



VDSL2/ ADSL2+ 802.11 N Modem/Gateway

NetVito 6800 Series
RTV1835W-D90

Wireless IAD

User Manual

Version released : 1.0

Copyright Notice

© 2011 All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of the seller.

Disclaimer

Information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. The seller therefore assumes no responsibility and shall have no liability of any kind arising from the supply or use of this document or the material contained herein.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, the seller reserves the right to make changes to the products described in this document without notice.

The seller does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Trademarks

All other product or service names mentioned in this document may be trademarks of the companies with which they are associated.

Safety and Precaution

For Installation

1. Use only the type of power source indicated on the marking labels.
2. Use only power adapter supplied with the product.
3. 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.
4. 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.
5. Do not place the product near any source of heat or expose it to direct sunlight.
6. Do not expose the product to moisture. Never spill any liquid on the product.
7. 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.
8. Do not place this product on unstable stand or table.

For Using

1. 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.

2. After powering off the product, power on the product at least 15 seconds later.
3. Do not block the ventilating openings of this product.
4. 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 :

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

Caution

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

FFC

This equipment must be installed and operated in accordance with provided instructions and a minimum 20cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

FCC Class B Notice

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.
- (2). This device must accept any interference received, including interference that may cause undesired operation.

Note :

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

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

TABLE OF CONTENTS

Before You Use.....	7
Unpacking.....	7
Features	8
ADSL Compliance	8
ADSL2 Compliance	8
ADSL2+ Compliance	8
VDSL Compliance.....	8
VDSL2 Compliance.....	8
Wireless LAN Compliance	8
ATM Features	9
Bridging Features.....	10
IP Functionalities	10
Security Features	10
USB Host Application.....	11
Configuration and Management	11
Subscription for ADSL or VDSL Service.....	12
Notes and Cautions.....	12
Chapter 1: Overview.....	13
Physical Outlook	13
Chapter 2 : System Requirement and Installation.....	15
System Requirement.....	15
Choosing a place for the Wireless IAD	15
Connecting the Wireless IAD.....	16
Wall Mounting	18
Setting up TCP / IP	19
For Windows XP 	19
Renewing IP Address on Client PC	23
For Windows NT/2000/XP 	23
Chapter 3 : Accessing the Internet.....	26
MER	27
PPP over ATM (PPPoA) Mode	29
PPP over Ethernet (PPPoE) Mode	31

Numbered IP over ATM (IPoA)	33
Numbered IP over ATM (IPoA) + NAT	35
Unnumbered IP over ATM (IPoA)	37
Unnumbered IP over ATM (IPoA) + NAT	39
Bridge Mode.....	41
Chapter 4 : Web Configuration.....	43
Using Web-Based Manager.....	43
Outline of Web Manager	44
Status	45
Advanced Setup	51
Local Network – IP Address	51
Local Network – DHCP Server	53
Local Network – UPnP	55
Local Network – IGMP Snooping	56
Internet – DNS Server	59
Internet – IGMP Proxy.....	60
Internet – ADSL / VDSL.....	62
IP Routing – Static Route	64
IP Routing – Dynamic Routing.....	68
Virtual Server – Port Forwarding	69
Virtual Server – Port Triggering	74
Virtual Server – DMZ Host	76
Virtual Server – Dynamic DNS	77
Firewall	78
Firewall – MAC Filtering	79
Firewall – IP Filtering	80
Quality of Service	83
Quality of Service – Qos Setup.....	85
Quality of Service – QoS Classification Setup.....	89
Interface Group.....	93
Wireless	96
Basic Settings	96
Security	101
Accesses Control.....	109
Repeater	111
Wireless QoS.....	114
USB App.....	116

Storage Service.....	116
Management	117
Diagnostics	117
Management Accounts	118
TR-069 Client Configuration.....	119
Identify the Validation of Certificate from ACS	122
Internet Time	123
System Log	124
Backup Configuration.....	128
Update Firmware.....	130
Reset Router	130
UPnP for XP.....	131
Chapter 5 : Troubleshooting.....	134
Problems with LAN.....	134
Problems with WAN.....	134
Problems with WAN.....	135
Chapter 6 : Glossary	137
ARP (Address Resolution Protocol)	137
DHCP (Dynamic Host Configuration Protocol)	137
LAN (Local Area Network) & WAN (Wide Area Network).....	137
NAT (Network Address Translation) IP Address	138
Private IP Address	138
Public IP Address.....	138
PVC (Permanent Virtual Circuit)	139
RIP (Routing Information Protocol)	139
UDP (User Datagram Protocol)	139
Virtual Server	139
VPI (Virtual Path Identifier) & VCI(Virtual Channel Identifier).....	139

Before You Use

Thank you for choosing the Wireless IAD. With the asymmetric technology, this device runs over standard copper phone lines.

RTV1835W Wireless IAD is a DSL broadband access device which allows ADSL and VDSL connectivity while providing 802.11b/g/n wireless LAN interface for home or office users.

It supports ADSL2/ADSL2+ and VDSL2, it's backward compatible to ADSL, even offers auto-negotiation capability for different flavors (G.dmt, G.lite, or T1.413 Issue 2 and G993.1 and G993.2) according to central office DSLAM's settings (Digital Subscriber Line Access Multiplexer).

To benefit users' access to the Internet, 4-port 10/100 Mbps Ethernet switch hub is equipped with this wireless IAD. Print server function is provided for sharing the printer in the home or office.

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 RTV1835W Wireless IAD.

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.

- ✓ **Wireless IAD**
- ✓ **Power Adapter and Cord**
- ✓ **RJ-11 ADSL Line Cable**
- ✓ **RJ-45 Ethernet Cable**
- ✓ **Phone Cable**
- ✓ **PSTN Cable**
- ✓ **Quick Start Guide**
- ✓ **Driver & Utility Software CD**

Features

ADSL Compliance

- ▶ 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
- ▶ Maximum Rate: 8 Mbps for downstream and 1 Mbps for upstream

ADSL2 Compliance

- ▶ ITU G.992.3 Annex A (G.dmt.bis)
- ▶ Maximum Rate: 12 Mbps for downstream and 1 Mbps for upstream

ADSL2+ Compliance

- ▶ ITU G.992.5 Annex A
- ▶ Maximum Rate: 24 Mbps for downstream and 1.2 Mbps for upstream

VDSL Compliance

- ▶ ITU G.993.1 Annex A
- ▶ Maximum Rate: 50Mbps for downstream and 10 Mbps for upstream

VDSL2 Compliance

- ▶ ITU G.993.2 Annex A
- ▶ Maximum Rate: 100 Mbps for downstream and 100 Mbps for upstream

Wireless LAN Compliance

- ▶ IEEE 802.11n, IEEE 802.11g and IEEE 802.11b
- ▶ IEEE 802.11g Data Rate: 54, 48, 36, 24, 18, 12, 9, 6 Mbps for 802.11g; 11, 5.5, 2, 1 Mbps for 802.11b
- ▶ IEEE 802.11n Data Rate: 14, 29, 43, 58, 87, 116, 130, 144Mbps in 20MHz
- ▶ 30, 60, 90, 120, 180, 240, 270, 300Mbps in 40MHz.
- ▶ 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 ~ 2.5 GHz
- Operating Channels: depending on local regulations. For example, 11 Channels (Northern America), 13 Channels (Europe), and 14 Channels (Japan)
- Support the selection of best quality channel automatically
- Antenna : Two internal antenna is provided
- Internal Antenna :
 - 2.4G~2.5GHz PIFA antenna with 2.78dBi and 2.72dBi peak gain.
- Coverage Area: 300 meters
- Support WEP (Wired Equivalent Privacy) mechanism which uses RC4 with 64-bit or 128-bit key length
- Support WPA and WPA2
- Support WiFi Protected Setup (WPS)
- Support the Access Control function: only registered WLAN clients are allowed to associate to this device.
- SSID can be hidden for the security issue (Don't broadcast SSID).
- Support multiple SSIDs
- Support the Repeater function to extend the coverage area
- Support wireless user isolation for the hotspot
- Support Wireless QoS (WMM)

ATM Features

- Compliant to ATM Forum UNI 3.1 / 4.0 Permanent Virtual Circuits (PVCs)
- Support up to 8 PVCs for UBR, CBR, VBR-nrt, VBR-rt with traffic shaping
- RFC2684 LLC Encapsulation and VC Multiplexing over AAL5
- RFC2364 Point-to-Point Protocol (PPP) over AAL5
- 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 among 10/100 Mb Ethernet and 802.11g wireless LAN
- Supports IGMP Snooping
- Supports 802.1Q VLAN packet pass-through

IP Functionalities

- 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 with multiple sessions, RTSP, SIP, etc.
- Port Forwarding: 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, Dynamic DNS
- DHCP Client/Relay/Server
- Time protocol can be used to get current time from network time server
- Support IGMP Proxy
- Support port mapping function which allows you to assign all data traffic transmitted among specific Internet connections and LAN ports
- Support IP/Bridge QoS for prioritize the transmission of different traffic classes
- Support 802.1Q VLAN Tagging

Security Features

- PAP (RFC1334), CHAP (RFC1994), and MS-CHAP/MS-CHAP2 for PPP session
- IP packets filtering based on IP address/Port number/Protocol type
- Bridge packet filtering
- 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)

USB Host Application

- ▶ Support Internet printing protocol 2.0 for print server function

Configuration and Management

- ▶ User-friendly embedded web configuration interface with password protection
- ▶ Remote management accesses control
- ▶ Telnet session for local or remote management
- ▶ Firmware upgrades through HTTP, TFTP, or FTP
- ▶ The boot loader contains very simple web page to allow the users to update the run-time firmware image.
- ▶ Configuration file backup and restore
- ▶ Support TR-069, TR-104, TR-111, and TR-098

Subscription for ADSL or VDSL Service

To use the IAD, you have to subscribe for ADSL or VDSL 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, such as using PPPoA, PPPoE, or MER mode.

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 IP address varies according to different ADSL service provider, such as using MER mode.

Notes and Cautions

Note and **Caution** in this manual are highlighted with graphics as below to indicate important information.



Contains information that corresponds to a specific topic.

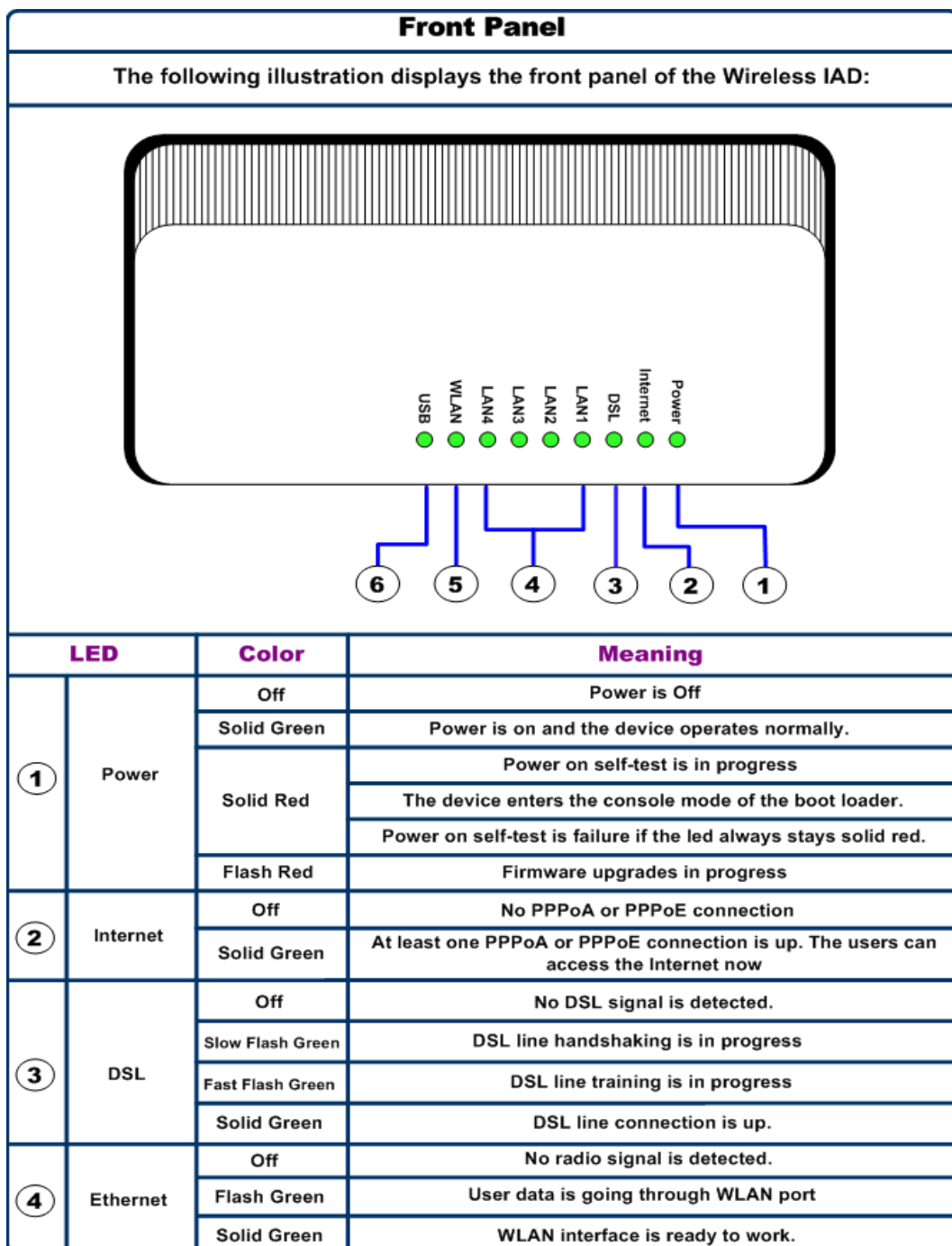


Represents essential steps, actions, or messages that should not be ignored.

Chapter 1: Overview

This chapter provides you the description for the LEDs and connectors on the front and rear surface of the router. Before you use/install this wireless IAD, please take a look at the information first.

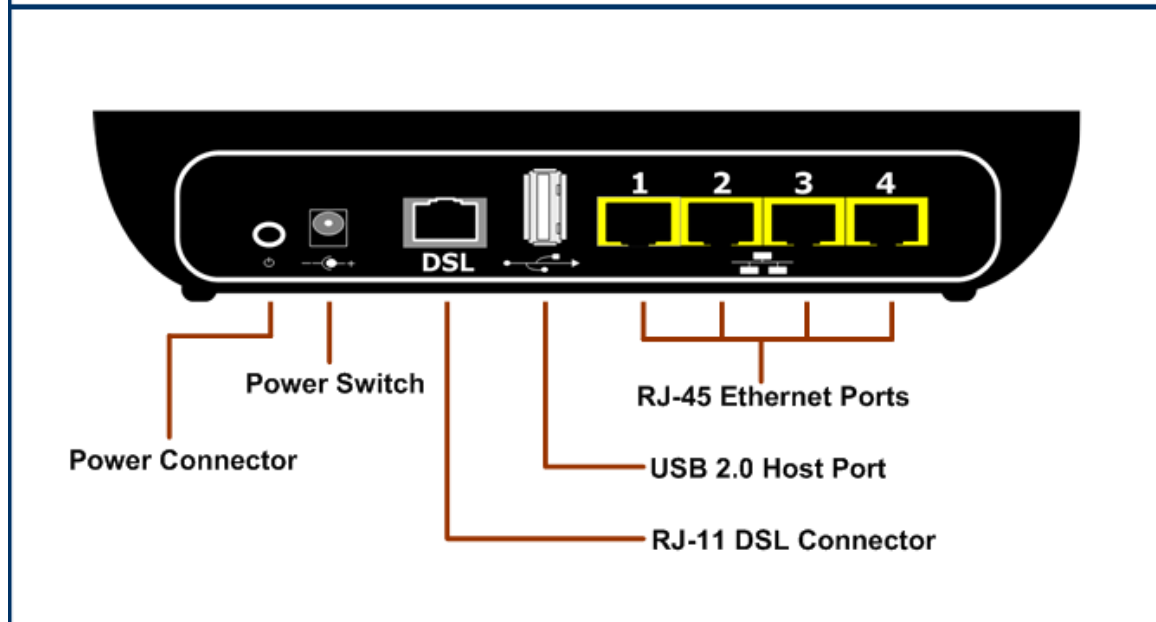
Physical Outlook



LED	Color	Meaning	
5	WLAN	Off	No radio signal is detected
	Flash Green	User data is going through WLAN port	
	Solid Green	WLAN interface is ready to work.	
6	USB	Off	No USB signal is detected
	Solid Green	USB interface is ready to work.	

Rear Panel

The following figure illustrates the rear panel of your Wireless IAD:



Chapter 2 : System Requirement and Installation

System Requirement

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

- ❖ Equipped with an Ethernet network interface.
- ❖ Have TCP/IP installed.
- ❖ Allow the client PC to obtain an IP address automatically or set a fixed IP address.
- ❖ With a web browser installed: Internet Explorer 5.x or later.

The Wireless IAD is configured with the default IP address of 192.168.1.1 and subnet mask of 255.255.255.0. Considering that the DHCP server is enabled by default, the DHCP clients should be able to access the Wireless IAD, or the host PC should be assigned an IP address first for initial configuration.

You also can manage the Wireless IAD through a web browser-based manager: [ADSL ROUTER CONTROL PANEL](#). The Wireless IAD manager uses the HTTP protocol via a web browser to allow you to set up and manage the device.

Choosing a place for the Wireless IAD

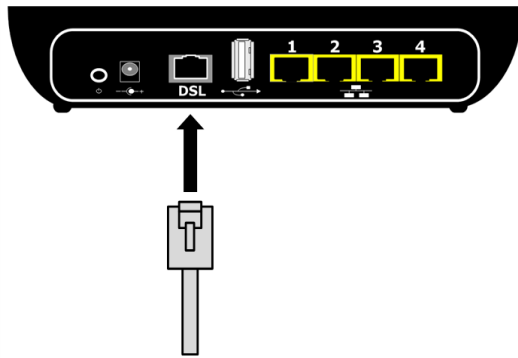
- ❶ Place the Wireless IAD close to ADSL wall outlet and power outlet for the cable to reach it easily.
- ❷ Avoid placing the device in places where people may walk on the cables. Also keep it away from direct sunlight or heat sources.
- ❸ Place the device on a flat and stable stand.

Connecting the Wireless IAD

Please follow the steps below to connect the related devices.

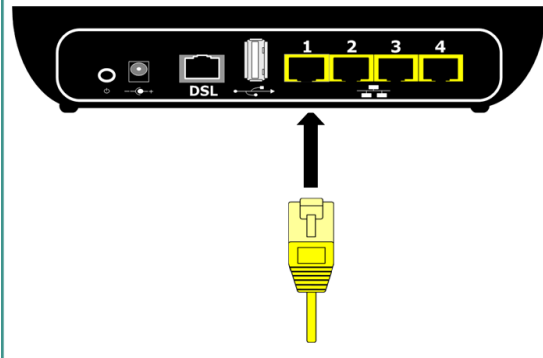
Step 1

Connecting the ADSL line : connect the DSL port of the device to your ADSL wall outlet with RJ-11 cable



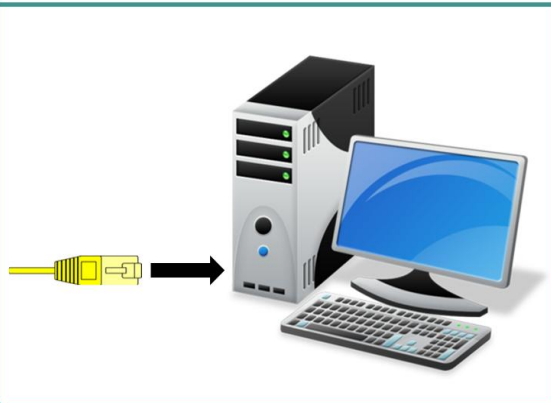
Step 2

Please attach one end of the Ethernet cable with RJ-45 connect to the LAN port of your Wireless IAD.



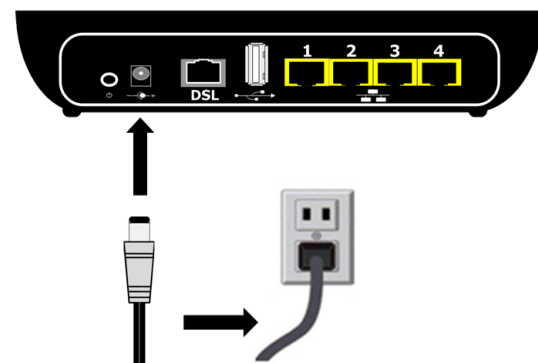
Step 3

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



Step 4

Connect the supplied power adapter to the **Power port** of your Wireless IAD , and plug the other end to a power outlet.



Step 5

Turn on the power switch. Here is an example for connecting the PC to the Wireless IAD



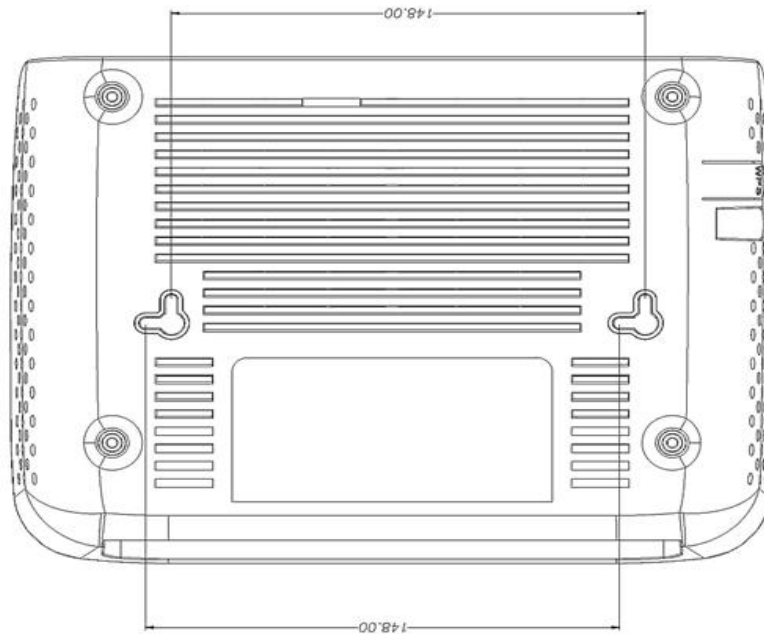
POWER ADAPTER

A. OUTPUT: 12V=====2.0A

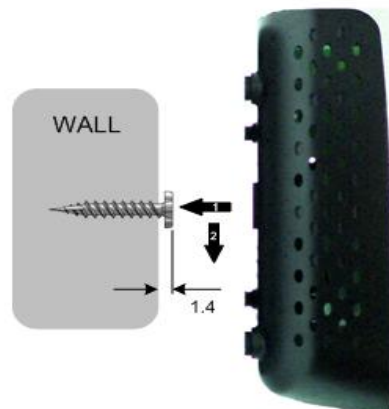
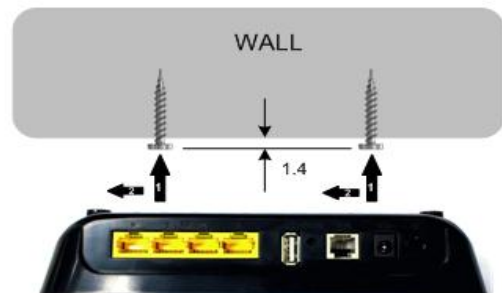
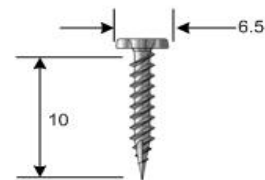
B. Max. Operation Temperature: 40°C



Wall Mounting



1. Please this template on the wall in the position the Router will be mounted. (It is recommended to mount the Router with the cable connections on the bottom)
2. Mark the mounting holes and drill holes for the screws. (It is recommended to use #8 Pan Head or Flat Head Screws. See picture to the right.)
3. Leave screws extended about 1.4 inches from the wall.
4. Hang the Router on the screws.



Setting up TCP / IP

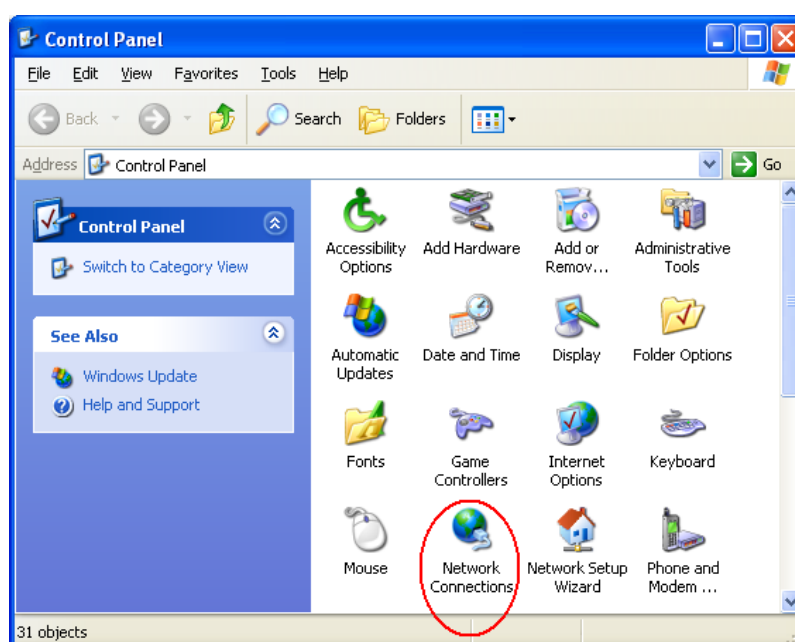
If the TCP/IP protocol has not been installed yet, please follow the steps below for installation. In the following illustrations, we will set the PC to get an IP address automatically at the same time.

For Windows XP

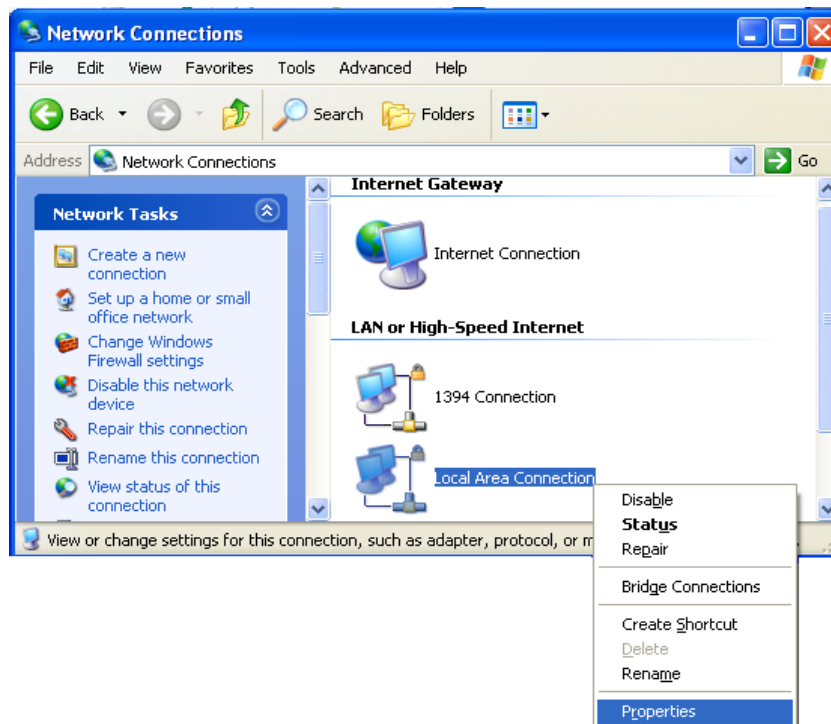
1. Open the Start menu, point to Control Panel and click it.



2. Double click the Network Connection.



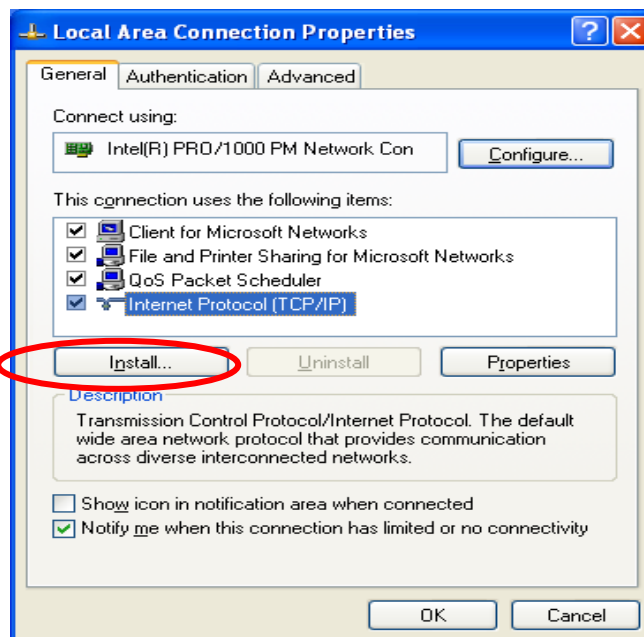
3. Right click Local Area Connection and then click Properties.



4. On the General tab, check out the list of installed network components.

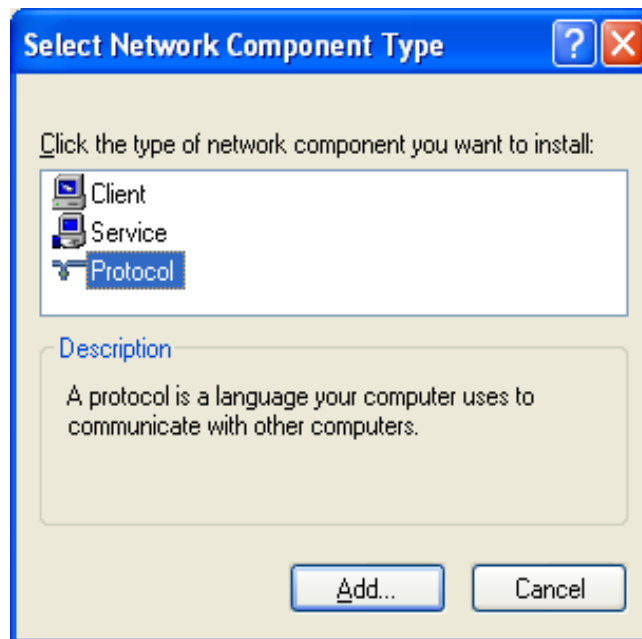
Option 1: If there is no TCP/IP Protocol, click Install.

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

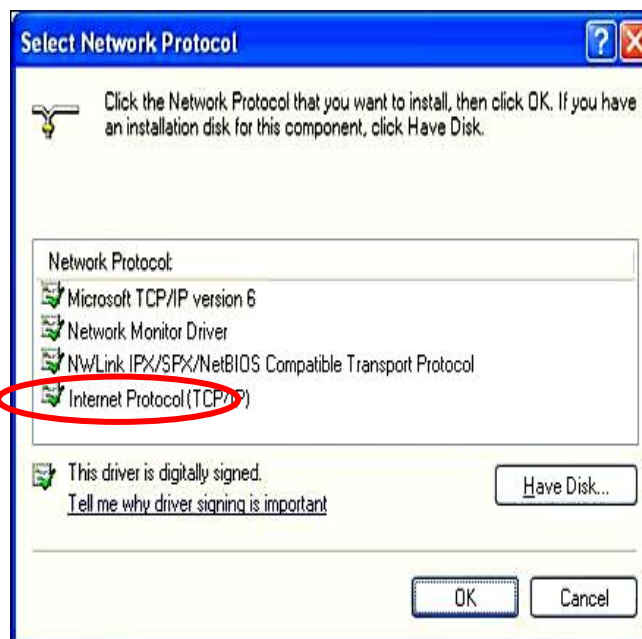


If there is no TCP/IP protocol installed on your PC, press "Install" to continue.

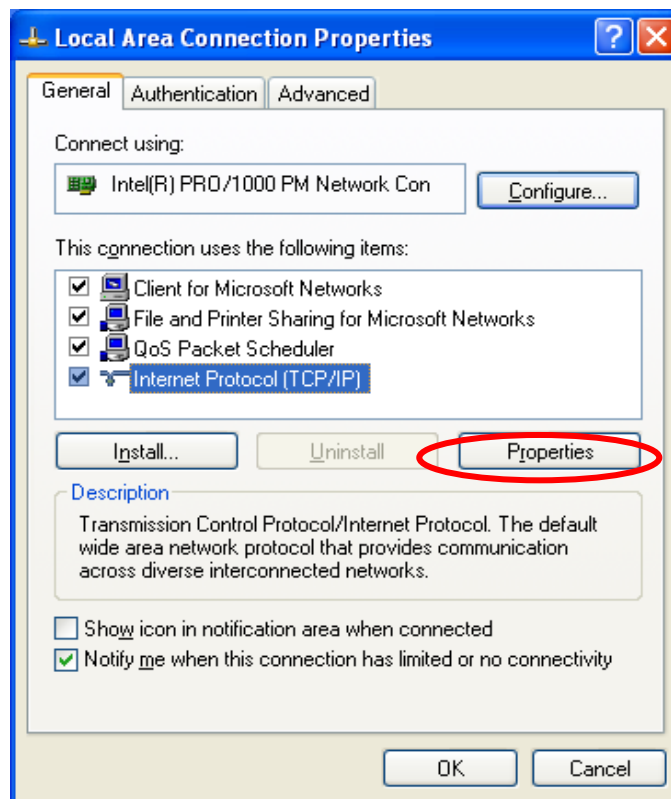
5. Highlight Protocol and then click Add.



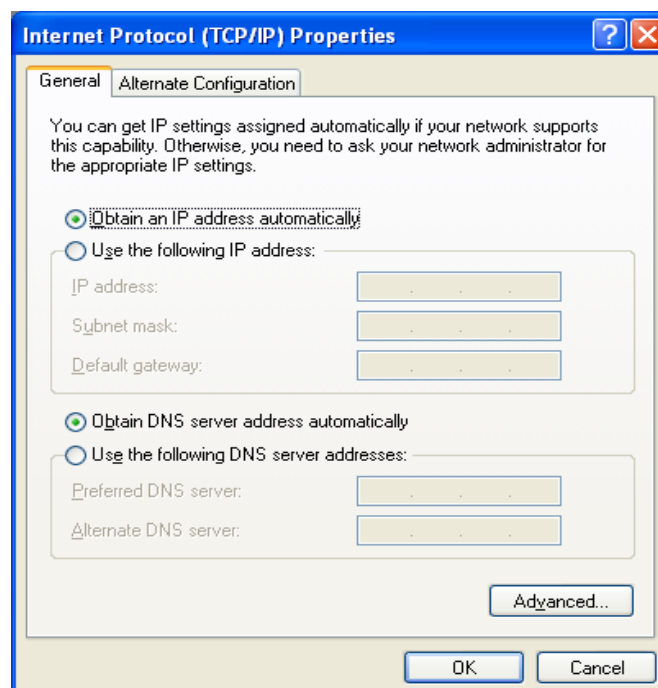
6. Click Internet Protocol(TCP/IP) and then click OK.



- When it returns to the **General Tab** on the **Local Area Connection Properties** window, highlight **Internet Protocol (TCP/IP)** and then click **Properties**.



- Under the **General** tab, select **Obtain an IP address automatically**, and **Obtain DNS server address automatically**. Then click **Ok**.

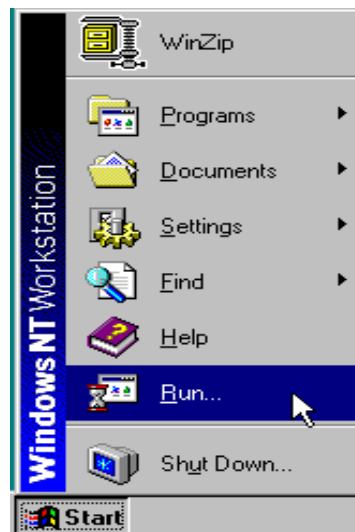


Renewing IP Address on Client PC

After the Wireless IAD gets on line, there is a chance that your PC does not renew its IP address and thus causes the PC not able to access the Internet. To solve this problem, please follow the procedures below to renew PC's IP address.

For Windows NT/2000/XP

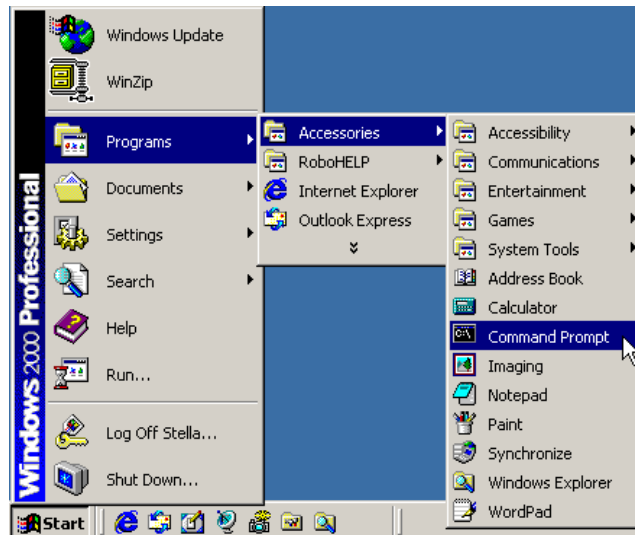
1. Open the Start menu, and click Run... on this menu.



2. Type cmd in the text box that appears and click OK. Then you will see the command prompt window.



- **Another way to open the command prompt:**
From Start menu, point to Programs, select Accessories, and then click Command Prompt.



3. Type `ipconfig` at the command prompt window and press Enter to view the computer's IP information from DHCP server.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

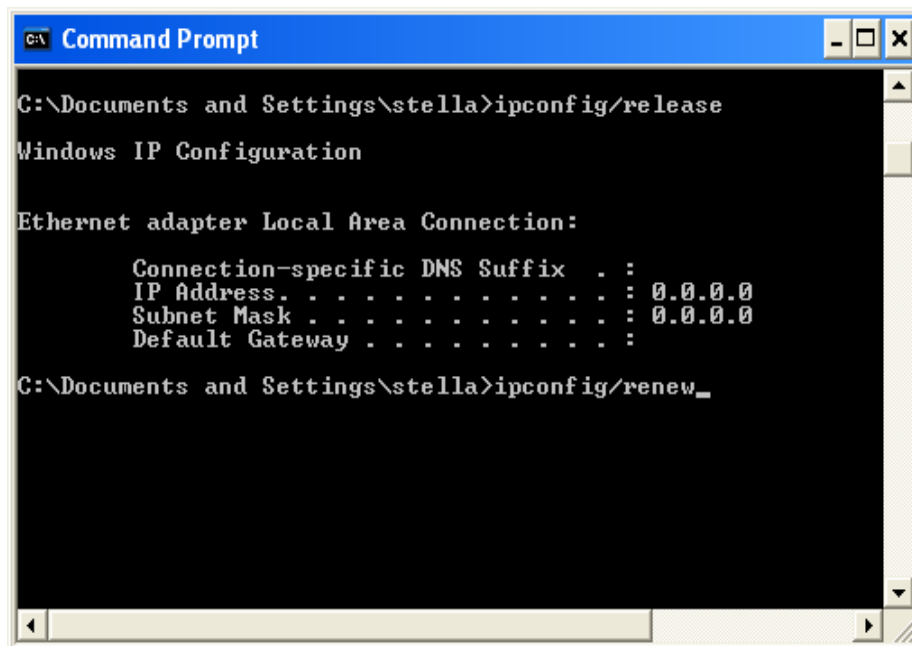
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : home
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Documents and Settings>_
```


4. If the computer is holding a current IP address, type `ipconfig /release` to let go of the address, then type `ipconfig /renew` to obtain a new one.



```
C:\Documents and Settings\stella>ipconfig/release
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . .               : 0.0.0.0
    Subnet Mask . . . . .             : 0.0.0.0
    Default Gateway . . . . .         :

C:\Documents and Settings\stella>ipconfig/renew_
```

Chapter 3 : Accessing the Internet

Before configuring the Wireless IAD, you must decide whether to configure the Wireless IAD 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)
- ◆ PPP over Ethernet (PPPoE)
- ◆ Numbered IP over ATM (IPoA)
- ◆ Numbered IP over ATM (IPoA) + NAT
- ◆ Unnumbered IP over ATM (IPoA)
- ◆ Unnumbered IP over ATM (IPoA) + NAT
- ◆ Bridge Mode
- ◆ MER (Bridge Mode + NAT)

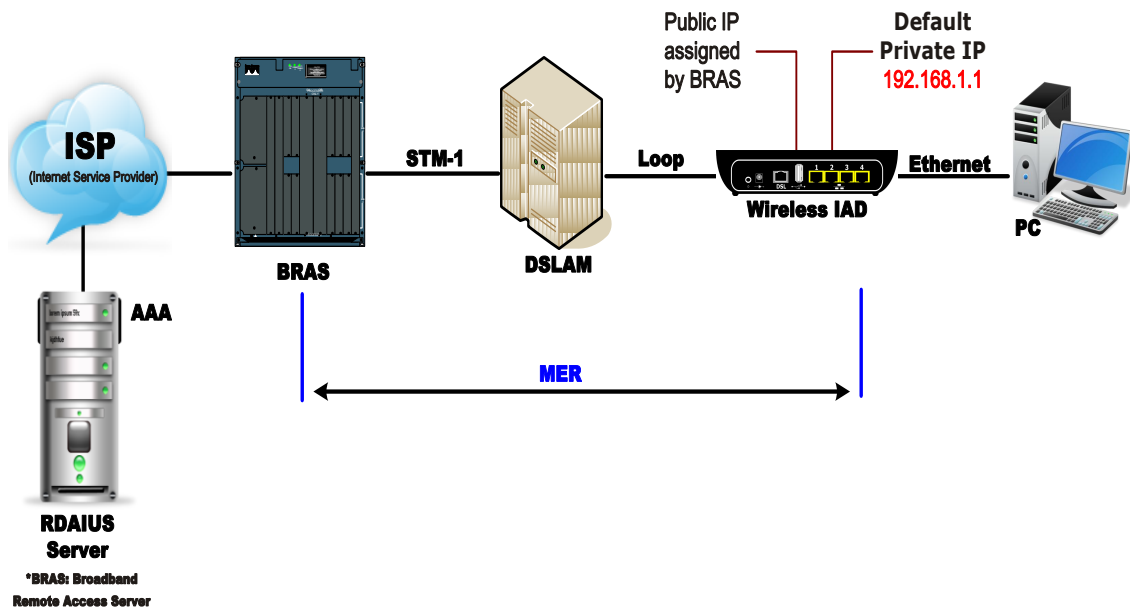
To ensure your PC accessing the Internet successfully, please check the following first.

- ◆ A network interface card is installed on your PC.
- ◆ The Wireless IAD is solidly connected with your computer.
- ◆ The TCP/IP protocol has been installed and the IP address setting is to obtain IP address automatically.

When all above preparations are ready, you can open the Browser and type "192.168.1.1" into the URL box and start to make the web configuration for different connection modes.

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

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 to Internet.

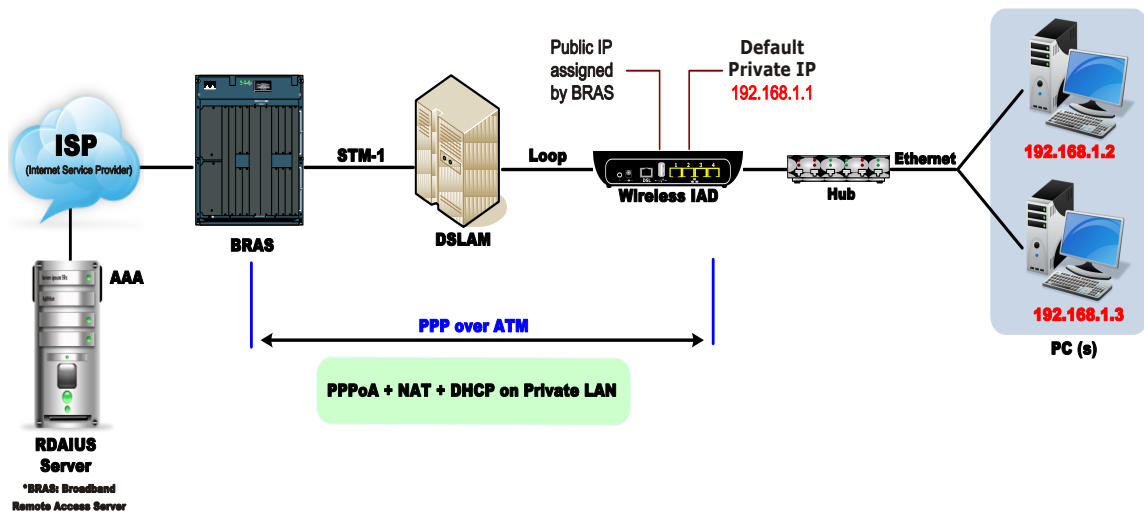
In this example, the Wireless IAD acts as a NAT device which translates a private IP address into a public address. Therefore multiple users can share with one public IP address to access the Internet through this IAD. The public address can be a static public address that is pre-assigned by ISP or a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

Configuration:

1. Start your browser and type 192.168.1.1 in the URL box to access ADSL web-based manager.
2. Go to Quick Start – Quick Setup. Uncheck Auto Scan Internet Connection (PVC). Key in the VCI and VPI value, e.g.,
VPI – 0 VCI – 37
Then click the Next button.
3. On the Configure Internet Connection – Connection Type page, select Bridging and then click the Next button.
4. On the WAN IP Settings page, select Obtain an IP address automatically; then, select Obtain DNS server address automatically.
5. Check Enable NAT. Then click Next.

6. On the Configure LAN side Settings page, key in the IP address and subnet mask for your LAN. Check DHCP Server On box, and enter the start and end points, e.g.:
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*
Then key in the leased time that you want. And click Next
7. Check the network information on the Summary page. Make sure the contents match the settings provided by your ISP. Click Finish.
8. Now the IAD is well-configured. You can access the Internet.

PPP over ATM (PPPoA) Mode



Description :

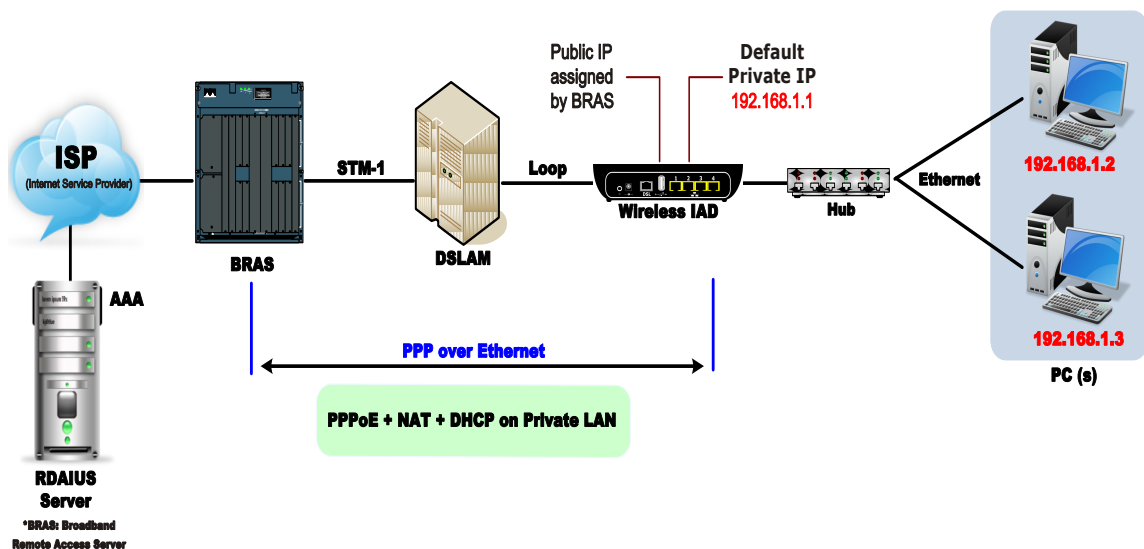
In this deployment environment, the PPPoA session is between the ADSL WAN interface and BRAS. The Wireless IAD gets a public IP address from BRAS when connecting to DSLAM. The multiple client PCs will get private IP address from the DHCP server enabled on private LAN. The enabled NAT mechanism will translate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

Configuration :

1. Start your browser and type 192.168.1.1 as the address to access ADSL web-based manager.
2. Go to Quick Start – Quick Setup. Uncheck Auto Scan Internet Connection (PVC). Key in the VCI and VPI value, e.g.:
VPI – 0
VCI – 38
Click the Next button.
3. On the Configure Internet Connection – Connection Type page, select PPP over ATM (PPPoA) then click the Next button.
4. On the WAN IP Settings page, select Obtain an IP address automatically and check Enable NAT box. Click Next.
5. On the PPP Username and Password page, enter the PPP username and password that you got from your ISP. Select Always on or select Dial on Demand and key in the inactivity timeout value. (The default value is 20 minutes.) Then click Next.

6. **On the Configure LAN side Settings page, key in the IP address and subnet mask for your LAN, e.g.:**
Primary IP address: 192.168.1.1
Subnet Mask: 255.255.255.0
Check DHCP Server on box. And key in the start and end IP address, e.g.:
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Then enter the leased time (the default is 1 day), and click Next.
7. **Check the network information on This Internet Connection -- Summary page. Make sure the settings match the information provided by your ISP. Click Finish.**

PPP over Ethernet (PPPoE) Mode



Description :

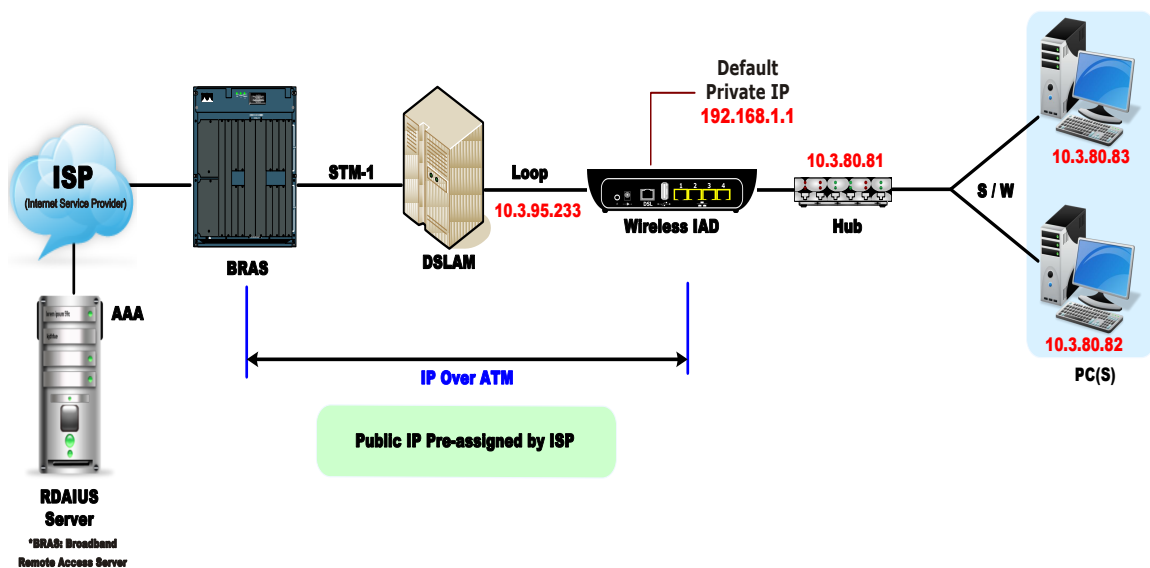
In this deployment environment, the PPPoE session is between the ADSL WAN interface and BRAS. The Wireless IAD gets a public IP address from BRAS when connecting to DSLAM. The multiple client PCs will get private IP address from the DHCP server enabled on private LAN. The enabled NAT mechanism will translate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

Configuration :

1. Start your browser and type 192.168.1.1 in the URL box to access ADSL web-based manager.
2. Go to Quick Start – Quick Setup. Uncheck Auto Scan Internet Connection (PVC). Key in the VCI and VPI value, e.g.:
VPI – 0
VCI – 39
Click the Next button.
3. On the Configure Internet Connection – Connection Type page, select PPP over Ethernet (PPPoE) then click the Next button.
4. On the WAN IP Settings page, select Obtain an IP address automatically and check Enable NAT box. Click Next.
5. On the PPP Username and Password page, enter the PPP username and password that you got from your ISP. Select Always on or select Dial on Demand and key in the inactivity timeout value. (The default value is 20 minutes.) Then click Next.

6. **On the Configure LAN side Settings page, key in the IP address and subnet mask for your LAN, e.g.:**
Primary IP address: 192.168.1.1
Subnet Mask: 255.255.255.0
Check DHCP Server on box. And key in the start and end IP address, e.g.:
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Then enter the leased time (the default is 1 day), and click Next.
7. **Check the network information on This Internet Connection -- Summary page. Make sure the settings match the information provided by your ISP. Click Finish.**

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 Wireless IAD and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as the IAD IP addresses and the last one is for subnet broadcasting. Other remaining IP addresses can be assigned to PCs on the LAN.

The following example uses the LAN IP address ranging from *10.3.80.81* to *10.3.80.86* and the subnet mask for LAN is *255.255.255.248*. The WAN IP address is *10.3.95.233*, and the subnet mask for WAN is *255.255.255.248*.

Configuration :

- (1). Start your browser and type 192.168.1.1 in the URL box to access ADSL web-based manager.
- (2). Go to Quick Start – Quick Setup. Uncheck Auto Scan Internet Connection (PVC). Key in the VCI and VPI value, e.g.:
VPI – 0
VCI – 32
Click the Next button.
- (3). On the Configure Internet Connection – Connection Type page, select IP over ATM (IPoA) then click “Next”.
- (4). On the WAN IP Settings page, select Use the following IP address and

Use the following DNS Server Address, then key in the information that your ISP offered, e.g.:

WAN IP Address: 10.3.95.233

WAN Subnet Mask: 255.255.255.248

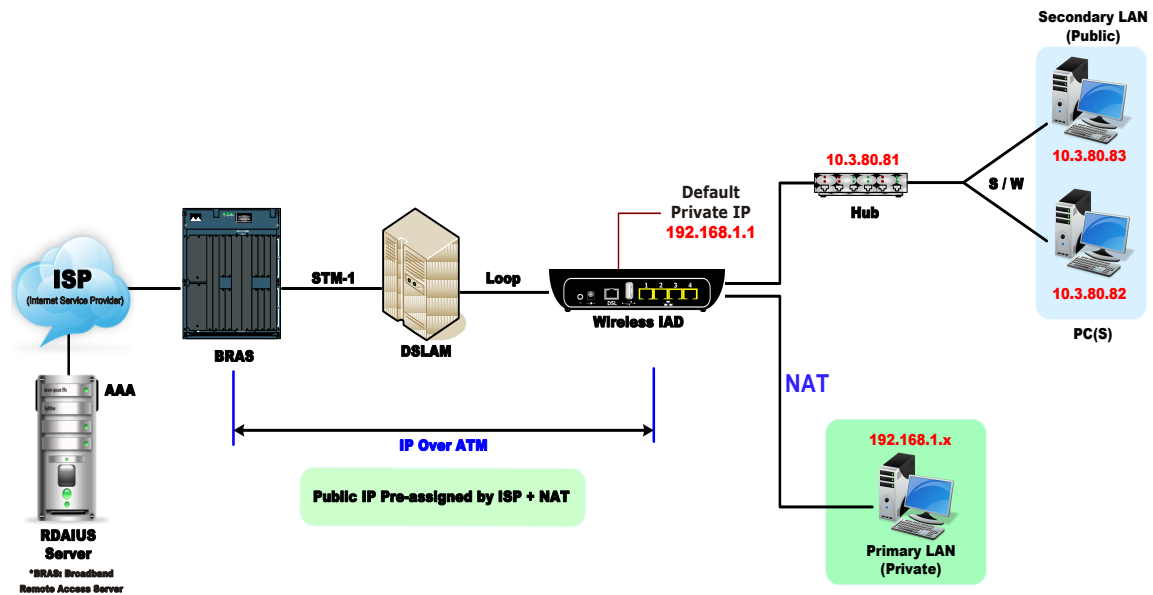
Primary DNS server: 168.95.1.1

Secondary DNS server: 168.95.192.1

Uncheck Enable NAT and click Next.

- (5). On the Configure LAN side Settings page, key in the information for your LAN, e.g.,
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 enter the information needed.
Secondary IP Address: 10.3.80.81
Subnet mask: 255.255.255.248
Click Next.
- (7). Check the network information on the Summary page. Make sure the settings match the settings provided by your ISP. Click Finish.
- (8). Refer to the TCP/IP properties, specify an IP Address, and fill in other information needed, e.g.:
IP Address: 10.3.80.82
Subnet Mask: 255.255.255.248
Gateway: 10.3.80.81
Preferred DNS server: 168.95.1.1
- (9). Now the IAD is well-configured. You can access the 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 the IAD or use another NAT box connected to hub) to support multiple clients to access the IAD 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 Wireless IAD and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as IAD IP address and the last one is subnet broadcasting. Other remaining IP addresses can be assigned to PCs on the LAN.

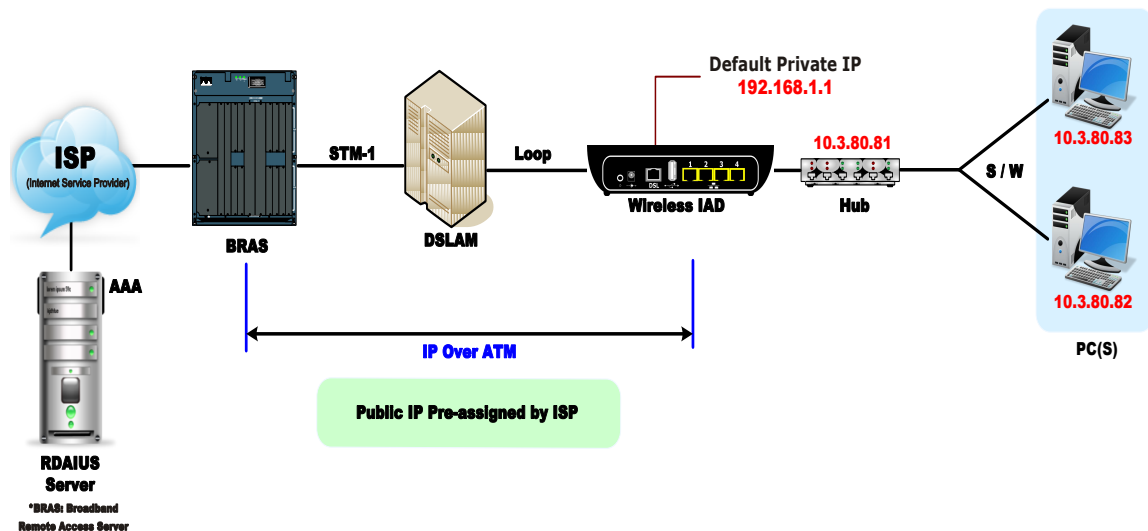
The following example uses the IP address ranging from 10.3.80.81 to 10.3.80.86 and the subnet mask is 255.255.255.248.

Description :

- (1). Start your browser and type 192.168.1.1 in the URL box to access ADSL web-based manager.
- (2). Go to Quick Start – Quick Setup. Uncheck Auto Scan Internet Connection (PVC). Key in the VCI and VPI value, e.g.:
 - VPI – 0
 - VCI – 32
 Click the Next button.

- (3). On the Configure Internet Connection – Connection Type page, select IP over ATM (IPoA) then click “Next”.
- (4). On the WAN IP Settings page, select Use the following IP address and Use the following DNS Server Address, then key in the information that your ISP offered, e.g.:
WAN IP Address: *10.3.80.81*
WAN Subnet Mask: *255.255.255.248*
Primary DNS server: *168.95.1.1*
Secondary DNS server: *168.95.192.1*
- (5). Check the Enable NAT box. And click” Next”.
- (6). On the Configure LAN side Settings page, key in the information for your LAN, e.g.,
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.
- (8). Now the IAD 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 Wireless IAD and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as IAD 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 IP address ranging from 10.3.80.81 to 10.3.80.86 and the subnet mask is 255.255.255.248. In such circumstance, we do not assign any WAN IP.

Configuration :

- (1). Start your browser and type 192.168.1.1 in the URL box to access ADSL web-based manager.
- (2). Go to Quick Start – Quick Setup. Uncheck Auto Scan Internet Connection (PVC). Key in the VCI and VPI value, e.g.:
VPI – 0
VCI – 32
Click the Next button.
- (3). On the Configure Internet Connection – Connection Type page, select IP over ATM (IPoA) then click “Next”.
- (4). On the WAN IP Settings page, select none for WAN IP address settings. Then, select Use the following DNS Server Address and key in the information that your ISP offered, e.g.:

Primary DNS server: 168.95.1.1
Secondary DNS server: 168.95.192.1
Uncheck Enable NAT and click Next.

- (5). **On the Configure LAN side Settings page, key in the information for your LAN, e.g.,**
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

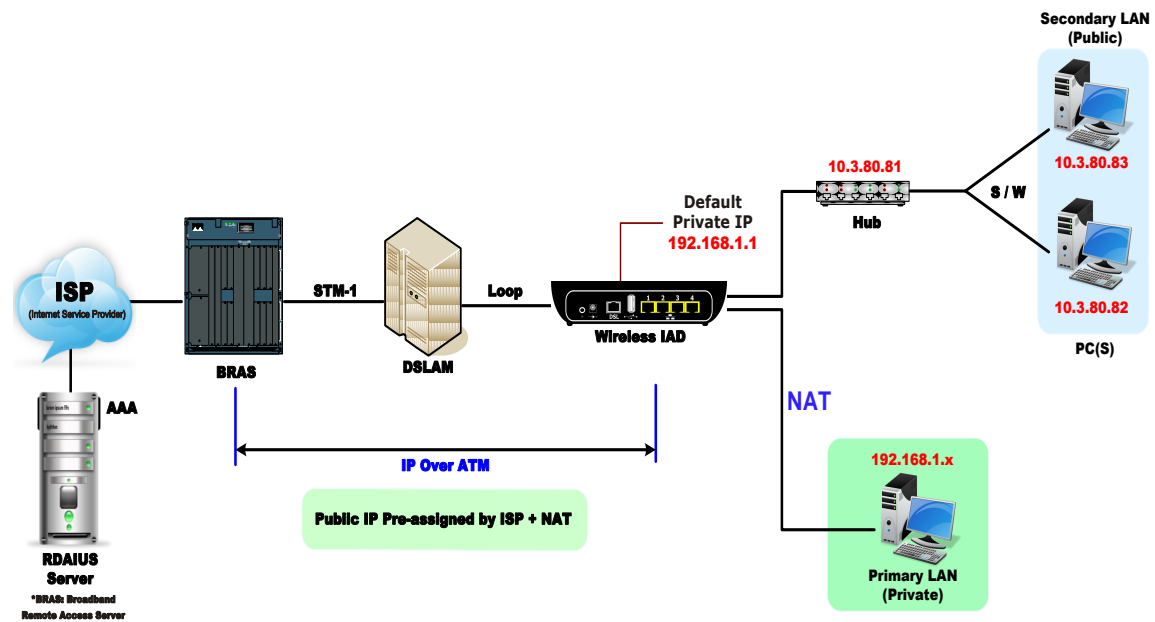
- (6). **Check Configure the second IP Address and Subnet Mask for LAN Interface and enter the information needed, e.g.,**
Secondary IP Address: 10.3.80.81
Subnet mask: 255.255.255.248
Check DHCP Server Off and click Next.

- (7). **Check the network information on the Summary page. Make sure the settings match the settings provided by your ISP. Click Finish.**

- (8). **Refer to the TCP/IP properties, specify an IP Address, and fill in other information needed, e.g.:**
IP Address: 10.3.80.82
Subnet Mask: 255.255.255.248
Gateway: 10.3.80.81
Preferred DNS server: 168.95.1.1

- (9). **Now the IAD is well-configured. You can access the Internet.**

Unnumbered IP over ATM (IPoA) + NAT



Configuration :

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

The following example uses the IP address ranging from 10.3.80.81 to 10.3.80.86 and the subnet mask is 255.255.255.248. In such circumstance, we enable NAT function but not assign any WAN IP.

Description :

- (1). Start your browser and type 192.168.1.1 in the URL box to access ADSL web-based manager.
- (2). Go to Quick Start – Quick Setup. Uncheck Auto Scan Internet Connection (PVC). Key in the VCI and VPI value, e.g.:
VPI – 0
VCI – 32
Click the Next button.
- (3). On the Configure Internet Connection – Connection Type page, select IP over ATM (IPoA) then click “Next”.
- (4). On the WAN IP Settings page, select none for WAN IP address

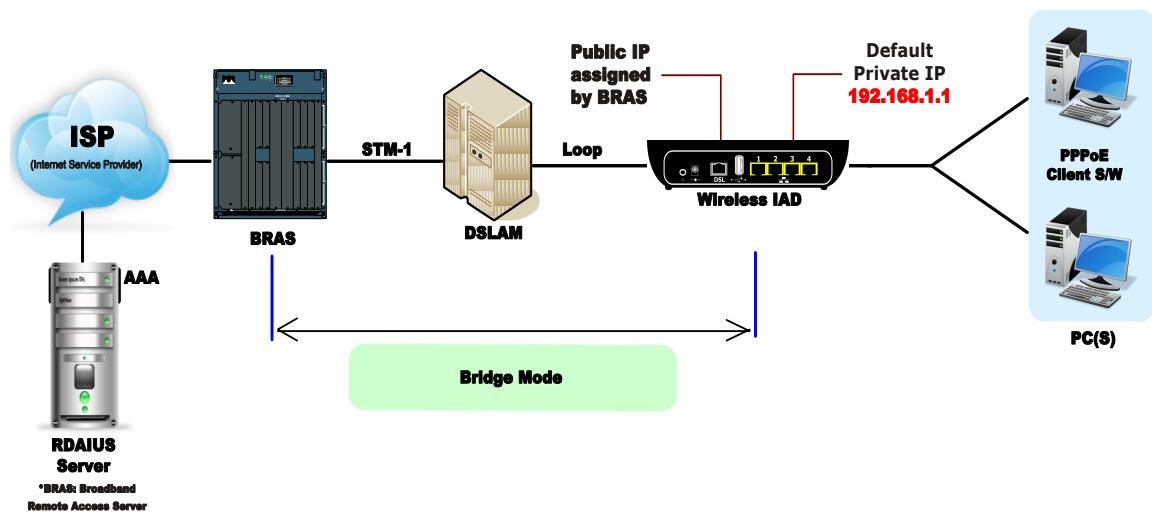
settings. Then, select **Use the following DNS Server Address** and key in the information that your ISP offered, e.g.:

Primary DNS server: 168.95.1.1

Secondary DNS server: 168.95.192.1

- (5). Check the **Enable NAT** box. And click **Next**.
- (6). On the **Configure LAN side Settings** page, key in the information for your LAN, e.g.,
 - 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 enter the information needed, e.g.,
 - Secondary IP Address: 10.3.80.81**
 - Subnet mask: 255.255.255.248**Click **Next**.
- (8). Check the network information on the **Summary** page. Make sure the contents match the settings provided by your ISP. Click **Finish**.
- (9). Now the IAD is well-configured. You can access the Internet.

Bridge Mode



Description :

In this example, the Wireless IAD acts as a bridge which bridging the PC IP addresses from LAN to WAN. The PC IP address can be a static public address that is pre-assigned by the ISP or a dynamic public address that is assigned by the ISP DHCP server, or an IP address received 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 your browser and type 192.168.1.1 in the URL box to access ADSL web-based manager.
3. Go to Quick Start – Quick Setup. Uncheck Auto Scan Internet Connection (PVC). Key in the VCI and VPI value, e.g.,
VPI – 0
VCI – 35
Then click the Next button.
4. On the Configure Internet Connection – Connection Type page, select Bridging then click the Next button.
5. On the WAN IP Settings page, select none for WAN IP address settings.

6. On the **Configure LAN side Settings** page, enter the IP address and subnet mask for your LAN, e.g.:
Primary IP address: 192.168.1.1
Subnet Mask: 255.255.255.0
Choose **DHCP Server Off** and click **Next**.
7. Check the network information on the **Summary** page. Make sure the contents match the settings provided by your ISP. Click **Finish**.
8. Refer to the **TCP/IP** properties, specify an IP Address, and fill in other information needed, e.g.:
IP Address: 10.3.86.81
Subnet Mask: 255.255.255.248
Gateway: 10.3.86.1
Preferred DNS server: 168.95.1.1
9. Click **OK**. Now the IAD is well-configured. You can access to the Internet.

Chapter 4 : Web Configuration

Using Web-Based Manager

After properly configuring you host PC, please proceed as follows:

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



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

Outline of Web Manager

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

The screenshot shows the NetVito VDSL2 web manager interface. On the left is a navigation menu with options: Device Info, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled 'Device Info' and contains two tables. The first table lists device specifications, and the second table shows WAN connection details. Below the tables is a note: 'This information reflects the current status of your WAN connection.'

Device Info	
Board ID:	RTV1835W
Symmetric CPU Threads:	2
Build Timestamp:	131202_1807
Software Version:	RTV1835W.41208.00.01.0005
Bootloader (CFE) Version:	1.0.38-114.185
DSL PHY and Driver Version:	A2pv6F039f1.d24j
Wireless Driver Version:	6.30.102.7.cpe4.12L08.0
Uptime:	0D 0H 15M 39S

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0

Title	The title of this management interface.
Main Menu	Including Quick Start, Status, Advanced, Wireless, Voice, USB APP, and Management.
Main Window	The current workspace of the web manager, containing configuration or status information.
Current Version	Here provides the version info for firmware, ADSL2+, and Wireless.

To Have the New Settings Take Effect

After selecting or adjusting the settings according to your needs, your customizations will be saved to the flash memory before you restart the IAD. And only after rebooting the IAD, your customizations may take effect.

Language

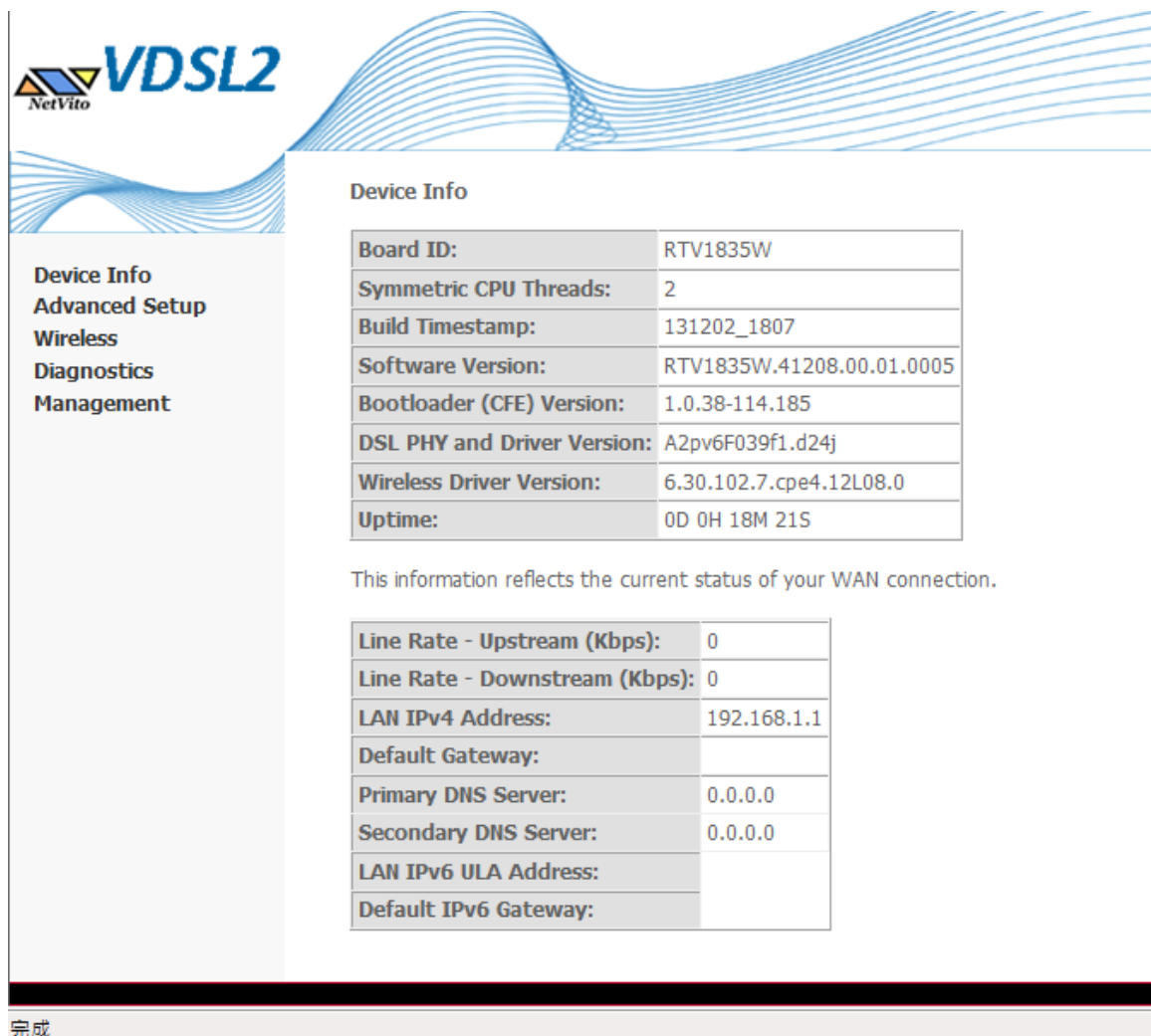
On the top to the right of this web page, it provides a drop-down menu for you to choose a proper language. (However, we only offer English at present.)



Status

Device Info

This page displays the current status for the ADSL connection, including the System Up Time, ADSL speed, LAN IP address, default gateway, DNS server, firmware version, boot loader version, ADSL driver version, wireless driver version, wireless BSSID, Ethernet MAC address, and memory size. The system status will be different according to the settings that you configured in the web pages.



The screenshot shows the NetVito VDSL2 web interface. On the left is a navigation menu with options: Device Info, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled 'Device Info' and contains two tables. The first table lists hardware and software details. Below it is a note: 'This information reflects the current status of your WAN connection.' The second table shows WAN connection parameters.

Device Info	
Board ID:	RTV1835W
Symmetric CPU Threads:	2
Build Timestamp:	131202_1807
Software Version:	RTV1835W.41208.00.01.0005
Bootloader (CFE) Version:	1.0.38-114.185
DSL PHY and Driver Version:	A2pv6F039f1.d24j
Wireless Driver Version:	6.30.102.7.cpe4.12L08.0
Uptime:	0D 0H 18M 21S

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
Default IPv6 Gateway:	

完成

xDSL Line :

- ▶ This page shows all information for xDSL. For knowing the quality of the xDSL connection, please click xDSL BER Test button to have advanced information. Click [More Information](#) hyperlink to show more detailed information about xDSL Line Status.

DSL

Statistics -- xDSL

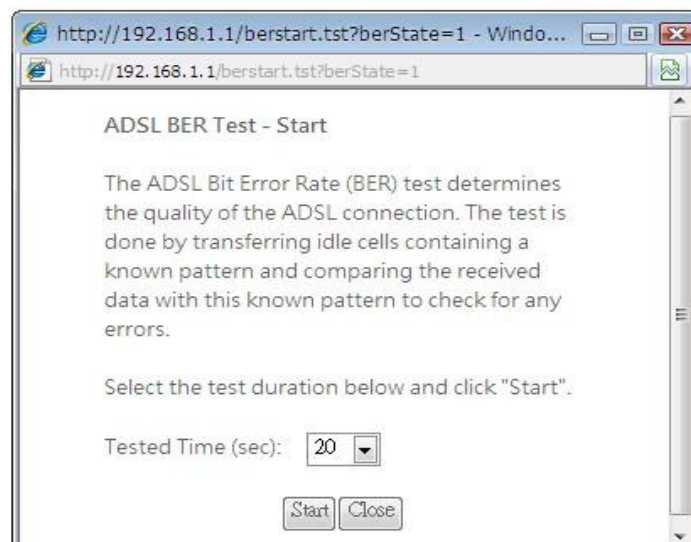
Device Info
Summary
WAN
Statistics
LAN
WAN Service
xTM
xDSL
Route
ARP
Advanced Setup
Wireless
Voice
Diagnostics
Management

Mode:		
Traffic Type:		
Status:	NoSignal	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		

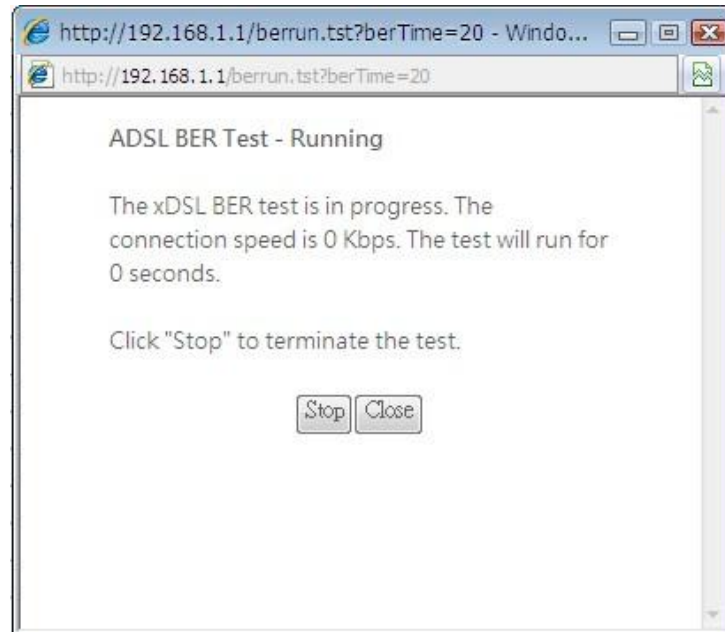
xDSL BER Test Reset Statistics

BER Test :

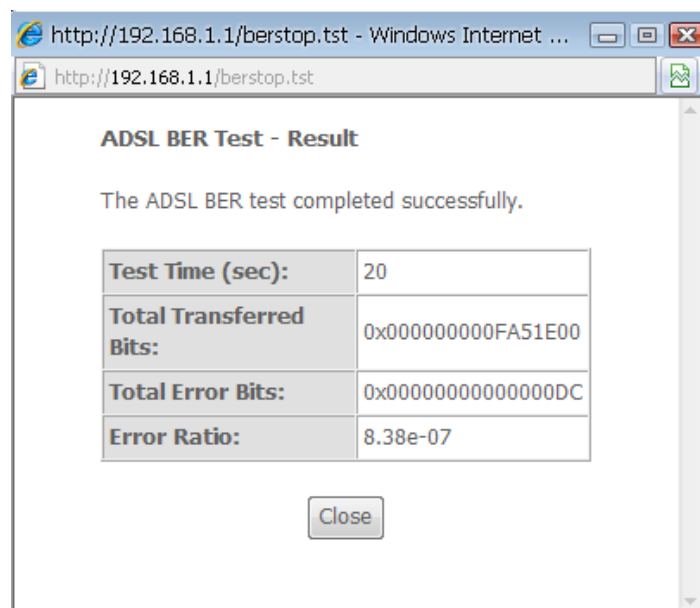
- (1). This test determines the quality of the ADSL connection. It is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for errors.



- (2). After selecting the test duration time and click Start, the following dialog appears to tell you the test is running. You can stop the test by clicking Stop or close this dialog window by pressing Close.



- (3). When the test is over, the result will be shown on the following dialog window for your reference. Click Close to close this window.



Internet Connection :

- ▶ This page displays the connection information for your wireless IAD, such as the PVC name, VPI/VCI value, service category, protocol, invoking NAT and QoS or not, IP address, linking status, and so on.

WAN Info											
Interface	Description	Type	VlanMuxdd	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ppp0.1	pppoe_0_0_35	PPPoE	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Unconfigured	(null)	(null)

Traffic Statistics :

- ▶ This table shows the records of data going through the LAN and WAN interfaces. For each interface, cumulative totals are displayed for Received and Transmitted. You may click Reset to reset the amount.

Statistics -- LAN								
Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	0	0	0	0
eth1	0	0	0	0	0	0	0	0
eth2	31669	221	0	0	75750	340	0	0
eth3	0	0	0	0	0	0	0	0
wl0	0	0	0	0	22290	226	289	0

DHCP Table :

- ▶ This table shows all DHCP clients who get their IP addresses from your Wireless IAD. For each DHCP client, it shows the Host Name, MAC Address, IP Address and the Lease Time.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
Haofun-NB	5c:26:0a:43:3a:23	192.168.1.2	23 hours, 11 minutes, 59 seconds
xpsp1	00:16:36:ea:31:b5	192.168.1.3	23 hours, 26 minutes, 2 seconds

Wireless Clients :

- ▶ This table shows the MAC address for all of the wireless LAN clients currently associated to your Wireless IAD.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
00:17:23:00:F8:B7			RTV1805VW	wl0

Refresh

Routing Table

- ▶ This table shows the routing rules that your router uses.

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.22.1.254	0.0.0.0	255.255.255.255	UH	0	pppoe_0_0_36	ppp0.1
192.168.2.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.0.0	192.168.1.2	255.255.0.0	UG	1		br0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe_0_0_36	ppp0.1

ARP Table :

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

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.3	Complete	00:16:36:ea:31:b5	br0

Advanced Setup

Local Network – IP Address

This page is the same as you can see on 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.

Disable DHCP Server
 Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
00:00:00:11:22:33	192.168.1.10	<input type="checkbox"/>

Enable DHCP Server Relay
 DHCP Server IP Address:

Configure the second IP Address and Subnet Mask for LAN interface

▶ **Primary IP Address:**

Key in the first IP address that you received from your ISP for the LAN connection.

▶ **Subnet Mask:**

Key in the subnet mask that you received from your ISP for the LAN connection.

▶ **Host Name:**

List the host name of this device.

▶ **Domain Name:**

List the name of the domain.

The screenshot displays a configuration window with the following elements:

- Enable LAN side firewall
- Disable DHCP Server
- Enable DHCP Server
 - Start IP Address:
 - End IP Address:
 - Leased Time (hour):
 - Static IP Lease List: (A maximum 32 entries can be configured)
 - Buttons: **MAC Address**, **IP Address**, **Remove**
 - Buttons: **Add Entries**, **Remove Entries**
- Configure the second IP Address and Subnet Mask for LAN interface
 - IP Address:
 - Subnet Mask:
-

- ▶ **Configure the second IP Address and Subnet Mask:**
Check this box to enter another set of IP Address and Subnet Mask to connect to your IAD if they are not included in the range that DHCP server accepts. After checking this box, the secondary IP address and subnet mask entries will show up, as shown in the right figure.
- ▶ **Secondary IP Address & Subnet Mask:** Enter the information provided by your ISP for your LAN connection.
- ▶ **MTU:**
It means the maximum size of the packet that transmitted in the network. The packet of the data greater than the number set here will be divided into several packets for transmitting. Type the value into the field of MTU. The default setting is 1500.
- ▶ **Apply:**
Click this button to activate the settings listed above.

Local Network – DHCP Server

This allows you to set DHCP server on LAN interface.

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName

IP Address:

Subnet Mask:

Enable IGMP Snooping

Standard Mode

Blocking Mode

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

DHCP Server On:

Check this item if DHCP service is needed on the LAN. The IAD will assign IP address and gateway address for each of your PCs. You have to key in Start IP Address, End IP Address, and Lease Time. The default lease time is 1day.

DHCP Server Configuration

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

DHCP Server On

Start IP:

End IP:

Lease Time: days hours minutes

Relay On

Relay to Server IP:

Server and Relay Off

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

Relay On:

Click this button to have a relay setting. And type the Server IP in the IP field. When the DHCP server is served by another device rather than the IAD itself, you can relay to that specific server and enter the IP address of it, as 10.3.95.2 in our example.

Server and Relay Off :

Check this item if DHCP service isn't needed on the LAN.

Apply :

Click this button to activate the settings listed above.

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/>		

DHCP Static IP Lease

Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address:

IP Address:

You can reserve one specific IP address for a certain PC for particular purpose. Simply add a mapping entry of MAC address & IP address for that PC by pressing the Reserved IP Address List button. The window as the one shown in the right column will appear.

Click the Add button to open another dialog window, shown as the right. On PC's MAC Address and Assigned IP Address boxes, please type the correct information according to your need and click Apply.

Static IP Lease List: (A maximum 32 entries can be configured)


MAC Address	IP Address	Remove
00:10:18:20:21:22	192.168.1.1	<input type="checkbox"/>
<input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/>		

The information added will be shown on the window right away, as the right figure illustrates. That is, the specified address will be reserved and not be assigned by DHCP for other computer(s).

You may click Add button to add another set or click close to exit

Local Network – UPnP

The UPnP is only available for Windows XP. If you are not a Windows XP user, you may ignore this page.



UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

Enable UPnP

Apply/Save

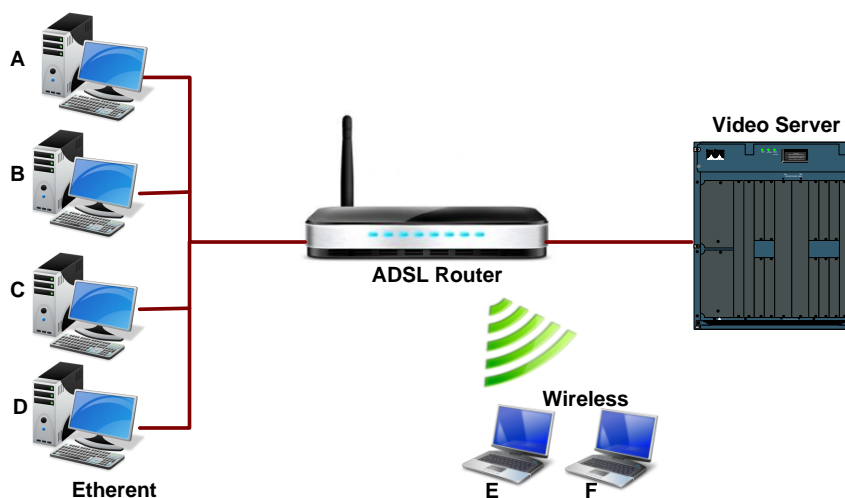
Enabling the UPnP IGD and NAT traversal function allows the users to perform more applications behind NAT without additional configuration settings or ALG support on your router.

You can enable the UPnP function through this web page by checking Enable UPnP and press Apply.

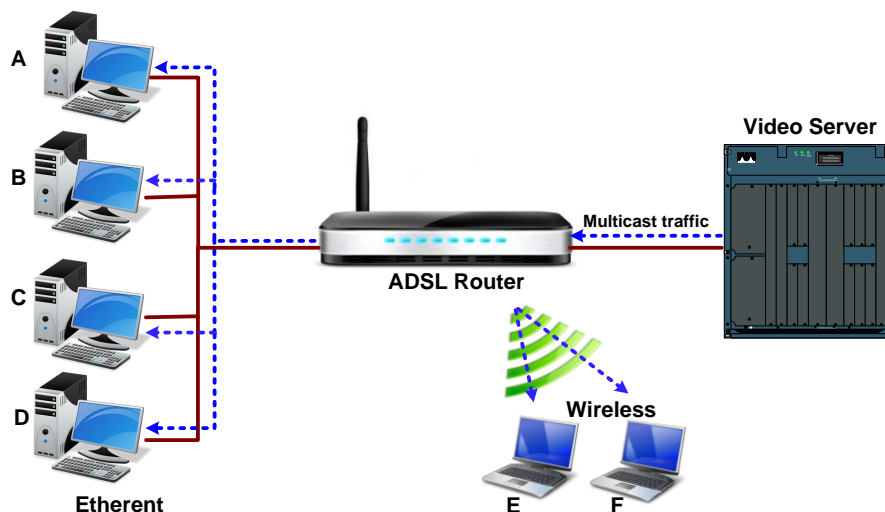
Local Network – IGMP Snooping

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everyone on the network). Multicast delivers IP packets to just a group of hosts on the network. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

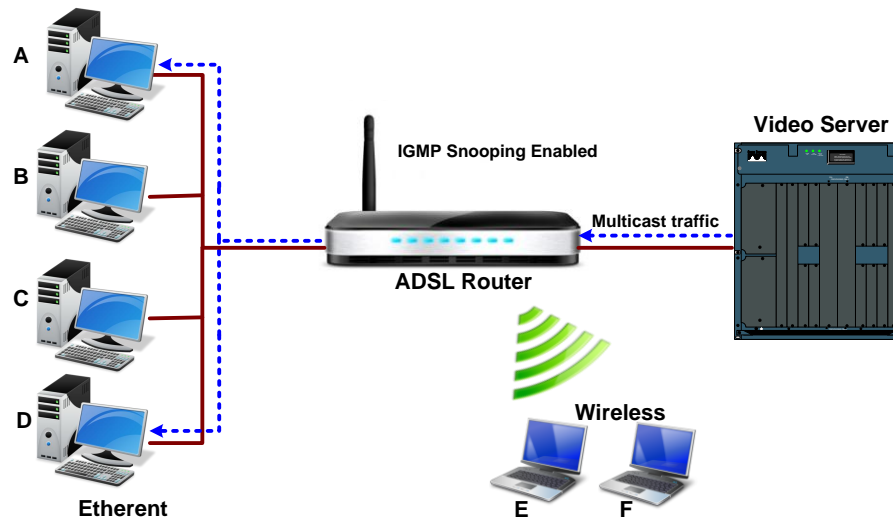
The figure below shows a simple network connected via the Wireless IAD. There are four Ethernet clients and two wireless clients.



Now suppose the video server is the multicast transmitter and host A and D are multicast receivers. If we do not turn on the IGMP snooping function, the IAD will forward the multicast traffic to all hosts on all interfaces and consequently block and interrupt the traffic of wireless users, shown as the following figure.



When IGMP snooping is invoked, it makes the system aware to establish the best path for multicast service to save LAN bandwidth. Refer the figure below, just as desired, only host A and D will actually receive multicast traffic when IGMP snooping is enabled.



While IGMP snooping is enabled, the IGMP packets will be monitored, the membership information will be recorded and processed, and the multicast traffic will only be forwarded to those LAN interfaces, such as Ethernet, Wireless, and USB, which are bonded to the subscribed multicast groups. Thus it helps to save the bandwidth and helps the devices to perform more effectively.

Check Enable IGMP Snooping and click Apply to invoke this function. When IGMP Snooping is enabled, you can check the box below to filter out multicast packets which will be sent to your local network if no user plays multimedia movies.

Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address:

Subnet Mask:

Enable IGMP Snooping

Note that the IGMP proxy must be enabled first. If the IGMP snooping function is not available as shown in the following figure, you have to enable the IGMP Proxy first.

When IGMP Snooping is enabled, you can check the box below to filter out multicast packets which will be sent to your local network if no user plays multimedia movies.

If the PVC you're using is NAT enabled, remember to turn on the IGMP Proxy at the same time. Please refer to Internet – IGMP Proxy for more information.

Internet – 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. Finish your setting and click the **Apply** button to save it and invoke it.

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

TODO: IPV6 ***** Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

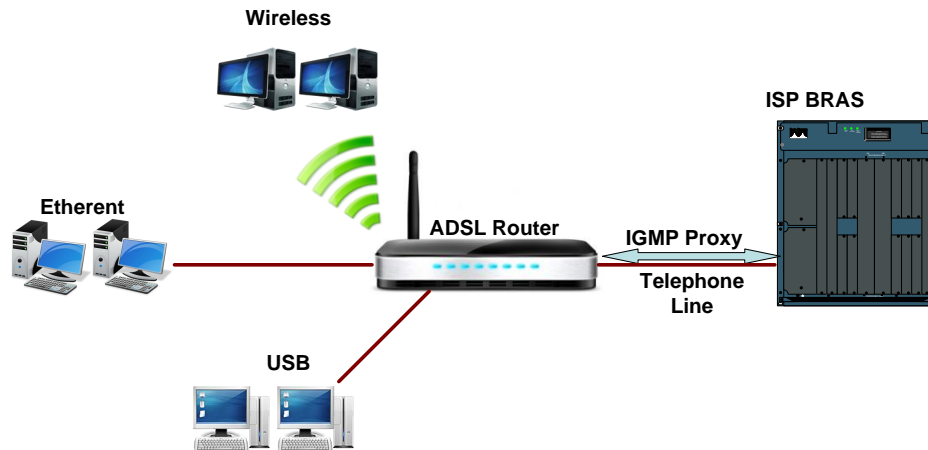
Enable Automatic Assigned DNS :

Check this box to enable this function, or uncheck this box to disable it. The default setting is checked. When this function is disabled, you have to offer the Primary DNS server and Secondary DNS server.

If you are satisfied with the settings, click Apply.

Internet – 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 routers 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 being queried, the system will send membership reports to the group.
 - ◆ When one of the hosts joins a multicast address group which none of other hosts belongs to, the system will send unsolicited membership reports to that group.
 - ◆ When the last host in a particular multicast group leaves the group, the system will send a leave group membership report to the router's group.
- ▶ If the PVC you're using is NAT enabled, remember to turn on the IGMP Proxy at the same time. Please refer to Internet – IGMP Proxy for more information.

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

Internet Connection :

This field displays the internet connection(s) set in this router.

IGMP Proxy Enabled :

Check this box to enable this function or uncheck this box to disable this function. After finish the settings, click Apply.

Internet – ADSL / VDSL

DSL Settings	
Select the modulation below.	Select the profile below.
<input checked="" type="checkbox"/> G.Dmt Enabled	<input checked="" type="checkbox"/> 8a Enabled
<input checked="" type="checkbox"/> G.lite Enabled	<input checked="" type="checkbox"/> 8b Enabled
<input checked="" type="checkbox"/> T1.413 Enabled	<input checked="" type="checkbox"/> 8c Enabled
<input checked="" type="checkbox"/> ADSL2 Enabled	<input checked="" type="checkbox"/> 8d Enabled
<input checked="" type="checkbox"/> AnnexL Enabled	<input checked="" type="checkbox"/> 12a Enabled
<input checked="" type="checkbox"/> ADSL2+ Enabled	<input checked="" type="checkbox"/> 12b Enabled
<input type="checkbox"/> AnnexM Enabled	<input checked="" type="checkbox"/> 17a Enabled
<input checked="" type="checkbox"/> VDSL2 Enabled	<input checked="" type="checkbox"/> 30a Enabled
	US0
	<input checked="" type="checkbox"/> Enabled

Enable ADSL Port :

Check this box to enable this function. It simply invokes the line mode that you choose here for the IAD.

Select the support of line modes :

There are several selections, and you may select them according to the line modes supported by your ISP and your needs.

Capability Enabled :

Two items are provided here for you to choose.

Select the phone line pair below.

Inner pair
 Outer pair

Capability

Bitswap Enable
 SRA Enable

Bitswap :

It is a mandatory receiver initiated feature to maintain the operating conditions of the modem during changing environment conditions. It reallocates the data bits and power among the allowed carriers without modification of the higher layer control parameters in the ATU. After a bit swapping reconfiguration, the total data rate and the data rate on each latency path is unchanged. Check this box to enable the function. If not, uncheck this box to close the function

Capability

Bitswap Enable
 SRA Enable

Seamless Rate Adaptation(SRA) :

It enables the ADSL2/ ADSL2+ Router to change the data rate of the connection while in operation without any service interruption or bit errors. Check this box to enable the function. If not, uncheck this box to close the function.

IP Routing – Static Route

The table shows all static route status and allows you to add new static IP route or delete static 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.

Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
------------	---------------------	---------	-----------	--------	--------

This page shows all the routing table of data packets going through your ADSL Router.

Destination Network Address :

Display the IP address that the data packets are to be sent.

Netmask, Gateway, WAN Interface :

Display the subnet mask, gateway, and WAN interface information that the transmitting data will pass through.

Delete :

Allow you to remove the static route settings.

Adding a New One :

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

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save"

IP Version:

Destination IP address/prefix length:

Interface:

(optional: metric number should be greater than or equal to zero)

Metric:

For **example**, type **192.168.1.1** in the field of the gateway IP address and leave the destination network blank.

Destination IP Address :

The destination IP address of the network indicates where data packets are to be sent. You may specify an IP, type 0.0.0.0, or leave it blank.

Netmask :

Enter the Netmask that you got from the ISP, type 0.0.0.0, or leave it blank.

Gateway IP Address :

Check it to forward packets to the specific gateway. Enter the gateway IP address that you want to use.

Forward Packets to

Gateway IP Address:

WAN Interface:

WAN Interface :


Click this button to forward packets to a specific WAN interface. Choose one from the drop-down menu.

If you have added an IPoA PVC from Advanced- Internet Connections webpage, you can forward packets to it now. Just select it from the WAN Interface drop down menu.

Click **Apply** to save the setting.

Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
4	192.168.0.0/16	192.168.1.2		1	<input type="checkbox"/>

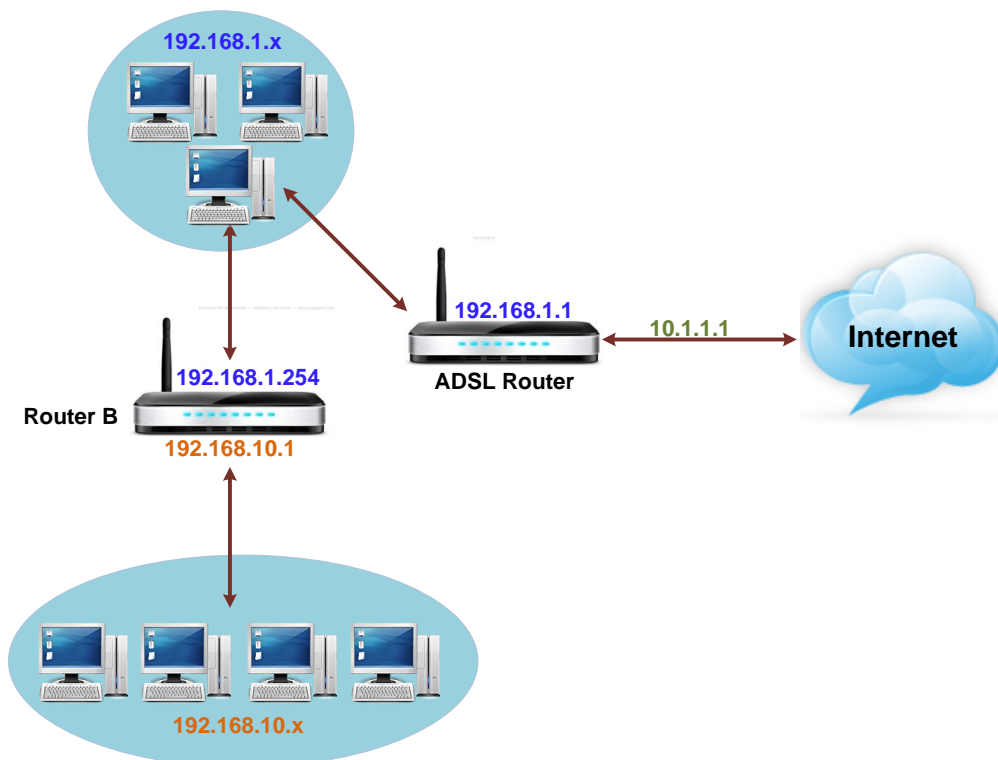
You will see the result shown as the right figure. If you don't want the static route that you created, please click the  icon in the Delete column from the table.



A dialog window will appear to confirm your action. Click OK to remove the static route, or click **Cancel** to keep the setting.

Example – Static Route :

Here provides you an example of Static Route.



For the LAN shown above, if the PC in the subnet of 192.168.1.x wants to access the PC in the subnet of 192.168.10.x, we can set a static route in the ADSL router, in which the destination is the PC in the subnet 192.168.10.x and the gateway is router B. The setting would be as follows:

Destination : 192.168.10.0

Netmask : 255.255.255.0 (Standard Class C)

Gateway : 192.168.1.254 (Router B)

IP Routing – Dynamic Routing

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

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm0.1	2	Passive	<input checked="" type="checkbox"/>

1
2
Both

Apply/Save

RIP Version :

It incorporates the RIP information when receiving and broadcasting the RIP packets. From the drop down menu, 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 :

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

Click Apply to invoke the settings set here.

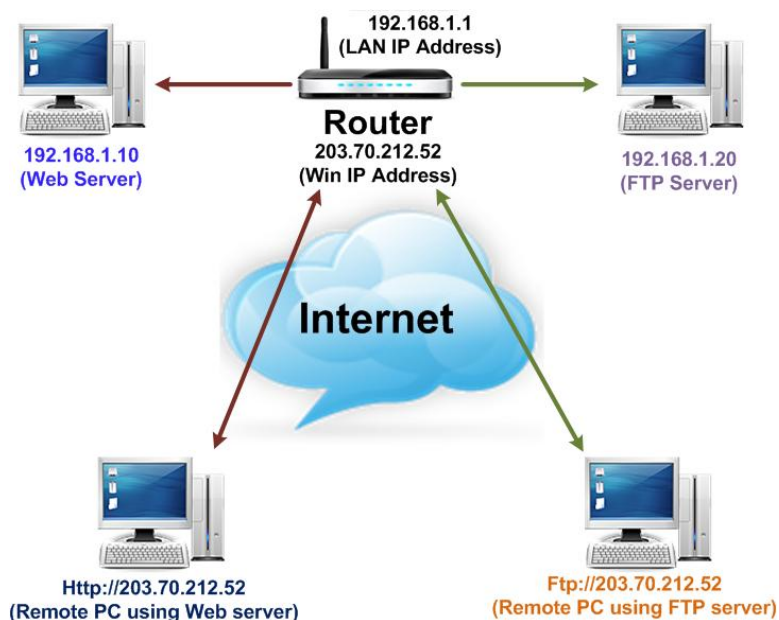
Virtual Server – Port Forwarding

The Router implements NAT to make 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.

Virtual Server function 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 :

Once configured, anyone on the Internet can connect to your Virtual Servers.

Please note that, in the above picture, both Internet users are connecting to the same IP address, but using different protocols, such as *Http://203.70.212.52* and *Ftp://203.70.212.52*.

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.

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).

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN. Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	R

Add New Port Forwarding :

To set a virtual server, please open the Virtual Server item from the Advanced setup menu.

To add a new Port Forwarding, please click Add from the Port Forwarding web page.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
1234	1234	TCP	21	21
		TCP		
		TCP		
		TCP		

Pre-defined :

Choose one of the service types from the first drop-down list, such as **Audio/Video**, **Games**, and so on. In the second drop-down list, choose the name of the application that you want to use with the type that you select in the first list.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
1723	1723	TCP	1723	1723
		TCP		
		TCP		

For example, if you choose **Audio/Video** in the first field, the corresponding contents of the second field would be like the drop-down list shown as the following figure.

Add New Port Forwarding Rule

Application Name:

Pre-defined:

User defined:

From Internet Host IP Address:

Forward to Internal Host IP Address:

By using the rules:

Protocol	External Packet		Forward to Internal Host	
	Port Start	Port End	Port Start	Port End
TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
TCP <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

User defined :

Type a new service name for building a customized service for specific purpose. There are three lines that you can enter settings into on this page. If you need more lines, just apply the settings and then add a new port forwarding rule.

Application Name:

Pre-defined:

User defined:

From Internet Host IP Address:

Forward to Internal Host IP Address:

For example, select the predefined application name *Audio/Video – Media Player 7*, set from *ALL* internet host IP addresses, and forward to *192.168.1.200*. Click *Apply*. Be sure to reboot your router for these changes to take effect.

Port Forwarding

Create the port forwarding rules to allow certain applications or server software to work on your computers if the Internet connection uses NAT.

Application Name	External Packet			Internal Host		Delete
	IP Address	Protocol	Port	IP Address	Port	
Media Player 7	ALL	TCP	1755	192.168.1.200	1755	<input type="checkbox"/>
Media Player 7	ALL	UDP	70 - 7000	192.168.1.200	70 - 7000	<input type="checkbox"/>

Select All

The result will be displayed as the following figure. If you do not want the server that you created, check the Delete box of that application and click the Delete button to discard it. Or if you want to add another one, click Add to add a new one.

Virtual Server – Port Triggering

When the wireless IAD detects outbound traffic on a specific port, it will set up the port forwarding rules temporarily on the port ranges that you specify to allow inbound traffic. It is supposed to increase the support for Internet gaming, video conferencing, and Internet telephony due to the applications require multiple connection.

<input type="button" value="Add"/> <input type="button" value="Remove"/>								
Application Name	Trigger				Open		WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

IAD -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text" value="1234"/>	<input type="text" value="1234"/>	TCP	<input type="text" value="21"/>	<input type="text" value="21"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

To add a new port triggering rule, click Add to open this web page. Then choose an application name from the Pre-defined list box.

Add New Port Triggering Rule

Application Name: Pre-defined: User defined:

The system provides 9 items for you to choose.

Port Triggering

Port triggering function is a conditional port forwarding feature. When your ADSL router detects outbound traffic on a specific port(trigger port), it will set up the port forwarding rules temporarily on the port ranges you specify to allow inbound traffic. This is supposed to increase the support for Internet gaming, video conferencing, and Internet telephony due to these applications require multiple connection.

Application Name	Trigger		Open		Delete
	Protocol	Port	Protocol	Port	
AIM Talk	TCP	4099	TCP	5090	<input type="checkbox"/>

Select All

You may also define by yourself, just type the name into the field of User defined.

Click Apply to complete the setting.

If you select *AIM Talk*, the result page will be like the demo figure in the right column.

You may delete the application by checking the delete box and pressing Delete.

Virtual Server – DMZ Host

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

NAT -- DMZ Host

The Broadband 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:

Once this feature is enabled, you must specify an IP address. It allows 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.
- ▶ The DMZ feature only works when the NAT function is enabled.

Virtual Server – Dynamic DNS

The Dynamic DNS (Domain Name System) combines both functions of DNS and DHCP to map a dynamic IP to a fixed domain name. This page allows you to access the virtual servers with a domain name and password.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org

Hostname: blajlin.dyndns.org

Interface: pppoe_0_0_36/ppp0.1

DynDNS Settings

Username: blajlin

Password: [masked]

Apply/Save

Dynamic DNS :

Select enable to enable Dynamic DNS; select Disabled to disable this function.

Dynamic DNS Provider :

Choose a provider (*DynDNS.org*, *TZO.com*, *Changelp.com*, or *No-IP.com*) from the drop-down list.

Internet Connection :

Select the interface from the drop-down list that you want to use for this function.

User Name & Password :

Type the user name and password that you registered with the provider.

Host Name, Domain Name :

Key in the domain name or host name to registered. 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.

When the setting is finished, click Apply to invoke them, or click Cancel if you want to discard the settings.

Firewall

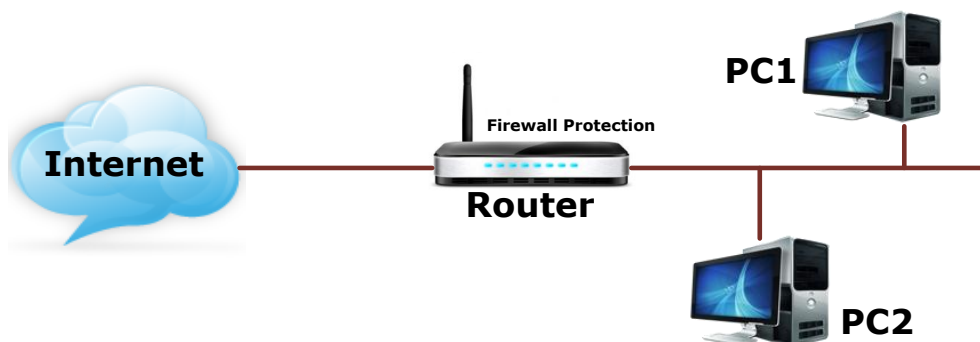
The firewall is a kind of software that interrupts the data between the Internet and your computer. It is the TCP/IP equivalent of a security gate at the entrance to your company. All data must pass through it, and the firewall (functions as a security guard) will allow only authorized data to be passed 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. The device supports logging of the TCP/UDP and IP packet headers and the first 129 bytes of the packet (including headers) whenever a packet is successfully passed through or blocked, and whenever a packet matches a rule being setup for suspicious packets.

An example for firewall setup :



This picture shows 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, setting the firewall is an important issue.

Firewall – MAC Filtering

The bridge filtering mechanism provides a way for the users to define rules to allow/deny packets through the bridge based on source MAC address and/or destination MAC address. When bridge filtering is enabled, each packet is examined against the each defined filter rules sequentially, and when a matched is determined, the packets will be blocked.

This page allows you to define the bridge packet filtering rules to block those redundant packets with specific protocols and MAC addresses.

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
atm0.1	FORWARD	<input type="button" value="Change"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

Select traffic direction from the drop down menu, and check the network interface which you want this rule to apply on. Then, choose a protocol and define the source or destination MAC address which you want to control.

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

For example, if we choose *Outbound*, check *br_0_35*, select *PPPoE* as protocol, and enter *00:90:96:01:2A:C3* into the Source MAC Address field, then after clicking Apply, we will see the result as shown in the right.

You can use Add or Delete button to maintain the bridge filtering rules.

Firewall – 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.

Choose Disabled to disable the firewall function. Click Enabled to invoke the settings that you set in this web page.

Filter Name:	<input type="text" value="ICMP"/>
IP Version:	<input type="text" value="IPv4"/>
Protocol:	<input type="text" value="ICMP"/>
Source IP address[/prefix length]:	<input type="text"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address[/prefix length]:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>

To initiate the IP Filtering, select the Enabled radio button and click Apply.
Select the direction to filter packets :

Inbound means the data is transferred from outside onto your computer.

Outbound means the data is transferred from your computer onto outside through Internet. Please choose Outgoing traffic or Incoming traffic as the direction for filtering packets.

Click Add to add a new IP Filtering rule.

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

Allow Traffic :

Choose **No** to stop the data transmission, **Yes** to permit the data pass through.

Protocol :

Here provides 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 according to the necessity.

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.

The setting **All** means that all the IP addressed in the network are allowed or denied to pass through in Internet.

If you choose **Single**, you will have to key in the specific IP address as the start/end point to let the router identify for granting or denying passing through.

If you choose **Subnet**, you will have to enter the specific IP address and netmask as the start/end point to let the router identify for granting or denying passing through.

Port Range :

The port range is from 0 to 65535. Please key in the start point and end point for the IP Filtering.

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

Here provides an example shown in the right column. Select **TCP** as the Protocol type, and make the Source and Destination IP address to include **All**, then type **0** and **65535** as the start and end port.

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:



Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All
 pppoe_0_0_36/ppp0.1
 br0/br0

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

To add a new Inbound IP Filtering, click "Inbound traffic" in the item of Select the direction to filter packets on the IP Filtering page. Use the same way to add a new one as stated above.

Quality of Service

QoS (Quality of Service) is an industry-wide initiative to provide preferential treatment to certain subsets of data, enabling that data to traverse the Internet or intranet with higher quality transmission service.

There have been two generations of quality of service architectures in the Internet. The interpretation of the *Type of Service Octet* in the Internet Protocol header varies between these two generations.

The First generation: Precedence and type of service bits The refined definition of the initial *Type of Service Octet* looks like this :

2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
Precedence			Type of Service Field				

The Second generation: Differentiated services code point

The *Differentiated Service Code Point* is a selector for router's per-hop behaviors (PHB). As a selector, there is no implication that a numerically greater DSCP implies a better network service. RFC2474 redefined the *Type of Service Octet* to be :

2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
Differentiated Services Code Point						ECT	CE

The fields *ECT* and *CE* are nothing to do with quality of service. They are spare bits in the IP header used by Explicit Congestion Notification. As can be seen, the *DSCP* totally overlaps the old *Precedence* field. So if values of *DSCP* are carefully chosen then backward compatibility can be achieved. This leads to the notions of "class", each class being the group of DSCP with the same *Precedence* value. Values within a class would offer similar network services but with slight differences. Classes were initially defined as :

DSCP	Precedence	Purpose
0	0	Best effort
8	1	Class 1
16	2	Class 2
24	3	Class 3
32	4	Class 4
40	5	Express forwarding
48	6	Control
56	7	Control

Now, DSCP is what we are using for the QoS configuration on this device.

Among the classes you will see on the webpage, the **BE** (*Best Effort*) class possesses no guaranteed rates; the **CS** (*Class Selector*) values enable backward compatibility with the older IP-Precedence scheme ranges 0~7; the **EF** (*Expedited Forwarding*) class is a low-loss, low-latency, low-jitter, assured-bandwidth, end-to-end service; **AF** (*Assured Forwarding*) provides for the delivery of IP packets in four independently forwarded AF classes, AF1x through AF4x. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. This class is used when a service (application) requires a high probability of packets being forwarded, so long as the aggregate traffic from each site does not exceed the subscribed information rate (profile). Each of the four AF classes allocates a certain amount of forwarding resources, such as buffer space and bandwidth in each network node. When congestion occurs, the drop precedence of a packet determines the relative importance of the packet within the AF class.

You can start to configure the Bridge QoS/IP-QoS rules on the Quality of Service webpage for your IAD.

Quality of Service – QoS Setup

To classify the upstream traffic by assigning the transmission priority for different users' data, please use Bridge QoS to prioritize the data transmission.

The Bridge QoS allows you to set the settings based on layer two bridge packets.

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
 In PTM mode, maximum 8 queues can be configured.
 For each Ethernet interface, maximum 3 queues can be configured.
 To add a queue, click the **Add** button.
 To remove queues, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the queue after page reload.
 Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Shaping Rate(bits/s)	Burst Size(bytes)	Enable	Remove
WMM Voice Priority	1	wl0	1	1/SP					Enabled	
WMM Voice Priority	2	wl0	2	2/SP					Enabled	
WMM Video Priority	3	wl0	3	3/SP					Enabled	
WMM Video Priority	4	wl0	4	4/SP					Enabled	
WMM Best Effort	5	wl0	5	5/SP					Enabled	
WMM Background	6	wl0	6	6/SP					Enabled	
WMM Background	7	wl0	7	7/SP					Enabled	
WMM Best Effort	8	wl0	8	8/SP					Enabled	
Default Queue	37	atm0	1	8/WRR/1	Path0				<input type="checkbox"/>	

QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)
- The precedence list shows the scheduler algorithm for each precedence level.
- Queues of equal precedence will be scheduled based on the algorithm.
- Queues of unequal precedence will be scheduled based on SP.

Queue Scheduler
 Weighted Round Robin
 Weighted Fair Queuing

Queue Weight: [1-63]

DSL Latency:

Traffic Class Name :

Key in a name as the traffic class for identification.

802.1p Priority :

Each incoming packet will be mapped to a specific priority level, so that these levels may be acted on individually to deliver traffic differentiation. Please choose the number (from 0 to 7, low to high priority) for the 02.1p Priority.

DiffServ Class (DSCP):	No Change
	No Change
	BE - 0x00
	AF13 - 0x38
	AF12 - 0x28
	AF11 - 0x24
	CS1 - 0x20
	AF23 - 0x58
	AF22 - 0x48
	AF21 - 0x44
	CS2 - 0x40
	AF33 - 0x78
	AF32 - 0x68
	AF31 - 0x64
	CS3 - 0x60
	AF43 - 0x98
	AF42 - 0x88
	AF41 - 0x84
	CS4 - 0x80
	EF - 0xB8
	CS5 - 0xA0
	CS6 - 0xCD
	CS7 - 0xED

DiffServ Class (DSCP) :

DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing QoS (quality of service) guarantees on modern IP networks. DiffServ can, for example, be used to provide low-latency, guaranteed service to critical network traffic such as voice or video while providing simple best-effort traffic guarantees to non-critical services such as web traffic or file transfers.

The higher position the item appears, the smaller DSCP value it is (i.e., *BE* is the lowest while *CS7* is the highest). The corresponding DSCP value in the IP header of the upstream packets will be overwritten by the selected value. The default setting is *No change*.

WAN 802.1p:	No Change ▾
	No Change
	0
	1
	2
	3
	4
	5
	6
	7

WAN 802.1p:

If 802.1p is enabled on Internet connection, WAN 802.1p value of the upstream packets can be overwritten by the selected value. You may select a priority from the drop-down menu.

If you set the LAN 802.1p Priority 0 as the traffic condition, choose *Low* traffic priority for this rule, set DSCP as BE, and WAN 802.1p as *no change*, after clicking Apply, you will get the result as the figure in the right column. Thus when the users' data matches the traffic condition, the transmission will get a low traffic priority.

You may check the Delete box and press Delete to discard it, or click Add to create more.

Quality of Service – QoS Classification Setup

To classify the upstream traffic by assigning the transmission priority of the data for different users, please use IP QoS to prioritize the data transmission.

QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.
 To remove rules, check their remove-checkboxes, then click the **Remove** button.
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

CLASSIFICATION CRITERIA													CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Rate Limit (kpbs)	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																		

The IP QoS allows you to set the settings based on layer three IP packets.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:

Ether Type:

Source MAC Address:

Source IP Address[/Mask]:

Destination IP Address[/Mask]:

Differentiated Service Code Point (DSCP) Check:

Protocol:

Specify Classification Results (A blank value indicates no operation)

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Set Rate Limit: [Kbits/s]

To add a new IP QoS setting, press **Add** in the page of Quality of Service – IP QoS, a page same as the right side will appear.

Traffic Class Name :

Type a name as the traffic class for identification.

LAN Ports which traffic come from :

The IP QoS rules will be applied on the LAN ports you checked here. The default setting includes all ports.

Source MAC Address & MAC Mask/ Destination MAC Address & MAC Mask :
 Key in the specific MAC Address or MAC Mask of the devices which you want the QoS rule to be applied to, or simply leave it blank to include all.

Protocol:	TCP/UDP ▼
	TCP/UDP
	TCP
	UDP
	ICMP

Protocol :

Choose a proper interface for this function. If you don't know how to select, simply use the default one.

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)	
Class Interface:	LAN ▼
Ether Type:	▼
Source MAC Address:	<input type="text"/>
Source MAC Mask:	<input type="text"/>
Destination MAC Address:	<input type="text"/>
Destination MAC Mask:	<input type="text"/>

Source IP/ Subnet Mask/ Port :

Key in the source IP address (ex.: 192.168.1.0) and subnet mask (ex.: 255.255.255.0) for the application (ex.: FTP, HTTP, and so on) that you want to invoke the QoS traffic rule. You may simply enter the source port, ranging from 0 to 65535, as the traffic condition.

Destination IP/ Subnet Mask/ Port :

Enter the destination IP address (ex.: 168.95.1.88) and subnet mask (ex.:255.255.255.0) for the application that you want to invoke the QoS traffic rule. Or simply enter the destination port for the traffic condition; it ranges from 1 to 65535.

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required): ▼
 - Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP): ▼

Mark 802.1p priority: ▼
 - Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

Traffic Priority/ DiffServ Class (DSCP)/ WAN 802.1p :

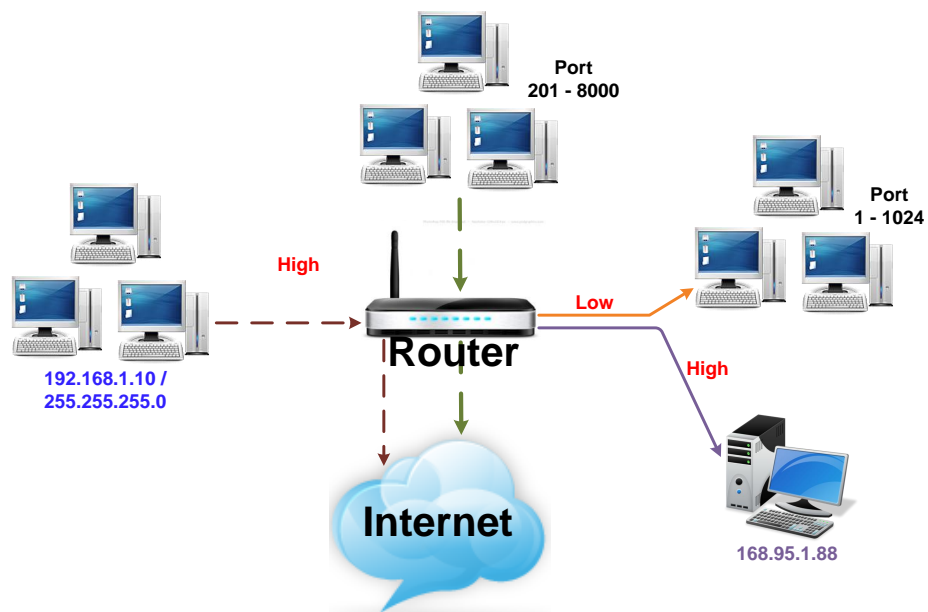
Please refer to the Bridge QoS section.

After finishing the settings, click Apply, the new QoS setting will be shown as the example.

According to the example, we set four rules for IP QoS. In traffic *A*, we set the destination port as *1-1024*, and the traffic priority is *low*; in traffic *B*, the source port is from *201 to 8000*, and the priority is *medium*; in traffic *C*, when the source IP is *192.168.1.0*, subnet mask is *255.255.255.0*, the traffic priority is *high*; in traffic *D*, when the traffic is heading to *168.95.1.88*, the priority is *high*.

To delete the rules you set, simply click the check button below Delete item and click Delete button.

According to our example, the IP QoS configuration can be illustrated by the following figure.



While there are many PCs getting online, the PCs using *port 201-8000* to access the internet will have medium traffic priority, the PCs carrying *192.168.1.x/ 255.255.255.0* as IP address will have high traffic priority. In addition, PCs heading to *port 1-1024* will have a low priority, while the PCs accessing *168.95.1.88* will have a high priority.

Interface Group

This page allows you to configure various *port mapping groups* which contains specific Internet connections and LAN ports. The user data will be only transmitted and received among the interfaces in the group.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	eth0.0	
			eth1.0	
			eth2.0	
			eth3.0	
			wlan0	

Add Remove

Virtual LAN Function on Ethernet :

If you click Disabled, the LAN ports for Ethernet ports will only be shown as an Ethernet interface.

After applying Enabled, the LAN ports will be viewed as four separated ports shown on the status chart like the second figure.

Normally, this function only needed when more than two PVCs are available, for example, if we have two PVCs, one uses PPPoE and the other uses Bridge mode, we may want to group certain connection to a specific port, especially when some devices may consume higher bandwidth.

In our following demonstration, we set up one more Internet connection in bridge mode; so we will have two PVCs: *pppoe_0_39_1* and *br_0_35*.

Click Add to create a new port mapping group.

Group Name :

Give a unique name here. The word length must not be over the length of the field. In our example, "*bridge*".

Available Interfaces :

The available interfaces (such as Ethernet1-4, wireless, etc.) will be displayed in the left side box. Choose one from them and click Add, the item will be transferred into the Grouped Interfaces box at the right side. You can click Remove to return the item back to the Default group (left side box).

When the setting is done, click Apply.

4. Click Apply/Save button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces

eth0.0
eth2.0
vlan0

Available LAN Interfaces

eth1.0
eth2.0
wl0_Crest1
wl0_Crest2
wl0_Crest3

Navigation buttons: > <

Now we are going to map Wireless and the first Ethernet port together with the bridge mode PVC. Click *br_0_35* and press Add button, then use the same way to add Wireless, and Ethernet1 to grouped interfaces. The four items are moved to the right box now.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

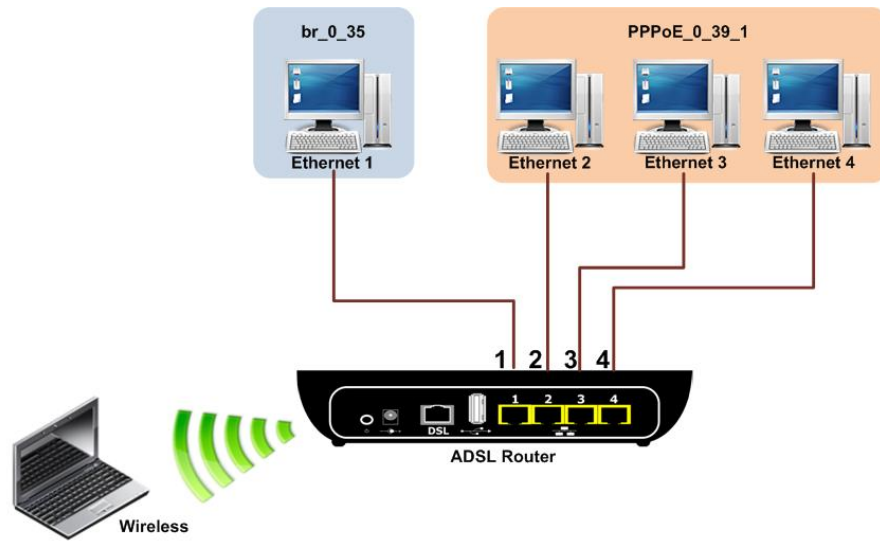
Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			eth2.0	
			eth3.0	
Internet	<input type="checkbox"/>	ppp0.1	eth0.0	
			eth1.0	
			vlan0	

Buttons: Add Remove

Now we can check the result of the port mapping configuration. We have a default group, in which PPPoE mode will be applied through Ethernet port 2, 3, and 4, and we have another group named bridge, in which the bridge mode will be applied on Wireless and Ethernet port1.

You may click  to edit the created group, press  to delete it, or click Add to create another group.

The following relationship figure illustrates the port mapping configuration.



Under this configuration, any devices that is connected to Wireless or Ethernet port 1 will connect to the internet through the bridge mode PVC `br_0_35`, while the PCs using Ethernet port 2, 3, and 4 will access the internet by the PPPoE connection `pppoe_0_39_1`.

Wireless

This page allows you to configure the wireless function on you IAD. You may setup the settings for security, access control, and repeater features for the device.

Basic Settings

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

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless network (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Max Clients:

Enable Wireless Network :

Click this check box to enable the wireless network function.

Wireless Main/Guest Network Name (SSID) :

This device supports multiple wireless networks. The system will detect the Main SSID of your router and displayed in this field for your reference.

SSID:

BSSID: 00:26:B2:DA:94:52

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wlo_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wlo_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wlo_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

The SSID is the identification characters of a router. The default words will be shown on this page. If you do not check “Hidden SSID” 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 note that if you want to communicate, all wireless clients should use the same SSID with the router or access point.

Two SSIDs are supported. One SSID can be used for main wireless network and the other SSID can be used for guest wireless network. Two wireless networks can be configured in different wireless security level.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 10:10:10:20:20:21

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:							
Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input checked="" type="checkbox"/>	wl0_Guest1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A
<input checked="" type="checkbox"/>	wl0_Guest2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A
<input checked="" type="checkbox"/>	wl0_Guest3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A

Apply/Save

Hide Wireless Main/Guest Network :

Check the box to hide the Main/Guest SSID of this AP (access point). Thus, other people in the network cannot find the Main/Guest SSID of this device.

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on wh fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon inte preambles are used.

Click "Apply/Save" to configure the advanced wireless options.

Band:	2.4GHz	
Channel:	1	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	Auto	
802.11n/EWC:	1	
Bandwidth:	2	Current: 20MHz
Control Sideband:	3	Current: N/A
802.11n Rate:	4	
802.11n Protection:	5	
Support 802.11n Client Only:	6	
RIFS Advertisement:	7	
OBSS Coexistence:	8	
RX Chain Power Save:	9	Power Save status: Full Power
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	

Channel :

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

The administrator of network has to search available channels and assign one as the communication channel. All the other clients that match the SSID and pass security authentication can access this device and will use the same channel set here.

802.11n/EWC:	Auto	
Bandwidth:	20MHz	Current: 20MHz
Control Sideband:	20MHz	Current: N/A
802.11n Rate:	40MHz	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	

Transmission Mode :

It decides the mode of data transmission. Choose the one that you want to use from the drop-down menu. There are 11n default but mixed 802.11b and 11g provided here.

Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz	Current: 20MHz
Control Sideband:	Lower	Current: N/A
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Use 54g Rate	
RIFS Advertisement:	0: 6.5 Mbps	
OBSS Coexistence:	1: 13 Mbps	
RX Chain Power Save:	2: 19.5 Mbps	
RX Chain Power Save Quiet Time:	3: 26 Mbps	
RX Chain Power Save PPS:	4: 39 Mbps	Power Save status: Full Power
54g™ Rate:	5: 52 Mbps	
Multicast Rate:	6: 58.5 Mbps	
Basic Rate:	7: 65 Mbps	
Fragmentation Threshold:	8: 13 Mbps	
RTS Threshold:	9: 26 Mbps	
	10: 39 Mbps	
	11: 52 Mbps	
	12: 78 Mbps	
	13: 104 Mbps	
	14: 117 Mbps	
	15: 130 Mbps	

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 transmission mode that you set above. The transmission rate settings under 802.11n:

Multicast Rate:	Auto
-----------------	------

Multicast Rate :

When the multicast transmitting traffics are large, the transmission will be delayed in some way. If you want to speed up the rate, modify from the drop-down list.

For example, you may select *802.11g only* as the transmission mode, and select high multicast rate like *54 Mbps*.

<input checked="" type="checkbox"/>	Clients Isolation						
<input type="checkbox"/>	Disable WMM Advertise						
<input type="checkbox"/>	Enable Wireless Multicast Forwarding (WMF)						
SSID:	<input type="text" value="RTV1805VW"/>						
BSSID:	<input type="text" value="10:10:10:20:20:21"/>						
Country:	<input type="text" value="UNITED STATES"/>						
Max Clients:	<input type="text" value="16"/>						
Wireless - Guest/Virtual Access Points:							
Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input checked="" type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input checked="" type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input checked="" type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="button" value="Apply/Save"/>							

Wireless User Isolation :

To make the communication between the clients, please choose Off. To cut the communication between the clients, please choose on.

Click Apply to invoke the settings.

Security

To configure security features for the Wireless interface, please open Security item from Wireless menu. This web page offers eight authentication protocols for you to secure your data while connecting to networks. There are nine selections including Wireless Protected Setup (WPS), 64-bit and 128-bit WEP, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, mixed WPA2/WPA, and mixed WPA2/WPA-PSK. Different item leads to different web page settings. Please read the following information carefully.

Select Wireless Network :

Select the wireless network which you want to configure the security settings from the drop down list.

WPS Security :

The Disabled item offers you the protection for wireless communication. By Manual Setup AP if you choose Disabled, the Encryption Keys will not be shown on this page.

There are nine wireless security modes for you to select.

For 64-Bit WEP/ 128-Bit WEP



Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Wireless Security :

Select the WEP mode for the security function; there are two options, 64-bit and 128-bit. Before being transmitted, the data will be encrypted using the encryption key. For example, if you set 64-bit in this field, then the receiving station must be set to use 64 Bit Encryption, and have the same Key value at the same time; otherwise, it will not be able to decrypt the data.

Authentication Type:

Open System
Open System
Shared Key

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 be attacked by 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.

WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	1
Network Key 1:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Format :

Choose the form of encryption key. You have to select either Hexadecimal digits or ASCII characters and type the keys on the fields of Key 1 to Key 4.

Key 1 to 4 :

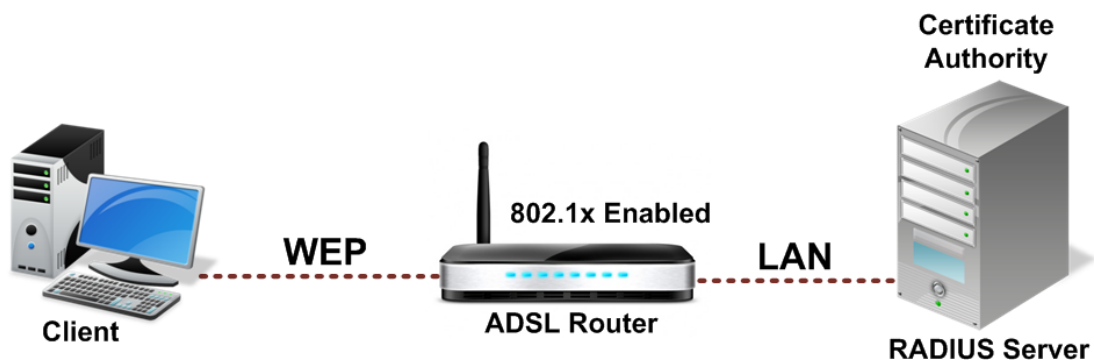
Fill out the WEP keys according to the key length. For 64-bit WEP mode, the content you can type is 5 characters or 10 hexadecimal digits; for 128-bit WEP, the content you can type is 13 characters or 26 hexadecimal digits.

Default Transmission Key :

Select one of the network keys as the default one.

Click Apply for activation when the settings are done.

For 802.1X Wireless Network



When a wireless client requests to access 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 those unauthorized will be blocked.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA2 Preauthentication:

Network Re-auth Interval:

WPA Group Rekey Interval:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WPA/WAPI Encryption:

WEP Encryption:

Wireless Security :

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 enter the IP Address for the RADIUS Server.

RADIUS UDP Port :

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 Shared Secret :

A shared 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. Enter the words for the share secret.

After finishing the settings, click Apply for activation.

Example for 802.1x environment Configuration

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

- ◆ **Windows 2000/2003/NT Server :** RADIUS server equipped with “Internet Authentication Service”. Certificate Services installed.
- ◆ **AP (Router) :** Connected to Windows 2000 Advanced Server through the LAN port with DHCP server and 802.1x enabled.
- ◆ **802.1x client :** a WLAN card supporting WEP.
- ◆ **Authentication Mechanism.**

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

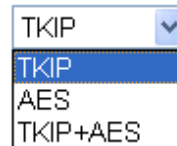
WPA/WAPI Encryption:

WEP Encryption:

For WPA (Wi-Fi Protected Access)

The WPA (Wi-Fi - Protected Access) authentication 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 provide stronger encryption and authentication solution than none WPA modes.

Data Encryption:



TKIP
TKIP
AES
TKIP+AES

Data Encryption :

Select the data encryption method for the WPA mode. There are three types that you can choose, TKIP, AES, TKIP+AES.

TKIP (Temporary Key Integrity Protocol) 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 never be used twice.

AES (Advanced Encryption Standard) 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 combine the features and functions of TKIP and AES.

WPA Group Rekey Interval :

Enter the time for the WPA group rekey interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced.

RADIUS Server IP Address, RADIUS UDP Port, and RADIUS Shared Secret :

Please refer to the elucidation in the previous 802.1x section.

After finishing the settings, click Apply for activation.

For WPA-PSK; WPA2-PSK; Mixed WPA2/WPA-PSK

WPA-PSK (WPA-Pre-Shared Key) is useful for small places without authentication servers such as the network at home. It allows the use of manually-entered keys or passwords and is designed to be easily set up for home users.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

Data Encryption :

Select the encryption type for the WPA mode. There are three types that you can choose, TKIP, AES, TKIP+AES. (For more information please refer to WPA section.)

Format :

Choose the form of encryption key. You have to select either Hexadecimal digits or ASCII characters and type the keys on the fields of Pre-Share Key.

Pre-Share Key :

Please enter the key 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 :

Enter the time for the WAP group rekey interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced.

After finished settings, click Apply for activation.

For WPA2; Mixed WPA2/WPA

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA2 Preauthentication:

Network Re-auth Interval:

WPA Group Rekey Interval:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WPA/WAPI Encryption:

WEP Encryption:

Wireless Security :

The WPA2 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 provide stronger encryption and authentication solution than other WPA mode.

Data Encryption :

Select the encryption type for the WPA2 mode. There are three types that you can choose, TKIP, AES, TKIP+AES. (For detailed information please refer to WPA section.)

WPA2 Pre-authentication :

The wireless client that has associated with one AP (router A) can do the authentication with another AP (router B) in advance. If the client roams to AP (B), it can associate with AP (B) quickly. Please click enabled to activate this function.

Network Re-auth Interval :

When a wireless client has associated with the AP for a period of time longer than the setting here, it would be disconnected and the authentication will be executed again. The default value is 36000, you may modify it.

WPA Group Rekey Interval :

Enter the time for the WPA group rekey interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced.

RADIUS Server IP Address, RADIUS UDP Port, and RADIUS Shared Secret:

Please refer to the elucidation in the previous 802.1x section.

When the settings are finished, click Apply for activation

Accesses Control

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

Wireless -- MAC Filter

Select SSID: RTV1805VW

MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address Remove

Add Remove

Access Control :

Click Off to disable this function. Click On in Allow mode to allow the devices using matched MAC address to link to the AP. And click On in Deny mode to disturb the listed wireless MAC address to access the AP.

View Access Control List :

Click this button to view the wireless access control list and to add a new MAC address.

Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address: 00:10:18:22:23:24

Apply/Save

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

To add a new MAC address to your wireless MAC address filter, click on the Add button

Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address: 00:10:18:22:23:24

Apply/Save


MAC Address of Wireless adaptor :


Key in the MAC Address to be filtered. And click Apply.

Wireless -- MAC Filter

Select SSID: RTV1805VW

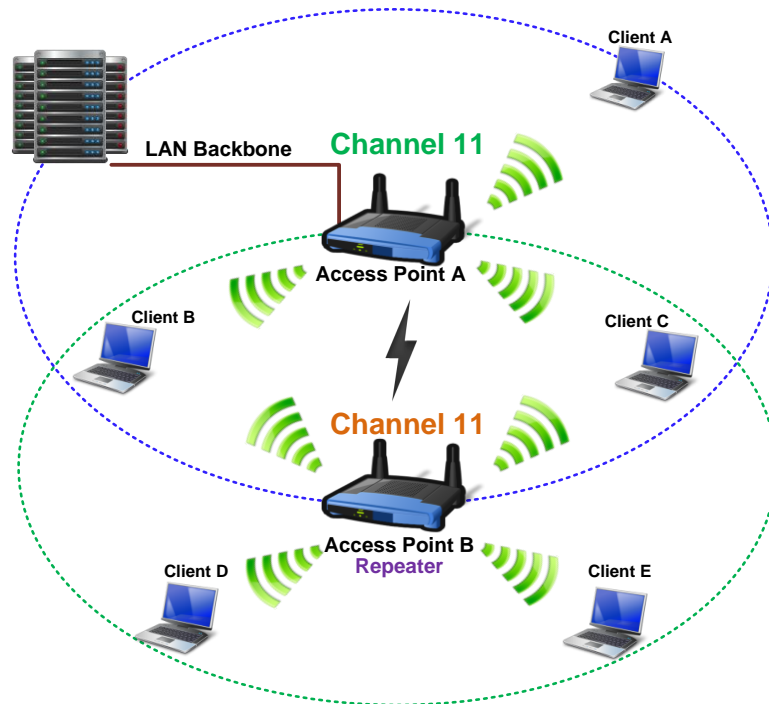
MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address	Remove
00:10:18:22:23:24	

The result of the added MAC address will be shown on the table. If you want to delete the added MAC address, simply click the delete button  , a dialog box will be prompted to confirm the deleting. Click Yes, and then the selected one will be erased.

Repeater

A repeater is an **electronic** device that **receives** a weak or low-level **signal** and **retransmits** it at a higher level or higher power, so that the signal can cover longer distances without degradation.



The example figure illustrates the relationship among the repeaters and the clients. In this example, client A, B, and C can access AP-A, but client D and E cannot? In this case, AP-B extends the coverage area of AP-A, thus allows client D and E to receive the signal smoothly.

The web page allows you to configure the wireless distribution system for the wireless network.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(S) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

AP Mode :

Choose an AP mode that you would like to use.

Search Other Repeaters :

You can configure other routers as your repeater by setting up repeater feature mutually. Click the Scan now button to search other repeater in the wireless network automatically. The result will be shown on the chart.

Note :

To configure the repeater function among routers, they must use the same channel, SSID and WEP key, so that they may work as repeaters for each other.

If you select Manual for Search Other Repeaters, you will need to type the MAC address for wireless repeaters in the boxes of MAC Address of Remote Wireless Repeaters.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution access point functionality). Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enable enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	LITEONIT	02:24:D6:00:06:00
<input type="checkbox"/>	HQ-Staff	00:1E:4A:E5:1C:E0
<input type="checkbox"/>	ASKRD-9F	00:30:BD:F6:FF:75
<input type="checkbox"/>	Askey-MIS2	00:1B:9E:65:AD:D9
<input type="checkbox"/>	ASKEY-10F	00:30:BD:F6:FB:47

The right figure shows an example result of executing the function of auto-searching repeaters.

You may select the routers (which use the same channel as yours) from the table and configure the same SSID and WEP key with the one you chose, so that the routers can function as repeaters for each other to extend the coverage area.

When you finish the settings, please click Apply to invoke them.

Wireless QoS

In the fields of wireless packet-switched networks and wireless networking, the Wireless QoS (Quality of Service) refers to control mechanisms that can provide different priority to different users or data flows for wireless networks, or guarantee a certain level of performance to a data flow transmitted through the wireless interface in accordance with requests from the application program. QoS guarantees are important if the network capacity is limited, especially for real-time streaming multimedia applications, for example voice over IP and IP-TV, since these often require fixed bit rate and may be delay-sensitive.

Wireless QoS is also referred to as Wi-Fi Multimedia (WMM), which is a subset of 802.11e developed by Wi-Fi Alliance. WMM prioritizes traffic according to 4 AC (Access Categories) - Voice, Video, Best Effort, and Background. However, it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi VoIP phone.

Access Categories (AC)

Voice Priority	Highest priority Allows multiple concurrent VoIP calls, with low latency and toll voice quality	7, 6
Video Priority	Prioritize video traffic above other data traffic	5, 4
Best Effort Priority	Traffic less sensitive to latency, but affected by long delays, such as Internet surfing. Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities	3, 0
Background Priority	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements	2, 1

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure wireless QoS on the device, you can select specific network traffic and prioritize it to provide preferential treatment. Implementing QoS on your WLAN makes network performance more predictable and bandwidth utilization more effective.

The Wireless QoS web configuration page allows you to classify wireless traffic by assigning the transmission priority for various user data.

WMM(Wi-Fi Multimedia):	Enabled ▾
WMM No Acknowledgement:	Disabled ▾
WMM APSD:	Enabled ▾

Wi-Fi Multimedia Function :

Wireless QoS is enabled by default.

To experience the full benefit of the WMM function, both the IAD and the client device must support WMM.

USB App

Storage Service

This device provides the **USB Storage** function. Connect your storage device to the **USB host port** on the rear panel of this IAD.

Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volumename	FileSystem	Total Space	Used Space
usb1_1	ntfs	76316	53827

Management

Diagnostics

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

Diagnostic Tests

This ADSL router is capable of testing your ADSL connection.

Select the Internet Connection:

Press **“Run Diagnostic Tests”** on the Diagnostic Tests page.

pppoe_0_0_36 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your eth2 Connection:	PASS	Help
Test your eth3 Connection:	FAIL	Help
Test your eth0 Connection:	FAIL	Help
Test your eth1 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

Test the connection to your Internet service provider

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

The Result would be shown on the same page.

For the item which passes through the diagnostics, a **“PASS”** will be displayed on the right side of that item.

If not, a **“FAIL”** will be presented there.

If there is no device using that port, a **“DOWN”** will be displayed.

Press the Help link to know what the result (Pass, Fail) represents for.

Management Accounts

This page allows you to change the user name and password for accessing your wireless IAD.

Access Control -- Passwords

Access to your broadband router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.

The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

User Name:

Old Password:

New Password:

Confirm Password:

For the Admin Account, the default setting for both username and password are admin. If you want to change the username and the password, please modify the User Name and New Password, and then retype the new password in the Confirm field for confirmation. Then click Apply.

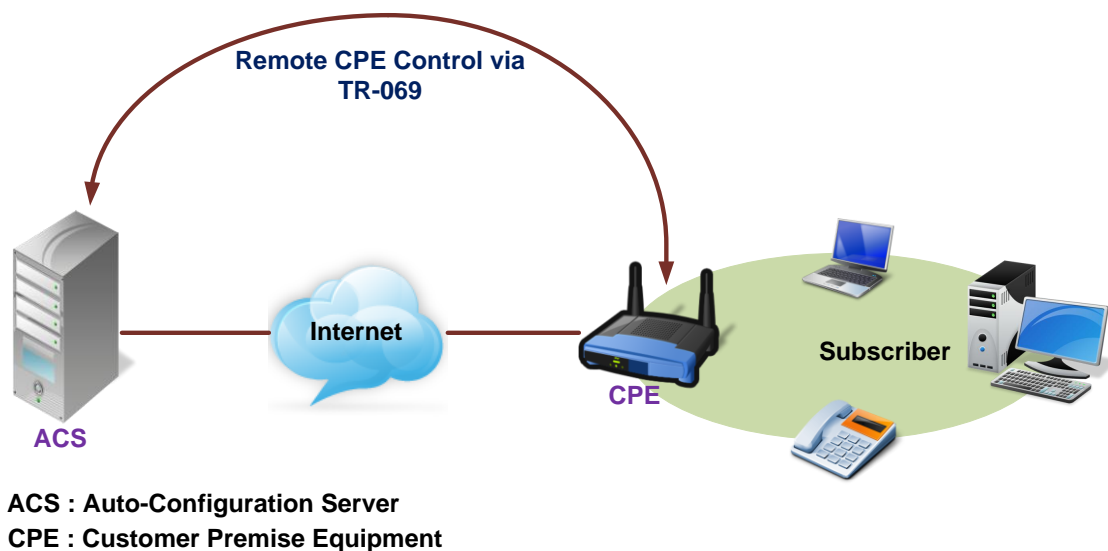
To create a user account, you may setup a username and password under User Account on the same page.

Note that the new user can merely access the Quick Start and Status page.

TR-069 Client Configuration

TR-069 is a CPE WAN Management Protocol (CWMP) intended for communication between Customer Premise Equipment (CPE) and an Auto-Configuration Server (ACS). It defines a mechanism that encompasses secure auto configuration of a CPE, and also incorporates other CPE management functions into an integrated framework.

Using TR-069 the CPE can get in contact with the ACS and establish the configuration automatically. Accordingly other service functions can be provided. TR-069 is the current standard for activation of CPE in the range of DSL broadband market.



Compliant with DSL's Forum's TR-069 Remote Management Specification, the wireless IAD is highly manageable with the default ACS for auto-configuration, dynamic service provisioning, firmware updates, status and performance monitoring, and diagnostics to a collection of routers. By these provision value-added services, the wireless IAD with TR-069 helps DSL service provider reduce operation effort as well as enhance customer satisfaction.

Normally, users do not have to modify the settings here. If you do not know how to set up, you can just accept the factory default settings on this page or contact your ISP.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

Connect to ACS :

Choose to connect to ACS with or without SSL (Secure Socket Layer) protocol according to your ISP.

If the ACS URL starts with `http://`, choose *without SSL* mode; if it begins with `https://`, select *with SSL*.

ACS URL Address :

Key in the Auto-Configuration Server URL Address provided by the ISP, e.g., <http://10.22.1.110:8082/askey/ACSServer> without SSL or <http://10.22.1.110:8082/askey/ACSServer> with SSL.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

ACS User Name/ ACS Password :

When connecting to ACS, this device must have correct user name and password for authentication. Key in the information provided by the ISP.

When the content of ACS URL Address, User Name, and Password match the ACS authorization, the router will send an online report to ACS.

Connection Request User Name/Password :

If the ACS wants to communicate with the device, it will have to offer the matching Connection Request User Name and Password. When the device sends the report to ACS for the first time, it will contain information for this.

Inform Disable Enable

Inform Interval:

Periodic Transmission of Inform Request :

If this function is enabled, the CPE will frequently report to ACS the status after a period of time set here. The default setting is 300 seconds, and the ISP can modify the value. Generally, users do not have to change the settings here.

If this function is disabled, the CPE will only report once when the connection between ACS and the device has been set up.

Identify the Validation of Certificate from ACS

When using SSL protocol to connect to ACS, a trusted CA and synchronic time setting with the server are used to identify the validation of the Certificate sent from ACS.

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
------	--------	---------	------	--------

When choosing with SSL for Connect to ACS, you will see a paragraph appear on the bottom of the window (as shown in the right column).

Press Import Certificate to Import Certificate obtained from your ISP, a window (as shown in the figure) will be prompted for you to import certificate.

Note :

The certificate may have been imported in this device already, please check with your ISP.

To synchronize your time with the server, go to Management->Internet Time to adjust the setting. Configure to set time by Time Server, and make sure the time zone is the same as the server's.

(Please refer to the next section for detailed information about Internet Time.)

Internet Time

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

Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Third NTP time server:

Fourth NTP time server:

Fifth NTP time server:

Time zone offset:

Update Now :

Click this button to refresh the current time.

Set Time by (Time Server or Manual) :

The default setting is Manual. Select this one, and set the start time by typing the date and the time manually to help the router perform tasks. If you select Time Server, the system will set time automatically.

Primary Time Server/ Secondary Time Server :

You may select the preferred time server from the drop-down list. The time will be adjusted by the time server.

Time Zone :

Choose the time zone of your location.

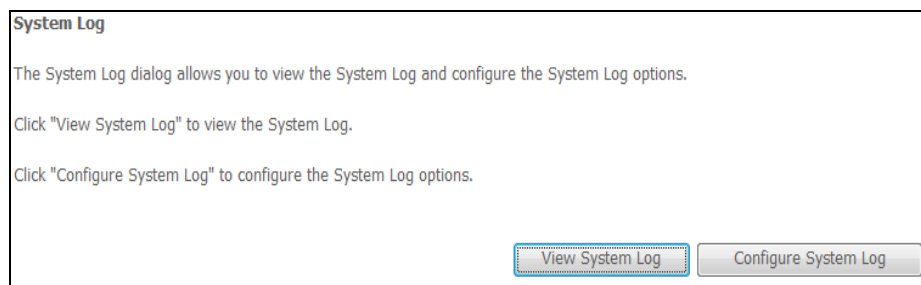
Apply :

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

Cancel :

Discard the new configuration and reserve the original settings.

System Log



System Log

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

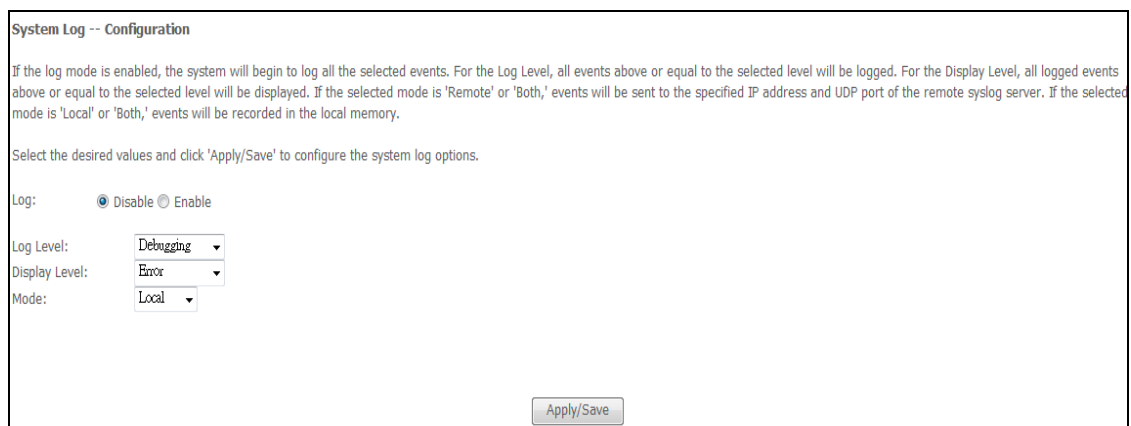
Click "View System Log" to view the System Log.

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

[View System Log](#) [Configure System Log](#)

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

To view the system log, you must configure system log first. Press **Configure System Log to start.**



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

Mode:

[Apply/Save](#)

Configuring System Log

You can enable or disable the log function, and choose log level, display level and proper mode as you like. Then click **Apply to invoke the settings or press **Cancel** to discard them.**

Log: Disable Enable

Log Level: Debugging

Display Level: Emergency

Mode:

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

There are 8 types of log level and display level for you to choose.

Log Level :

This function enables you to decide how detailed the messages will be stored. Set a proper level according to your needs. The default Log Level is Debugging.

The Debugging Level logs all messages to the file, while the Emergency Level logs fatal messages only. The lower the item is, the more detailed information it provides; i.e., *debugging* level stores the most detailed information.

Owing to the limitation of the storage on the ADSL router, the former information will be erased and replaced by the latest message automatically when the buffer is overflowed.

Display Level: Error

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

Display Level :

For the convenience of the users, the display level can function as a filter. It decides the level for the messages to exhibit when the user wants to view the logs on the local side. For example, for a programmer or engineer, he/she may want to know about *debugging* or *informational* level message; for general users, they may only need or want to learn about *error*, *critical*, *alert*, or *emergency* messages only. The default Display Level is Error.

Therefore, when the log level is “Debugging” and the display level is “Error”, the CPE logs the most detailed message but shows error level data only.

Mode:	Local
	Local
	Remote
	Both

Mode :

You can choose where to store the logs; the options include **Local**, **Remote** and **Both**. *Local* means the CPE, i.e., the ADSL Router. *Remote* means the log server you specified to forward the log information to. The default mode is **Local**.

Log Level:	Debugging
Display Level:	Error
Mode:	Remote
Server IP Address:	0.0.0.0
Server UDP Port:	514

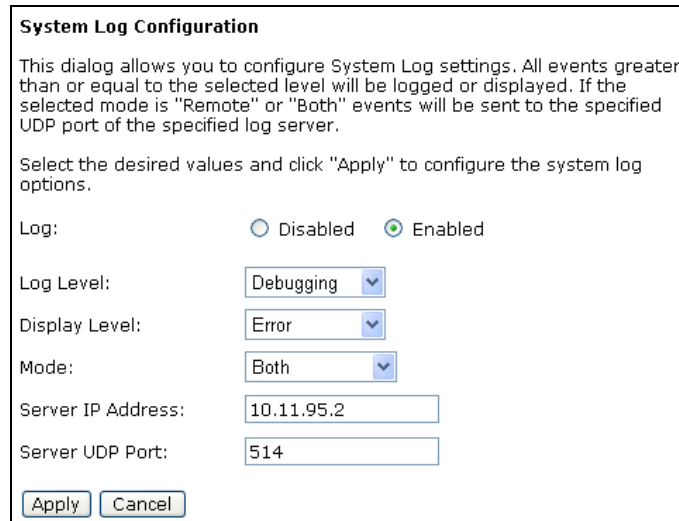
If you choose **Remote** or **Both**, you have to specify the **Server IP Address** and **UDP Port**, and all the events will be sent to the specified UDP port of the specified log server.

Note :

Display Level only filters for the *local* side. All the messages will be displayed on the remote Log Server.

Example

Suppose we are going to record the system logs on both the ADSL Router and the Server bearing IP address **10.11.95.2**, the procedures below illustrate the situation:



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:

Server IP Address:

Server UDP Port:

1. **Choose Enabled Log.**
2. **Select *Debugging* as the Log Level, and *Error* as the Display Level. (Or select other level according to your needs.)**
3. **Set the Mode as *Both*, key in the Server IP Address as *10.11.95.2*, and leave the Server UDP Port as the default value *514*.**
4. **Press Apply to invoke the settings.**

Backup Configuration

Backup Configuration

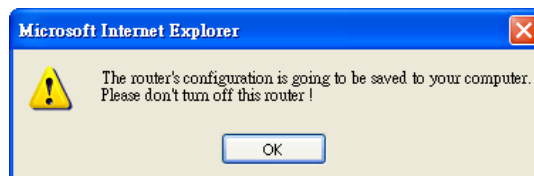
Use to save your ADSL router's current settings into the computer.

Restore Configuration

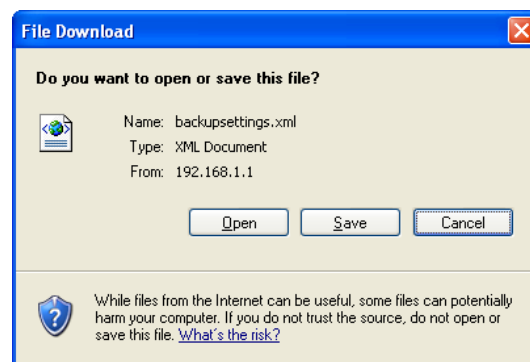
Use to reset your ADSL router with settings previously saved on the computer.

Backup File:

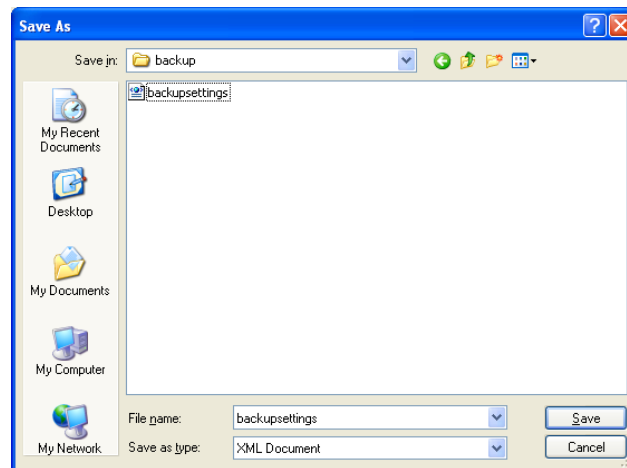
To backup your settings of the wireless IAD, you can use Backup Config web page to save the configuration.



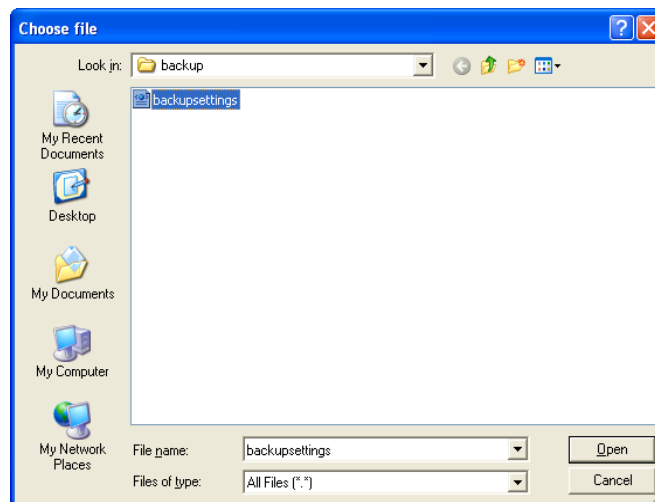
Click Backup button and the warning window will be prompted. Click OK to continue the backup procedure.



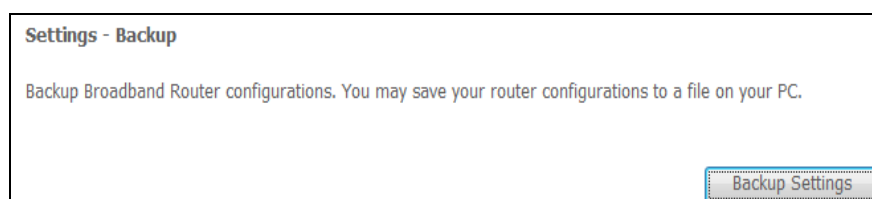
The system will ask your command about the next procedure. Click **Save** to backup.



You may change the file name and choose a place to save the backup file.



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



After opening the backup file, click Restore.

Update Firmware

Update Firmware

Warning: DO NOT turn off your router during firmware updates.

Current Firmware Version: 3.61k

New Firmware File Name:

The update process takes about 2 minutes to complete, then your ADSL router will reboot.

If you have to or want to upgrade the firmware for this IAD, you can open the Update Firmware web page and choose the correct file by pressing Browse. Then click the Update Firmware button.

Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

The system will execute the update procedure automatically.

Note: The IAD must not turn off during firmware updates.

When it is finished, the system will tell you the update is successfully.

Reset Router

Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

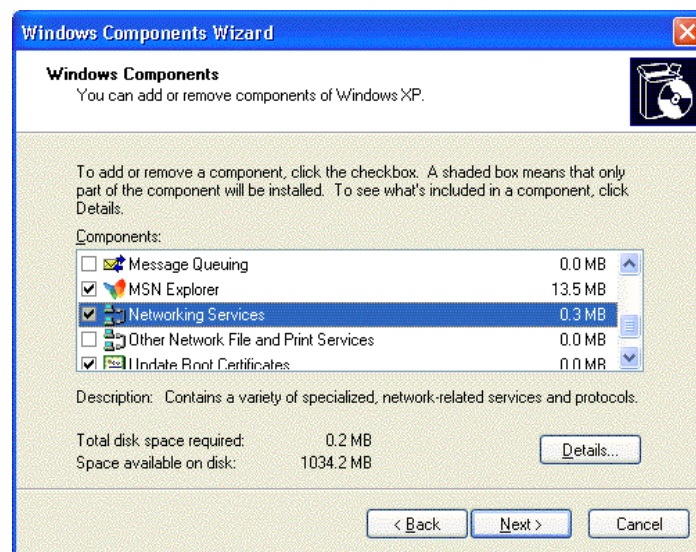
You can restore your web pages with default settings. Simply check Reset to factory default settings and click Reboot.

UPnP for XP

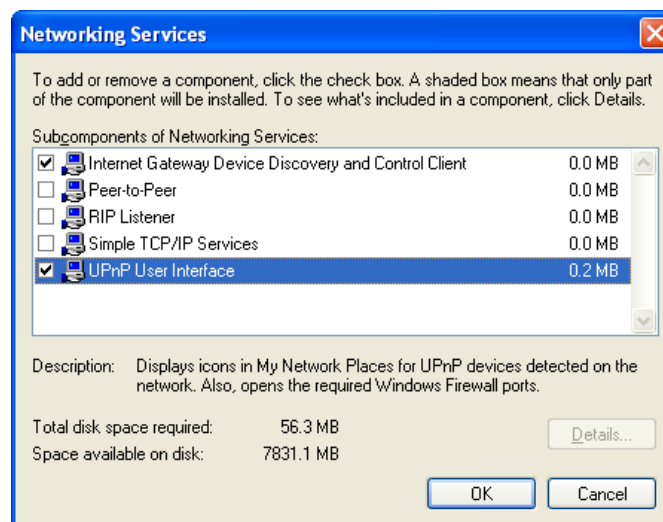
Universal plug and play (UPnP) is architecture for pervasive peer to peer network connectivity of intelligent appliances and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public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

Only **Windows XP** supports UPnP function.

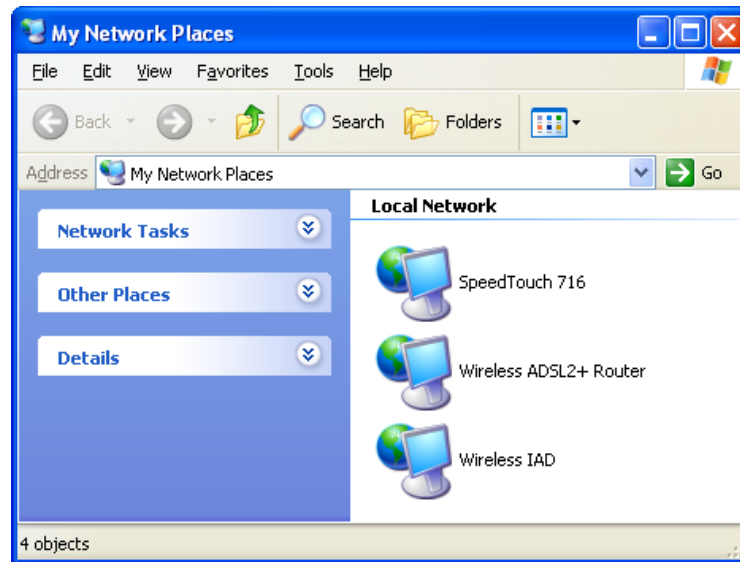
Please follow the steps below for installing UPnP components



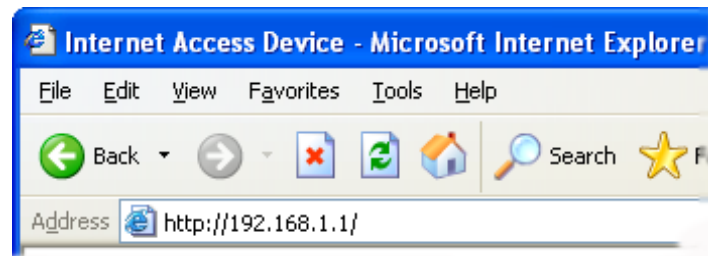
1. Click on the Start menu, point to Settings and click on Control Panel.
2. Select Add or Remove Programs > Add/Remove Windows Components to open Windows Components Wizard dialog box.



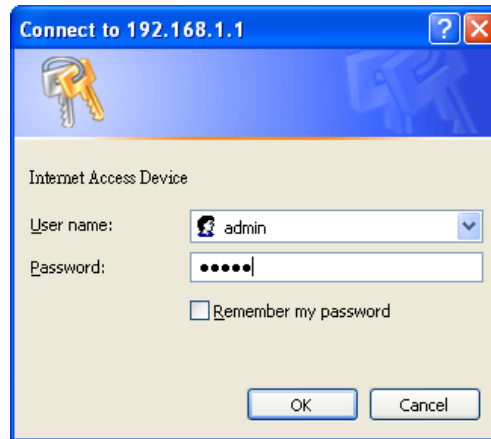
3. Select **Networking Services** and click **Details**. Click the **UPnP User Interface** check box.
4. Click **Ok**. The system will install UPnP components automatically.



5. After finishing the installation, go to **My Network Places**. You will find an icon (e.g., **Wireless IAD**) for UPnP function.



6. Double click on the icon, and the IAD will open a web page via the port for UPnP function. The IE address will be directed to the IP address for the configuration main page as shown in the graphic.



7. **After entering the user name and password, you may access the IAD through the webpage.**
8. **Now, the NAT traversal function has already been provided. The ADSL router will create a new virtual server automatically when the router detects that some internet applications is running on the PC.**

Chapter 5 : 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 does 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.

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 addresses of the ADSL Router, e.g., ping 192.168.1.1. If the following response occurs :

Reply 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 timed 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 addresses 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:

Reply 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 timed out

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

Problems with WAN

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

Error message : All the ADSL LEDs light up and cannot light off as usual.
Possible cause : When users are executing firmware upgrade and saving 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 :

Setup your PC with a static IP address, such as 192.168.1.2, and then access the router's web page by entering <http://192.168.1.1>. Then update the firmware again.

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

- ◆ **Possible cause: The firmware file format is invalid.**
- ◆ **Action: Check to see whether 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 6 : 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.

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 192.168.2.2 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, met signaling channel or a generic broadcast signaling channel. Your ISP should supply you with the values.

FCC Statement:

Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.