protocol)

UDP is a connectionless transport service that does not own 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.

Appendix: Specifications

Software

Router Features

- NAT let multiple users on LAN to access the Internet for the cost of only one IP address and enjoy various multimedia applications.

- ALGs(Application Level Gateways) support. (NetMeeting, MSN Messenger, MSN Game Zone, Battle.net and else)

- Trigger port mechanism support that can allow new application through NAT

- UPnP support (include NAT traversal)

- DMZ hosting, Multiple Virtual Servers (e.g., Web, FTP, Mail servers) can be setup in local network

- Static Route, RIP v1, v2

- Multiple kind of WAN connection: PPPoE, DHCP Client, Fixed IP, PPTP

- DHCP Server, DNS Relay, SNTP (Time Zone) setup, DDNS support

- Mac cloning (for WAN connection is DHCP client)

- Support VPN PPTP pass through, IPSec Pass through

- IGMP support Router mode and Proxy mode

Bridging Features

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

- ◆ Transparent Bridging between 4-port 10/100 MB Ethernet switch and 802.11b Wireless LAN interface.

Wireless LAN Features

- Fully compatible to 802.1lb standard, allowing up to 11Mbps wireless rate with distance up to 300 feet/90 meters.

- The 2.4 GHz Direct Sequence Spread Spectrum (DSSS) technology is exploited.

- Seamless roaming within wireless LAN infrastructure.

- Wireless clients association list

- Wireless clients Mac address filter

- Support disable the broadcast of SSID

Security Features

- PAP(RFC1334), CHAP(RFC1994) for PPPoE session

- Wireless support WEP (Wired Equivalent Privacy) uses RC4 with 40/64 and 128 bit key length. Passphrase key generation support.

- 802.1x support (also include WEP key distribution support)

- Mac address Filter

- Schedule and Group base content filtering, URL filtering and IP filtering

Configuration and Management

- Enable/disable Remote Management (ping and web browse)

- Login / Logout of web management

- Configurable through Web Browser

- HTTP firmware upgrades via Web browser directly

- Support DHCP Server function for IP distribution to local network users

- E-mail Alert and Event Logging. Also provide different level of event alert and log

Hardware

Interface
- One 10/100 Base-T RJ-45 port for Broadband connection (Cable/DSL or direct Ethernet)

- Four RJ-45 ports for 10/100Base-TX Ethernet Switch LAN connection.

- Build-in PCMCIA card for 802.11b that include two internal patch antenna

Regulatory Approvals and Compliance
- EMI: FCC part 15 Class B

- Safety: Dentori, IEC950

- Immunity: VCCI class B

- PTT: JATE

Power Requirement and Operation Environment Requirement
- Power Adaptor: Input 100±10 VAC; Output 12 VDC, 1A

- Power Consumption: less than 10 Walt

- Ambient Temperature: Operating - 0°C to 40°C, Storage - -20°C to 70°C

- Relative Humidity: 5% to 90% (non-condensing)

LED Indicators
- Power (Green)

- Diagnose (Green)

- 10Mbps / 100Mbps Ethernet Link (Green)

- WLAN(Green)

- WAN(Green)

Physical
- Dimensions: 152 mm (L) × 113 mm (W)

- Weight: less than 700 g

Certification
- Wi-Fi Certified