



ADSL Router/Modem User Manual

RTA770/RTA770W



No part of this publication may be reproduced in any form by any means without the prior written permission. Other trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective companies.

2004/4/14

Rev:04

This manual currently suits for RTA770W/RTA770BW.

000230-rita

Safety Notes

For Installation

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

For Using

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

For Service

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

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

Warning

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

Caution

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

Contents

Before You Use	ix
Features	ix
Unpacking.....	xi
Subscription for ADSL Service.....	xi
 Chapter 1.....	 1
Physical Outlook	1
<i>Front Panel</i>	1
<i>Rear Panel</i>	2
 Chapter 2.....	 3
Choosing a place for the ADSL Router.....	3
Connecting the ADSL Router.....	3
USB Driver Installation	4
<i>For Windows ME</i>	4
<i>For Windows 2000</i>	4
<i>For Windows XP</i>	5
Uninstall the USB Driver	5
<i>For Windows ME</i>	5
<i>For Windows 2000</i>	5
<i>For Windows XP</i>	6
 Chapter 3.....	 7
Setting TCP/IP on Client PC	7
<i>For Windows 98</i>	8
<i>For Windows ME</i>	11
<i>For Windows NT</i>	12
<i>For Windows 2000</i>	15
<i>For Windows XP</i>	17
Configure PC to get IP address from DHCP	18
<i>For Windows 98</i>	18
<i>For Windows ME</i>	18
<i>For Windows NT</i>	19
<i>For Windows 2000</i>	19
<i>For Windows XP</i>	20
Renew IP Address on Client PC	20
<i>For Windows 98ME</i>	20
<i>For Windows NT</i>	21
<i>For Windows 2000</i>	22
<i>For Windows XP</i>	22
 Chapter 4.....	 23
Using Web-Based Manager	23
<i>Outline of Web Manager</i>	24
<i>To Have the New Settings Take Effect</i>	24
Quick Start.....	25
<i>Connect to Internet</i>	25
<i>Quick Setup</i>	25

<i>Connection Type</i>	25
<i>PPP over ATM/ PPP over Ethernet</i>	26
<i>MAC Encapsulated Routing (MER)</i>	28
<i>IP over ATM</i>	30
<i>Bridging</i>	32
Status	33
<i>Overview</i>	33
<i>ADSL Line</i>	34
<i>Internet Connection</i>	35
<i>Traffic Statistics</i>	35
<i>DHCP Table</i>	35
<i>Wireless Client</i>	36
<i>Routing Table</i>	36
<i>ARP Table</i>	36
Advanced Setup.....	37
<i>LAN- IP Address</i>	37
<i>LAN-DHCP Server</i>	37
<i>WAN - Internet Setting</i>	38
<i>WAN - ADSL Settings</i>	39
<i>IP Routing - Static Route</i>	40
<i>IP Routing – Dynamic Routing</i>	42
<i>DNS Server</i>	42
<i>NAT - Virtual Servers</i>	43
<i>NAT - DMZ Host</i>	45
<i>NAT - Dynamic DNS</i>	45
<i>Firewall</i>	47
<i>IGMP Proxy</i>	49
Wireless.....	51
<i>Basic</i>	51
<i>Security</i>	53
<i>Access Control</i>	59
Diagnostics	60
Management	61
<i>Admin Account</i>	61
<i>Remote Access</i>	61
<i>Date and Time</i>	62
<i>System Log</i>	62
<i>SNMP Setting</i>	64
<i>Backup Config</i>	65
<i>Update Firmware</i>	65
<i>Reset Router</i>	65
<i>UPnP for XP</i>	66

Chapter 5..... 69

PPP over ATM (PPPoA) Mode.....	70
PPP over ATM (PPPoA) IP Extension Mode	71
PPP over Ethernet (PPPoE) Mode.....	72
PPP over Ethernet (PPPoE) IP Extension Mode.....	73
MER	74
Numbered IP over ATM (IPoA)	75
Numbered IP over ATM (IPoA)+NAT	77
Unnumbered IP over ATM (IPoA).....	79
Unnumbered IP over ATM (IPoA)+NAT.....	81
Bridge Mode	83

Chapter 6	85
Problems with LAN	85
Problems with WAN	85
Problems with Upgrading	86
Chapter 7	87
Appendix A	91
<i>Software</i>	91
<i>Hardware</i>	93
Appendix B	95
<i>Getting Client Certificate</i>	95
<i>Enable 802.1x authentication and Encryption for wireless card</i>	97

Before You Use

Thank you for choosing the Asymmetric Digital Subscriber Line (ADSL) Router. With the asymmetric technology, this device runs over standard copper phone lines. In addition, ADSL allows you to have both voice and data services in use simultaneously all over one phone line.

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

Features

ADSL Compliance

For Annex A model (RTA770W)

- ✧ ANSI T1.413 Issue 2
- ✧ ITU G.992.1 Annex A (G.dmt)
- ✧ ITU G.992.2 Annex A (G.lite)
- ✧ ITU G.994.1 (G.hs)
- ✧ Support dying gasp

For Annex B model (RTA770BW)

- ✧ ITU G.992.1 Annex B (G.dmt)
- ✧ ITU G.994.1 (G.hs)

ATM Features

- ✧ Compliant to ATM Forum UNI 3.1 / 4.0 Permanent Virtual Circuits (PVCs)
- ✧ Support UBR and CBR with traffic shaping
- ✧ RFC2684 LLC Encapsulation and VC Multiplexing over AAL5
- ✧ RFC2364 Point-to-Point Protocol (PPP) over AAL5
- ✧ RFC2225 Classical IP and ARP over ATM
- ✧ RFC2516 PPP over Ethernet: support Relay (Transparent Forwarding and Client functions)
- ✧ Support PPPoA or PPPoE Bridged mode (the IP address got from ISP can be passed to the user's PC and behave as the IP address of the user's PC.)
- ✧ OAM F4/F5 End-to-End/Segment Loopback Cells

Bridging Features

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

- ✧ Supports up to 4096 learning MAC addresses
- ✧ Transparent Bridging between 10/100 Mb Ethernet and USB

Routing Features

- ✧ NAT (Network Address Translation) / PAT (Port Address Translation) let multiple users on the LAN to access the internet for the cost of only one IP address.
- ✧ ALGs (Application Level Gateways): such as NetMeeting, MSN Messenger, FTP, Quick Time, mIRC, Real Player, CuSeeMe, VPN pass-through, etc.
- ✧ Port Mapping: the users can setup multiple virtual servers (e.g., Web, FTP, Mail servers) on user's local network.
- ✧ Support DMZ
- ✧ UPnP IGD (Internet Gateway Device) with NAT traversal capability
- ✧ Static routes, RFC1058 RIPv1, RFC1723 RIPv2
- ✧ DNS Relay
- ✧ ARP Proxy

Security Features

- ✧ PAP (RFC1334), CHAP (RFC1994) for PPP session
- ✧ Firewall support IP packets filtering based on IP address/Port number/Protocol type
- ✧ Support DoS (Deny of Services) which detect & protect a number of attacks (such as SYN/FIN/RST Flood, Smurf, WinNuke, Echo Scan, Xmas Tree Scan, etc)

Wireless LAN Compliance Features

- ✧ IEEE 802.11g and IEEE 802.11b
- ✧ Data Rate: 54, 48, 36, 24, 18, 12, 9, 6 Mbps for 802.11g/11, 5.5, 2, 1 Mbps for 802.11b
- ✧ Modulation Technique: OFDM for 802.11g; CCK (11 Mbps, 5.5 Mbps) for 802.11b; DQPSK (2Mbps) for 802.11b; DBPSK (1 Mbps) for 802.11b
- ✧ Network Architecture: infrastructure
- ✧ Operating Frequency: 2.4 ~ 2.497 GHz
- ✧ Operating Channels: depending on local regulations. For example, 11Channels (Northern America), 13 Channels (Europe), and 14 Channels (Japan)
- ✧ RF Output Power: 15dBm maximum
- ✧ Antenna Connectors: Hardware diversity support. One external antenna and one internal antenna are provided.
- ✧ Coverage Area:
802.11g: LOS (Outdoors): Max. 50 meters; Indoors: Max. 20 meters
802.11b: LOS (Outdoors): Max. 180 meters; Indoors: Max. 60 meters
- ✧ Power Consumption:
TX peak: 550 mA @ 3.3 VDC; RX peak: 350 mA @ 3.3 VDC
Idle: 225 mA @ 3.3 VDC; Radio disabled: < 10 mA @ 3.3 VDC
- ✧ Support WEP (Wired Equivalent Privacy) mechanism which uses RC4 with 64-bit or 128-bit key length
- ✧ Support WPA, WPA-PSK, WPA-802.1X
- ✧ Support the Access Control function: only registered WLAN clients can be allowed to associate to the router.
- ✧ SSID can be hidden for the security issue (Don't broadcast SSID).

Configuration and Management

- ✧ User-friendly embedded web configuration interface with password protection
- ✧ Remote management accesses control
- ✧ Telnet session for local or remote management
- ✧ HTTP firmware upgrades via web browser GUI directly
- ✧ Distribute IP addresses to end users via DHCP server provided by ADSL router
- ✧ SNMPv1/v2 agent with MIB-II, ADSL Line MIB

Unpacking

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

- ✧ ADSL Router
- ✧ Power Adapter and Cord
- ✧ RJ-11 ADSL Line Cable
- ✧ RJ-45 Ethernet Cable
- ✧ Quick Start Guide
- ✧ Driver & Utility Software CD
- ✧ USB Cable (for model with USB interface only)

Subscription for ADSL Service

To use the ADSL 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 ISP.

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 ISP. The number of IP addresses varies according to different ADSL service provider.

Chapter 1

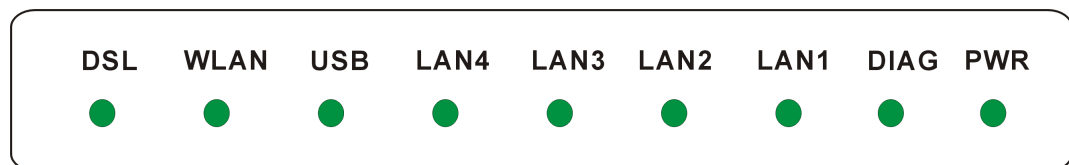
Overview

This chapter provides you the description for the LED and connector for front and rear view of the router. Before you use/install this router, please take a look at this information first.

Physical Outlook

Front Panel

The following illustrations show the front panel of the ADSL Router (with USB interface and without USB interface):



LED Indicators

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

LED	Color	Status	Description
DSL	Green	Unlit	Power off or ADSL line connection is handshaking or training is in progress.
		Blinking	User data is going through ADSL port.
		Solid	ADSL line connection is OK.
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.
USB	Green	Unlit	Power off or wait for USB connection going up.
		Blinking	User data is going through USB port.
		Solid	USB connection is OK.
LAN 1 - 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.

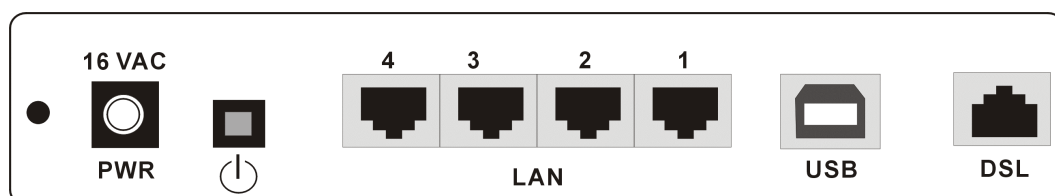
LED	Color	Status	Description
DIAG	Green	Unlit	Power off or initial self-test of the unit is OK.
		Blinking	When software downloading or updating operation parameters located in FLASH memory is in progress.
		Solid	Initial self-test failure or programming FLASH memory failure.
PWR	Green	Unlit	Power off.
		Solid	Power on.




Note: The USB LED is useful for the model with USB interface only.

Rear Panel

The following figures illustrate the rear panel of your ADSL Router (with USB interface and without USB interface).



Connector	Description
16VAC	16VAC Power connector
	Power switch
LAN 1- 4	Ethernet RJ-45 connector
USB	USB connector (for the model with USB interface only)
DSL	RJ-11 connector

Chapter 2

Installation

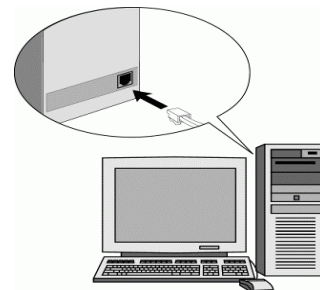
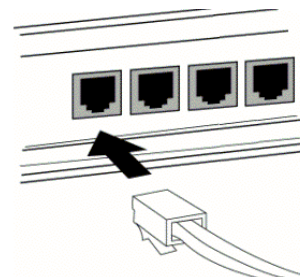
Choosing a place for the ADSL Router

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

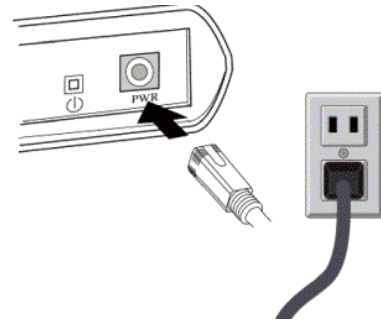
Connecting the ADSL Router

Follow the steps below to connect the related devices.

- ❶ Please attach one end of the Ethernet cable with RJ-45 connector to the **LAN** port of your ADSL Router.
- ❷ Connect the other end of the cable to the Ethernet port of the client PC.



- ③ Connect the supplied power adapter to the **PWR** port of your ADSL Router, and plug the other end to a power outlet.



- ④ Turn on the power switch.

USB Driver Installation

If the ADSL Router is connected to a PC through USB interface, you will be prompted for the USB drivers when plugging the USB cable to the PC. Refer to the relevant operating system to install the USB drivers. Otherwise, you may skip this chapter.



Note: This section is for the model with USB interface only. If your router does not support USB interface, please skip this section.

For Windows ME

- ① Run the USB installation program from the CD provided by your router package.
- ② An InstallShield Wizard will appear. Please wait for a moment.
- ③ When the InstallShield Wizard Complete appears, click Finish.
- ④ Plug the USB cable between your router and PC.



Note: If the USB device is not detected, check the USB cable between the PC and the device. Also verify that the device is power on.

- ⑤ The USB driver installation finished. You can use the router now.

For Windows 2000

- ① Run the USB installation program from the CD provided by your router package.
- ② An InstallShield Wizard will appear. Please wait for a moment.
- ③ When the welcome screen appears, click **Next** for next step.
- ④ When the InstallShield Wizard Complete appears, click **Finish**.
- ⑤ Plug the USB cable between your router and PC.



Note: If the USB device is not detected, check the USB cable between the PC and the device. Also verify that the device is power on.

- ⑥ The system will detect the USB driver automatically. When the system detects it, a dialog

of Digital Signature Not Found will appear. Click **Yes** for next step.

- 7 Now, the system will copy the proper files for this router.
- 8 When the file copying finished, the dialog above will close. Now the USB driver is installed properly. You can use the router.

For Windows XP

- 1 Run the USB installation program from the CD provided by your router package.
- 2 An InstallShield Wizard will appear. Please wait for a moment.
- 3 When the welcome screen appears, click **Next** for next step.
- 4 When the InstallShield Wizard Complete appears, click **Finish**.
- 5 Plug the USB cable between your router and PC.



Note: If the USB device is not detected, check the USB cable between the PC and the device. Also verify that the device is power on.

- 6 The system will detect the USB driver automatically. When the system detects it, a dialog of Welcome to the Found New Hardware Wizard will appear. Click **Next** for next step.
- 7 The system is trying to find proper driver for your router and copying the files automatically.
- 8 After the file copying is finished, a completing dialog will appear. Click **Finish**.
- 9 You can use the router now.

Uninstall the USB Driver

For Windows ME

For uninstall the USB driver, please do the following.

- 1 Run the USB installation program from the CD provided by your router package. The InstallShield Wizard screen will appear.
- 2 The system will search all the USB drivers on your computer. Please wait for a minute. Then, a dialog appears to ask you confirm if you want to remove the USB driver or not. Please click **Ok**.
- 3 When the Maintenance Complete screen appears, the USB driver is removed successfully. Please click **Finish**.
- 4 Unplug the USB cable between your router and your PC.

For Windows 2000

For uninstall the USB driver, please do the following.

- 1 Run the USB installation program from the CD provided by your router package. The InstallShield Wizard screen will appear. Please wait for a moment.
- 2 A dialog appears to ask you confirm if you want to remove the USB driver or not. Please

click **Ok**.

- ③ When the Maintenance Complete screen appears, the USB driver is removed successfully. Click Finish.
- ④ Unplug the USB cable between your router and your PC.

For Windows XP

For uninstall the USB driver, please do the following.

- ① Run the USB installation program from the CD provided by your router package. The InstallShield Wizard screen will appear. Please wait for a moment.
- ② A dialog appears to ask you confirm if you want to remove the USB driver or not. Please click **Ok**.
- ③ When the Maintenance Complete screen appears, the USB driver is removed successfully. Click Finish.
- ④ Unplug the USB cable between your router and your PC.

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 ADSL 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 ADSL 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 ADSL Router. Or you could assign an IP address to the host PC first for initial configuration.

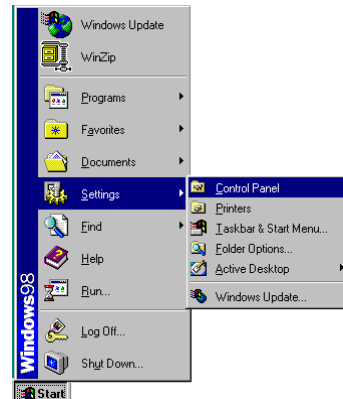
You also can manage the ADSL Router through a web browser-based manager: **ADSL ROUTER CONTROL PANEL**. The ADSL Router manager uses the HTTP protocol via a web browser to allow you to set up and manage the device.

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

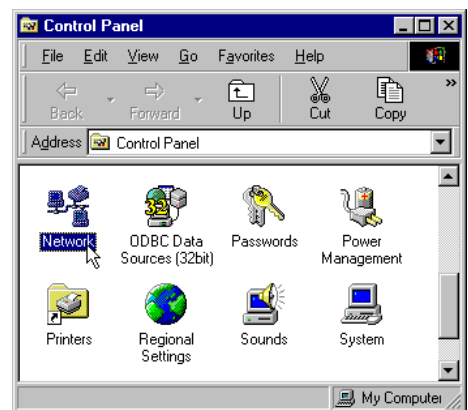
If TCP/IP is not already installed, follow the steps below for installation.

For Windows 98

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



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



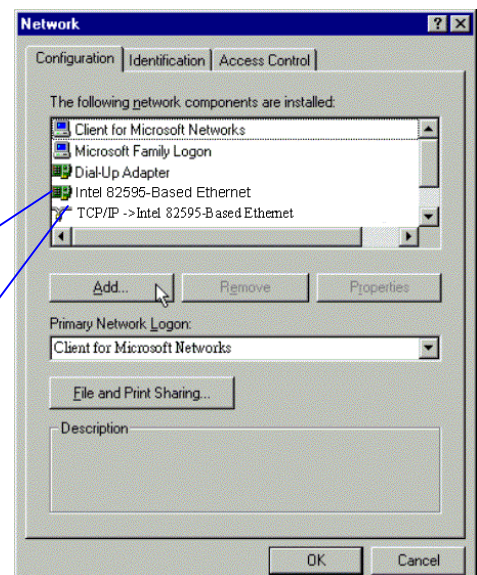
3. The **Network** window appears. On the **Configuration** tab, check out the list of installed network components.

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

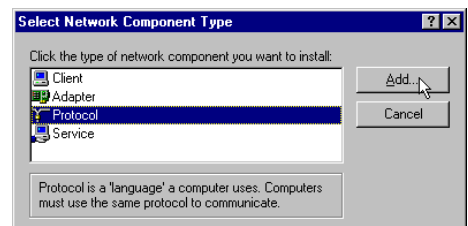
Option 2: If you have TCP/IP protocol, go to Step 6

Your network interface card.

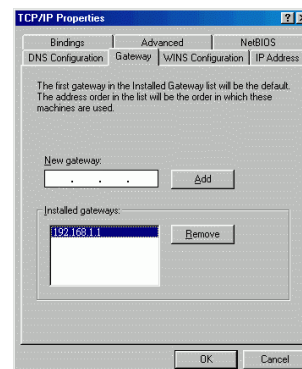
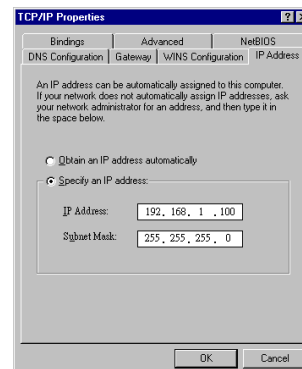
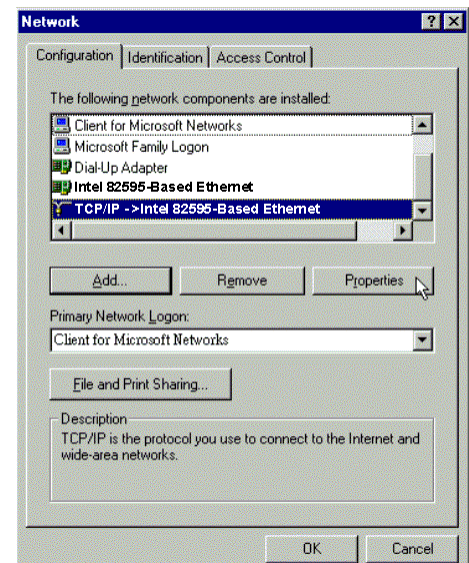
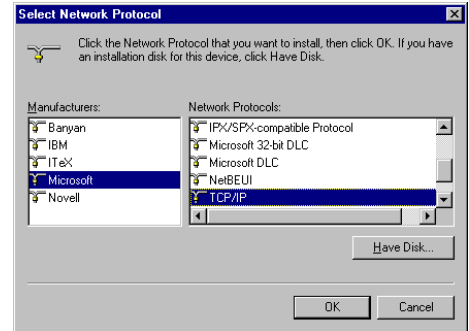
Check out if TCP/IP for your NIC is installed or not.



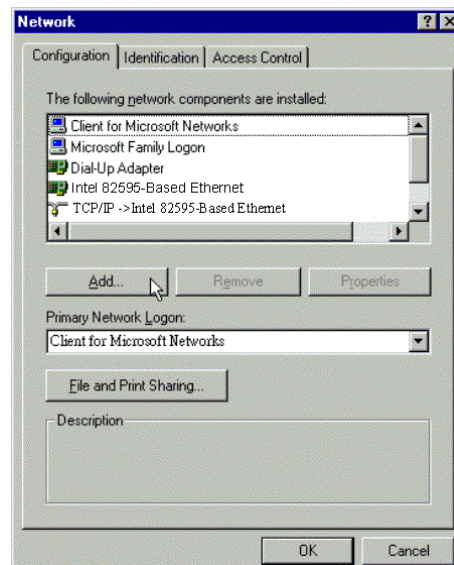
4. Highlight **Protocol** and click **Add**.



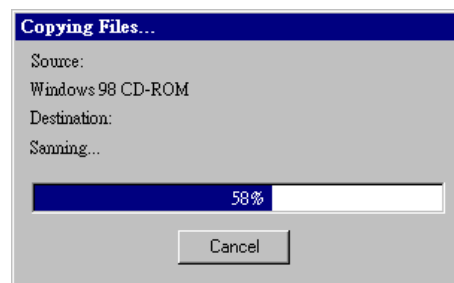
5. On the left side of the windows, highlight **Microsoft** and then select **TCP/IP** on the right side. Then click **OK**
6. When returning to **Network** window, highlight **TCP/IP** protocol for your NIC and click **Properties**.
7. On **IP Address** tab:
Enable **Specify an IP address** option. 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**



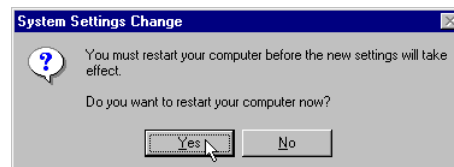
8. When returning to **Network** window, click **OK**



9. Wait for Windows copying files.

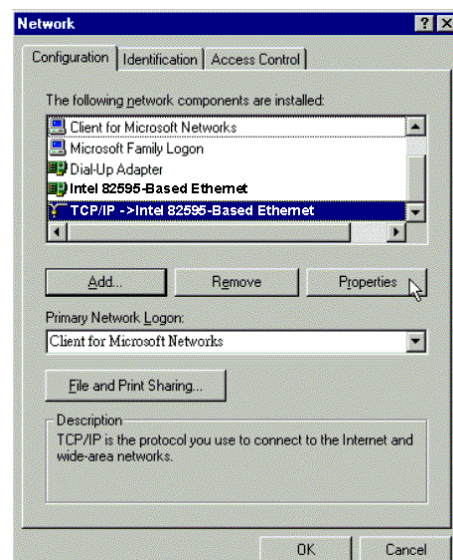


10. When prompted with **System Settings Change** dialog box, click **Yes** to restart your computer.

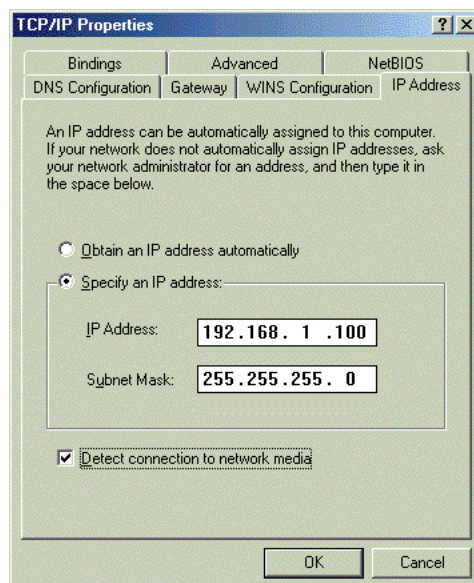


For Windows ME

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**.

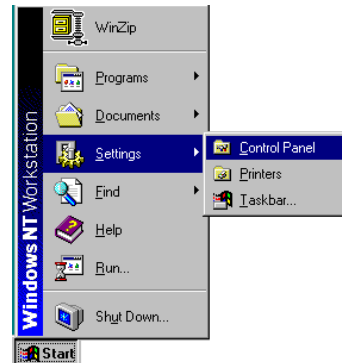


8. While returning to the **Network** window, click **OK**.

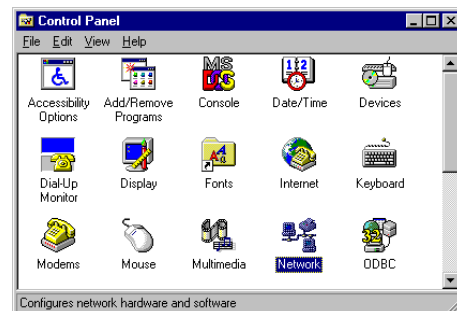
9. Wait for Windows copying files.
10. When prompted with the **System Settings Change** dialog box, click **Yes** to restart your computer.

For Windows NT

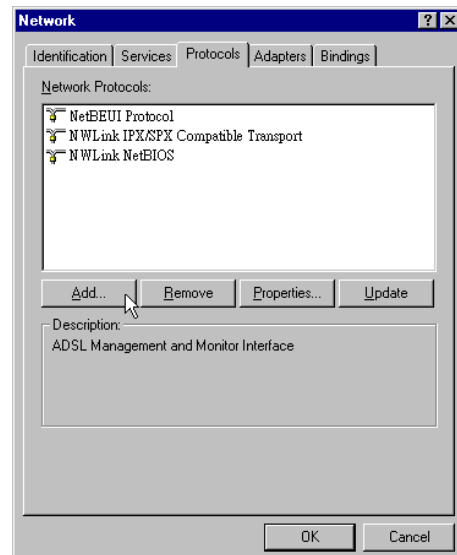
1. Click **Start**, point to **Settings**, and then click **Control Panel**.



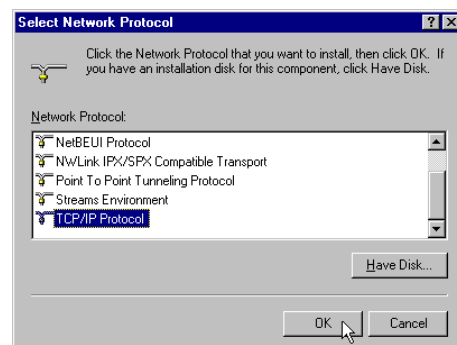
2. Double-click the **Network** icon.



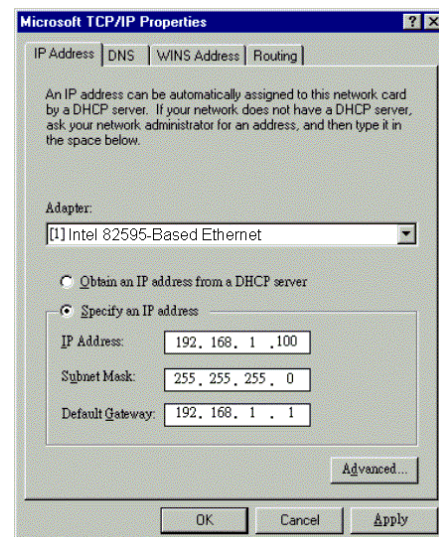
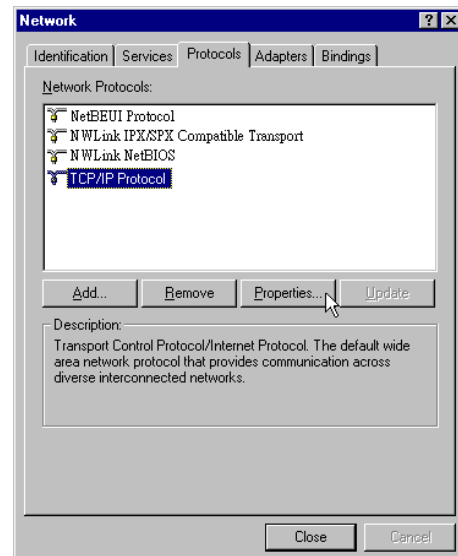
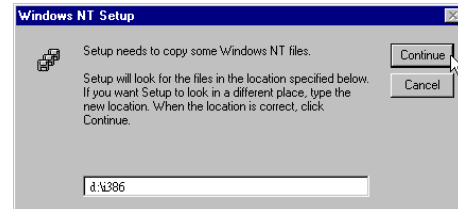
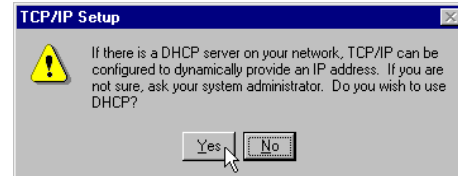
3. The **Network** window appears. On the **Protocols** tab, check out the list of installed network components.
Option 1: If you have **no** TCP/IP Protocol, click **Add**.
Option 2: If you have TCP/IP Protocol installed, go to Step 7.



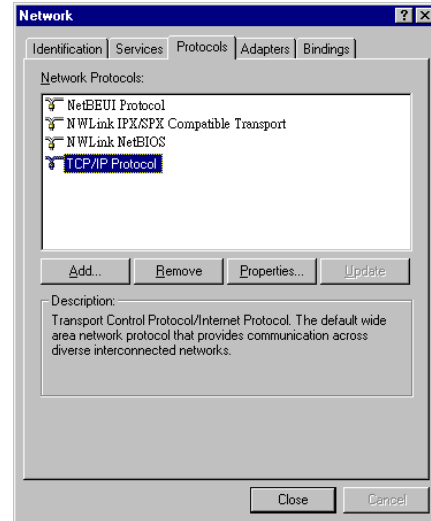
4. Highlight **TCP/IP Protocol** and click **OK**.



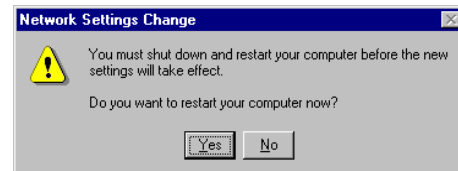
5. Click **Yes** to use DHCP.
6. Insert the Windows NT CD into your CD-ROM drive and type the location of the CD. Then click **Continue**.
7. Returning to the **Network** window, you will find the **TCP/IP Protocol** among the list. Select **TCP/IP Protocol** and click **Properties**.
8. Enable **Specify 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**.

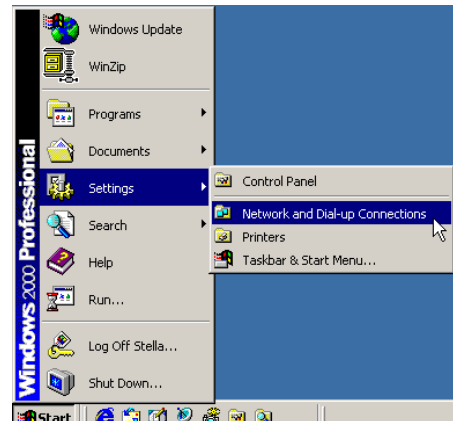


10. When prompted with **Network Settings Change** dialog box, click **Yes** to restart your computer.

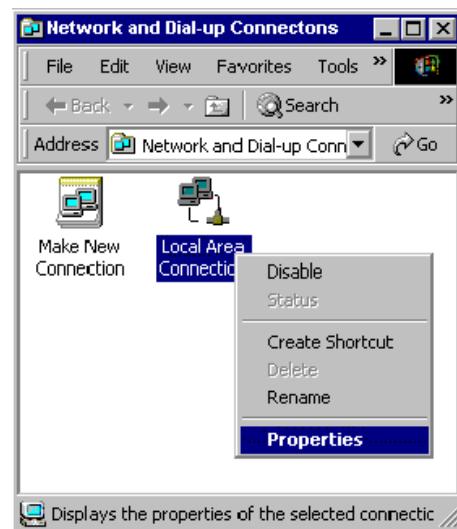


For Windows 2000

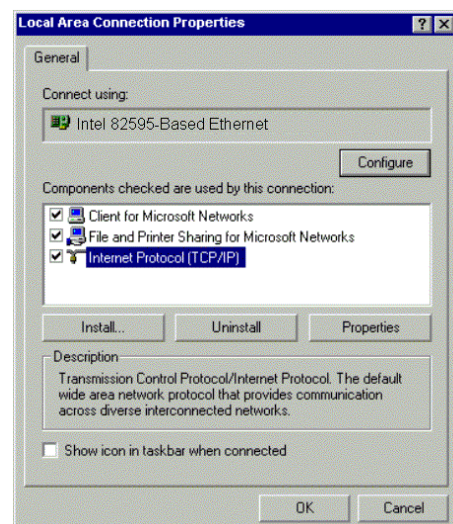
1. From the Start menu, point to Settings and then click Network and Dial-up Connections.



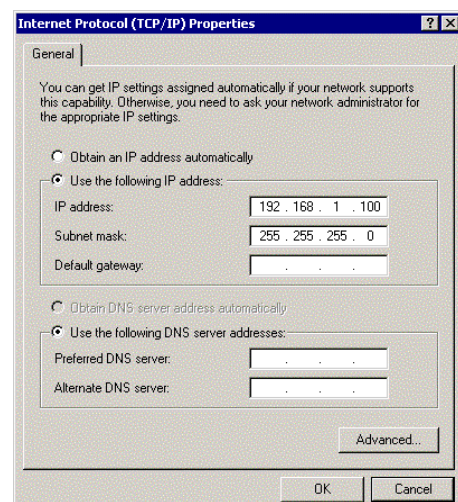
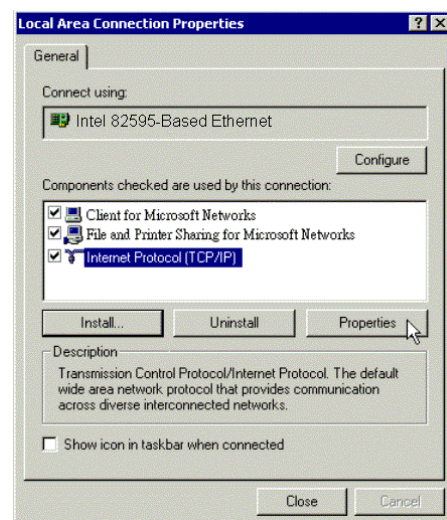
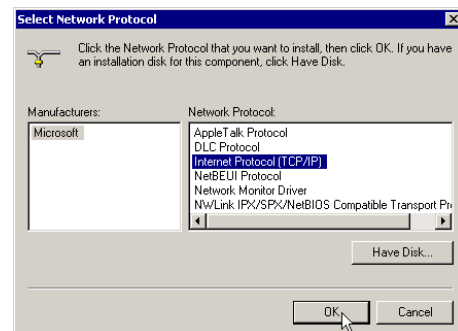
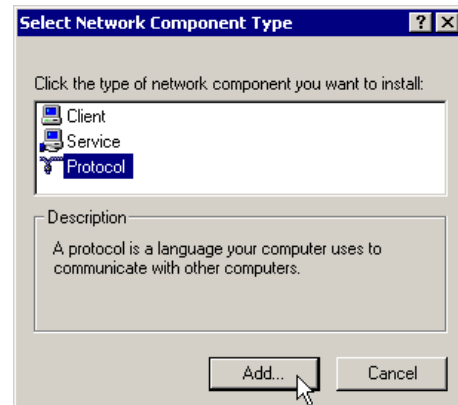
2. Right-click the **Local Area Connection** icon and then click **Properties**.



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.

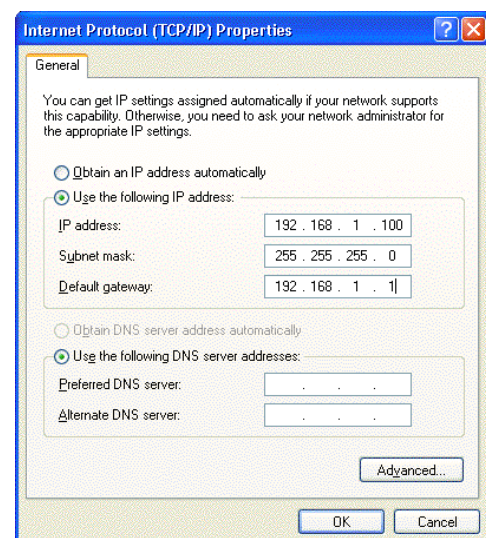
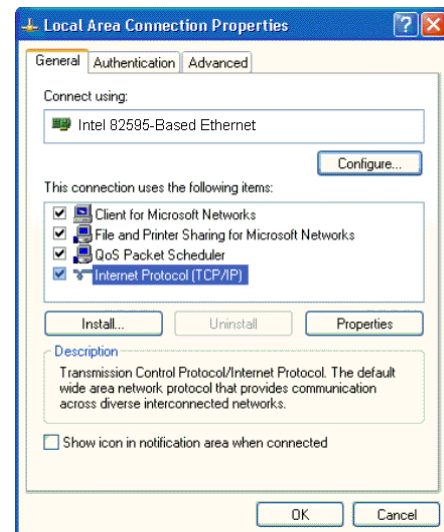


4. Highlight **Protocol** and then click **Add**.
5. Click **Internet Protocol (TCP/IP)** and then click **OK**.
6. When returning to **Local Area Connection Properties** window, highlight **Internet Protocol (TCP/IP)** and then click **Properties**.
7. Under the **General** tab, enable **Use the following 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**.



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. 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**.



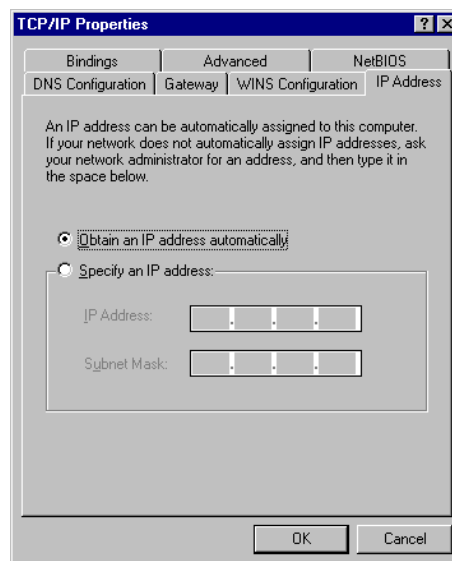
Configure PC to get IP address from DHCP

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:

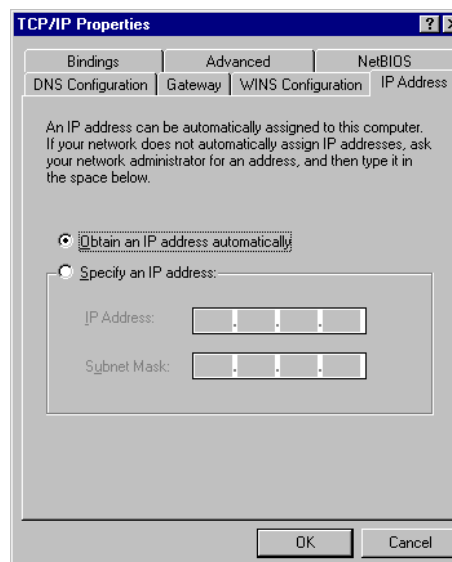
For Windows 98

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



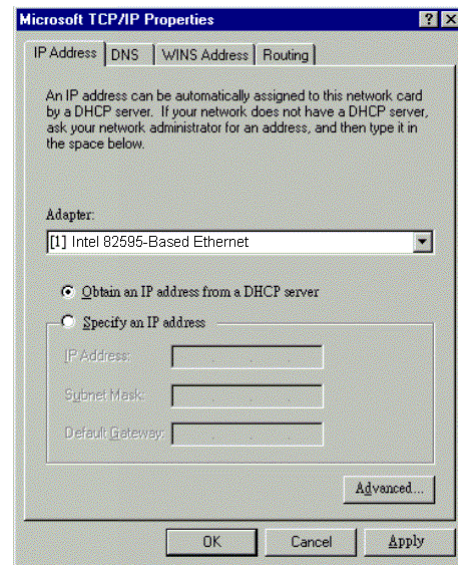
For Windows ME

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

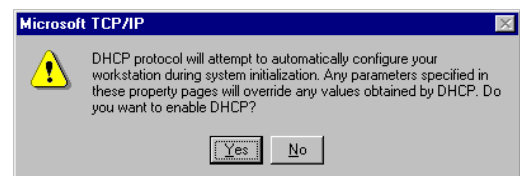


For Windows NT

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..**

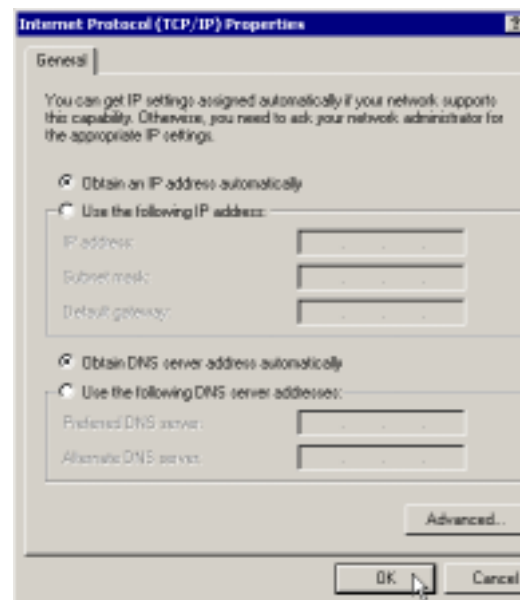


When prompted with the message below, click **Yes** to continue.



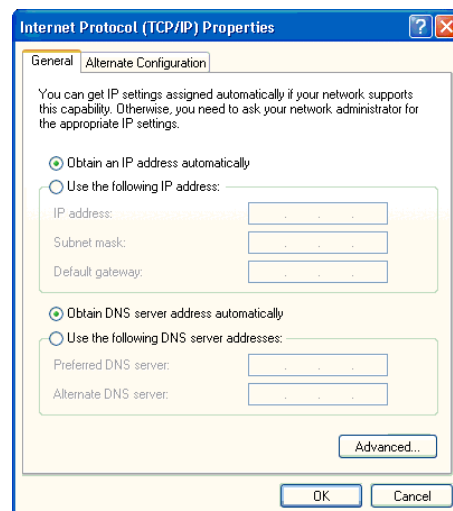
For Windows 2000

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**.

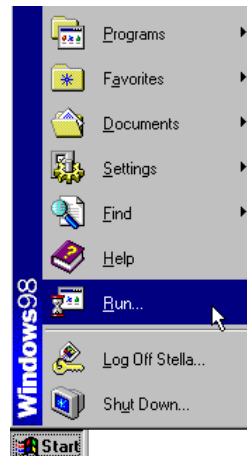


Renew IP Address on Client PC

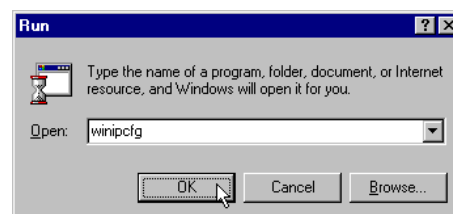
There is a chance that your PC does not renew its IP address after the ADSL Router is on line and the PC cannot access the Internet. Please follow the procedures below to renew PC's IP address.

For Windows 98ME

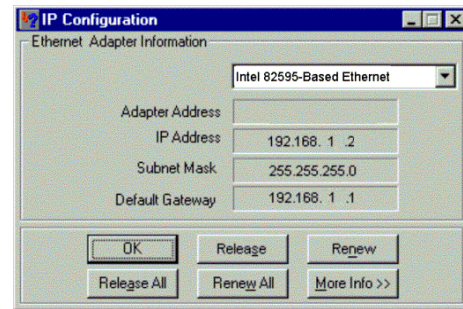
1. Select **Run** from the **Start** menu.



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

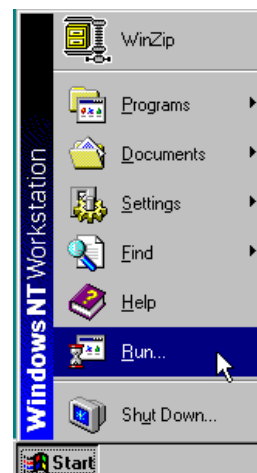


3. When the figure below appears, click Release and then Renew to get an IP address.

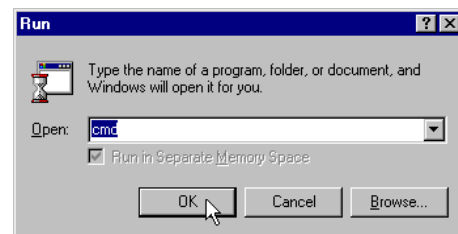


For Windows NT

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



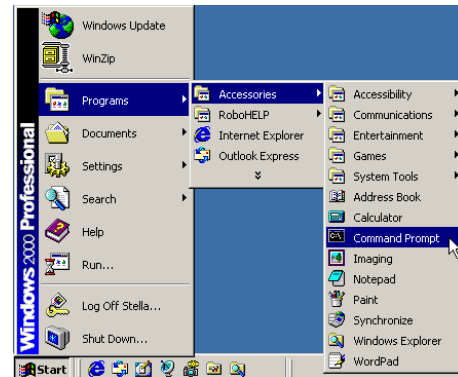
2. Select **Run** from the **Start** menu.
3. Type **cmd** in the dialog box and then click **OK**.



4. Type **ipconfig** at prompt. Then you will see the IP information from DHCP server.
5. 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

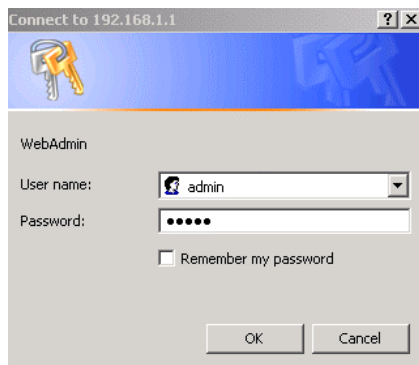
1. Type **ipconfig** at prompt. Then you will see the IP information from DHCP server.
2. From the **Start** menu, point to **Programs, Accessories** and then click **Command Prompt**.
3. Type **ipconfig** at prompt. Then you will see the IP information from DHCP server.
4. If you want to get a new IP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

Chapter 4

Web Configuration

Using Web-Based Manager

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



1. Start your web browser and type the private IP address of the ADSL Router in the URL field: **192.168.1.1**.
2. After connecting to the device, you will be prompted to enter username and password. By default, the username is **admin** and the password is **admin**. See the example for running under Windows XP.

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

Outline of Web Manager

For configure the web page, please use **admin** as the username and the password. The main screen will be shown as below.

DSL Quick Start Status Advanced Diagnostics Management Language: English

Connect to Internet Quick Setup

Connect to Internet

Your DSL router is **not ready to connect** to ADSL.
Status: Down

Enter your ADSL user name and password, then click "Connect".

Internet Connection: pppoe_8_35
Total Online Time: 0 secs
ADSL User Name:
Password:

Connect

Title: It indicates the title of this management interface.

Main Menu: Includes Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics and Management.

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

To Have the New Settings Take Effect

After select or adjust the settings to your desire, your customizations will be saved to the flash memory before you restart the router. And only after restarting the router, your customizations take effect.

Quick Start

Connect to Internet

A quick way to connect to Internet by using PPPoE interface, click **Connect to Internet** to open the web page.

Enter the user name and password for your ADSL router and click **Connect**.

The system will connect automatically.

Connect to Internet

Your DSL router is **not ready to connect to ADSL**.
Status: Down

Enter your ADSL user name and password, then click "Connect".

Internet Connection:	pppoe_8_35
Total Online Time:	0 secs
ADSL User Name	<input type="text"/>
Password	<input type="password"/>

Quick Setup

The quick setup wizard will guide you to configure the DSL router through some steps.

VPI (Virtual Path Identifier): Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255.

VCI (Virtual Channel Identifier): Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols).

After finished entering the VPI/VCI value, please click **Next** for next step

Quick Setup

This Quick Setup will guide you through the steps necessary to configure your DSL Router.

NOTE: All of original settings will be replaced by new settings after you finish these steps.

Select the check box below to scan the Internet connection automatically. It is recommended that there is no any PVC configured in your DSL Router before performing auto-scanning connection.

☐ Auto Scan Internet Connection (PVC)

Configure Internet Connection -- ATM PVC

Please enter VPI and VCI numbers for the Internet connection which is provided by your ISP.

VPI: (0-255)
VCI: (32-65535)

Connection Type

After clicking on the **Next** button from the VPI/VCI web page, the following screen will appear. Please choose the connection type and encapsulation mode that you want to use and click **Next** for next page.

For example, PPP over Ethernet (PPPoE) in this screen is selected.

Configure Internet Connection - Connection Type

Select the protocol and encapsulation type over the ATM PVC that your ISP has instructed you to use.

Protocol:

- ☐ PPP over ATM (PPPoA)
- ☒ PPP over Ethernet (PPPoE)
- ☐ MAC Encapsulation Routing (MER)
- ☐ IP over ATM (IPoA)
- ☐ Bridging

Encapsulation Type:

PPP over ATM/ PPP over Ethernet

If the type you choose is PPP over ATM or PPP over Ethernet, please refer to the following information.

According to the ISP's configuration on the server, you can choose PPPoE and PPPoA modes.

Choose **PPPoA** or **PPPoE** and click **Next**.

In this screen, you have to choose the settings for WAN IP. To get the IP address automatically, click the **Obtain an IP address automatically** radio button. Or click **Use the following IP address** button and enter the IP address for WAN interface.

Click **Enable NAT** if you want.

Click **Next** for next screen.

PPP Username:

Type in the username that you got from your ISP.

PPP Password:

Type in the password that you got from your ISP.

Always On:

Check this button to make the connection is always active.

Dial on Demand:

Click this button to make a connection while in demand. Enter the timeout to cut off the network connection if there is no activity for this router.

Manually Connect:

Click this button to make a connection by pressing the Connect button on the Advanced Setup- WAN - Internet web page.

PPP IP extension:

Check this box to invoke the PPP IP extension. When you check this box, only one user is allowed to access into the web page for configuration at one time.

Configure Internet Connection - Connection Type

Select the protocol and encapsulation type over the ATM PVC that your ISP has instructed you to use.

Protocol: ☐ PPP over ATM (PPPoA)
☒ PPP over Ethernet (PPPoE)
☐ MAC Encapsulation Routing (MER)
☐ IP over ATM (IPoA)
☐ Bridging

Encapsulation Type:

< Back Next >

Configure Internet Connection - WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

WAN IP Address:

☒ Enable NAT

< Back Next >

Configure Internet Connection - PPP User Name and Password

In order to establish the Internet connection, please enter PPP user name and password that your ISP has provided.

PPP User Name:

PPP Password:

Session established by: ☐ Always On

☒ Dial on Demand

Disconnect if no activity for minutes

☐ Manually Connect

< Back Next >

Please type the username and password that you got from your ISP. Then click **Next**.

Primary IP Address:

Type in the first IP address that you got from your ISP for your LAN connection.

Subnet Mask:

Type in the subnet mask that you got from your ISP for your LAN connection.

Configure the second IP Address and Subnet Mask for LAN interface:

Check this box to make another set of IP Address and Subnet Mask to connect to your router if they are not included in the range that DHCP server accepts.

Secondary IP Address:

Type in the second IP address that you got from your ISP for your LAN connection.

Subnet Mask:

Type in the subnet mask that you got from your ISP for your LAN connection.

Enable DHCP server on the LAN:

Check this item if DHCP service is needed on the LAN. The router will assign IP address, gateway address for each of your PCs.

Start IP Address:

Type in the start point IP address.

End IP Address:

Type in the end point IP address.

Leased Time:

Type in the duration for the time. The default is 1 day.

You can check it at this time. If you find something is incorrect, click **Back** to change the settings.

If everything is OK, click **Finish** to accept these settings.

Now, the system will reboot to activate the new settings that you have done in this section.

Please wait for 2 minutes for restarting the router.

Configure LAN side Settings**LAN side IP Address**

Enter the DSL Router IP Address and Subnet Mask for LAN interface.

Primary IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Host Name:	RTA230
Domain Name:	home

☐ Configure the second IP Address and Subnet Mask for LAN interface.

DHCP Server

Enabling DHCP Server on LAN interface can provide the proper IP Address settings to your computers.

☒ Enable DHCP Server on the LAN

Start IP Address:	192.168.1.2
End IP Address:	192.168.1.254
Leased Time:	1 days 0 hours 0 minutes

< Back Next >

On the Configure LAN side Settings web page, the IP address and subnet mask will be shown on it. You can modify them if needed.

Type in all the necessary settings and click **Next** for next page.

Quick Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Internet (WAN) Configuration:

VPI / VCI	8 / 35
Connection Type	PPPoA LLC/SNAP, Dial on Demand, Idle Timer 20 mins
NAT	On
WAN IP Address	Automatically Assigned
Default Gateway	Automatically Assigned
DNS Server	Automatically Assigned

LAN Configuration:

Primary LAN IP	192.168.1.1 / 255.255.255.0
Secondary LAN IP	0.0.0.0 / 0.0.0.0
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 ~ 192.168.1.254
DHCP Lease Time	1 days 0 hours 0 minutes

Click "Finish" to accept these settings, and reboot the system.
Click "Back" to make any modifications.

< Back Finish

Reboot DSL Router

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

MAC Encapsulated Routing (MER)

If the type you choose is MAC Encapsulated Routing (MER), please refer to the following information.

MER mode is used in business environment where static IP address and subnet are assigned by your ISP.

Choose **MER** and click **Next**.

Configure Internet Connection - Connection Type

Select the protocol and encapsulation type over the ATM PVC that your ISP has instructed you to use.

Protocol:

- ☐ PPP over ATM (PPPoA)
- ☐ PPP over Ethernet (PPPoE)
- ☒ MAC Encapsulation Routing (MER)
- ☐ IP over ATM (IPoA)
- ☐ Bridging

Encapsulation Type:

[< Back](#) [Next >](#)

Obtain an IP address automatically: Click this button to make the system get an IP address automatically.

Use the following IP address:

If you want to set WAN IP address by yourself, you have to click on this button to invoke the following entries.

WAN IP Address:

Type in the IP address that you got from ISP for the WAN interface.

WAN Subnet Mask:

Type in the subnet mask address that you got from ISP for the WAN interface.

Default Gateway:

Type in the default gateway that you got from ISP for the WAN interface.

Obtain DNS server address automatically:

Click this button to make the system get DNS server automatically.

Use the following DNS server address:

If you want to set DNS server by yourself, you have to click on this button to invoke the following entries.

Preferred DNS server:

Type in your preferred DNS server that you got from ISP.

Alternate DNS server:

Type in the alternate DNS server that you got from ISP.

Enable NAT:

Check **Enable NAT** to enable this function.

Primary IP Address:

Type in the first IP address that you got from your ISP for your LAN connection.

Subnet Mask:

Type in the subnet mask that you got from your ISP for your LAN connection.

Configure Internet Connection - WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

WAN IP Address:

WAN Subnet Mask:

Default Gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

☒ Enable NAT

[< Back](#) [Next >](#)

Please type in the WAN IP address, Subnet Mask, Default Gateway and DNS server addresses. Then Click **Next** to get the following page.

Configure the second IP Address and Subnet Mask for LAN interface:

Check this box to make another set of IP Address and Subnet Mask to connect to your router if they are not included in the range that DHCP server accepts.

Secondary IP Address:

Type in the second IP address that you got from your ISP for your LAN connection.

Subnet Mask:

Type in the subnet mask that you got from your ISP for your LAN connection.

Enable DHCP server on the LAN:

Check this item if DHCP service is needed on the LAN. The router will assign IP address, gateway address for each of your PCs.

Start IP Address:

Type in the start point IP address.

End IP Address:

Type in the end point IP address.

Leased Time:

Type in the duration for the time. The default is 1day.

You can check it at this time. If you find something is incorrect, click **Back** to change the settings. If everything is OK, click **Finish** to accept these settings. And the following page will appear.

Now, the system will reboot to activate the new settings that you have done in this section.

Please wait for 2 minutes for restarting the router.

Configure LAN side Settings

LAN side IP Address

Enter the DSL Router IP Address and Subnet Mask for LAN interface.

Primary IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Host Name:	RTA230
Domain Name:	home

☐ Configure the second IP Address and Subnet Mask for LAN interface.

DHCP Server

Enabling DHCP Server on LAN interface can provide the proper IP Address settings to your computers.

☒ Enable DHCP Server on the LAN

Start IP Address:	192.168.1.2
End IP Address:	192.168.1.254
Leased Time:	1 days 0 hours 0 minutes

[< Back](#) [Next >](#)

On the **Configure LAN side Settings** web page, the IP address and subnet mask will be shown on it. You can modify them if needed. Click **Next** for next page.

Quick Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Internet (WAN) Configuration:

VPI / VCI	8 / 35
Connection Type	MER LLC/SNAP
NAT	On
WAN IP Address	10.3.95.3
Default Gateway	10.3.95.1
DNS Server	168.95.1.1 ; 168.95.192.1

LAN Configuration:

Primary LAN IP	192.168.1.1 / 255.255.255.0
Secondary LAN IP	0.0.0.0 / 0.0.0.0
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 ~ 192.168.1.254
DHCP Lease Time	1 days 0 hours 0 minutes

Click "Finish" to accept these settings, and reboot the system.
Click "Back" to make any modifications.

[< Back](#) [Finish](#)

Reboot DSL Router

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

IP over ATM

If the type you choose is IP over ATM, please refer to the following information.

IPoA is an alternative of LAN emulation. It allows TCP/IP network to access ATM network and uses ATM quality of service's features.

Choose **IPoA** and click **Next**

Configure Internet Connection - Connection Type

Select the protocol and encapsulation type over the ATM PVC that your ISP has instructed you to use.

- Protocol:
- ☐ PPP over ATM (PPPoA)
 - ☐ PPP over Ethernet (PPPoE)
 - ☐ MAC Encapsulation Routing (MER)
 - ☒ IP over ATM (IPoA)
 - ☐ Bridging

Encapsulation Type: LLC/SNAP

[< Back](#) [Next >](#)

None:

If it is not necessary to set the WAN IP address, please click this button.

Obtain an IP address automatically: Click this button to make the system get an IP address automatically.

WAN IP Address:

Type in the IP address that you got from ISP for the WAN interface.

WAN Subnet Mask:

Type in the subnet mask address that you got from ISP for the WAN interface.

Obtain DNS server address automatically:

Click this button to make the system get DNS server automatically.

Use the following DNS server address:

If you want to set DNS server by yourself, you have to click on this button to invoke the following entries.

Primary DNS server:

Type in your preferred DNS server that you got from ISP.

Secondary DNS server:

Type in the alternate DNS server that you got from ISP.

Enable NAT:

Check **Enable NAT** to enable this function.

Please type in the WAN IP address, Subnet Mask and DNS server addresses. Then Click **Next** to get the following page.

Configure Internet Connection - WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

- ☐ None
- ☒ Obtain an IP address automatically
- ☐ Use the following IP address:
- WAN IP Address:
- WAN Subnet Mask:
- ☒ Obtain DNS server address automatically
- ☐ Use the following DNS server addresses:
- Primary DNS server:
- Secondary DNS server:
- ☒ Enable NAT

[< Back](#) [Next >](#)

Primary IP Address:

Type in the first IP address that you got from your ISP for your LAN connection.

Subnet Mask:

Type in the subnet mask that you got from your ISP for your LAN connection.

Configure the second IP Address and Subnet Mask for LAN interface:

Check this box to make another set of IP

Configure LAN side Settings

LAN side IP Address

Enter the DSL Router IP Address and Subnet Mask for LAN interface.

Primary IP Address:

Subnet Mask:

Host Name:

Domain Name:

☒ Configure the second IP Address and Subnet Mask for LAN interface.

Secondary IP Address:

Subnet Mask:

Address and Subnet Mask to connect to your router if they are not included in the range that DHCP server accepts.

Secondary IP Address:

Type in the second IP address that you got from your ISP for your LAN connection.

Subnet Mask:

Type in the subnet mask that you got from your ISP for your LAN connection.

Enable DHCP server on the LAN:

Check this item if DHCP service is needed on the LAN. The router will assign IP address, gateway address for each of your PCs.

Start IP Address:

Type in the start point IP address.

End IP Address:

Type in the end point IP address.

Leased Time:

Type in the duration for the time. The default is 1 day.

You can check it at this time. If you find something is incorrect, click **Back** to change the settings. If everything is OK, click **Finish** to accept these settings. And the following page will appear.

Now, the system will reboot to activate the new settings that you have done in this section.

Please wait for 2 minutes for restarting the router.

Configure LAN side Settings

LAN side IP Address

Enter the DSL Router IP Address and Subnet Mask for LAN interface.

Primary IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Host Name:	<input type="text" value="RTA230"/>
Domain Name:	<input type="text" value="home"/>

☒ Configure the second IP Address and Subnet Mask for LAN interface.

Secondary IP Address:	<input type="text" value="0.0.0.0"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>

DHCP Server

Enabling DHCP Server on LAN interface can provide the proper IP Address settings to your computers.

☒ Enable DHCP Server on the LAN

Start IP Address:	<input type="text" value="192.168.1.2"/>
End IP Address:	<input type="text" value="192.168.1.254"/>
Leased Time:	<input type="text" value="1"/> days <input type="text" value="0"/> hours <input type="text" value="0"/> minutes

[< Back](#) [Next >](#)

On the Configure LAN side Settings web page, the IP address and subnet mask will be shown on it. You can modify them if needed. Click **Next** for next page.

Quick Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Internet (WAN) Configuration:

VPI / VCI	8 / 35
Connection Type	IPoA LLC/SNAP
NAT	On
WAN IP Address	Automatically Assigned
Default Gateway	Automatically Assigned
DNS Server	Automatically Assigned

LAN Configuration:

Primary LAN IP	192.168.1.1 / 255.255.255.0
Secondary LAN IP	0.0.0.0 / 0.0.0.0
DHCP Server	Enabled
DHCP IP Range	192.168.1.2 ~ 192.168.1.254
DHCP Lease Time	1 days 0 hours 0 minutes

Click "Finish" to accept these settings, and reboot the system.
Click "Back" to make any modifications.

[< Back](#) [Finish](#)

Reboot DSL Router

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Bridging

If the type you choose is Bridging, please refer to the following information.

The bridging mode can configure your router to send packets received on any port such as ATM PVC or Ethernet with a broadcast MAC address to all other ports.

Choose **Bridging** and click **Next**.

Configure Internet Connection - Connection Type

Select the protocol and encapsulation type over the ATM PVC that your ISP has instructed you to use.

Protocol:

- ☐ PPP over ATM (PPPoA)
- ☐ PPP over Ethernet (PPPoE)
- ☐ MAC Encapsulation Routing (MER)
- ☐ IP over ATM (IPoA)
- ☒ Bridging

Encapsulation Type: LLC/SNAP

< Back Next >

Primary IP Address:

Type in the IP address that you got from your ISP for LAN interface.

Subnet Mask:

Type in the subnet mask that you got from your ISP for LAN interface.

You can modify them if needed. Click **Next** for next step.

Configure LAN side Settings

This step is optional.

LAN side IP Address

Enter the DSL Router IP Address and Subnet Mask for LAN interface.

Primary IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

< Back Next >

You can check it at this time. If you find something is incorrect, click **Back** to change the settings. If everything is OK, click **Finish** to accept these settings. And the following page will appear.

Quick Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Internet (WAN) Configuration:

VPI / VCI	8 / 35
Connection Type	Bridge LLC/SNAP

LAN Configuration:

Primary LAN IP	192.168.1.1 / 255.255.255.0
DHCP Server	Disabled

Click "Finish" to accept these settings, and reboot the system.
Click "Back" to make any modifications.

< Back Finish

Now, the system will reboot to activate the new settings that you have done in this section.

Please wait for 2 minutes for restarting the router.

Reboot DSL Router

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Status

Overview

This page is displaying the current status for the DSL connection.

Overview of Device Information

This information reflects the current status of your DSL Router.

Wireless Network	Enabled
ADSL Port	Enabled

Downstream Line Rate	
Upstream Line Rate	
LAN IP Address	192.168.1.1
Default Gateway	
Primary DNS Server	192.168.1.1
Secondary DNS Server	192.168.1.1
Firmware Version	2.12.3.15_a023g
System Up Time Duration	00:00:23:30

ADSL Line

This page shows all information for ADSL. For knowing the quality of the ADSL connection, please click ADSL BER Test button to have advanced information.

Click More Information to show more detailed information about ADSL Line Status.

ADSL Line Status

Current adsl line status is as the below.

Line Mode		Line State	Down
Latency Type		Line Up Time Duration	N/A
Line Coding		Line Up Count	0

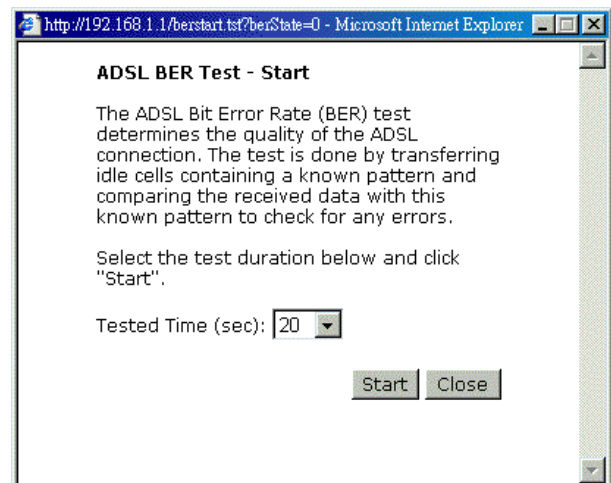
Statistics	Downstream	Upstream
Line Rate		
Attainable Line Rate		
Noise Margin		
Line Attenuation		
Output Power		

[More Information](#) »

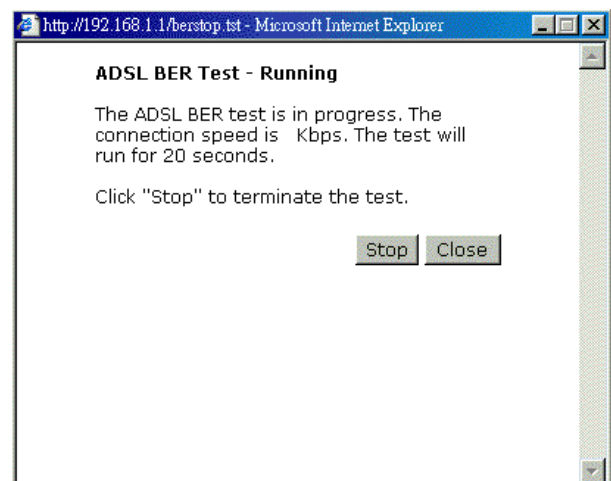
ADSL BER Test

ADSL BER Test

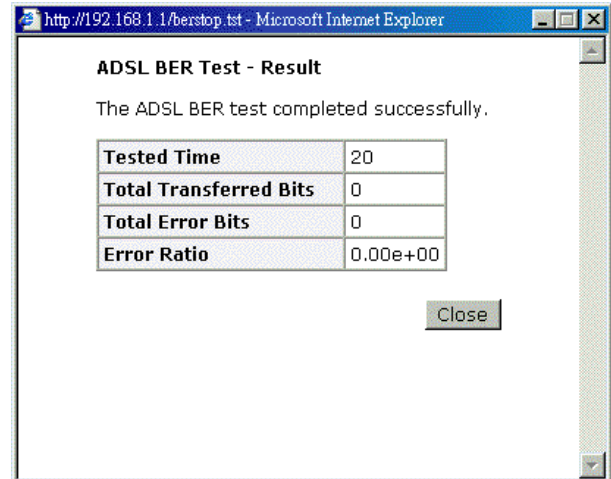
This test determines the quality of the ADSL connection. It is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for errors.



After select the test duration time and click **Start**, the following dialog appears to tell you the test is running. You can stop the test by click **Stop** or close this dialog by click **Close**.



When the test is over, the result will be shown on the following dialog for your reference. Click **Close** to close this dialog.



Internet Connection

This page displays the connection information for your router, such as PVC name, category, protocol, invoking NAT or not, IP address, link status and so on.

Internet Connection

Current Internet connections are listed below.

PVC Name	VPI/VCI	Category	Protocol	NAT	WAN IP Address	Status / Online Time
pppoe_8_35	8/35	UBR	PPPoA LLC/SNAP	On		ADSL Link Down 00:00:00:00

Traffic Statistics

This table shows the records of data going through the LAN and WAN interface. For each interface, cumulative totals are displayed for **Received** and **Transmitted**.

Traffic Statistics

The statistics of user data going through your DSL Router are listed below.

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
Ethernet	183244	1723	0	0	537115	1974	0	0
USB	0	0	0	0	0	0	0	0
Wireless	0	0	0	0	14540	91	0	0
WAN	0	0	0	0	0	0	0	0

Reset

DHCP Table

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

DHCP Table

Those devices which get their IP addresses from your DSL Router are listed below.

Host Name	MAC Address	IP Address	Lease Time
CN	00:C1:26:0A:69:2B	192.168.1.2	00:23:55:31

Wireless Client

This table shows the MAC address for all of wireless LAN clients currently associated to your DSL Router.

Wireless Clients Table

All of wireless LAN clients currently associated to your DSL Router are listed below.

NOTE: The list below might include wireless clients which are no longer connected to your DSL Router. You need to wait for a few seconds for the list to be fully updated.

MAC Address	On-line Time
-------------	--------------

Routing Table

This table shows the routing method that your router uses.

Routing Table

All of current routing rules in your DSL Router are listed below.

Destination	Netmask	Gateway	Interface	Metric
192.168.1.0	255.255.255.0	0.0.0.0	br0	0

ARP Table

This table shows the IP address record for IP-to-Physical translation in your router.

ARP Table

The IP-to-Physical address translation entries recorded in your DSL Router are listed below.

IP address	Physical Address	Interface	Type
192.168.1.2	00:C1:26:0A:69:2B	br0	Dynamic

Advanced Setup

LAN- IP Address

This page is the same as you can see in the **Configure LAN side Settings** page while running the **Quick Setup**. It allows you to set IP Address and Subnet Mask values for LAN interface.

Primary IP Address:

Type in the first IP address that you got from your ISP for your LAN connection.

Subnet Mask:

Type in the subnet mask that you got from your ISP for your LAN connection.

Configure the second IP Address and Subnet Mask for LAN interface:

Check this box to make another set of IP Address and Subnet Mask to connect to your router if they are not included in the range that DHCP server accepts.

Secondary IP Address:

Type in the second IP address that you got from your ISP for your LAN connection.

Subnet Mask:

Type in the subnet mask that you got from your ISP for your LAN connection.

Apply:

Click this button to activate the settings listed above.

LAN IP Address Configuration

NOTE: New settings only take effect after the router is rebooted. If necessary, reconfigure your PC's IP address to match new settings.

Enter the DSL Router IP Address and Subnet Mask for LAN interface.

Primary IP Address:
 Subnet Mask:
 Host Name:
 Domain Name:

☒ Enable UPNP

☒ Configure the second IP Address and Subnet Mask for LAN interface.

Secondary IP Address:
 Subnet Mask:

LAN-DHCP Server

This allows you to set DHCP server on LAN interface.

Enable DHCP server on the LAN:

Check this item if DHCP service is needed on the LAN. The router will assign IP address, gateway address for each of your PCs.

Start IP Address:

Type in the start point IP address.

End IP Address:

Type in the end point IP address.

Leased Time:

Type in the duration for the time. The default is 1day.

Apply:

Click this button to activate the settings listed above.

DHCP Server Configuration

Enabling DHCP Server on LAN interface can provide the proper IP address settings to your computer.

NOTE: New settings only take effect after the router is rebooted. If necessary, reconfigure your PC's IP address to match new settings.

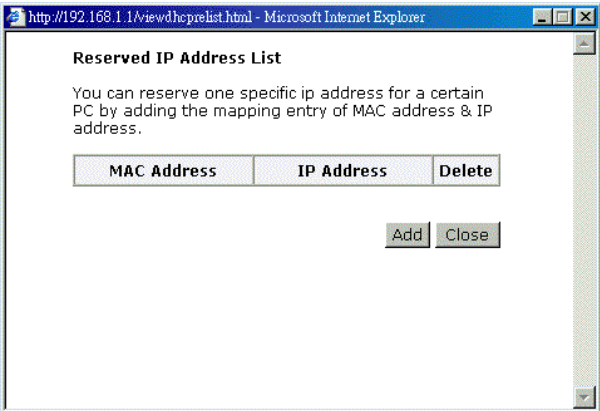
☒ Enable DHCP Server on the LAN

Start IP Address:

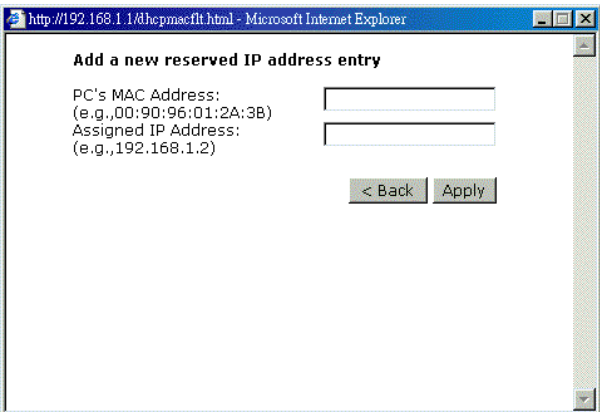
End IP Address:

Leased Time: days hours minutes

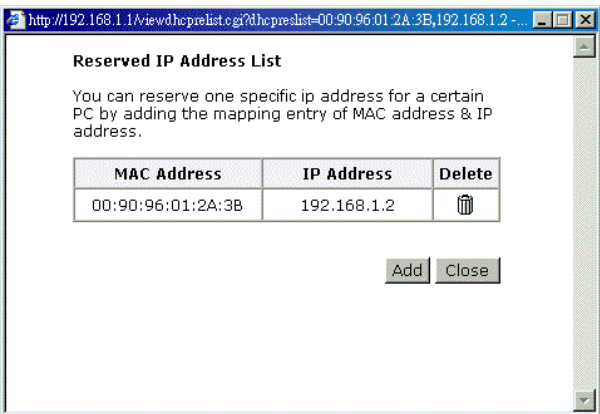
You can reserve one specific IP address for a certain PC for certain purpose. Simply add a mapping entry of MAC address & IP address for that PC by pressing the **View Reserved IP Address List** button. The following picture will appear.



Click the Add button to open another dialog as follows. On PCs MAC Address and Assigned IP Address boxes, please type in the correct information for the one that you want to add and click **Apply**.



The new one will be shown on the dialog right away. That is, the specified address will be reserved and not be assigned by DHCP for other computer.





WAN - Internet Setting

To set WAN settings for each service, please open **Advanced Setup – WAN**. This page allows you to add new WAN settings, to edit or remove created WAN settings.

If you click the **Connect** line under the PVC Name item, the system will connect to WAN automatically. If the WAN connection is OK, you can check the detailed information directly.

Internet Connection Configuration
Choose Add or Edit to configure Internet connection.
Choose Finish to apply the changes and reboot the system.
NOTE: The Internet connection is NOT active if the PVC name is maked with (?). You need to click "Finish" to apply the changes and reboot the system for activating this PVC.

PVC Name	VPI/VCI	Category	Protocol	NAT	WAN IP Address	Edit
pppoa_8_35 Connect	8/35	UBR	PPPoA LLC/SNAP	On	Auto assingd	 

Add Finish

Adding a New One

To add a new WAN connection, please click the **Add** button. The following screen appears.

VPI (Virtual Path Identifier):

Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255.

VCI (Virtual Channel Identifier):

Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols).

Service Category:

There are five categories provided here for your selection. Please choose any one of it as you desired.

Configure Internet Connection -- ATM PVC

Please enter VPI and VCI numbers for the Internet connection which is provided by your ISP.

VPI: (0-255)
VCI: (32-65535)

Service Category:

< Back Next >

If you choose Non Realtime VBR, you have to type in the following data.

The range for Peak Cell Rate is from 1 to 1690.

The range for Sustainable Cell Rate is from 1 to 1689 and must be smaller than Peak Cell Rate.

The range for Maximum Burst Size is from 1 to 100.

Configure Internet Connection -- ATM PVC

Please enter VPI and VCI numbers for the Internet connection which is provided by your ISP.

VPI: (0-255)
VCI: (32-65535)

Service Category:
Peak Cell Rate: cells/s (1-1690)
Sustainable Cell Rate: cells/s (1-1689)
Maximum Burst Size: cells/s (1-100)

< Back Next >

You have to type in the VPI and VCI values in the entry boxes. Then click **Next**. The screen will get into the **Connection Type** page of **Quick Setup** and ask you to fill in the data according to the request of the screen. Refer to **Quick Setup** for more information if you don't know how to set the configuration.

WAN - ADSL Settings

Modulation:

There are five selections for your choosing. Select the one that you need.

ADSL Settings

☒ Enable ADSL Port

Select the line mode below.

- ☒ Auto mode (G.dmt, G.lite or T1.413)
- ☐ G.dmt / G.lite
- ☐ T1.413
- ☐ G.dmt
- ☐ G.lite

Apply

IP Routing - Static Route

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

Destination Network Address:
Display the IP address that the data packets are to be sent.

Netmask:
Display the subnet mask that the data transmitting is passing through.

Gateway:
Display the gateway that the data transmitting is passing through.

WAN Interface:
Display the interface that the data transmitting is passing through.

Remove:
Allow you to remove the selected static route settings.

Static Route

Current static routes:

Destination	Netmask	Gateway	WAN Interface	Delete

Add

Adding a New One

To add a static route, please choose Static Route - Add. Type the destination network address, subnet mask and gateway that you get from ISP and click **Apply**.

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

Subnet Mask:
Type in the subnet mask that you got from ISP.

Gateway IP Address:
Check this box to invoke this function. Type in the gateway that you got from ISP.

WAN Interface:
Check this box to invoke this function and choose the one from the drop down menu.

Add New Static Route

Enter the Destination Network Address, Netmask, Gateway or available WAN interface then click "Apply" to add the entry to the routing table.

Destination Network (For default route, type 0.0.0.0 or leave blank)

IP Address: 192.168.1.10

Netmask: 255.255.255.0

Forward Packets to

☒ Gateway IP Address:

☐ WAN Interface: pppoa_8_35

Apply

Click **Apply** to view the routing result. This page shows all the routing table of data packets going through your ADSL Router.

Remove Static Route

If you don't want the static route that you created, please click the icon under **Delete** from Routing Table.

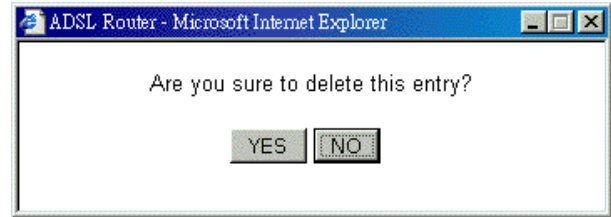
Static Route

Current static routes:

Destination	Netmask	Gateway	WAN Interface	Delete
0.0.0.0	255.255.255.0	192.168.1.1		

Add

A dialog appears to ask you to confirm the action. Click Yes to remove the static route, or click No to keep the setting.



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.

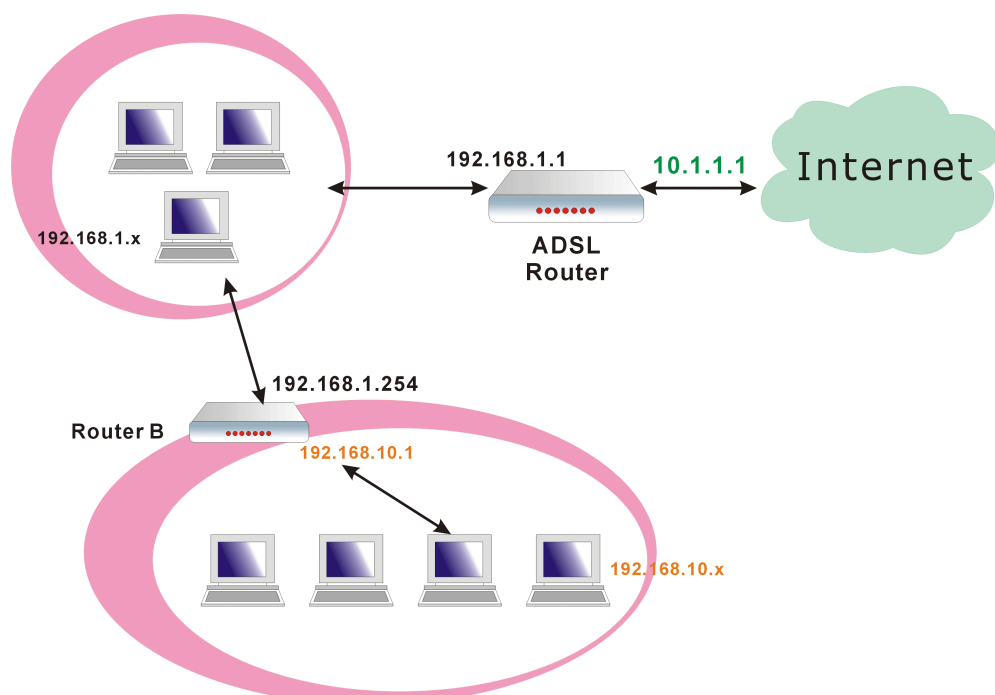
Other Routers on the Local LAN

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

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

ADSL Router	Destination	192.168.10.0
	Subnet Mask	255.255.255.0 (Standard Class C)
	Gateway	192.168.1.254 (Router B)

IP Routing – Dynamic Routing

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

Version: It incorporates the RIP information when receiving and broadcasting the RIP packets. From the radio buttons, select a RIP version to be accepted, 1, 2 or both.

Operation:

There are two modes for you to choose, Active and Passive. Select Active for transmitting and receiving data, or select Passive for receiving data only.

Enabled:

Click Enabled to enable the RIP function on different interface. Otherwise, disable this function.

Click **Apply** to invoke the settings set here.

Dynamic Routing

You can enable RIP function on several interfaces of your DSL router. Select the desired RIP version and operation, followed by ticking the 'Enabled' checkbox to do so when clicking "Apply", or leave unticked if you would like to disable RIP on those interfaces.

Interface	Version	Operation	Enabled
LAN	2	Active	<input type="checkbox"/>
pppoe_8_35	2	Passive	<input type="checkbox"/>

Apply

DNS Server

If **Enable Automatic Assigned DNS** checkbox is selected, this router will accept the **first** received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, it is necessary for you to enter the primary and optional secondary DNS server IP addresses. After type in the address, click **Apply** button to save it and invoke it.

Enable Automatic Assigned DNS:

Check this box to enable this function, or uncheck this box to disable it.

Primary DNS server:

Type in your primary DNS server.

Secondary DNS server:

Type in the secondary DNS server.

If you are satisfied the settings, click **Apply**.

DNS Server Configuration

If Enable Automatic Assigned DNS checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click "Apply" to save it.

NOTE: If changing from unselected Automatic Assigned DNS to selected Automatic Assigned DNS, You must reboot the router to get the automatic assigned DNS addresses.

☐ Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

Apply

NAT - Virtual Servers

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

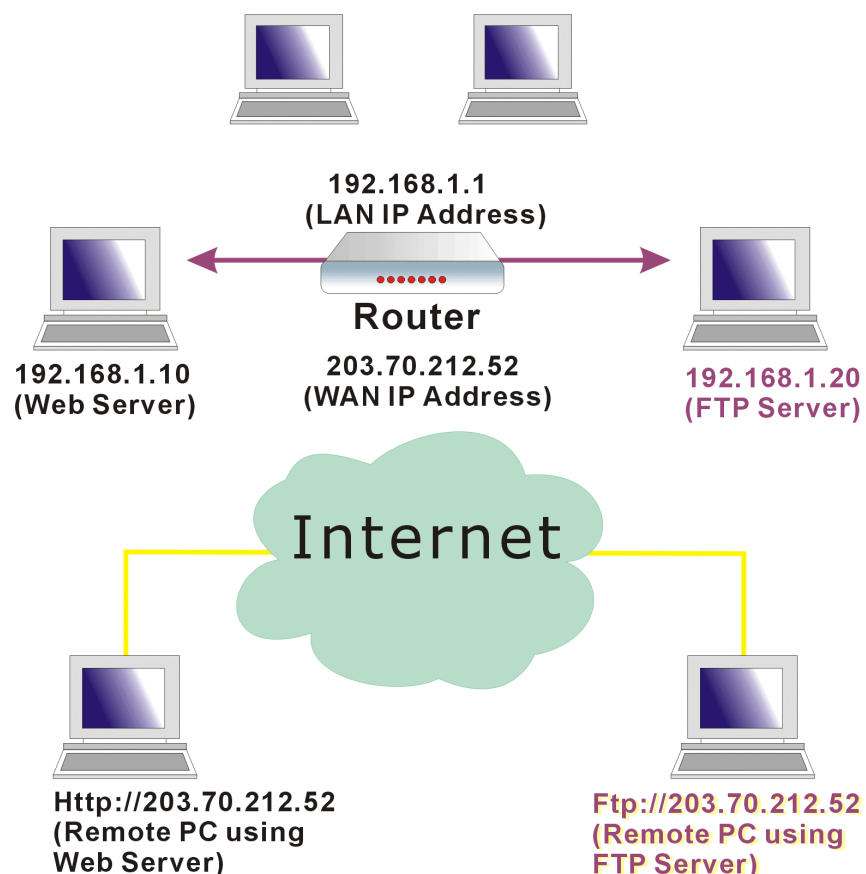
When the router receives an incoming IP packet requesting for access to your local server, the router will recognize the service type according to the port number in this packet (e.g., port 80 indicates HTTP service and port 21 indicates FTP service). By specifying the port number, you tell the router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

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

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:

- ☐ Your 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 than 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.

To set a virtual server, please open the **Virtual Servers** item from the **Advanced Setup - NAT** menu.

Virtual Servers

Server Name	Protocol	External Port	Internal Port	Server IP Address	Remove
<div style="text-align: right;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>					

Add New Virtual Servers

To add a new Virtual Server, please click **Add**. In the “**Select from the following list**” drop-down list, you can select required entry

Select from the following list:

Choose one of the services from the list, such as SMTP, WEB, FTP, DNS and so on. The corresponding data will be shown on the data boxes below.

Customized service:

Type a new service name for building a customized service for specific reason.

Protocol:

Select a protocol for the service that you choose.

External port for this service:

The port number will be shown automatically when you select a service for using. You can type a new number if you want to do a customized service.

Internal port for this service:

The port number will be shown automatically when you select a service for using. You can type a new number if you want to do a customized service.

Internal server IP address:

Type in the server IP address when you want to specify a certain address for the virtual server.

1. Select the protocol type from the drop-down list.
2. Enter the TCP/IP port information in the External and Internal Port for this service fields.
3. Enter the IP address of the internal server in the Internal server IP Address field.
4. Click **Apply**.

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).

Virtual Servers

Select the service name, server IP address and click "Apply" to forward IP packets for this service to the specified server.

Service Name:

☒ Select from the following list:

☐ Customized service:

Protocol:

External port (port or port:port):

Internal port (port or port:port):

Internal server IP address:

After adding a new virtual server, click **Apply** to view the new virtual server. The following screen will be shown to display the status for this new one.

If you do not want the new server that you added, please check the one and click **Remove** to discard it. Or if you want to add another one again, click **Add** to add a new one. And if you are satisfied with all settings that you configure here, click **Save**.

Virtual Servers

Server Name	Protocol	External Port	Internal Port	Server IP Address	Remove
FTP	TCP	21	21	192.168.1.4	<input type="checkbox"/>

Add **Remove**

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 Fixed 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.

NAT - DMZ Host

Direct Mapping Zone (DMZ) uses a technology that makes Router forwarding all incoming packet to internal specific server.

To activate a DMZ host, please type in the DMZ Host IP Address and click **Apply**.

DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host. Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Apply

This feature allows 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.

NAT - Dynamic DNS

This page allows you to access into virtual servers with a domain name and password.

Dynamic DNS:

Selects Enable to enable DDNS; select Disabled to disable this function.

Internet Connection:

Selects the interface that you want to use for connecting Internet.

User Name:

Type in the user name that you registered in www.dyndns.org.

Password:

Type in the password that you registered in www.dyndns.org.

Domain Name:

Type in the domain name that you registered in www.dyndns.org. You can use letters and dash for naming, yet other characters are not allowed to use for preventing from making troubles.

Status:

It displays current status for DDNS.

Dynamic DNS Configuration

This page allows you to provide Internet users with a domain name (instead of an IP address) to access your virtual servers. This DSL router supports dynamic DNS provided by the provider <http://www.dyndns.org>. Please register this service at www.dyndns.org.

The user name is configured when you register the service and then the password will be sent to you via email. Domain name is allocated to you by www.dyndns.org.

Dynamic DNS: ☐ Disabled ☒ Enabled

Internet Connection:

User Name:

Password:

Domain Name:

Status:

Firewall

The firewall is a software that interrupts the data between the Internet and your computer. It is the TCP/IP equivalent of a security gate at the entrance to your company. All data must pass through it, and the firewall (functions as a security guard) will allow only authorized data to be passed into the LAN.

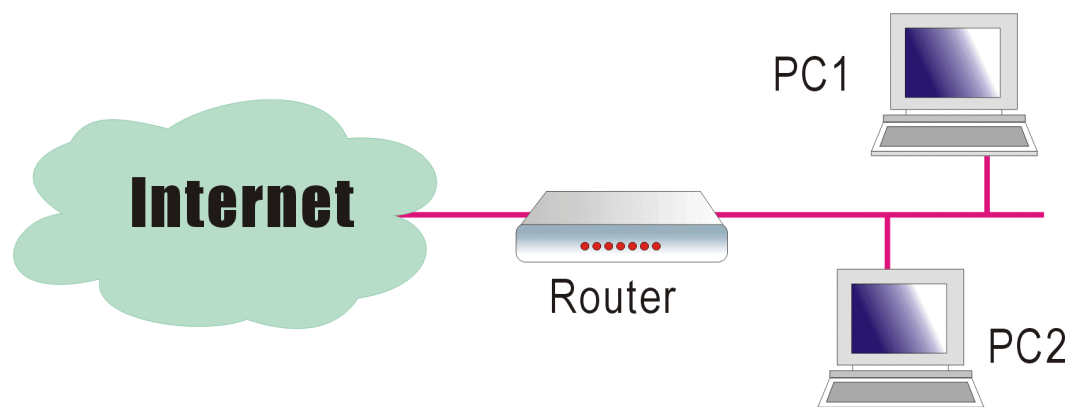
What the firewall can do? It can:

- ☐ deny or permit any packet from passing through explicitly
- ☐ distinguish between various interfaces and match on the following fields:
 - ◆ source and destination IP address
 - ◆ port

To keep track of the performance of IP Filter, a logging device is used which supports logging of the TCP/UDP and IP packet headers and the first 129 bytes of the packet (including headers) when a packet is successfully **passed** through, a packet is **blocked** from passing through and it matches a rule setup to look for suspicious packets

IP Filtering

An example for firewall setup:



This picture is the most common and easiest way to employ the firewall. Basically, you can install a packet-filtering router at the Internet gateway and then configure the filter rule in the router to block or filter protocols and addresses. The systems behind the router usually have a direct access to the Internet, however some dangerous services such as NIS and NFS are usually blocked.

For the security of your router, set the firewall is an important issue.

Choose **Disabled** to disable the firewall function.

IP Filtering

This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts.

IP Filtering: ☒ Disabled ☐ Enabled

Apply

To open the IP Filtering, please click the **Enabled** radio button. The web page will be shown as the right picture.

Select the direction to filter packets:

The way of the data transmission. In Bound means the data is transferred from outside onto your computer. Out Bound means the data is transferred from your computer onto outside through Internet. Please choose **Outbound traffic** or **Inbound traffic** as the direction for filtering packets

IP Filtering

This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts.

IP Filtering: ☐ Disabled ☒ Enabled

Apply

Select the direction to filter packets: ☒ Outbound traffic ☐ Inbound traffic

Protocol	Source IP addr	Dest IP addr	Port Range		Allow	Edit
			Start	End		

Add

direction for filtering packets.

Then, to add a new IP Filtering, click **Add**.

This page provides some settings for you to adjust for adding a new outbound IP Filtering.

Allow Traffic:
No stops the data transmission, **Yes** lets the data pass through.

Protocol:
Here provide several default policies for security levels for you to choose. If you don't want to use the predefined setting, you can use **User Defined** to set a customized protocol for your necessity. When you choose **User Defined** setting, you have to type in a port number in the "as" field.

Source/Destination IP address:
To specify IP address to allow or deny data transmission, please pull down the drop-down menu to choose a proper one.
All: This setting means that all the IP addressed in the network are allowed or denied to pass through in Internet. If you choose **Single**, an IP addr field will appear to the right side. You have to type in the specific IP address as the start/end point to let the router identify for granting or denying pass through. If you choose **Subnet**, the IP address and Netmask will appear to the right side. Please type in the specific IP address and netmask as the start/end point to let the router identify for granting or denying pass through.

Port Range:
The port range is from 0 to 65535. Please type in the start point and end point for the IP Filtering.

After finish the settings, click **Apply**. A new one will be added and shown on the web page.

Add New Outbound IP Filtering Rule

Allow Traffic ☒ Yes ☐ No

Protocol: TCP

Source IP address: ALL

Destination IP address: ALL

Port Range: Start End

Apply

Protocol:

TCP

TCP

UDP

ICMP

AH

ESP

GRE

ALL

User Defined

Add New Outbound IP Filtering Rule

Allow Traffic ☒ Yes ☐ No

Protocol: User Defined as

Source IP address:

ALL

ALL

SINGLE

SUBNET

Add New Outbound IP Filtering Rule

Allow Traffic ☒ Yes ☐ No

Protocol: TCP

Source IP address: SUBNET IP addr: Netmask:

Destination IP address: ALL

Port Range: Start End

Apply

A new IP filtering setting for Outbound traffic is created in the web page. To edit the setting, please click the pencil mark to get into the editing page. To delete the setting, click the trash mark to erase it. To set another IP filtering, click **Add** again.

IP Filtering
This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts.

IP Filtering: ☐ Disabled ☒ Enabled Apply

Select the direction to filter packets: ☒ Outbound traffic ☐ Inbound traffic

Protocol	Source IP addr	Dest IP addr	Port Range		Allow	Edit
			Start	End		
UDP	ALL	ALL	0	65535	<input checked="" type="checkbox"/>	

Add

For adding a new Inbound IP Filtering, click **Inbound traffic** in the item of **Select the direction to filter packets**. Use the same way to add a new one as stated above.

Add New Inbound IP Filtering Rule

Allow Traffic ☒ Yes ☐ No

Protocol:

TCP

Source IP address:

ALL

Destination IP address:

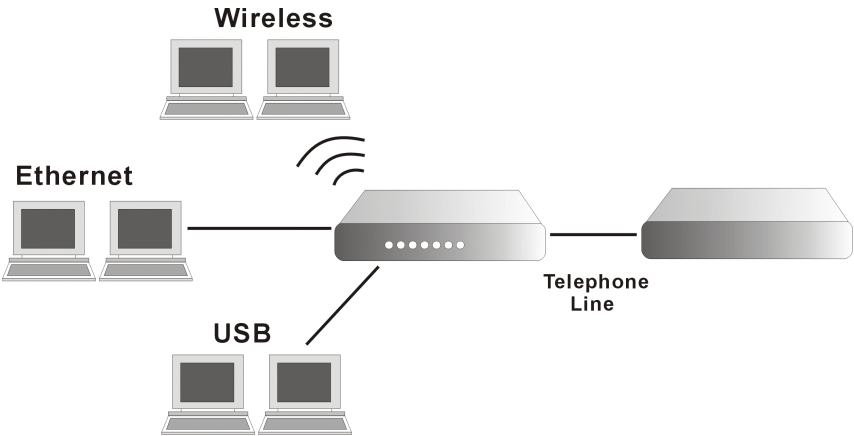
ALL

Port Range: Start End

Apply

IGMP Proxy

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.



The hosts interact with the system through the exchange of IGMP messages. When you want to configure IGMP proxy, the system will interact with other router through the exchange of IGMP messages. However, when acting as the proxy, the system performs the host portion of the IGMP task as follows:

- When it is queried, the system will send group membership reports to the group.
- When one of the hosts joins a multicast address group to which none of other hosts belong, the system will send unsolicited group membership reports to that group.
- When the last of hosts in a particular multicast group leaves the group, the system will send a leave group membership report to the routers group.

Internet Connection:
This field displays the internet connection that you currently use.

IGMP Proxy Enabled:
Check this box to enable this function or uncheck this box to disable this function.

After finish the settings, click **Apply**.

IGMP Proxy Configuration

Enabling IGMP proxy function can allow the users on your local network to play the multimedia (video or audio) which sent from the servers on the Internet.

Internet Connection	IGMP Proxy Enabled
ppoe_8_35	<input checked="checked" type="checkbox"/>

Apply

Wireless

The Wireless setting must match the other Wireless stations.

Basic

To set the basic configuration for the wireless features, please open Basic item from the Wireless menu.

Enable Wireless Network:

Click this check box to enable the wireless network function.

Hide Access Point:

Checking this box can hide the SSID of this access point. Then other people in the network cannot find the SSID of this device.

Wireless Network Name (SSID):

The system will detect the SSID of your router and displayed in this field for your reference.

The SSID is the identification characters of a router. The default words will be shown on this page. If you do not check the Hide Access Point item, the router will periodically broadcasts its SSID to allow the wireless clients within the range to recognize its presence. This can create a security hole since any wireless clients which got the broadcast might associate to your system.

Please be noted that if you want to communicate, all wireless clients should use the same SSID with the router or access point.

Channel:

The frequency in which the radio links are about to be established. Select one channel that you want from the drop down list.

As an administrator of network, he/she must search which channels are available and then assign one available channel as the communication channel. All the other clients that want to transmission through this device should choose the same channel that you set in this field.

Transmission Mode:

It decides the mode of data transmission. Choose the one that you want to use from the drop-down menu. There are **802.11b only**, **802.11g only** and **Mixed Mode** provided here.

Transmission Rate:

It decides the speed of data transmission. Choose any one of it by using the drop-down menu. This setting will change by the

Wireless Basic Settings

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and select the working channel. Click "Apply" to configure the wireless basic options.

☒ Enable Wireless Network:

☐ Hide Access Point:

Wireless Network Name (SSID): RTA770W-52289E

Channel: 6

Transmission Mode: mixed mode

Transmission Rate: Auto

Apply

Wireless Network Name (SSID): RTA770W-52289E

Channel: 6

Transmission Mode: 802.11b only

Transmission Rate: mixed mode
802.11b only
802.11g only

Apply

Transmission Mode: 802.11b only

Transmission Rate: Auto

Apply

Transmission Mode: 802.11g only

Transmission Rate: Auto

Apply

transmission mode that you set above. If you choose **802.11b only** as the transmission mode, the transmission rate settings include 1, 2, 5.5, 11Mbit/s and auto. If you choose **802.11g**, the transmission rate settings include 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbit/s and auto. If you choose mixed mode, only Auto is available.

Click **Apply** to invoke the settings.

Transmission Mode:

mixed mode ▼

Transmission Rate:

Auto ▼

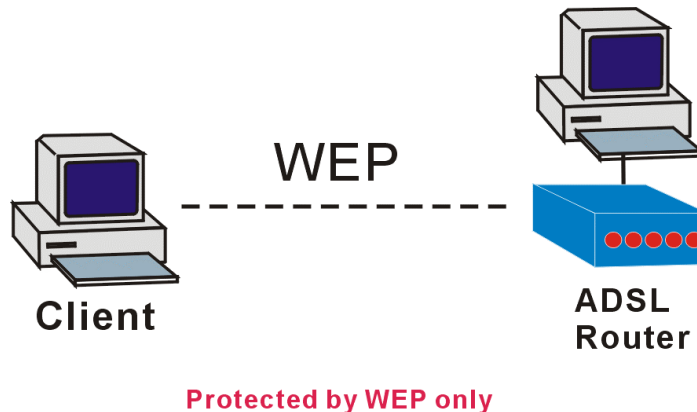
Auto

Apply

Security

To configure security features for the Wireless interface, please open Security item from Wireless menu. This web page offers four authentication protocols for you to secure your data while connecting to networks. There are four selections including None WPA, 802.1X, WPA, and WPA-PSK. Different item leads different web page settings. Please read the following information carefully.

For None WPA



WiFi-Protected Access: The **None** item offers you the less protection for wireless communication.

Authentication Type:

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

Open System means that it allows any client to authenticate and attempt to communicate with a bridge. The client can only communicate if its WEP keys match the router's WEP keys.

Shared Key means that a bridge or router will send an unencrypted text string to any client attempting to communicate with the router. The client requesting authentication encrypts the text and sends back to the router. Both unencrypted and encrypted can be monitored, yet it leaves the bridge open to attack from any intruder if he calculates the WEP key by comparing the text strings. That is why shared key authentication can be less secure than open authentication.

Data encryption (WEP):

Select the WEP mode for the WEP key function. You can choose **64-bit** or **128-bit** for your necessity. If you choose **Off**, the Encryption Keys will not be shown on this page. If selected, data is encrypted using the key before being transmitted. For example, if

Wireless Security

This page allows you to configure security features of the wireless LAN interface. You can specify whether an encryption key is required to authenticate this wireless network, enable data encryption(WEP) with the encryption strength(64-bit or 128-bit). Click "Apply" to configure the wireless security options.

Wi-Fi Protected Access:

Authentication Type:

Data encryption (WEP):

For Open System (or Shared Key), 64-bit

Wi-Fi Protected Access:

Authentication Type:

Data encryption (WEP):

Encryption Keys

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

Format: ☐ Hexadecimal digits (0-9,A-F, and a-f are valid)
☒ ASCII characters (any printable characters are valid)

Key1:

Key2:

Key3:

Key4:

Default Transmission Key:

you set 128-bit in this field, then the receiving station must be set to use 128 Bit Encryption, and have the same Key value too. Otherwise, it will not be able to decrypt the data.

Format:

Choose the typing method of encryption key. You have to click either **Hexadecimal digits** or **ASCII characters** and type the keys on the fields of Key 1 to Key 4.

Key 1 to 4:

Type the encryption key length and fill out WEP keys. The system allows you to type in 4 kinds of the WEP key. For **64-bit WEP** mode, the number you can type is that 5 characters or 10 hexadecimal digits. As for **128-bit WEP** mode, the number you can type is that 13 characters or 26 hexadecimal digits.

Default Transmission Key:

Select one of network key that you set on the Key boxes as the default one.

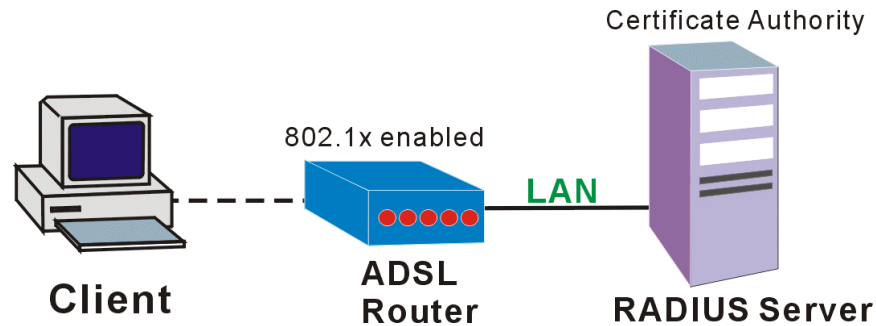
After finished settings, click **Apply** for activation.

For Open System (or Shared Key), 128-bitWi-Fi Protected Access: Authentication Type: Data encryption (WEP): **Encryption Keys**

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.

Format: ☐ Hexadecimal digits (0-9,A-F,and a-f are valid)☒ ASCII characters (any printable characters are valid)Key1: Key2: Key3: Key4: Default Transmission Key:

For 802.1X Wireless Network



When a wireless client requests access to a network, it is required to be authenticated by a central authentication server (RADIUS Server). Only an authenticated user can be granted by the network access and thereby unauthorized is blocked.

WiFi-Protected Access: Choose 802.1x as the authentication protocol, your data transmission between the router and the clients will be protected with the settings that you set in this web page.

RADIUS Server IP Address: RADIUS Server 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. Please type in the IP Address for the RADIUS Server.

RADIUS UDP Port: Except for the IP address of the RADIUS Server, you have to enter the port number for the server. Port 1812 is the reserved RADIUS-authentication port described in RFC 2138. Earlier AP (RADIUS clients) use port 1945. The default value will be shown on this box. You can keep and use it.

RADIUS Share Secret: A share secret is like a password, which is used between RADIUS Server and the specific AP (RADIUS client) to verify identity. Both RADIUS Server and the AP (RADIUS client) must use the same shared secret for successful communication to occur. Type in the words for the share secret.

Authentication Type:

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

Data encryption (WEP):

Select the WEP mode for the WEP key function. You can choose **64-bit** or **128-bit** for your necessity. If you choose **Off**, the Encryption Keys will not be shown on this page. If selected, data is encrypted using the

Wireless Security

This page allows you to configure security features of the wireless LAN interface. You can specify whether an encryption key is required to authenticate this wireless network, enable data encryption(WEP) with the encryption strength(64-bit or 128-bit). Click "Apply" to configure the wireless security options.

Wi-Fi Protected Access:

RADIUS Server IP Address:

RADIUS UDP Port:

RADIUS Share Secret:

Authentication Type:

Data encryption (WEP):

For Open System (or Shared Key), 64-bit

Wi-Fi Protected Access:

RADIUS Server IP Address:

RADIUS UDP Port:

RADIUS Share Secret:

Authentication Type:

Data encryption (WEP):

Encryption Keys

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

Format: ☐ Hexadecimal digits (0-9,A-F, and a-f are valid)

☒ ASCII characters (any printable characters are valid)

Key1:

Key2:

Key3:

Key4:

Default Transmission Key:

For Open System (or Shared Key), 128-bit

key before being transmitted. For example, if you set 128-bit in this field, then the receiving station must be set to use 128 Bit Encryption, and have the same Key value too. Otherwise, it will not be able to decrypt the data.

Format:

Choose the typing method of encryption key. You have to click either **Hexadecimal digits** or **ASCII characters** and type the keys on the fields of Key 1 to Key 4.

Key 1 to 4:

Type the encryption key length and fill out WEP keys. The system allows you to type in 4 kinds of the WEP key. For **64-bit WEP** mode, the number you can type is that 5 characters or 10 hexadecimal digits. As for **128-bit WEP** mode, the number you can type is that 13 characters or 26 hexadecimal digits.

Default Transmission Key:

Select one of network key that you set on the Key boxes as default one.

After finished settings, click **Apply** for activation.

Wi-Fi Protected Access:

RADIUS Server IP Address:

RADIUS UDP Port:

RADIUS Share Secret:

Authentication Type:

Data encryption (WEP):

Encryption Keys

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.

Format: ☐ Hexadecimal digits (0-9,A-F, and a-f are valid)
☒ ASCII characters (any printable characters are valid)

Key1:

Key2:

Key3:

Key4:

Default Transmission Key:

Example for Configuration 802.1x environment

You will need the following components for establishing an 802.1x environment in your network.

- ☐ Windows 2000 Server: RADIUS server installed using “Internet Authentication Service”. Certificate Services is installed
- ☐ AP (Router): It should be connected to Windows 2000 Advanced Server through the LAN port. The DHCP server for the router is used and 802.1x must be enabled.
- ☐ 802.1x client: A WLAN card supporting WEP is used.
- ☐ Authentication Mechanism

For WPA-PSK

WiFi-Protected Access: WPA-PSK is useful for small places such as home environment without having authentication servers. It allows the use of manually-entered keys or passwords and is designed to be easy to set up for home users.

Format:

Choose the typing method of encryption key. You have to click either **Hexadecimal digits** or **ASCII characters** and type the keys on the field of Pre-Share Key.

Pre-Share Key: Please type the key to be between 8 and 63 characters, or 64 hexadecimal digits. Only the devices with a matching key that you set here can join this network.

WPA Group Rekey Interval: Type in the time for the WAP group rekey interval. The unit is second.

Data Encryption (WPA): Select the data encryption for the WPA mode. There are three types that you can choose, TKIP, AES, TKIP+AES.

TKIP takes the original master key only as a starting point and derives its encryption keys mathematically from this master key. Then it regularly changes and rotates the encryption keys so that the same encryption key will be never used twice.

AES provides security between client workstations operating in ad hoc mode. It uses a mathematical ciphering algorithm that employs variable key sizes of 128, 192 or 256 bits.

TKIP+AES combines the features and functions of TKIP and AES.

After finished settings, click **Apply** for activation.

Wireless Security

This page allows you to configure security features of the wireless LAN interface. You can specify whether an encryption key is required to authenticate this wireless network, enable data encryption(WEP) with the encryption strength(64-bit or 128-bit). Click "Apply" to configure the wireless security options.

Wi-Fi Protected Access:

WPA Pre-Shared Key

Enter the key to be between 8 and 63 ASCII characters, or 64 hexadecimal digits

Format: ☐ Hexadecimal digits (0-9,A-F, and a-f are valid)
☒ ASCII characters (any printable characters are valid)

Pre-Share Key:

WPA Group Rekey Interval: seconds

Data Encryption (WPA):
 TKIP
 AES
 TKIP+AES

For WPA (Wi-Fi Protected Access)

WiFi-Protected Access: The WPA is suitable for enterprises. It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It can provides stronger encryption and authentication solution than others WPA mode.

WPA Group Rekey Interval: Type in the time for the WAP group rekey interval. The unit is second.

RADIUS Server IP Address: RADIUS Server 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. Please type in the IP Address for the RADIUS Server.

RADIUS UDP Port: Except for the IP address of the RADIUS Server, you have to enter the port number for the server. Port 1812 is the reserved RADIUS-authentication port described in RFC 2138. Earlier RADIUS clients use port 1945. The default value will be shown on this box. You can keep and use it.

RADIUS Share Secret: A share secret is like a password, which is used between IAS and the specific RADIUS client to verify identity. Both IAS and the RADIUS client must be use the same shared secret for successful communication to occur. Type in the words for the share secret.

Data Encryption (WPA): Select the data encryption for the WPA mode. There are three types that you can choose, TKIP, AES, TKIP+AES.

TKIP takes the original master key only as a starting point and derives its encryption keys mathematically from this mater key. Then it regularly changes and rotates the encryption keys so that the same encryption key will be never used twice.

AES provides security between client workstations operating in ad hoc mode. It uses a mathematical ciphering algorithm that employs variable key sizes of 128, 192 or 256 bits.

TKIP+AES combines the features and functions of TKIP and AES.

After finished settings, click **Apply** for activation.

Wireless Security

This page allows you to configure security features of the wireless LAN interface. You can specify whether an encryption key is required to authenticate this wireless network, enable data encryption(WEP) with the encryption strength(64-bit or 128-bit). Click "Apply" to configure the wireless security options.

Wi-Fi Protected Access:	<input type="text" value="WPA"/>
WPA Group Rekey Interval:	<input type="text" value="0"/> seconds
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS UDP Port:	<input type="text" value="1812"/>
RADIUS Share Secret:	<input type="text"/>
Data Encryption (WPA):	<input type="text" value="TKIP+AES"/> <input type="text" value="TKIP"/> <input type="text" value="AES"/> <input type="text" value="TKIP+AES"/>
<input type="button" value="Apply"/>	

Access Control

The web page allows you to enable the wireless MAC control configuration.

Access Control:

Click **Off** to disable this function. Click **On in Allow mode** to make any wireless MAC address can be linked to. And click **On in Deny mode** to disturb any wireless MAC address to be linked to.

View Access Control List: Click this button to view the wireless access control list and to add a new access control.

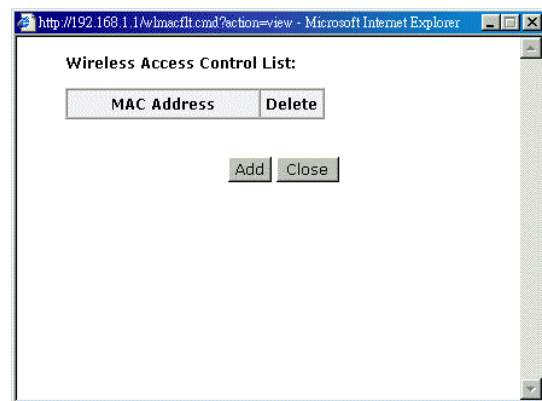
Wireless MAC Access Control

This page lets you to specify the wireless adaptors that are allowed to connect to your DSL Router. This offers additional protection against unwanted connections. Click "Apply" to configure the wireless access control mode.

- Access Control:
- ☒ Off
 - ☐ On in Allow mode (Only those wireless adaptors listed in the access control table are allowed to connect to your DSL Router, others are denied.)
 - ☐ On in Deny mode (Only those wireless adaptors listed in the access control table cannot connect to your DSL Router, others are allowed.)

[View Access Control List](#) [Apply](#)

The Wireless Access Control List dialog allows you to add a new MAC address and view current MAC address that you had added.



To add a new MAC address to your wireless MAC address filters, click on the Add button from the Wireless Access Control List dialog to show next page.

MAC Address of Wireless:

You have to type in the MAC Address that you want it to be linked to your router. And click **Apply**.



The result of adding a new MAC address will be shown the example as the right picture.

If you want to delete the added MAC address, simple click the delete button (like a trash can), a dialog box will be shown to ask you. Click Yes, then the new one will be erased.



Diagnostics

To check the link status for the network and your computer, a diagnostic test can guide you to detect the network problem. The testing items are listed and accomplished one by one. If the previous one is failed, than the items below that failed one will be failed too. Use this diagnostic test to detect the connectivity mistakes whenever you happen to the linked problem.

For the item which pass through the diagnostics, a PASS word will be shown on the right side of that item.

If not, a Fail word will be there.

N/A means that item is not necessary for the system to test.

Diagnostic Tests

This DSL Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic tests" again to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Select the Internet Connection: pppoe_8_35 Run Diagnostic Tests

Test the connection to your local network

Test your Ethernet Connection: PASS Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	N/A	Help
Test ATM OAM F5 end-to-end ping:	N/A	Help
Test ATM OAM F4 segment ping:	N/A	Help
Test ATM OAM F4 end-to-end ping:	N/A	Help

Test the connection to your Internet service provider

Test PPP server connection:	N/A	Help
Test authentication with ISP:	N/A	Help
Test the assigned IP address:	N/A	Help
Ping default gateway:	N/A	Help
Ping primary Domain Name Server:	N/A	Help

The Help link lets you know what the result (Pass, Down, Fail) represents for. In this page you still can rerun diagnostic test at any time.

ADSL Synchronization Test

Pass:	Indicates that the DSL router has detected a DSL signal from the telephone company. A solid DSL LED on the router also indicates the detection of a DSL signal from the telephone company.
Fail:	Indicates that the DSL router does not detect a signal from the telephone company's DSL network. The DSL LED will continue to flash green.

If the test fails, follow the troubleshooting procedures listed below and rerun the diagnostics tests by clicking "Rerun Diagnostic Tests" at the bottom of this page. If all the tests pass, close and restart your Web browser to access the Internet.

Troubleshooting:

1. Make sure your phone line is plugged into the router.
2. After turning on your DSL router, wait for at least one minute to establish a connection. Run the diagnostic tests again by clicking "Rerun Diagnostic Tests" at the bottom of this page.
3. Make sure there is no DSL micro filter on the phone cord connecting the DSL router to the wall jack.
4. Make sure you are using the phone cord that was supplied with your DSL router or another similar phone cord with four copper wires visible in the plug.
5. If your DSL has been functioning properly for a long period of time and you suddenly are experiencing this problem, there may be a problem with the DSL network. You may need to wait from 30 minutes to a couple of hours, and if you still do not have a solid DSL LED on your router, call Technical Support.
6. Turn off the power to the DSL router, wait 10 seconds and turn it back on. Wait at least one minute and if the DSL LED on the router remains a solid color, close your Web browser and restart it.

Rerun Diagnostic Tests

Contact ISP Technical Support if you have tried all of the above and still are experiencing a fail condition.

Management

Admin Account

This page allows you to type in the password for accessing into your DSL Router.

For the **Admin Account**, the default setting for user password is **admin**. If you want to change the username and the password, please retype the new password in the Confirm field for confirmation. Then click **Apply**.

Admin Account

Admin account has unrestricted access to change and view configuration of your DSL Router.

User Name:

New Password:

Confirm New Password:

Remote Access

There are four interfaces for the remote access. Please choose one of them if you want to enable the remote access control.

Select the Internet Connect:

Select one connection item from the drop down list to enable the function.

Web Browser:

Choose this box if you want to have remote control through HTTP. The default port number will be shown in the box. Modify this number whenever you want.

Telnet:

Choose this box if you want to have remote control through telnet.

SNMP:

Choose this box if you want to have remote control through SNMP agent.

Ping:

Choose this box if you want to have remote control through ping command under DOS prompt.

Remote Access Control

Enable remote access to let an expert, e.g. helpdesk, configure your DSL Router remotely.

Select the Internet Connection:

To allow remote access to your router via

☐ Web Browser

Web server port on WAN interface:

☐ Telnet

☐ SNMP

☐ Ping

Date and Time

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

Update:

Click this button to refresh the current time.

Set Time by:

The default setting is Manual. If you select Time Server, you don't need to type in the time setting manually. The system will set automatically.

Time:

Set the start time by typing the year, the month, the day, the hour, and the date to help the router perform tasks.

Timezone:

Choose the time zone of your country where you are going to use the router.

Apply:

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

Date & Time

To synchronize your router among other network devices you can set up its time manually or by a time server.

Current time: 1970/01/01, 01:29

Set Time by: ☐ Time Server ☒ Manual

Year Month Day

Time: Hour Minute

Timezone:

Date & Time

To synchronize your router among other network devices you can set up its time manually or by a time server.

Current time: 1970/01/01, 01:29

Set Time by: ☒ Time Server ☐ Manual

Time Server:

Timezone:

System Log

As shown in the web page, you can view the system log and configure system log whenever you want.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

Configure System Log

After you click **Configure System Log**, the following screen will appear. You can enable or disable the log function, choose log level, display level and proper mode as you like. Then click **Apply**.

System Log Configuration

This dialog allows you to configure System Log settings. All events greater than or equal to the selected level will be logged or displayed. If the selected mode is "Remote" or "Both" events will be sent to the specified UDP port of the specified log server.

Select the desired values and click "Apply" to configure the system log options.

Log: ☒ Disabled ☐ Enabled

Log Level:

Display Level:

Mode:

There are 8 types for log level and display level for your choose. The default is **Debugging**.

Log Level: Informational

Display Level:

Mode:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational**
- Debugging

Apply

The mode selection includes **Local**, **Remote** and **Both**. The default one is Local. If you choose **Remote** or **Both**, all the events will be sent to the specified UDP port of the specified log server.

Log Level: Informational

Display Level: Error

Mode: Local

Local

Remote

Both

Apply

Viewing System Log

For viewing the system log, please click the **View System Log** button.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

View System Log

Configure System Log

The screen will be shown immediately for your reference.

http://192.168.1.1/logview.cfm - Microsoft Internet Explorer

System Log

Refresh Close

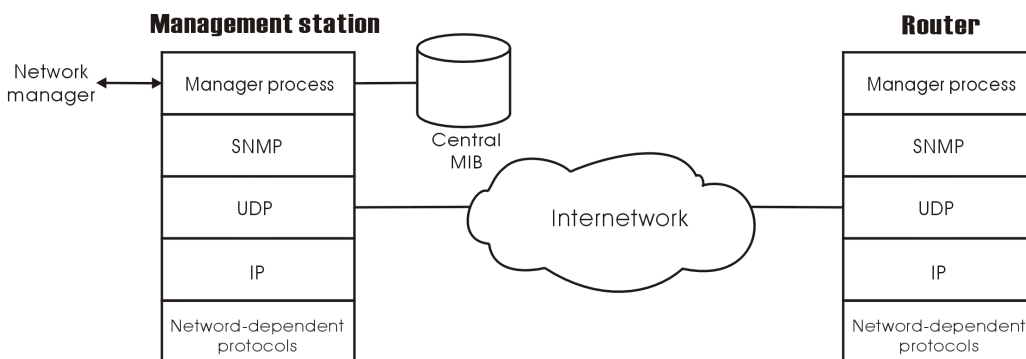
Date/Time	Facility	Severity	Message
-----------	----------	----------	---------

SNMP Setting

The SNMP, the abbreviation of Simple Network Management Protocol, is used to refer to a collection of specifications for network management that include the protocol itself, the definition of data structures and associated concepts.

A management station performs the monitoring function by retrieving the value of MIB objects. The management station and agents are linked by a network management protocol that is SNMP. The SNMP includes three key capabilities, get, set and trap. A single management station can handle many agents as long as SNMP remains relatively “simple”, so the number can be high (hundreds or so).

The **following picture** is the typical configuration of protocols for SNMP. As for a stand-alone management station, a manager process controls access to a central MIB at the management station and provides an interface to the network manager. The manager process achieves network management by using SNMP, which will be implemented on top of the UDP, IP and the relevant network-dependent protocols (e.g., Ethernet).



For an agent device that supports other applications, such as FTP, both TCP and UDP are required. An agent may issue a trap message in response to an event that effects the MIB and the underlying managed resources.

Note: There are no ongoing connections are maintained between a management station and its agents. Instead, each exchange is a separate transaction between a management station and an agent.

Each agent is responsible for notifying the management station of any **unusual event**; for example, if the agent crashes and is rebooted, a link fails or an overload condition as defined by the packet load crosses some threshold. These events are communicated in SNMP messages known as traps.

Please select the **SNMP** menu from **Management**. The dialog will appear.

SNMP Agent:

Choose Disable to close this function; choose Enabled to open this function.

Read Community:

The default setting is **public**, please type in the data that your ISP provided.

Write Community:

The default setting is **private**, please type in the data that your ISP provided.

Enable TRAP Service:

Check this box to enable this function, otherwise uncheck this box to disable this function.

TRAP Manager IP:

Type in an IP address as the remote workstation. If there is any abnormal condition happened, you can advice remote

SNMP Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent ☒ Disabled ☐ Enabled

Read Community

Write Community

☒ Enable Trap Service

Trap Manager IP

workstation by way of SNMP agent.

Backup Config

To backup your configuration for the router to your computer, you can use **Backup Config** web page to save the settings.

And when you want to restore the settings in the future, simply open Backup Config web page and use **Browse** button to located the file and click **Restore**.

Backup Configuration

Use to save your DSL Router's current settings into the computer.

Backup

Restore Configuration

Use to reset your DSL Router with settings previously saved on the computer.

Backup File: **Browse**

Restore

Update Firmware

If you have to or want to update the firmware for this router, you can open the update software web page and choose the correct file by pressing **Browse**. Then click the **Update Software** button. The system will execute the update procedure automatically. When it is finished, the system will tell you the update is successfully.

Update Firmware

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click "Browse" to locate the image file.

Step 3: Click "Update Firmware" once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Current Firmware Version: 2.12.3.15_a023g

New Firmware File Name: **Browse**

Update Firmware

Reset Router

To make effect the settings that you set for this router, please open the **Reset Router** web page and click the **Reboot** button to invoke all settings.

Reset Router

To reboot your DSL Router, just click "Reboot".

To restore your DSL Router settings to the factory defaults, please tick the checkbox below and then click "Reboot".

☐ Reset to factory default settings

Reboot

You can restore your web pages default settings. Simply check **Reset to factory default settings** and click **Reboot**.

Restore Factory Default Settings

The DSL Router configuration has been restored to factory default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

UPnP for XP

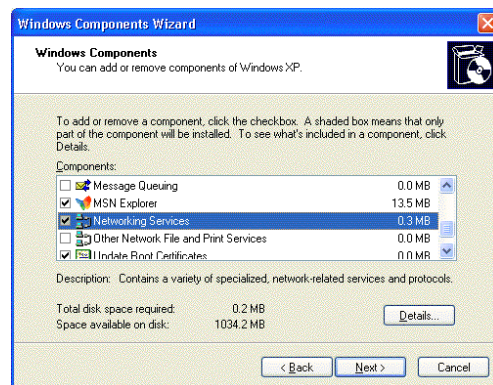
Universal plug and play (UPnP) is an architecture for pervasive peer to peer network connectivity of intelligent appliances and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business,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

Only **Windows XP** supports UPnP function.

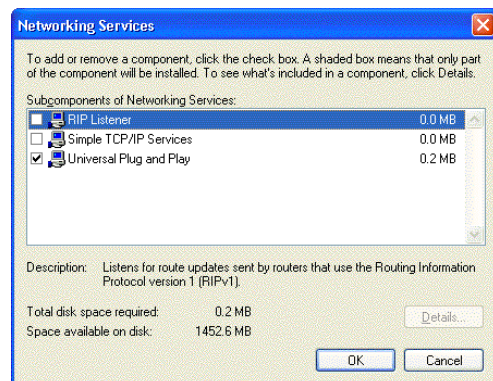
Please follow the steps below for installing UPnP components.

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

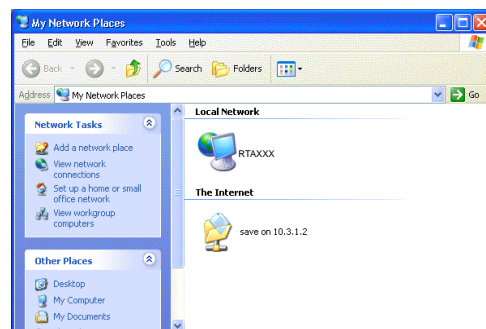
2. Select **Add or Remove Programs > Add/Remove Windows Components** to open **Windows Components Wizard** dialog box



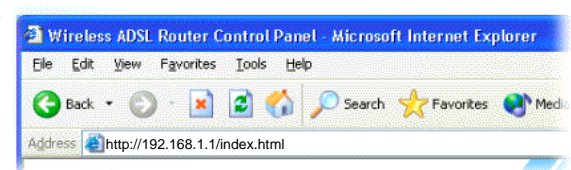
3. Select **Network Services** and click **Details**. Click the **Universal Plug and Play** check box.



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 (e.g., RTAXXX) for UPnP function.



6. Double click on the icon, the ADSL router will open another web page with port for UPnP function. The IE address will be changed as shown as the graphic.



7. Now, the NAT traversal function will be provided. The ADSL router will create a new virtual server automatically for mapping while the router detecting the computer running some Internet applications.

Chapter 5

Connection Mode

Prior to configuring the ADSL Router, you must decide whether to configure the ADSL Router as a bridge or as a router. This chapter presents some deployment examples for your reference. Each mode includes its general configure procedures. For more detailed information about web configuration, refer to "Web Configuration".

- ☐ PPP over ATM (PPPoA)
- ☐ PPPoA IP Extension
- ☐ PPP over Ethernet (PPPoE)
- ☐ PPPoE IP Extension
- ☐ MER Mode
- ☐ Numbered IP over ATM (IPoA)
- ☐ Numbered IP over ATM (IPoA)+NAT
- ☐ Unnumbered IP over ATM (IPoA)
- ☐ Unnumbered IP over ATM (IPoA)+NAT
- ☐ Bridging

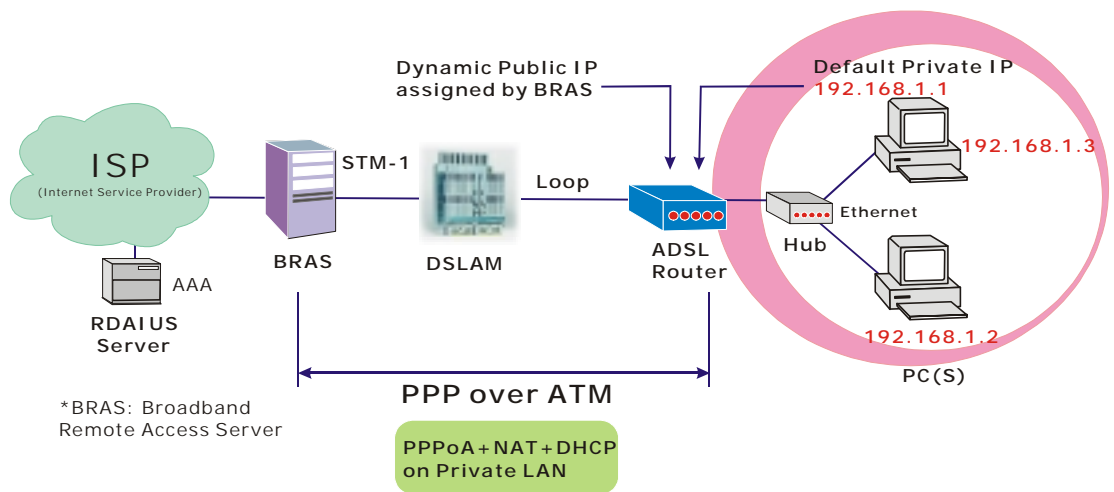
For making sure that you can connect the ADSL to your computer well and get into Internet successfully, please make sure the following first.

- ☐ Make sure you have installed a network interface card into your computer.
- ☐ Make sure the connection between the ADSL and your computer is OK.
- ☐ Check to see the TCP/IP protocol and set the IP address as "Auto Get IP Address".

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

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

PPP over ATM (PPPoA) Mode



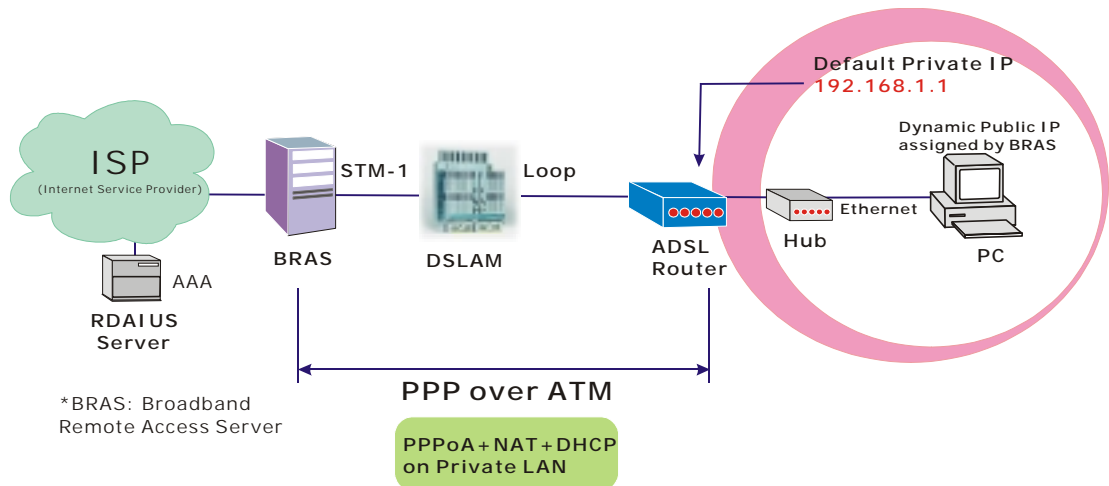
Description:

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

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button. eg:
VPI – 0
VCI – 38
3. On the **Configure Internet Connection -Connection Type** page, select the **PPP over ATM (PPPoA)** then click the **Next** button.
4. In the **PPP Username and Password** page, enter the PPP username and password that you got from your ISP.
5. Select **Dial on Demand** and type in the number for inactivity timeout. The default is 20. Or select **Always on** Then click **Next**.
6. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN. Check **Enable DHCP Server on the LAN** box. And type in the start and end points. Then type in the leased time that you want. And click **Next**. eg:
Primary IP address:192.168.1.1
Subnet Mask:255.255.255.0
Start IP Address:192.168.1.2
End IP Address: 192.168.1.254
7. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.

PPP over ATM (PPPoA) IP Extension Mode



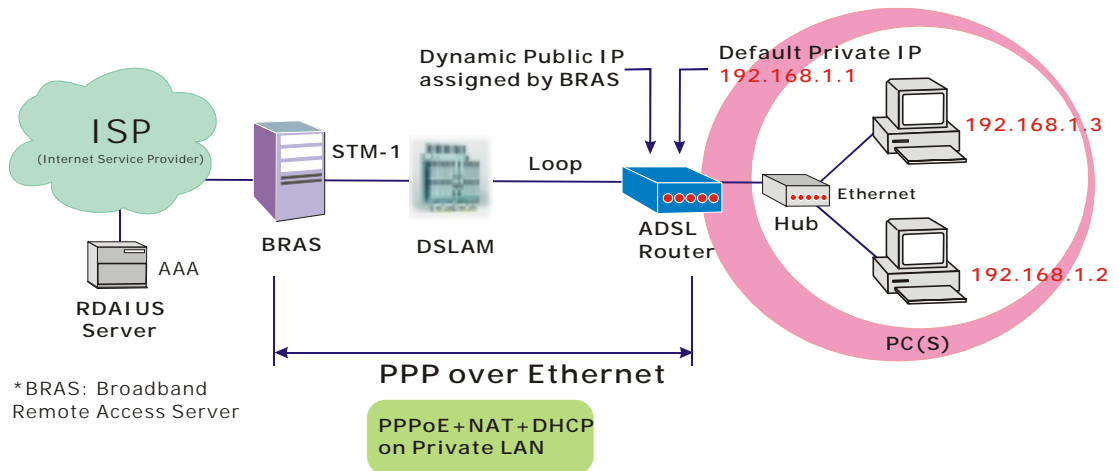
Description:

In this deployment environment, the PPPoA session is between the ADSL WAN interface and BRAS. The ADSL Router acts as a bridge and gets a public IP address from BRAS for your computer. And only the one that got the public IP address is allowed to access into Internet. Moreover, no NAT translation will be done at this case.

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button. eg:
VPI – 0
VCI – 38
3. On the **Configure Internet Connection -Connection Type** page, select the **PPP over ATM (PPPoA)** then click the **Next** button.
4. In the **PPP Username and Password** page, enter the PPP username and password that you got from your ISP.
5. Select **Dial on Demand** and type in the number for inactivity timeout. The default is 20. Or select **Always on**.
6. Check **PPP IP extension** then click **Next**.
7. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN. And click **Next**. eg:
Primary IP address:192.168.1.1
Subnet Mask:255.255.255.0
8. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.

PPP over Ethernet (PPPoE) Mode



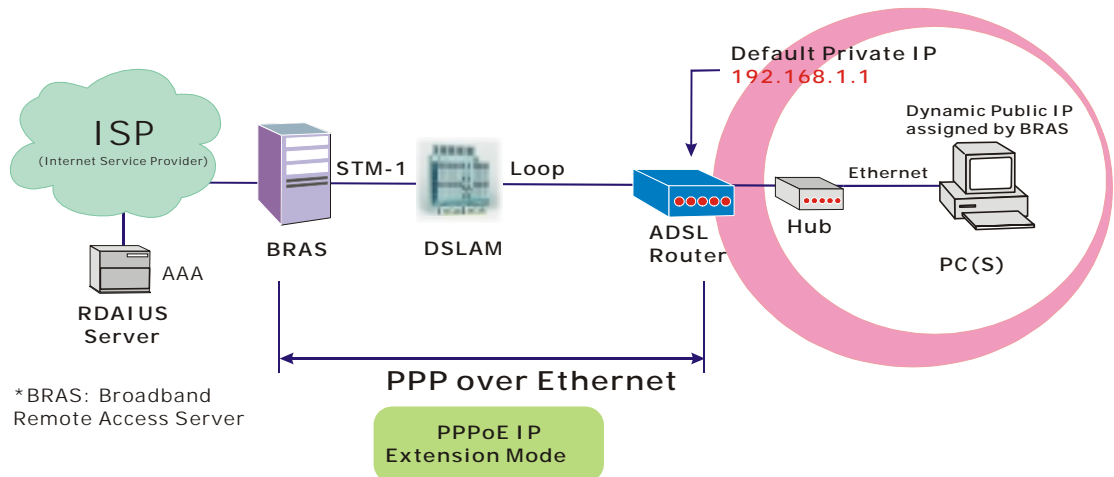
Description:

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

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button. eg:
VPI – 0
VCI – 39
3. On the **Configure Internet Connection -Connection Type** page, select the **PPP over ATM (PPPoA)** then click the **Next** button.
4. In the **PPP Username and Password** page, enter the PPP username and password that you got from your ISP.
5. Select **Dial on Demand** and type in the number for inactivity timeout. The default is 20. Or select **Always on**.
6. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN. Check **Enable DHCP Server on the LAN** box. And type in the start and end points. Then type in the leased time that you want. Finally click **Next**. eg.:
Primary IP address:192.168.1.1
Subnet Mask:255.255.255.0
Start IP Address:192.168.1.2
End IP Address: 192.168.1.254
7. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.

PPP over Ethernet (PPPoE) IP Extension Mode



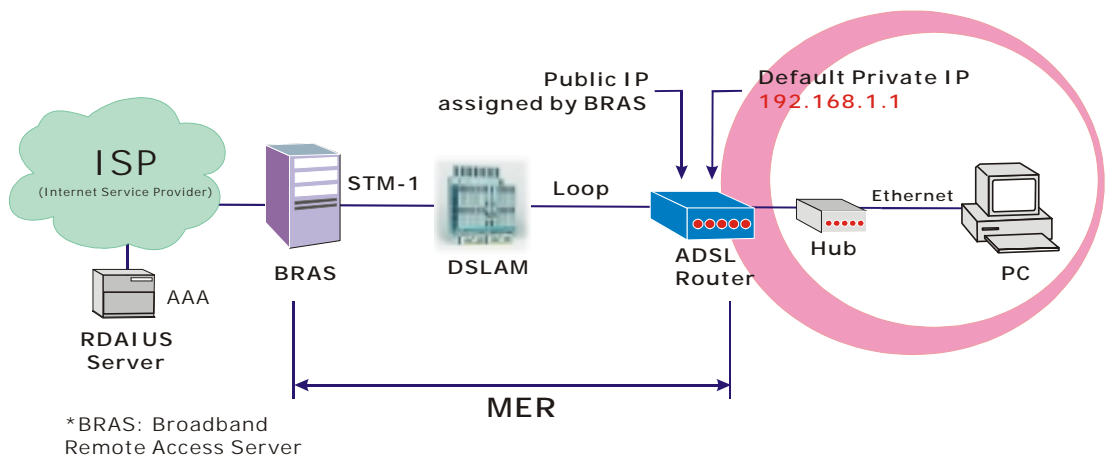
Description:

In this deployment environment, the PPPoE session is between the ADSL WAN interface and BRAS. The ADSL Router acts as a bridge and gets a public IP address from BRAS for your computer. And only the one that got the public IP address is allowed to access into Internet. The real IP that you got is acquired from ISP. Moreover, no NAT translation will be done at this case.

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button. eg:
VPI – 0
VCI – 39
3. On the **Configure Internet Connection -Connection Type** page, select the **PPP over ATM (PPPoA)** then click the **Next** button.
4. In the **PPP Username and Password** page, enter the PPP username and password that you got from your ISP.
5. Select **Dial on Demand** and type in the number for inactivity timeout. The default is 20. Or select **Always on**.
6. Check **PPP IP extension** then click **Next**.
7. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN. Finally click **Next**. eg:
Primary IP address:192.168.1.1
Subnet Mask:255.255.255.0
8. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.

MER



Description:

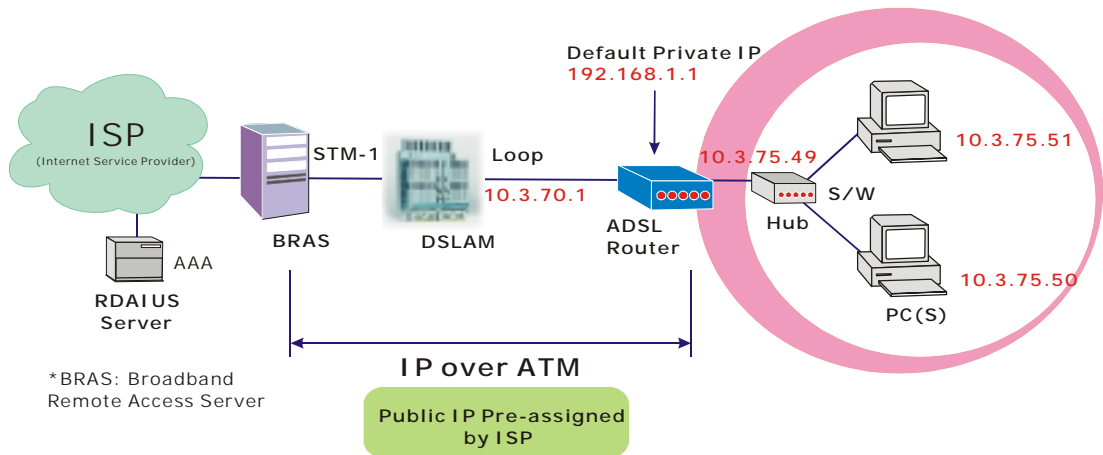
In this deployment environment, we make up a private IP network of 192.168.1.1. NAT function is enabled to support multiple clients to access Internet.

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

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button. ex:
VPI – 0
VCI – 37
3. On the **Configure Internet Connection -Connection Type** page, select the **MAC Encapsulated Routing (MER)** then click the **Next** button.
4. In the **WAN IP Settings** page, select **Use the following IP address** and type in the IP address, subnet mask and gateway that you got from ISP. Then, select **Use the following DNS Server Address**. Type in the Primary DNS server and Secondary DNS server.
WAN IP Address: 10.3.95.3
WAN Subnet Mask: 255.255.255.0
Default Gateway:10.3.95.1
Primary DNS server: 168.95.1.1
Secondary DNS server: 168.95.192.1
5. Check the **Enable NAT** if you want. Then click **Next**.
6. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN. Uncheck **Enable DHCP Server on the LAN** box. And click **Next**.
7. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.
8. Now the router is well configured. You can access into Internet.

Numbered IP over ATM (IPoA)



Description:

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

The following example uses the LAN IP address ranging from 10.3.75.49 to 10.3.75.54 and the subnet mask for LAN is 255.255.255.248. The WAN address is 10.3.70.1, and the subnet mask for WAN is 255.255.255.252.

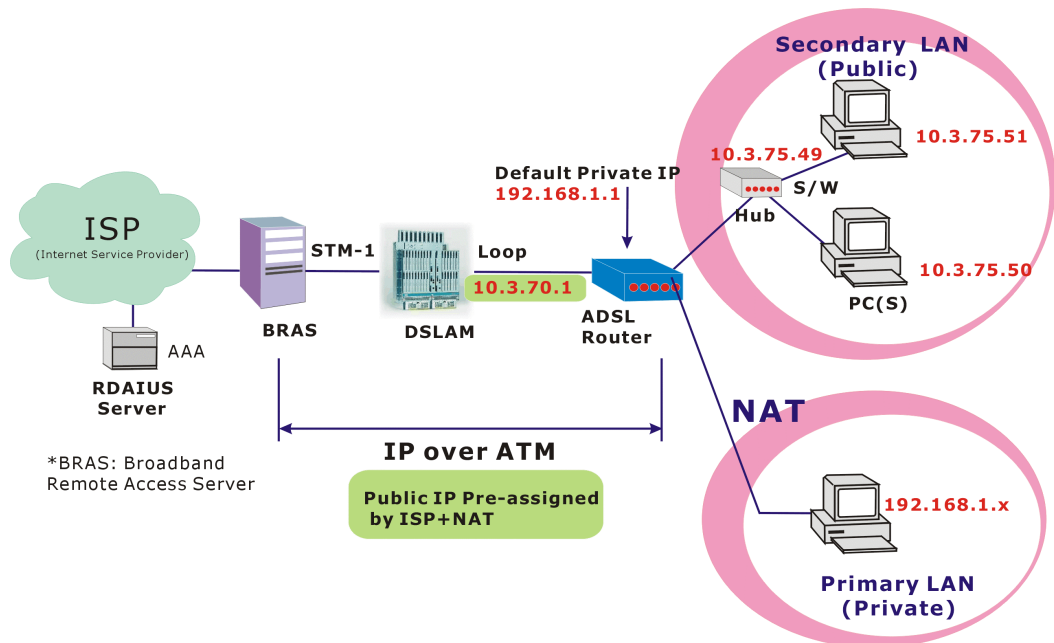
Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button.
VPI – 0
VCI – 32
3. On the **Configure Internet Connection -Connection Type** page, select the **IP over ATM (IPoA)** then click the **Next** button.
4. In the **WAN IP Settings** page, select **Use the following IP address** and type in the IP address, subnet mask and gateway that you got from ISP. Then, select **Use the following DNS Server Address**. Type in the Primary DNS server and Secondary DNS server. Click **Next** for next page.
WAN IP Address: 10.3.70.1
WAN Subnet Mask: 255.255.255.252
Primary DNS server: 168.95.1.1
Secondary DNS server: 168.95.192.1
5. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN.
Primary IP Address: 192.168.1.1
Subnet mask: 255.255.255.0
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
6. Check **Configure the second IP Address and Subnet Mask for LAN Interface** and type in the second IP address and subnet mask. Then click **Next**.
Secondary IP Address: 10.3.75.49
Subnet mask: 255.255.255.248
7. Check the network information. Make sure the settings match the settings provided by ISP.

Click **Finish**.

8. Set TCP/IP for your computer. Specify an IP Address, subnet mask and set default gateway. eg:
IP Address: 10.3.75.51
Subnet Mask: 255.255.255.248
Gateway: 10.3.75.49
9. Now the router is well configured. You can access into Internet.

Numbered IP over ATM (IPoA) + NAT



Description:

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

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

The following example uses the LAN IP address ranging from 10.3.75.49 to 10.3.75.54 and the subnet mask for LAN is 255.255.255.248. The WAN address is 10.3.70.1, and the subnet mask for WAN is 255.255.255.252.

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button.
VPI – 0
VCI – 32
3. On the **Configure Internet Connection -Connection Type** page, select the **IP over ATM (IPoA)** then click the **Next** button.
4. In the **WAN IP Settings** page, select **Use the following IP address** and type in the IP address, subnet mask and gateway that you got from ISP. Then, select **Use the following DNS Server Address**. Type in the Primary DNS server and Secondary DNS server.
WAN IP Address: 10.3.70.1
WAN Subnet Mask: 255.255.255.252
Primary DNS server: 168.95.1.1
Secondary DNS server: 168.95.192.1
5. Check the **Enable NAT** box. And click **Next**.
6. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN.

Primary IP Address: 192.168.1.1

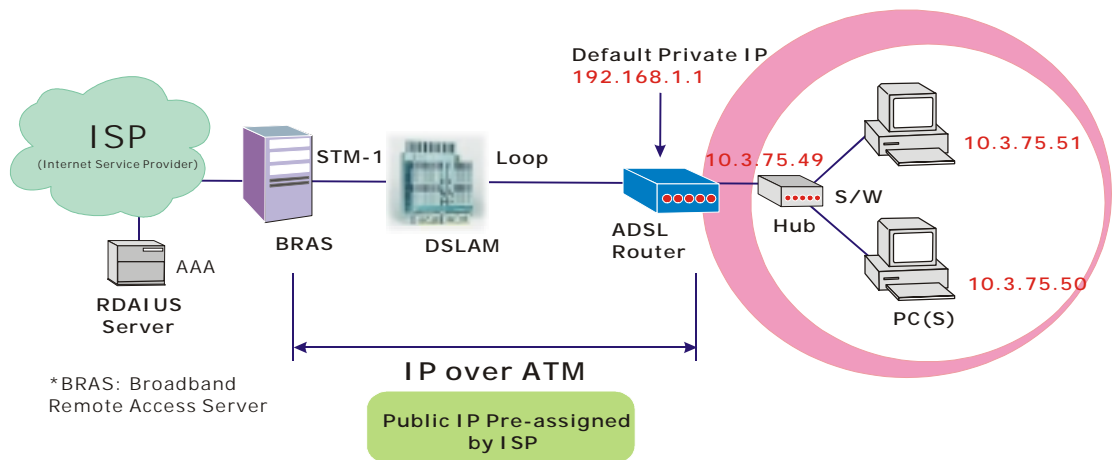
Subnet mask: 255.255.255.0

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

7. Check **Configure the second IP Address and Subnet Mask for LAN Interface** and type in the second IP address and subnet mask. Then click **Next**.
Secondary IP Address: 10.3.75.49
Subnet mask: 255.255.255.248
8. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.
9. Now the router is well configured. You can access into Internet.

Unnumbered IP over ATM (IPoA)



Description:

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

The following example uses the LAN IP address ranging from 10.3.75.49 to 10.3.75.54 and the subnet mask for LAN is 255.255.255.248. The WAN address is 10.3.70.1, and the subnet mask for WAN is 255.255.255.252.

Configuration:

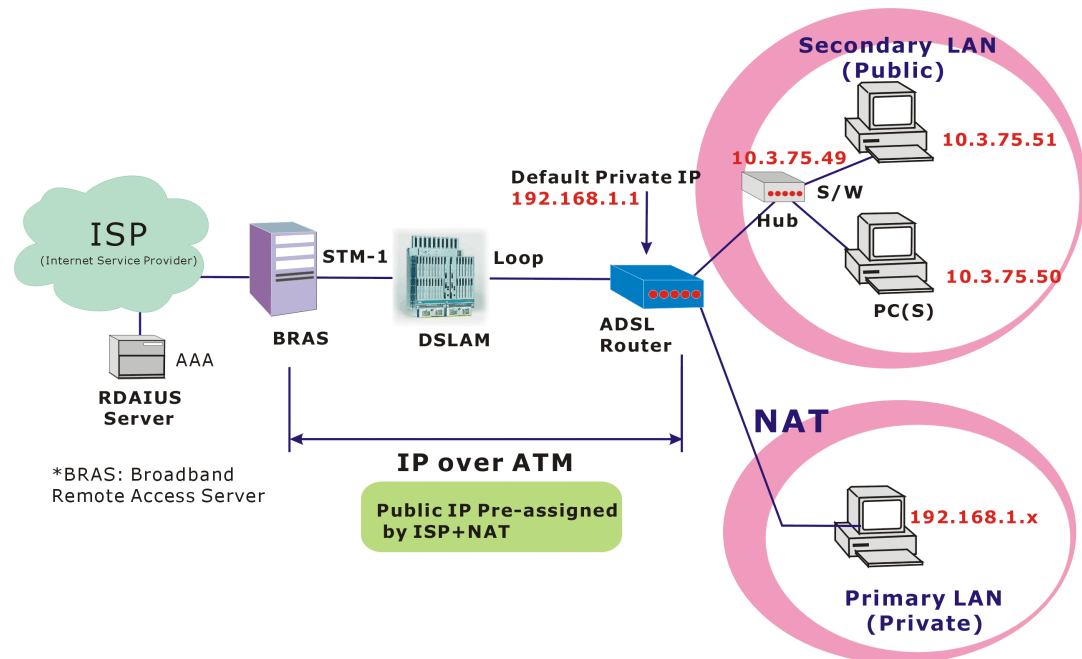
1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button.
VPI – 0
VCI – 32
3. On the **Configure Internet Connection -Connection Type** page, select the **IP over ATM (IPoA)** then click the **Next** button.
4. In the **WAN IP Settings** page, select **None** for WAN IP address settings. Then, select **Use the following DNS Server Address**. Type in the Primary DNS server and Secondary DNS server. Click **Next** for next page.
Primary DNS server: 168.95.1.1
Secondary DNS server: 168.95.192.1
5. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN.
Primary IP Address: 192.168.1.1
Subnet mask: 255.255.255.0
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
6. Check **Configure the second IP Address and Subnet Mask for LAN Interface** and type in the second IP address and subnet mask. Then click **Next**.
Secondary IP Address: 10.3.75.49
Subnet mask: 255.255.255.248
7. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.
8. Set TCP/IP for your computer. Specify an IP Address, subnet mask and set default gateway. eg:
IP Address: 10.3.75.51

Subnet Mask: 255.255.255.248

Gateway: 10.3.75.49

9. Now the router is well configured. You can access into Internet.

Unnumbered IP over ATM (IPoA) + NAT



Description:

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

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

The following example uses the LAN IP address ranging from 10.3.75.49 to 10.3.75.54 and the subnet mask for LAN is 255.255.255.248. The WAN address is 10.3.70.1, and the subnet mask for WAN is 255.255.255.252.

Configuration:

1. Start up your browser and type **192.168.1.1** as the address to enter this ADSL web-based manager.
2. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button.
VPI – 0
VCI – 32
3. On the **Configure Internet Connection -Connection Type** page, select the **IP over ATM (IPoA)** then click the **Next** button.
4. In the **WAN IP Settings** page, select **None** for WAN IP address settings. Then, select **Use the following DNS Server Address**. Type in the Primary DNS server and Secondary DNS server. Click **Next** for next page.
Primary DNS server: 168.95.1.1
Secondary DNS server: 168.95.192.1
5. Check the **Enable NAT** box. And click **Next**.
6. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN.
Primary IP Address: 192.168.1.1

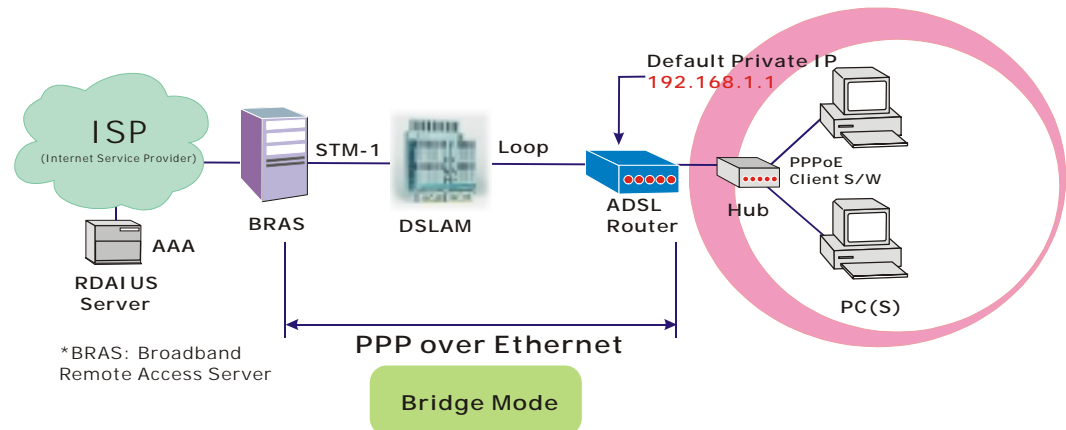
Subnet mask: 255.255.255.0

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

7. Check **Configure the second IP Address and Subnet Mask for LAN Interface** and type in the second IP address and subnet mask. Then click **Next**.
Secondary IP Address: 10.3.75.49
Subnet mask: 255.255.255.248
8. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.
9. Now the router is well configured. You can access into Internet.

Bridge Mode



Description:

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

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

Configuration:

1. Choose a client PC and set the IP as 192.168.1.x (x is between 2 and 254) and the gateway as 192.168.1.1.
2. Start up your browser and type **192.168.1.1** as the address to enter the web-based manager.
3. Go to **Quick Setup**. Type in the **VCI** and **VPI** value. Then click the **Next** button. eg:
VPI – 0
VCI – 32
4. On the **Configure Internet Connection -Connection Type** page, select the **Bridging** then click the **Next** button.
5. In the **Configure LAN side Settings** page, type in the IP address and subnet mask for your LAN. Finally click **Next**. eg:
Primary IP address:192.168.1.1
Subnet Mask:255.255.255.0
6. Check the network information. Make sure the settings match the settings provided by ISP. Click **Finish**.
7. Set TCP/IP for your computer. Specify an IP Address, subnet mask and set default gateway. eg:
IP Address: 10.3.86.81
Subnet Mask: 255.255.255.248
Gateway: 10.3.86.1
8. Click **OK**. Now the router is well configured. You can access into Internet.

Chapter 6

Troubleshooting

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

Problems with LAN

PCs on the LAN cannot get IP addresses from the ADSL 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 ADSL Router.

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

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

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

Problems with WAN

You cannot access the Internet.

- Check the physical connection between the ADSL Router and the LAN.

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

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

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

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

If you get a failed ping with the response of:

```
Request time out
```

Then the connection is fail. Check the cable between the ADSL Router and the network.

- Check the DNS setting of the ADSL Router.

At the DOS prompt, ping the IP address of the DNS provided by your ISP. For example, if your

DNS IP is 168.95.1.1, then ping 168.95.1.1. If the following response occurs:

`Relay from 168.95.1.1 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 ADSL Router.

Problems with Upgrading

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

- **Error:** All the ADSL LEDs light up and cannot light off as usual.

Possible cause: When users execute firmware upgrade and save settings to the router, the power for the router is lost for some unknown reasons, the normal web page for the router might be damaged. After power on your router, the LEDs might not work normally.

Boot Loader, Version 1.0.37-5.5.05

This device is currently running on the boot loader.

Update Firmware

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click "Browse" to locate the image file.

Step 3: Click "Update Firmware" once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

New Firmware File Name:

Action: Use the browser to connect to the router for executing image upgrade.

- **Error Message:** Image uploading failed. The selected file contains an illegal image.

Possible cause: The firmware file format is invalid.

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

- **Error Message:** Image uploading failed. The system is out of memory.

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

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

- **Error Message:** Image uploading failed. No image file was selected.

Possible cause: You did not select a file correctly.

Action: Download a compatible firmware from the web.

Chapter 7

Glossary

ARP (Address Resolution Protocol)

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

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

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

DHCP (Dynamic Host Configuration Protocol)

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

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

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

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

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

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

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

NAT (Network Address Translation) IP Address

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

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

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

Private IP Address

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

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

Public IP Address

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

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

PVC (Permanent Virtual Circuit)

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

RIP (Routing Information Protocol)

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

UDP (User Datagram Protocol)

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

Virtual Server

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

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

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

Appendix A

Specifications

Software

ADSL Compliance	For Annex A
	<ul style="list-style-type: none"> ● ANSI T1.413 Issue 2 ● ITU G.992.1 Annex A (G.dmt) ● ITU G.992.2 Annex A (G.lite) ● ITU G.994.1 (G.hs) ● Support dying gasp
	For Annex B
	<ul style="list-style-type: none"> ● ITU G.992.1 Annex B (G.dmt) ● ITU G.994.1 (G.hs)
ATM Features	<ul style="list-style-type: none"> ● Compliant to ATM Forum UNI 3.1 / 4.0 Permanent Virtual Circuits (PVCs) ● Support UBR and CBR with traffic shaping ● RFC2684 LLC Encapsulation and VC Multiplexing over AAL5 ● RFC2364 Point-to-Point Protocol (PPP) over AAL5 ● RFC2225 Classical IP and ARP over ATM ● RFC2516 PPP over Ethernet: support Relay (Transparent Forwarding and Client functions) ● Support PPPoA or PPPoE Bridged mode (the IP address got from ISP can be passed to the user's PC and behave as the IP address of the user's PC.) ● OAM F4/F5 End-to-End/Segment Loopback Cells
Bridging Features	<ul style="list-style-type: none"> ● Supports self-learning bridge specified in IEEE 802.1D Transparent Bridging ● Supports up to 4096 learning MAC addresses ● Transparent Bridging between 10/100 Mb Ethernet and USB
Routing Features	<ul style="list-style-type: none"> ● NAT (Network Address Translation) / PAT (Port Address Translation) let multiple users on the LAN to access the Internet for the cost of only one IP address. ● ALGs (Application Level Gateways): such as NetMeeting, MSN Messenger, FTP, Quick Time, mIRC, Real Player, CuSeeMe, VPN pass-through, etc.

	<ul style="list-style-type: none"> ● Port Mapping: the users can setup multiple virtual servers (e.g., Web, FTP, Mail servers) on user's local network. ● Support DMZ ● UPnP IGD (Internet Gateway Device) with NAT traversal capability ● Static routes, RFC1058 RIPv1, RFC1723 RIPv2. ● DNS Relay ● ARP Proxy
Security Features	<ul style="list-style-type: none"> ● PAP (RFC1334), CHAP (RFC1994) for PPP session ● Firewall support IP packets filtering based on IP address/Port number/Protocol type ● Support DoS (Deny of Services) which detect & protect a number of attacks (such as SYN/FIN/RST Flood, Smurf, WinNuke, Echo Scan, Xmas Tree Scan, etc) ● WEP (Wired Equivalent Privacy) encryption uses RC4 with 64/128 bit key length (for wireless ADSL router only) ● Support WPA, WPA-PSK, WPA-802.1X
Wireless Features	<ul style="list-style-type: none"> ● IEEE 802.11g and IEEE 802.11b ● Data Rate: 54, 48, 36, 24, 18, 12, 9, 6 Mbps for 802.11g/11, 5.5, 2, 1 Mbps for 802.11b ● Modulation Technique: OFDM for 802.11g; CCK (11 Mbps, 5.5 Mbps) for 802.11b; DQPSK (2Mbps) for 802.11b; DBPSK (1 Mbps) for 802.11b ● Network Architecture: infrastructure ● Operating Frequency: 2.4 ~ 2.497 GHz ● Operating Channels: depending on local regulations. For example, 11Channels (Northern America), 13 Channels (Europe), and 14 Channels (Japan) ● RF Output Power: 15dBm maximum ● Antenna Connectors: Hardware diversity support. One external antenna and one internal antenna are provided. ● Coverage Area: 802.11g: LOS (Outdoors): Max. 50 meters; Indoors: Max. 20 meters 802.11b: LOS (Outdoors): Max. 180 meters; Indoors: Max. 60 meters ● Power Consumption: TX peak: 550 mA @ 3.3 VDC; RX peak: 350 mA @ 3.3 VDC Idle: 225 mA @ 3.3 VDC; Radio disabled: < 10 mA @ 3.3 VDC ● Support WEP (Wired Equivalent Privacy) mechanism which uses RC4 with 64-bit or 128-bit key length. ● Support WPA, WPA-PSK, WPA-802.1X ● Support the Access Control function: only registered

	<p>WLAN clients can be allowed to associate to the router.</p> <ul style="list-style-type: none"> ● SSID can be hidden for the security issue (Don't broadcast SSID).
Configuration and Management	<ul style="list-style-type: none"> ● Configuration and Management ● User-friendly embedded web configuration interface with password protection ● Remote management accesses control ● Telnet session for local or remote management ● HTTP firmware upgrades via web browser GUI directly ● Distribute IP addresses to end users via DHCP server provided by ADSL router ● SNMPv1/v2 agent with MIB-II, ADSL Line MIB

Hardware

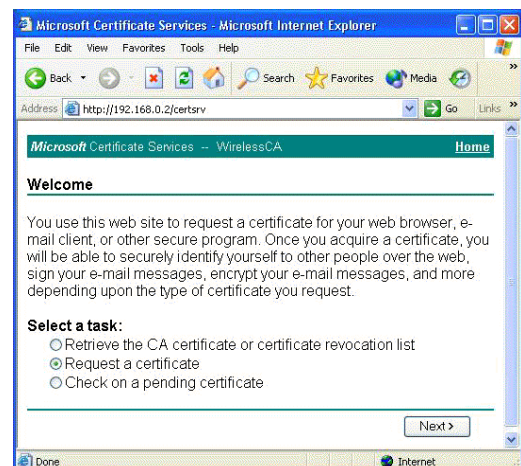
Interface	<ul style="list-style-type: none"> ● One RJ-11 port for ADSL connection ● One RJ-45 port for IEEE 802.3/802.3u 10/100 Base-T auto-sensing Ethernet connection ● One USB port compliant to USB v1.1 for 12 Mbps connection rate ● One hidden reset button for restoring to factory default settings
Regulatory Approvals and Compliance	<p>EMI: FCC part 15 Class B</p> <p>Immunity: FCC part 68 Class B</p> <p>Safety: UL, CE</p>
Power Requirement and Operation Environment Requirement	<p>Power Adaptor: Input 110±10 or 230±10 VAC; Output 16 VDC, 1A</p> <p>Power Consumption: less than 10 Walt</p> <p>Ambient Temperature: 0 to 45°C (32 to 113°F)</p> <p>Relative Humidity: 20% to 90% (non-condensing)</p>
Physical	<p>Dimensions: 215mm(L) x 160mm(W) x 40mm(H)</p> <p>Weight: 407g</p>

Appendix B

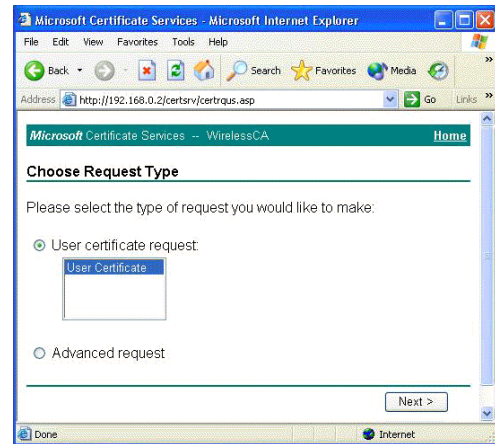
Server Setup for 802.1x Client

Getting Client Certificate

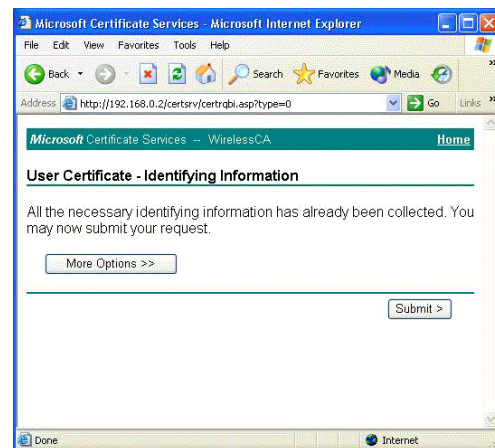
1. Please connect the client to a network that doesn't require port authentication.
2. Open up Microsoft Explorer in Windows XP, and go to `http://<yourserver>/certsrv`.
3. Authenticate to the server using your account that you created at the end of the server setup. (e.g. 123) and click OK. A dialog box might appear for you to choose.
4. Make sure that **Request a certificate** is selected, and click **Next**.



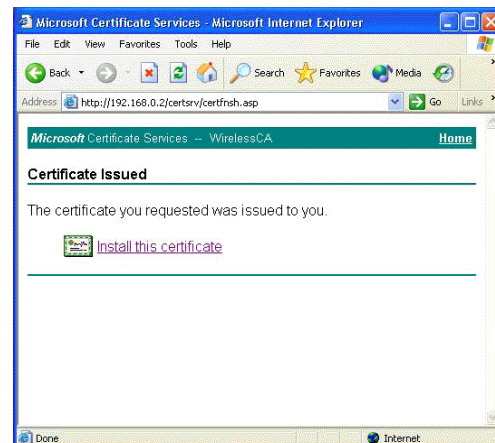
5. Make sure that **User certificate request: User Certificate** is selected, and click **Next**.



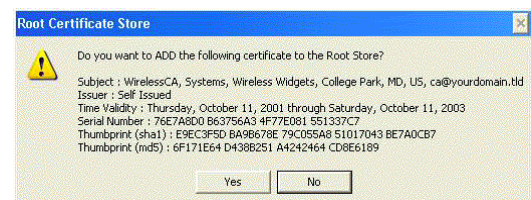
6. Click **Submit** in this dialog.



7. Now, you'll see status messages on the screen, then your certificate will be returned to you. Click **Install this certificate**.



8. You'll receive a confirmation message about accepting the certificate, click **Yes**

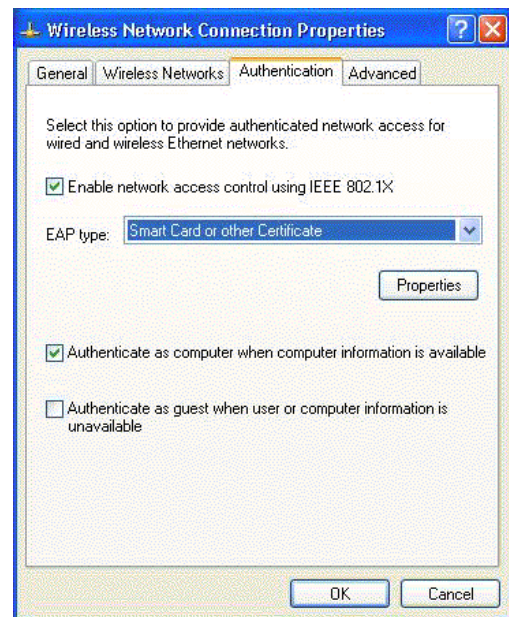


Enable 802.1x authentication and Encryption for wireless card

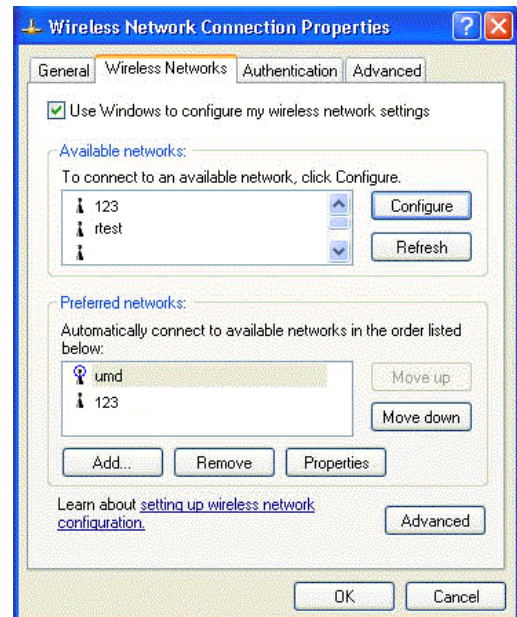
1. Open up the properties for your wireless connection, either by

Right-click on **My Network Places** on the desktop, select **Properties**, *or* Open up the **Control Panel**, select **Network Connections** (located under **Network and Internet Connections** if in Category View)

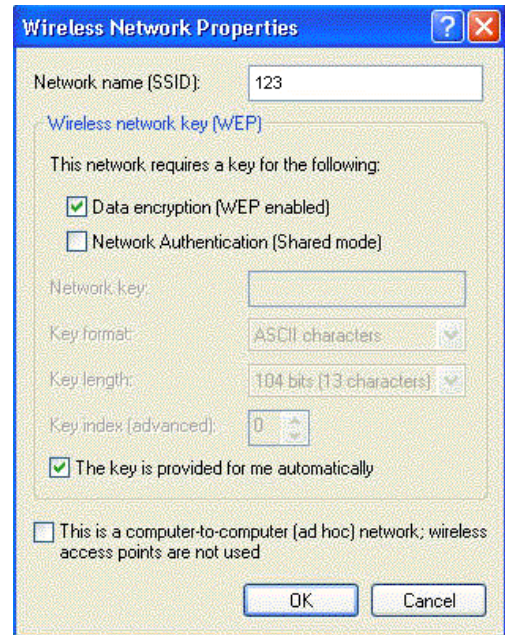
2. Right Click on the **Wireless Network Connection**, and select **Properties**.
3. Select the **Authentication Tab**, and ensure that **Enable network access control using IEEE 802.1X** is selected, and **Smart Card or other Certificate** is selected from the EAP type.



4. Click on the Wireless Networks tab.
5. Select the wireless network on which you want to enable dynamic WEP from under **Available Networks**, and select **Configure**.



6. Select **Data encryption (WEP enabled)**, and ensure **The key is provided for me automatically** is also selected.



7. Now you're ready to configure your router (AP) with 802.1x authentication.