# **Dynalink** ADSL2+ Wireless Modem Router User Manual

**RTA1025W** 



## U – RTA1025W

## **ADSL Router**

# **User's Manual**

Version 2.4

Mar. 3, 2007

### **Copyright Notice**

© 2005 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		Use only the type of power source indicated on the marking labels.	
		Use only power adapter supplied with the product.	
		Do not overload wall outlet or extension cords as this may increase the risk of electric shock or fire. If the power cord is frayed, replace it with a new one.	
		Proper ventilation is necessary to prevent the product overheating. Do not block or cover the slots and openings on the device, which are intended for ventilation and proper operation. It is recommended to mount the product with a stack.	
		Do not place the product near any source of heat or expose it to direct sunlight.	
		Do not expose the product to moisture. Never spill any liquid on the product.	
		Do not attempt to connect with any computer accessory or electronic product without instructions from qualified service personnel. This may result in risk of electronic shock or fire.	
		Do not place this product on unstable stand or table.	
For Using		Power off and unplug this product from the wall outlet when it is not in use or before cleaning. Pay attention to the temperature of the power adapter. The temperature might be high.	
		After powering off the product, power on the product at least 15 seconds later.	
		Do not block the ventilating openings of this product.	
		When the product is expected to be not in use for a period of time, unplug the power cord of the product to prevent it from the damage of storm or sudden increases in rating.	
should you attempt to service the produc		not attempt to disassemble or open covers of this unit by yourself. Nor uld you attempt to service the product yourself, which may void the user's nority to operate it. Contact qualified service personnel under the following ditions:	
		If the power cord or plug is damaged or frayed.	
		If liquid has been spilled into the product.	
		If the product has been exposed to rain or water.	
		If the product does not operate normally when the operating instructions are followed.	
		If the product has been dropped or the cabinet has been damaged.	
		If the product exhibits a distinct change in performance.	
Caution		Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.	

### FCC

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

#### 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.

## Contents

Before You Use I>	(
UnpackingI>	
Features	Χ
ADSL Compliance	Χ
ADSL2 Compliance	Χ
ADSL2+ Compliance	Χ
Wireless LAN Compliance	
ATM Features	
Bridging Features	
Routing FeaturesX	
Security Features	
Configuration and ManagementX	
Subscription for ADSL ServiceXI	
	_
Chapter 1: Overview1	
Physical Outlook	
Front Panel	
Rear Panel	2
Chapter 2: System Requirement and Installation	3
System Requirement	
Choosing a place for the ADSL Router	
Connecting the ADSL Router	
USB Driver Installation	
For Windows ME	
For Windows 2000	
For Windows XP	
For Windows Vista	
Uninstalling the USB Driver	
For Windows ME	
For Windows 2000	
For Windows XP	
For Windows Vista	
Setting up TCP/IP	
For Windows 98	
For Windows ME	
For Windows NT	
For Windows 2000	
For Windows XP	
For Windows Vista	
Renewing IP Address on Client PC	
For Windows 98/ME	
For Windows NT/2000/XP	
For Windows Vista	
Chapter 3: Accessing the Internet	

PPF	Pover ATM (PPPoA) Mode	52
	Pover ATM (PPPoA) IP Extension Mode	
	Pover Ethernet (PPPoE) Mode	
PPF	Pover Ethernet (PPPoE) IP Extension Mode	55
Num	nbered IP over ATM (IPoA)	56

Numbered IP over ATM (IPoA)+NAT	
Unnumbered IP over ATM (IPoA)	60
Unnumbered IP over ATM (IPoA)+NAT	62
Bridge Mode	
MER	

apter 4: Web Configuration	67
Using Web-Based Manager	67
Outline of Web Manager	
To Have the New Settings Take Effect	
Language	
Quick Start	
Connect to Internet	
Quick Setup	
Connection Type	
PPP over ATM/ PPP over Ethernet	
IP over ATM.	
Bridging	
Status	
Overview	
ADSL Line	
Internet Connection	
Traffic Statistics	
DHCP Table	
Wireless Clients	
Routing Table	
ARP Table	
Advanced Setup	
Local Network – IP Address	
Local Network – DHCP Server	
Local Network – UPnP	82
Local Network – IGMP Snooping	82
Internet – Connections	84
Internet – DNS Server	87
Internet – IGMP Proxy	87
Internet – ADSL	88
IP Routing – Static Route	
IP Routing – Dynamic Routing	
Virtual Server – Port Forwarding	
Virtual Server – Port Triggering	
Virtual Server – DMZ Host	
Virtual Server – Dynamic DNS	
Virtual Server – Static DNS	
NAT ALG Configuration	
Firewall – Bridge Filtering	
Firewall – IP Filtering	
Quality of Service – Bridge QoS	102
	102
•	105
	105
	107
	109
Access Control	
Repeater	
Management	
Diagnostics	117

Management Accounts110Management Control – From Remote110Management Control – From Local110TR-069 Client Configuration110Internet Time120System Log120Backup Config120Update Firmware120Reset Router120UPnP for XP120	29 29 29 29 29 29 29 29 29 29 29 29 29 2
Chapter 5: Troubleshooting	1
Problems with LAN	1
Problems with WAN	
Problems with Upgrading 132	2
Chapter 6: Glossary	3
Annondiu A. Charifications	
Appendix A: Specifications	Э
Appendix B: Client Setup for 802.1x, WPA, and WPA-PSK	7
Retreiving Client Certificate	87
Enabling 802.1x Authentication and Security 140	
Enabling WPA Authentication and Security	
Enabling WPA-PSK Authentication and Security 14	5

## **Before You Use**

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

RTA1025W Wireless ADSL2+ Router is a DSL broadband access device which allows ADSL connectivity while providing 802.11g wireless LAN capabilities for home or office users. It supports ADSL2/ADSL2+ and is backward compatible to ADSL, even offers auto-negotiation capability for different flavors (G.dmt, G.lite, or T1.413 Issue 2) according to central office DSLAM's settings (Digital Subscriber Line Access Multiplexer). Also the feature-rich routing functions are seamlessly integrated to ADSL service for existing corporate or home users. Now users can enjoy various bandwidth-consuming applications via RTA1025W Wireless ADSL2+ Router.

## Unpacking

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

- ✓ ADSL Router
- Power Adapter and Cord
- ✓ USB Cable
- ✓ RJ-11 ADSL Line Cable
- RJ-45 Ethernet Cable
- ✓ Quick Start Guide
- Driver & Utility Software CD

## Features

## **ADSL Compliance**

- ANSI T1.413 Issue 2
- S ITU G.992.1 Annex A (G.dmt)
- S 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)
- Support dying gasp
- Maximum Rate: 12 Mbps for downstream and 1 Mbps for upstream

## **ADSL2+ Compliance**

🖉 🛛 ITU G.992.5 Annex A

- Support dying gasp
- S Maximum Rate: 24 Mbps for downstream and 1.2 Mbps for upstream

## Wireless LAN Compliance

- IEEE 802.11g and IEEE 802.11b
- Data Rate: 54, 48, 36, 24, 18, 12, 9, 6 Mbps for 802.11g; 11, 5.5, 2, 1 Mbps for 802.11b
- Modulation Technique: OFDM for 802.11g; CCK (11 Mbps, 5.5 Mbps) for 802.11b; DQPSK (2Mbps) for 802.11b; DBPSK (1 Mbps) for 802.11b
- S Network Architecture: infrastructure
- S 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
- 8 RF Output Power: 13.5+/-1.5dBm for 802.11g; 17.5+/-1.5dBm for 802.11b
- Antenna Connectors: Hardware diversity support. One external antenna and one internal antenna are provided.
- Coverage Area: 300 meters
- Support WEP (Wired Equivalent Privacy) mechanism which uses RC4 with 64-bit or 128-bit key length
- Support 802.1x and WPA/WPA2
- 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).
- Two SSIDs are supported currently. 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.
- 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 16 PVCs for UBR, CBR, VBR-nrt, VBR-rt with traffic shaping
- RFC2684 LLC Encapsulation and VC Multiplexing over AAL5
- S RFC2364 Point-to-Point Protocol (PPP) over AAL5
- S RFC2225 Classical IP and ARP over ATM
- RFC2516 PPP over Ethernet: support Relay (Transparent Forwarding) and Client functions
- Support PPPoA or PPPoE Bridged mode (the IP address got from ISP can be passed to the user's PC and behave as the IP address of the user's PC.)
- S 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, USB, and 802.11g wireless LAN
- Supports IGMP Snooping
- Supports 802.1Q VLAN packet pass-through

## **Routing Features**

- NAT (Network Address Translation) / PAT (Port Address Translation) let multiple users on the LAN to access the internet for the cost of only one IP address.
- ALGs (Application Level Gateways): such as NetMeeting, MSN Messenger, FTP, Quick Time, mIRC, Real Player, CuSeeMe, VPN pass-through 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
- S DNS Relay, Dynamic DNS
- C DHCP Client/Relay/Server
- S 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
- Firewall support IP packets filtering based on IP address/Port number/Protocol type
- Bridge packet filtering (optional)
- URL filtering (optional)
- 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)

## **Configuration and Management**

- S User-friendly embedded web configuration interface with password protection
- Remote management accesses control
- Telnet/SSH 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-111, and TR-098<sup>1</sup>

## Subscription for ADSL Service

To use the ADSL Router, you have to subscribe for ADSL service from your broadband service provider. According to the service type you subscribe, you will get various IP addresses:

**Dynamic IP:** If you apply for dial-up connection, you will be given an Internet account with username and password. You will get a dynamic IP by dialing up to your ISP, such as under 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 IPoA or 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.

<sup>&</sup>lt;sup>1</sup> TR-098 can be supported since April, 2007.

## **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 router, please take a look at the information first.

## **Physical Outlook**

## **Front Panel**

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



## **LED Indicators**

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

Function	Color	Definition
Power	Off	Power is off.
	Solid Green	Power is on and the device operates normally.
	Solid Red	Power on self-test in progress
		The device enters the console mode of the boot loader.
		Power on self-test failure if the led always stays solid red.
	Flash Red	Firmware upgrades in progress
	Off	No DSL signal is detected.
DSL	Slow Flash Green	DSL line is handshaking in progress
DGL	Fast Flash Green	DSL line is training in progress
	Solid Green	DSL line connection is up.
	Off	No PPPoA or PPPoE connection
PPP	Solid Green	At least one PPPoA or PPPoE connection is up. The users can
		access the Internet now.
	Off	No Ethernet signal is detected.
Ethernet	Flash Green	User data is going through Ethernet port
	Solid Green	Ethernet interface is ready to work.
USB WLAN	Off	No USB signal is detected.
	Flash Green	User data is going through USB port
	Solid Green	USB interface is ready to work.
	Off	No radio signal is detected.
	Flash Green	User data is going through WLAN port
	Solid Green	WLAN interface is ready to work.

## **Rear Panel**

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



Connector	Description
12VAC	12VAC Power connector
	Power switch
Ethernet 1-4	Ethernet RJ-45 connector
USB	USB client port
DSL	RJ-11 connector

Note: For use only with power supply OEM type AA-121ABN, AA-121AD, AA-121AE; Leader type A48120100-C5, A48120100-B2, and A48120100-A3.

## **Chapter 2: System Requirement and Installation**

## System Requirement

To access the ADSL Router 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 ADSL Router 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 **Enable** by default, the DHCP clients should be able to access the ADSL Router, or the host PC should be assigned an IP address first for initial configuration.

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



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

## Choosing a place for the ADSL Router

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



## Connecting the ADSL Router

Follow the steps below to connect the related devices.

0 Connecting the ADSL line. Connect the DSL port of the device to your ADSL wall outlet with RJ-11 cable. 0 Please attach one end of the Ethernet cable with RJ-45 connector to the LAN port of your ADSL Router. ₿ Connect the other end of the cable to the Ethernet port of the client PC. • Connect the supplied power adapter to the PWR port of 0 your ADSL Router, and plug the other end to a power outlet. **5** Turn on the power switch. Here provides an example for hardware connection. Power Cord

## USB Driver Installation

If the ADSL router is connected to a PC through the USB interface, you will be prompted for the USB drivers when plugging the USB cable to the PC. Refer to the relevant operating system to install the USB drivers.

## For Windows ME

0 Run the USB installation program from the CD provided in your router package.

- 0 An InstallShield Wizard will appear. Please wait for a moment.
- Ø When the welcome screen appears, click Next for the next step.
- 4 When the complete window of the InstallShield Wizard appears, click Finish.
- 6 Link your router and the PC with a USB cable.
- 6 The system will detect the USB driver automatically. Then, the system will copy the proper files for this router.

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

0 When the file copying finished, the dialog above will close. Now the USB driver is installed properly. You can use the router.

## For Windows 2000

- O Run the USB installation program from the CD provided in your router package.
  - An InstallShield Wizard will appear. Please wait for a moment. InstallShield Wizard Askey ADSL Router USB Driver Setup is preparing the InstallShield® Wizard, which will guide you through the rest of the setup process. Please wait.
- ₿

0

When the welcome screen appears, click Next for the next step.

Cancel

InstallShield Wizard		×
	Welcome to the InstallShield Wizard for Askey ADSL Router USB Driver This Installation Wizard will install Askey ADSL Router USB driver on your computer. To continue, click Next.	<
	< <u>₿</u> ack <b>Next&gt;</b> Cancel	



InstallShield Wizard	
and the second	Askey ADSL Router USB Driver
4	Setup has finished installing Askey ADSL Router USB driver on your computer.
	To continue, click Finish, then insert the USB cable.
and the second s	The system will then automatically detect the device.
	< Back Finish Cancel



Link your router and the PC with a USB cable.

The system will detect the USB driver automatically. And then, the system will copy the proper files for this router.





0

**Note:** If the USB device is not detected automatically, check the USB cable between the PC and the device. Besides, make sure that the device is power on.

When the file copying finished, the dialog above will close. Now the USB driver is installed properly. You can use the router.

To make sure that your router is properly installed, please do the following steps.

1. Right-click on My Computer and press Properties.

My Computer	
	Active Desktop 🔸
My Network Places	Arrange Icons Line Up Icons Refresh
1	Paste Paste Shortcut
Recycle Bin	New 🕨
	Properties

2. On the Hardware tap, click Device Manager.



3. Confirm that the Askey ADSL Router USB Remote NDIS Device is on the Network adapters list.



## For Windows XP



0

Run the USB installation program from the CD provided in your router package.





₿	When the welcome screen appears, click <b>Next</b> for the next step.
	InstallShield Wizard
	Welcome to the InstallShield Wizard for Askey ADSL Router USB Driver
	This Installation Wizard will install Askey ADSL Router USB driver on your computer. To continue, click Next.
	< Back Next > Cancel
4	When the finish installing message of InstallShield Wizard appears, click <b>Finish</b> .
6	Link your router and the PC with a USB cable.
6	The system will detect the USB driver automatically.
	USB Device
	Note: If the USB device is not detected, check the USB cable between the PC and the device. Also make sure that the device is power on.
0	Then the system will try to find the proper driver for your router and copy the files automatically.
	Found New Hardware Askey ADSL Router USB Remote NDIS Device (BCM63xx Based) CF
8	After the file copying finished, a completing message will appear.
	Image: Second
Ø	You can use the wireless router now.

To make sure your router is properly installed, please do the following steps.

1. Right-click on My Computer and press Properties.



2. On the Hardware tab, click Device Manager.

tem Prope	rties			?
System Restore		Automa	Remote	
General	Comp	iter Name Hardware		Advanced
Device Manager The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.  Device Manager Drivers Driver Signing lets you make sure that installed drivers are				
Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set how Windows connects to Windows Update for drivers.           Driver Signing         Windows Update				you set up drivers.
Hardware Pr	ofiles			
		iles provide a v vare configurat	vay for you to set up ions.	and store
			Hardware <u>F</u>	Profiles
		ОК	. Cancel	Apply

3. Confirm that the Askey ADSL Router USB Remote NDIS Device is on the Network adapters list.



## **For Windows Vista**

For Vista users, please press **Continue** whenever a prompted window asking for permission to continue during USB driver installation process (see the figure below for example).

User Account	Control	×
💎 Wind	dows needs your permission to continue	
If you starte	d this action, continue.	
	Advanced System Settings Microsoft Windows	
🕑 Details	Continue Can	cel
User Account	t Control helps stop unauthorized changes to your comp	uter.

To install the USB driver before connect the router to the PC, here provides two methods.

Method One – Use the driver CD came with the product package.



Run the USB installation program on the CD provided in your router package.



An **InstallShield Wizard** will appear. Please wait for a moment.

Preparing Setup		Citing Of T
Please wait while	the InstallShield Wizard prepares the setup.	

Askey ADSL Router through the rest of th	USB Driver Setup e setup process. F	is preparing the li Please wait.	nstallShield Wizard	, which will guide yo
_				
stallShield ———				



When the welcome screen appears, click Next for the next step.

Askey ADSL Router USB Driver	Setup 🗾
	Welcome to the InstallShield Wizard for Askey ADSL Router USB Driver This Installation Wizard will install Askey ADSL Router USB driver on your computer. To continue, click Next.
	< <u>B</u> ack Next> Cancel

4	When the complete message of InstallShield Wizard appears, click <b>Finish</b> .
	Askey ADSL Router USB Driver         Setup has finished installing Askey ADSL Router USB driver on your computer.         To continue, click Finish, then insert the USB cable.         The system will then automatically detect the device.
<b>6</b>	Link your router and the PC with a USB cable. The system will detect the USB driver automatically.
	Installing device driver software Click here for status.
	Note: If the USB device is not detected, check the USB cable between the PC and the device. Also make sure that the device is power on.
0	After the file copying finished, a completing message will appear.
	Askey ADSL Router USB Remote NDIS Device × Device driver software installed successfully.
8	You can use the router now.

Method Two - Run a silent installation.



Copy the USB driver folder from the driver CD to somewhere on the PC. (In our example, the driver files are put under D:\Askey ADSL USB WHQLed.)

**e** c

Open Start menu, key in *cmd* in the blank and press enter. Then click **cmd**.



₿

When the Command Prompt screen appears, point to the driver folder on your PC, and then enter *setup -s*. Press enter to start silent installation.



- The system will install the driver automatically. You can connect your router and the PC with a USB cable now.
- 6

The system will detect the USB driver automatically.



If the USB driver has not been installed yet, you can also connect the router to the PC with a USB cable and wait for *Universal Plug and Play* device to detect the router, and then install the driver.



Plug the USB cable into the USB port on the PC.

A Found New Hardware window will appear. Press Locate and install driver software (recommended).



₿

Then insert the USB driver CD provided in your router package into the PC, and press **Next**.



4

The system will search disc for the USB driver needed and then complete the installation.



<sup>0</sup> 

Or if you do not have a disc, but have the driver files on your PC, you can follow the steps below:



## 4

Select Browse my computer for driver software (advanced).

	Found New Hardware - USB Network Interface	
Wir	ndows couldn't find driver software for your device	
•	Check for a solution Windows will check to see if there are steps you can take to get your device working.	
•	Browse my computer for driver software (advanced) Locate and install driver software manually.	
		Cancel



Press **Browse** to set the path for the driver file, and then press **Next**.

0	Found New Hardware - USB Network Interface
	Browse for driver software on your computer
	Search for driver software in this location:
	D:\Askey ADSL USB Driver  Browse
	☑ Include subfolders
	Next Cancel



0

6

Now the driver software is installed successfully. Press **Close** to start using the router.



To make sure the USB driver for your router is properly installed, please do the following steps.

1. Open the Start menu and press Control Panel.





2. On the Control Panel folder, click System and Maintenance.

3. Press System.



4. Click Device Manager.



5. Confirm that the Askey ADSL Router USB Remote NDIS Device is on the Network adapters list.

📲 Device Manager	
File Action View Help	
⇐ ⇒   ☶   🖬   🖬 📖 🔍 🗎 🕵 🖏	
ASKEY-PC	
i 👝 Disk drives i 🎭 Display adapters	
a 🔮 DVD/CD-ROM drives a 🛁 Floppy disk drives	
Floppy drive controllers	
EEE 1394 Bus host controllers     EEE Tage     Keyboards	
Mice and other pointing devices	
Network-adapters     Askey ADSL Router USB Remote NDIS Device     Broadcom NetLink (TM) Graabit Ethernet	
Ports (COM & LPT)	
ia 🋄 Processors ia 🐗 Sound, video and game controllers	
🖶 🖟 Universal Serial Bus controllers	
Uninstalls the driver for the selected device.	

## Uninstalling the USB Driver

## For Windows ME

To uninstall the USB driver, please follow the procedures below.

## Method One:

- Unplug the USB cable from the USB port on your PC.
- Choose Programs Askey Broadband Uninstall Askey ADSL Router USB Driver from the Start menu.
- 6 The InstallShield Wizard dialog will appear.
- A dialog appears to confirm whether you really want to remove the USB driver or not. Please click Ok.
- When the Maintenance Complete screen appears, the USB driver is removed successfully. Click **Finish.**

#### Method Two:

- Unplug the USB cable between your router and your PC. Then click **OK**.
- Choose Settings Control Panel from the Start menu. Choose Add/Remove Programs.
- A dialog appears to ask you to choose the program that you want to remove. Please select **Askey ADSL Router USB Driver** and click **Change/Remove**.
- The InstallShield Wizard dialog will appear.
- When the Maintenance Complete screen appears, the USB driver is removed successfully. Click Finish

## For Windows 2000

To uninstall the USB driver, there are two ways to do it. Please do the following procedures.

### Method One:

3.



To safely unplug the USB cable from the USB port on your PC:

1. Go to the right lower corner for **Unplug and Eject Hardware** and left click on it.



2. Click the dialog for Stop Askey ADSL Router USB Remote NDIS Device.



OK

Choose Programs – Askey Broadband – Uninstall Askey ADSL Router USB Driver from the Start menu.

	*	Windows Update					
	Ð.	WinZip					
		CRT 3.4					
<i></i>	<b>1</b>	Programs 🕨		Accessories Administrative Tools	•		
	<u></u>	Documents •		Startup	•		
erver	Б.	Settings 🕨 🕨	کار ا	Internet Explorer Outlook Express			
S S		Search 🕨	ē	CRT 3.4	×		
20	2	Help		WinZip Askey Broadband	•	<u>ال</u>	Uninstall Askey ADSL Router USB Driver
ows	2	Run	Γ				
Windows 2000 Server	Ì	Shut Down					

**6** The InstallShield Wizard dialog will appear.



A dialog appears to confirm whether you want to remove the USB driver or not. Please click **Ok**.

Confirm Uninstall		
Do you want to remove the Askey ADSL Router USB driver ?		
Warning: Please unplug the USB cable now before proceeding with uninstall.		
For Windows 2000 users, before unplugging the cable please click the "Unplug/Remove Hardware" icon in your Windows system tray to stop Askey ADSL router USB driver. Please refer to your Windows Help for help about unplugging hardware.		
Cancel		



4

When the Maintenance Complete screen appears, the USB driver is removed successfully. Click **Finish.** 

InstallShield Wizard	
	Maintenance Complete
	Askey ADSL Router USB driver has now been uninstalled.
	Click Finish to exit the un-installation process.
	< Back Finish Cancel

#### Method Two:

O

- To safely unplug the USB cable from the USB port on your PC:
  - 1. Go to the right lower corner for **Unplug and Eject Hardware** and left click on it.



2. Click the dialog for **Stop Askey ADSL Router USB Remote NDIS Device**.

Stop Askey ADSL Router USB Remote NDIS Device (BCM63xx Based)	
📢 🛞 📖 🌒 🥸	\$ 10:25 AM

3. The Router is safely removed, click **OK** to continue.



0

Choose **Settings – Control Panel** from the **Start** menu. Choose **Add/Remove Programs**.



Ø

A dialog appears to ask you to choose the program that you want to remove. Please select **Askey ADSL Router USB Driver** and click **Change/Remove**.





4

6

The InstallShield Wizard will guide you till the USB driver is removed.



When the Maintenance Complete screen appears, the USB driver is removed successfully. Click Finish.

InstallShield Wizard	
	Maintenance Complete
	Askey ADSL Router USB driver has now been uninstalled.
	Click Finish to exit the un-installation process.
	< Back Finish Cancel

## For Windows XP

To uninstall the USB driver, there are two ways to do it. Please do as follows.

Method One:

0



Choose Programs – Askey Broadband – Uninstall Askey ADSL Router USB Driver from the Start menu.

23	Windows Catalog											
2	Windows Update											
Ð	CRT 3.0											
	Set Program Access and Defaults											
N	Netscape 7.1											
2	Programs		Accessories	•	1							
	Programs		CommView	÷								
	Documents		Ethereal	Ĺ								
			Askey Broadband		63			10.01				
		1000	Askey Broadband	•	217	Uninsta	ill Askey	' ADSL	. Koute	r usb	Driver	
1.0	Settings											
1	Settings		×									
₩ 	Settings Search											
<ul> <li>✓</li> <li>✓</li></ul>												
<ul> <li>✓</li> <li>✓</li></ul>	Search I											
<ul> <li>✓</li> <li>✓</li></ul>	Search Help and Support											
	Search I Help and Support Run											



#### The InstallShield Wizard dialog will appear.



4

A dialog appears to confirm whether you want to remove the USB driver or not. Unplug the USB cable from your PC, and click **Ok**.

Confirm Uninstall
Do you want to remove the Askey ADSL Router USB driver ?
Warning: Please unplug the USB cable now before proceeding with uninstall.
Cancel

• When the Maintenance Complete screen appears, the USB driver is removed successfully. Click **Finish.** 

#### Method Two:

0

Unplug your USB cable between your router and your PC.

0

₿

6

6

Choose Settings –Control Panel from the Start menu. Choose Add or Remove Programs.

Control Panel			
Be Edit Yew Pavorites Iou			1
Address Dr Control Panel	interest interest	🛩 🔂 Go	Noton Antihus 😣 •
Control Panel	Accessibility Options	Add Hardware	
🕞 Switch to Category Vew	Add or Remove Programs	Administrative Tools	
See Also (2) Windows Update (2) Help and Support	Automatic Updates	Dute and Time	
	Display	Folder Options	
	Fonts	Game Controllers	
	Internet Options	Keyboard	
	Mouse	Network	
	Network Setup Witterd	Phone and Modern Options	
	Power Options	Printers and Faxes	

A dialog appears to ask you to choose the program that you want to remove. Please select **Askey ADSL Router USB Driver** and click **Change/Remove**.

🐻 Add or Re	nove Programs			
1	Currently installed programs:	Show updates	Sort by: Name	*
Change or Remove	ACDSee 5.0 PowerPack		Size	30.66MB 🛆
Programs	Adobe Acrobat 5.0		Size	25.17MB
	Alcohol 120%		Size	4.29MB
Add New	🚰 Askey ADSL Router USB Driver		Size	0.05MB
Programs	To change this program or remove it from your o	omputer, click Change/Remove.	Chang	e/Remove
6	CommView		Skee	4.34MB
Add/Remove Windows	🕞 Dr. Eye 6.0 SP2 (~by X-X-S-S)		Size	708.00MB
Components	Ethereal 0.10.4		Size	29.00MB
	FlashGet(JetCar)		Size	2.58MB
Set Program	FTDI USB Serial Converter Drivers			
Access and Defaults	GRIColal 3.3.2		Size	5.32MB
Defaults	Service Call Analyzer		Size	15.23MB
	15 Intel(R) Integrated Performance Primitives RTI 3	.0	Size	14.21MB
	LiveReg (Symantec Corporation)		Size	1.82MB
	1 LiveUpdate 2.5 (Symantec Corporation)		Size	7.85MB
	R Microsoft .NET Framework 1.1		Size	37.46MB
	My Web Search (Smiley Central)		Size	2.13MB 🥃

**4** The InstallShield Wizard dialog will appear.



A dialog appears to confirm whether you want to remove the USB driver or not. Unplug the USB cable from your PC, and click **Ok**.

Confirm Uninstall
Do you want to remove the Askey ADSL Router USB driver ?
Warning: Please unplug the USB cable now before proceeding with uninstall.
OK Cancel

When the Maintenance Complete screen appears, the USB driver is removed successfully. Click **Finish.**
### For Windows Vista

For Vista users, please press **Continue** whenever a prompted window asking for permission to continue during USB driver uninstallation process (see the figure below for example).



To uninstall the USB driver, there are two ways to do it. Please follow the instructions.

Method One: Remove from Device Manager.





Click System and Maintenance.



0

Choose Start menu, and then select Control Panel.





4

#### Click Device Manager.

and the second second		Film and party land strong	
🚱 🔍 🔻 🕨 Control Panel 🕨	System and Maintenance      System	stem 👻 🍫 Search	٩
Tasks  Device Manager  C Benote settings  System protection  Advanced system settings	Windows edition Windows Vista™ Enterpris	n about your computer se oft Corporation. All rights reserved.	
See also Windows Update	System Rating: Processor: Memory (RAM): System type: Computer name, domain, an Computer name: Full computer name: Computer description:	askey-PC askey-PC	
<u>S</u> ecurity Center <u>P</u> erformance	Workgroup: Windows activation	WORKGROUP	

6

Right click **Askey ADSL Router USB Remote NDIS Device** on the **Network adapters** list, and press Uninstall.

6

Click **OK** when the Confirm Uninstall window appears.



Remember to unplug the USB cable before continue the uninstallation, or you will see the reminder as follows. Unplug and press **OK**.

Confirm Uninstall
Please unplug the USB cable now before proceeding with uninstall.
OK Cancel

0

When the **Confirm Device Uninstall** screen show up, check **Delete the driver software for the device** and click **OK** to continue.

Confirm Device Uninstall				
Askey ADSL Router USB Remote NDIS Device				
Warning: You are about to uninstall this device from your system.				
Delete the driver software for this device.				
OK Cancel				

8

Wait while the system is uninstalling.

Confirm Device Uninstall			
1	Askey ADSL Router USB Remote NDIS Device		
Uninstalling devices			
	OK Cancel		

0

When the uninstallation is finished, the icon of this router under network adapter list will disappear.



#### Method Two - uninstall from program list

**Note:** If your USB driver is installed by UPnP device, you can only use method one (via the **Device Manager**) to uninstall, because the installed driver will not be shown on the program list.



Unplug your USB cable between your router and your PC.

0

Choose Start menu, and open Control Panel folder. Click Uninstall a program.



Ø

If the driver name is not on the list, click **Refresh** button or **F5** to update the information. To remove the driver, select it, and then press **Uninstall**.

G v 🖾 > Control Panel >	Programs   Programs and Features	<ul> <li>✓ ✓ Search</li> </ul>	
<b>Tasks</b> View installed updates	Uninstall or change a program To uninstall a program, select it from the lis		esh button
Get new programs online at Windows Marketplace View purchased software (digital locker)	🖓 Organize 🗸 🏢 Views 📿 Uninstall	-	Installed On
<ul> <li>Turn Windows features on or off</li> </ul>	Tame	Askey Computer	2/26/2007
	<u>د</u>		•



Then the system will start to uninstall the USB driver software automatically.

Setup Status		
Askey ADSL Router US	B Driver is configuring your ne	w software installation.
InstallShield		





The USB driver is successfully removed now.

## Setting up TCP/IP



In order to access the Internet through the ADSL Router, each host on your network must install/setup TCP/IP first. Please follow the steps below to set your network adapter.

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 98

 Open the Start menu, point to Settings and click on Control Panel.



2. Double-click the Network icon.



3.	The Network window appears. On the Configuration tab, check out the list of installed network components. Option 1: If there is no TCP/IP protocol, click Add. Option 2: If you have TCP/IP protocol, skip to Step 6. Your network interface card. Check out if TCP/IP for your NIC is installed or not.	Network       2 ×         Configuration       Identification       Access Control         The following getwork components are installed:       Image: Client for Microsoft Networks         Microsoft Family Logon       Image: Client for Microsoft Networks         Intel 82595-Based Ethernet       Image: Client for Microsoft Networks         Add       Remove       Properties         Primary Network Logon:       Client for Microsoft Networks       Image: Client for Microsoft Networks         Elle and Print Sharing       Description       OK       Cancel
4.	Highlight <b>Protocol</b> and click <b>Add</b> .	Select Network Component Type
5.	Highlight <b>Microsoft</b> on the left	Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate. Select Network Protocol
	side of the window, and select <b>TCP/IP</b> on the right side. Then click <b>OK</b> .	Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk. Manufacturers: Network Protocols: Banyan BM BM IBM Improved Microsoft 32-bit DLC Microsoft 22-bit D
6.	When returning to the <b>Network</b> window, highlight <b>TCP/IP</b> protocol for your NIC and click <b>Properties</b> .	Network       ? ×         Configuration       Identification       Access Control         The following network components are installed       Image: Client for Microsoft Networks         Microsoft Family Logon       Dial-Up Adapter         Dial-Up Adapter       Image: Client for Microsoft Networks         Intel 82595-Based Ethernet       Image: Client for Microsoft Networks         Add       Rgmove       Properties         Primary Network Logon:       Image: Client for Microsoft Networks       Image: Client for Microsoft Networks         Ele and Print Sharing       Description       TCP/IP is the protocol you use to connect to the Internet and wide-area networks.         OK       Cancel

7.	On the <b>IP Address</b> tab: Enable <b>Obtain an IP address</b> <b>automatically</b> and click OK.	CCP/IP Properties       Image: Advanced NetBIOS         Bindings       Advanced NetBIOS         DNS Configuration       Gateway         WINS Configuration       IP Address         An IP address can be automatically assigned to this computer.       If your network does not automatically assigned to this computer.         If your network does not automatically assigned to this computer.       If your network does not automatically assigned to this computer.         If point network does not automatically assigned to this computer.       If your network does not automatically assigned to this computer.         If point an IP address automatically       If point and IP address:         IP Address:       If point and IP address:         IP Address:       If point and IP address:         Sybnet Mask:       If point and point address
		OK Cancel
8.	When returning to the <b>Network</b> window, click <b>OK</b>	Network       ? X         Configuration       Identification       Access Control         The following network components are installed:          Client for Microsoft Networks          Microsoft Family Logon          Dial-Up Adapter          Intel 82595-Based Ethernet          TCP/IP ->Intel 82595-Based Ethernet          Add       Remove       Properties         Primary Network Logon:           Eile and Print Sharing        Description         Dk       Cancel
9.	Wait for Windows when copying files.	Copying Files Source: Windows 98 CD-ROM Destination: Sanning 58% Cancel
10.	When prompted with <b>System</b> <b>Settings Change</b> dialog box, click <b>Yes</b> to restart your computer.	System Settings Change       Image: Change         You must restart your computer before the new settings will take effect.         Do you want to restart your computer now?         Image: Monopole

### For Windows ME

 Open the Start menu, point to Settings and click on Control Panel.

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

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

**Option 1:** If there is **no** TCP/IP protocol, click **Add**.

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

Your network jinterface card.

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

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



Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate. 5. Highlight **Microsoft** on the left side of the windows, and select **TCP/IP** on the right side. Then click **OK**.

anufacturers:	Network Protocols:
Banyan	FIPX/SPX-compatible Protocol
■IBM ■ITeX	Generation Sector Microsoft 32-bit DLC
Microsoft	🧃 NetBEUI
Novell	
	,
	<u>H</u> ave Disk
	OK Cano
twork	
Configuration	entification Access Control
	Access Conton
The following ne	stwork components are installed:
Pung	crosoft Networks
B Microsoft Fa	
📑 Dial-Up Ada	apter
223	Based Ethemet
TCP/IP ->I	ntel 82595-Based Ethemet
•	
<u>A</u> dd	Remove Properties
Primary Network	Lanor
and the second se	
Client for Micro	DSOTT NETWOIKS
<u></u>	
Eile and Prin	
Eile and Prin	it Sharing
Eile and Prin Description TCP/IP is the	it Sharing
Eile and Prin Description TCP/IP is the	it Sharing protocol you use to connect to the Internet and works.
Eile and Prin Description TCP/IP is the	tt Sharing protocol you use to connect to the Internet and works. OK Cance
Eile and Prin Description TCP/IP is the wide-area net	t Sharing protocol you use to connect to the Internet and works. OK Cance
Eile and Prin Description TCP/IP is the wide-area net P/IP Propertie Bindings	t Sharing protocol you use to connect to the Internet and works. OK Cance s Advanced NetBIOS
Eile and Prin Description TCP/IP is the wide-area net P/IP Propertie Bindings	t Sharing protocol you use to connect to the Internet and works. OK Cance s Advanced NetBIOS
Eile and Prin Description TCP/IP is the wide-area nets P/IP Propertie Bindings DNS Configuration	t Sharing protocol you use to connect to the Internet and works. OK Cance s Advanced NetBIDS n Gateway WINS Configuration IP Addr
File and Prin Description TCP/IP is the wide-area netwide-area netwide- Bindings DNS Configuration An IP address of If your network	t Sharing protocol you use to connect to the Internet and works. OK Cance S I Advanced NetBIDS Advanced NetBIDS Gateway WINS Configuration IP Addr san be automatically assigned to this computer. does not automatically assign IP addresses, asl
Eile and Prin Description TCP/IP is the wide-area netwide-area netwide- Bindings DNS Configuration An IP addresso If your network at	t Sharing protocol you use to connect to the Internet and works. OK Cance s Advanced NetBIOS n Gateway WINS Configuration IP Addr ran be automatically assigned to this computer. does not automatically assigned to this computer.
File and Prin Description TCP/IP is the wide-area netwide-area netwide- Bindings DNS Configuration An IP address of If your network	t Sharing protocol you use to connect to the Internet and works. OK Cance s Advanced NetBIOS n Gateway WINS Configuration IP Addr ran be automatically assigned to this computer. does not automatically assigned to this computer.
Eile and Prin Description TCP/IP is the wide-area netwide-area netwide- Bindings DNS Configuration An IP addresso If your network at	t Sharing protocol you use to connect to the Internet and works. OK Cance s Advanced NetBIOS n Gateway WINS Configuration IP Addr san be automatically assigned to this computer. does not automatically assign IP addresses, asl ministrator for an address, and then type it in
Eile and Prin Description TCP/IP is the wide-area netwide-area netwide- Bindings DNS Configuration An IP address c If your network your network at the space below	t Sharing protocol you use to connect to the Internet and works. OK Cance s Advanced NetBIOS n Gateway WINS Configuration IP Addr san be automatically assigned to this computer. does not automatically assign IP addresses, ast dministrator for an address, and then type it in w.
Eile and Prin Description TCP/IP is the wide-area netwide-area netwide- Bindings DNS Configuration An IP address of If your network as the space below	t Sharing protocol you use to connect to the Internet and works. OK Cance Cance Advanced NetBIOS Advanced NetBIOS Advanced IP Addr this computer. does not automatically assigned to this computer. does not automatically assign IP addresses, ast fministrator for an address, and then type it in w. IP address automatically
Eile and Prin Description TCP/IP is the wide-area netwide-area netwide- Bindings DNS Configuration An IP address c If your network your network at the space below	t Sharing protocol you use to connect to the Internet and works. OK Cance Cance Advanced NetBIOS Advanced NetBIOS Advanced IP Addr this computer. does not automatically assigned to this computer. does not automatically assign IP addresses, ast fministrator for an address, and then type it in w. IP address automatically
Eile and Prin Description TCP/IP is the wide-area netwide-area netwide-area netwide-area netwide-area netwide Bindings DNS Configuration An IP address of If your network your network as the space below © Obtain an	t Sharing protocol you use to connect to the Internet and works. OK Cance Cance Advanced NetBIOS Advanced NetBIOS Advanced NetBIOS I Gateway WINS Configuration IP Addr san be automatically assigned to this computer. does not automatically assign IP addresses, ask fministrator for an address, and then type it in w. IP address automatically 1P address:
Eile and Prin Description TCP/IP is the wide-area netwide-area netwide- Bindings DNS Configuration An IP address of If your network as the space below	t Sharing protocol you use to connect to the Internet and works. OK Cance Cance Advanced NetBIOS Advanced NetBIOS Advanced NetBIOS I Gateway WINS Configuration IP Addr san be automatically assigned to this computer. does not automatically assign IP addresses, ask fministrator for an address, and then type it in w. IP address automatically 1P address:
Eile and Prin Description TCP/IP is the wide-area netwide-area netwide-area netwide-area netwide-area netwide Bindings DNS Configuration An IP address of If your network your network as the space below © Obtain an	t Sharing protocol you use to connect to the Internet and works. OK Cance s OK Cance s Advanced NetBIOS n Gateway WINS Configuration IP Addr san be automatically assigned to this computer. does not automatically assigned to this computer. N. IP address automatically n IP address:

ОK

Cancel

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

7. On IP Address tab: Enable Obtain an IP address automatically and click OK. 8. While returning to the **Network** window, click **OK**.

The following petwork components are installed:         Client for Microsoft Networks         Microsoft Family Logon         Diał-Up Adapter         Diał-Up Adapter         Intel 82595-Based Ethernet         TCP/IP ->Intel 82595-Based Ethernet         Add       Remove         Properties	vork	
Client for Microsoft Networks Microsoft Family Logon Dial-Up Adapter Intel 82595-Based Ethernet TCP/IP ->Intel 82595-Based Ethemet  Add Remove Properties Primary Network Logon: Client for Microsoft Networks Eile and Print Sharing	nfiguration Identification Access Control	
Client for Microsoft Networks Microsoft Family Logon Dial-Up Adapter Intel 82595-Based Ethernet TCP/IP ->Intel 82595-Based Ethemet  Add Remove Properties Primary Network Logon: Client for Microsoft Networks Eile and Print Sharing	The following network components are installed:	
Microsoft Family Logon  Microsoft Family Logon  Itel 82595-Based Ethernet  TCP/IP ->Intel 82595-Based Ethemet  Add  Remove Properties  Primary Network Logon:  Client for Microsoft Networks  Eile and Print Sharing		
Intel 82595-Based Ethernet TCP/IP ->Intel 82595-Based Ethernet  Add Remove Properties Primary Network Logon: Client for Microsoft Networks Eile and Print Sharing		
TCP/IP ->Intel 82595-Based Ethemet  Add  Remove Properties Primary Network Logon: Client for Microsoft Networks Eile and Print Sharing	Dial-Up Adapter	
Add Remove Properties Primary Network Logon: Client for Microsoft Networks Eile and Print Sharing	Intel 82595-Based Ethernet	
Primary Network Logon: Client for Microsoft Networks	TCP/IP ->Intel 82595-Based Ethemet	<b>_</b>
Primary Network Logon: Client for Microsoft Networks		<u>.</u>
Primary Network Logon: Client for Microsoft Networks	Add N Bernove Bronetter	
Client for Microsoft Networks	Honove Libbenes	
Eile and Print Sharing	Primary Network Logon:	
	Client for Microsoft Networks	•
	File and Dist Charles	
Description	Elle and Frint Sharing	
	Description	

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



## For Windows NT

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



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



3.	The <b>Network</b> window appears. On the <b>Protocols</b> tab, check out the list of installed network components. <b>Option 1:</b> If there is <b>no</b> TCP/IP Protocol, click <b>Add</b> . <b>Option 2:</b> If you have TCP/IP Protocol installed, skip to Step 7.	Network       Protocols       Adapters       Bindings         Network Protocols:       Image: Comparison of the second
4.	Highlight <b>TCP/IP Protocol</b> and click <b>OK</b> .	Select Network Protocol       ? ×         Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.         Network Protocol:         * NetBEUI Protocol         * NwLink IPX/SPX Compatible Transport         * Streams Environment         * TCP/IP Protocol         * TCP/IP Protocol         * Cancel
5.	Insert the Windows NT CD into your CD-ROM drive and type the location of the CD. Then click <b>Continue</b> .	Windows NT Setup       Image: Continue Setup will look for the files in the location specified below. If you want Setup to look in a different place, type the new location. When the location is correct, click Continue.       Continue Cancel         d/u386       d/u386

6. When returning to the **Network** window. Open the **Protocols** tab, then select **TCP/IP Protocol** and click **Properties**.

work			1
entification Se	rvices Protocol	S Adapters Bind	lings
Network Protoco	ols:		
¥ NetBEUI Pr ¥ NWLink IP; ¥ NWLink Ne ¥ <mark>TCP/IP Pro</mark> l	X/SPX Compatibl :tBIOS	le Transport	
<u>A</u> dd	<u>R</u> emove	Properties	<u>U</u> pdate
area network p		net Protocol. The d ides communication s.	
		Close	Cance
An IP address c by a DHCP serv	an be automatica er. If your netwo k administrator fo	ss Routing ally assigned to this rk does not have a r an address, and t	DHCP server,
Address DNS An IP address c by a DHCP serv ask your networ	an be automatica er. If your netwo k administrator fo	ally assigned to this rk does not have a	network card DHCP server,
Address DNS An IP address c by a DHCP serv ask your networ the space below Adapter:	an be automatica er. If your netwo k administrator fo	Ily assigned to this rk does not have a r an address, and t	network card DHCP server, hen type it in
Address DNS An IP address c by a DHCP serv ask your networ the space below Adapter: [1] Intel 82594	WINS Addre an be automatica er. If your netwo k administrator fo  5-Based Etherm IP address from a n IP address	elly assigned to this rk does not have a r an address, and th et	network card DHCP server,
Address DNS An IP address c by a DHCP serv ask your networ the space below Adapter: [1] Intel 82598 © Obtain an © Specify as [P Address:	WINS Addre an be automaticz er. If your netwo k administrator fo v. 5-Based Etherm IP address from i n IP address	elly assigned to this rk does not have a r an address, and th et	network card DHCP server, hen type it in
Address DNS An IP address c by a DHCP serv ask your networ the space below Adapter: [1] Intel 82598 © Obtain an © Specify at IP Address: Subnet Mask	WINS Addre an be automaticz er. If your netwo k administrator fo v. 5-Based Etherm IP address from i n IP address	elly assigned to this rk does not have a r an address, and th et	network card DHCP server, hen type it in
Address DNS An IP address c by a DHCP serv ask your networ the space below Adapter: [1] Intel 82598 © Obtain an © Specify at IP Address: Subnet Mask	WINS Addre an be automaticz er. If your netwo k administrator fo v. 5-Based Etherm IP address from i n IP address	elly assigned to this rk does not have a r an address, and th et	network card DHCP server, hen type it in
Address DNS An IP address c by a DHCP serv ask your networ Adapter: [1] Intel 82594 © Obtain an © Specify as IP Address: Sybnet Mask Default Gate	WINS Addre an be automatica er. If your netwo k administrator for 5-Based Etherm IP address from in n IP address way:	ally assigned to this rk does not have a r an address, and the et a DHCP server	network card DHCP server, hen type it in
Address DNS An IP address c by a DHCP serv ask your networ Adapter: [1] Intel 82594 © Obtain an © Specify as IP Address: Sigbnet Mask Default Gate	WINS Addre an be automaticz er. If your netwo k administrator fo v. 5-Based Etherm IP address from i n IP address wey OK	ally assigned to this rk does not have a r an address, and the et a DHCP server	network card DHCP server, hen type it in Advanced <u>Advanced</u> <u>aure your</u> neters specified

7. Enable Obtain an IP address from a DHCP server and click OK.

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

When returning to Network Network ? × window, click Close. Identification Services Protocols Adapters Bindings Network Protocols: 🐨 NetBEUI Protocol 🐨 N WLink IPX/SPX Compatible Transport 🍞 NWLink NetBIOS TCP/IP Protocol <u>A</u>dd.. <u>R</u>emove Properties.. Description: Transport Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Close 10. When prompted with **Network** Network Settings Change Settings Change dialog box, You must shut down and restart your computer before the new settings will take effect. <u>^</u>} click Yes to restart your computer. Do you want to restart your computer now? Yes <u>N</u>o

### For Windows 2000

9.

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



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



General

Connect using:

Install.

Description

Intel 82595-Based Ethernet

Internet Protocol (TCP/IP)

Show icon in taskbar when connected

Components checked are used by this connection:

☑ 🚚 File and Printer Sharing for Microsoft Networks

Uninstall

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK

Configure

Properties

Cancel

 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 6.

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

Select Network Component Type 🛛 🔹 🔀
Click the type of network component you want to install:
📃 Client
Service
Trotocol
Description
A protocol is a language your computer uses to
communicate with other computers.
Add Cancel
N

Click Internet Protocol (TCP/IP) and then click OK.	Select Network Protocol Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.
	Manufacturers:         Network Protocol           Microsoft         AppleTalk Protocol           DLC Protocol         DLC Protocol           Internet Protocol (TCP/IP)         NetBEUL Protocol           NetWork Monitor Driver         NW/Link IPX/SPX/NetBIOS Compatible Transport Private           Image: State St
	OK Cancel
When returning to the Local Area Connection Properties window, highlight Internet Protocol (TCP/IP) and then click Properties.	Local Area Connection Properties       ? ×         General       Connect using:         Image: Intel 82595-Based Ethernet       Configure         Components checked are used by this connection:       Configure         Components checked are used by this connection:       Configure         Components checked are used by this connection:       Image: Configure         Components checked are used by this connection:       Image: Configure         Components checked are used by this connection:       Image: Configure         Image: Client for Microsoft Networks       Image: Client for Microsoft Networks         Image: Client for Microsoft Internet Protocol (ICP/IP)       Image: Client for Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.         Show icon in taskbar when connected       Close       Cencel
Under the <b>General</b> tab, enable <b>Obtain an IP address</b> <b>automatically</b> . Then click <b>OK</b> .	Internet Protocol (TCP/IP) Properties       ?         General

7.

5.

6.

nternet Protocol (TCP/IP) Properti	es ? 🗙
General	
You can get IP settings assigned auto this capability. Otherwise, you need to the appropriate IP settings.	
Obtain an IP address automatica	ally
$\square^{\mathbb{C}}$ Use the following IP address: —	
IP address:	
Subnet mask:	
Default gateway:	
Obtain DNS server address auto	omatically
C Use the following DNS server a	· · · · · · · · · · · · · · · · · · ·
Preferred DNS server:	
Alternate DNS server:	· · · ·
	Advanced
	OK Cancel

### **For Windows XP**

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



Elle Edit View Favorites Iools Help

Address 🔂 Control Panel

Control Panel

See Also

Switch to Category

Windows Update
 Help and Support

🔇 Back 👻 🕥 👻 🏂 🔎 Search 🌔 Folders 🔢 🕇

Ġ,

Accessibility Options

4

Automatic Updates

Ż

Add Hardware

P

Date and Time

ter and the second s

ø

Add or Remov...

8

Display

ø

🖌 🄁 Co

**1** 

Administrative Tools

N

Folder Options

1

2. Double click the Network Connection.

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



the <b>General</b> tab, check out list of installed network	Local Area Connection Properties
tion 1: If there is <b>no</b> TCP/IP ptocol, click <b>Install</b> .	Connect using: B Intel(R) PR0/1000 PM Network Con
tion 2: If you have TCP/IP otocol, skip to Step 7.	This connection uses the following items:
If there is <b>no TCP/IP</b> protocol installed on your PC, press <b>Install</b> to continue.	Install       Properties         Description       Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.         Show icon in notification area when connected         ✓ Notify me when this connection has limited or no connectivity
	OK Cancel
k Ádd.	Select Network Component Type  Click the type of network component you want to install:  Client Service Protocol  Description  A protocol is a language your computer uses to communicate with other computers.  Add Cancel
ck Internet btocol(TCP/IP) and then ck OK.	Select Network Protocol         Image: Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.         Network Protocol:         Image: Network Protocol         Image: Network Protocol         Network Protocol:         Network Protocol:         Network Monitor Driver         Network Monitor Driver         Network Protocol(TCP/IP)         Internet Protocol(TCP/IP)         Internet Protocol(TCP/IP)         Internet Protocol(TCP/IP)         Ital me why driver signing is important         UK         Cancel
	List of installed network inponents. tion 1: If there is no TCP/IP intocol, click Install. tion 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. chlight Protocol and then k Add. ck Internet protocol (TCP/IP) and then

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



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

nternet Protocol (TCP/IP) Prop	erties 🛛 📝 🛂
General Alternate Configuration	
You can get IP settings assigned auto this capability. Otherwise, you need to the appropriate IP settings.	
Obtain an IP address automatica	ally
$\bigcirc \bigcirc$ Use the following IP address: –	
IP address:	
S <u>u</u> bnet mask:	
Default gateway:	
Obtain DNS server address auto	maticallu
O Use the following DNS server address date	
Preferred DNS server:	
	Ad <u>v</u> anced
	OK Cancel

### **For Windows Vista**

2.

3.

Internet.

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



4.

5.

6.

Click Manage Network 🕒 🕞 = 😫 « Network and Int Connection on the left ork and Sharing Center side. <u>.</u> ASKEY-PC (This comput (Private network) Local and Internet Local Area Co Sharing and Discovery Network discovery e On File sharing o Off • Public folder sharing e Off • Printer sharing € Off (r  $\odot$ Darr word pr • On • Media sharing e off Right click Local Area net + Nets • 49 S 🕡 ee Ne **Connection** and select Properties. Тур Local Area Connection Disable Status PPTP(Nortel) L2TP Diagnose Bridge Cor Create Shortcut Rename Properties On the **Networking** tab, X Local Area Connection Properties you will find Internet Networking Protocol Version 6 and Version 4. Contact your Connect using: ISP to confirm which one 👰 Broadcom NetLink (TM) Gigabit Ethernet will be used. (We take TCP/IPv4 for example Configure... here.) This connection uses the following items: Select Internet Protocol Client for Microsoft Networks Version 4 (TCP/IPv4) and press Properties. ☑ 📮 File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) 🗹 📥 Internet Protocol Version 4 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder Install. Uninstall **Properties** ( Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. OK Cancel

7. Under the General tab, select Obtain an IP address automatically, and Obtain DNS server address automatically. Then click Ok to exit.

nternet Protocol Version 4 (TCP/IPv4)	
General Alternate Configuration	
You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings.	
Obtain an IP address automatical	y.
Use the following IP address:	
IP address:	
S <u>u</u> bnet mask:	
Default gateway:	
Obtain DNS server address autom	natically
Use the following DNS server add	resses:
Preferred DNS server:	
Alternate DNS server:	
	Ad <u>v</u> anced
	OK Cancel

2 2

## Renewing IP Address on Client PC

After the ADSL Router 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 98/ME

1. Select Run from the Start menu.



- 2. Type **winipcfg** in the text box and click **OK**.
- Run
   ? ×

   Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
   Internet

   Open:
   winipcfg
   Image: Cancel Browse...

   Image: Proofiguration
   Image: Cancel Cancel
- 3. When the figure below appears, click **Release** to let go of the address and then click the **Renew** button to obtain a new IP address.

Adapter Address           IP Address           Subnet Mask           255.255.255.0           Default Gateway           192.168.1	IP Address 192.168. 1 .2 Subnet Mask 255.255.0		Intel 82595	-Based Ethernet
Subnet Mask 255.255.0	Subnet Mask 255.255.0	Adapter Address		
205.205.255.0	200.200.200.0	IP Address	192.	168. 1 .2
Default Gateway 192.168, 1, 1	Default Gateway 192.168. 1 .1	Subnet Mask	255.	255.255.0
		Default Gateway	192.	168. 1 .1
OK Release Renew		Release All Re	new All	More Info >>

### For Windows NT/2000/XP

- Open the Start menu, and click 1. Run... on this menu.
- 8 WinZip **Programs** Þ Documents <u>S</u>ettings <u>F</u>ind <u>H</u>elp 24 <u>R</u>un. 🛐 🛛 Sh<u>u</u>t Down.. 🚮 Start

Run

2

cmd Open:

indows IP Configuration

nnectio Add

adapter Local Area Connection:

n-specific DNS Suffix

- 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.



Type the name of a program, folder, or document, and Windows will open it for you.

Cancel

🔽 Run in Separate Memory Space

? ×

•

Browse..

 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.



### **For Windows Vista**

1. Open the **Start** menu, and type **cmd** in the text box then click **OK**.



- 2. The command prompt window will appear.
- 3. Type **ipconfig** at the command window and press **Enter** to view the computer's IP information from DHCP server.
- 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.

#### Note:

If you cannot release the IP address successfully and see the message "The requested operation requires elevation," please go to the Start menu and right click Command Prompt, then set Run as administrator.

Press **Continue** when a dialog asking for permission to continue prompts.

After then, repeat the above instruction to release and renew the IP address.



# **Chapter 3: Accessing the Internet**



This chapter aims to help you access the Internet in a quick and convenient way. If you need more detailed information for web configuration, please refer to the next chapter for the advanced configuration.

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

- □ PPP over ATM (PPPoA)
- PPPoA IP Extension
- PPP over Ethernet (PPPoE)
- PPPoE IP Extension
- □ 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 ADSL Router 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.

## PPP over ATM (PPPoA) Mode



#### **Description:**

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

- 1. Start your browser and type **192.168.1.1** as the address to access ADSL web-based manager.
- 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**.
- 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.
- 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 ATM (PPPoA) IP Extension Mode

#### **Description:**

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

- 1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
- 2. Go to Advanced Internet Connections. And click Add.
- Key in the VCI and VPI value, e.g.:
   VPI 0
   VCI 38
   Click the Next button.
- On the Configure Internet Connection Connection Type page, select PPP over ATM (PPPoA) then click the Next button.
- On the WAN IP Settings page, select Obtain an IP address automatically, check PPP IP extension (and Enable NAT would become disabled automatically) then click Next.
- 6. On the **PPP Username and Password** page, enter the PPP username and password offered by your ISP. Select **Always on**, and then click **Next**.
- 7. Check the network information on **This Internet Connection Summary** page. Make sure the settings match the settings provided by the ISP. Click **Apply**.
- 8. Press Finish.



## PPP over Ethernet (PPPoE) Mode

#### **Description:**

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

- 1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
- 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**.
- 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) IP Extension Mode

#### **Description:**

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

- 1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
- 2. Go to Advanced Internet Connections. And click Add.
- Key in the VCI and VPI value, e.g.:
   VPI 0
   VCI 39
   Click the Next button.
- 4. On the **Configure Internet Connection Connection Type** page, select **PPP over Ethernet (PPPoE)** then click the **Next** button.
- 5. On the WAN IP Settings page, select Obtain an IP address automatically, check PPP IP extension (and Enable NAT would become disabled automatically) then click Next.
- 6. On the **PPP Username and Password** page, enter the PPP username and password offered by your ISP. Select **Always on**, and then click **Next**.
- 7. Check the network information on **This Internet Connection -- Summary** page. Make sure the settings match the settings provided by the ISP. Click **Apply**.
- 8. Press 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 ADSL Router and public server, e.g., Web or FTP server. Typically the first IP is network address, the second is used as router IP address and the last one is 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 10.11.80.81 to 10.11.80.86 and the subnet mask for LAN is 255.255.248. The WAN IP address is 10.11.95.233, 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.
- 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**.
- 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: 10.11.95.233
  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: 10.11.80.81

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: 10.11.80.82
  Subnet Mask: 255.255.255.248
  Gateway: 10.11.80.81
  Preferred DNS server: 168.95.1.1
- 9. Now the router 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 ADSL Router or use another NAT box connected to hub) to support multiple clients to access the Router and some public servers (WWW, FTP).

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

The following example uses the IP address ranging from 10.11.80.81 to 10.11.80.86 and the subnet mask is 255.255.255.248.

- 1. Start your browser and type **192.168.1.1** in the URL box to access ADSL web-based manager.
- 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**.
- 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: 10.11.80.81
   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 router is well configured. You can access into Internet.
# Unnumbered IP over ATM (IPoA)



# **Description:**

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

The following example uses the IP address ranging from 10.11.80.81 to 10.11.80.86 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.
- 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.
- On the Configure Internet Connection Connection Type page, select IP over ATM (IPoA) then click Next.
- 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
- Check Configure the second IP Address and Subnet Mask for LAN Interface and enter the information needed, e.g., Secondary IP Address: 10.11.80.81 Subnet mask: 255.255.258.248 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: 10.11.80.82
  Subnet Mask: 255.255.255.248
  Gateway: 10.11.80.81
  Preferred DNS server: 168.95.1.1
- 9. Now the router is well-configured. You can access the Internet.



# Unnumbered IP over ATM (IPoA)+NAT

### **Description:**

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

The following example uses the IP address ranging from 10.11.80.81 to 10.11.80.86 and the subnet mask is 255.255.255.248. In such circumstance, we enable NAT function but 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.
- 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**.
- 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.
- 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

- Check Configure the second IP Address and Subnet Mask for LAN Interface and enter the information needed, e.g., Secondary IP Address: 10.11.80.81 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 router is well-configured. You can access the Internet.



# **Description:**

In this example, the ADSL Router 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.
- 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.
- 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: 10.11.86.81
  Subnet Mask: 255.255.255.248
  Gateway: 10.11.86.1
  Preferred DNS server: 168.95.1.1
- 9. Click OK. Now the router is well-configured. You can access to the Internet.

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

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.
- 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 router is well-configured. You can access the Internet.

# **Chapter 4: Web Configuration**



Some users might want to set specific configuration for the router such as firewall, data transmission rate..., and so on. This chapter will provide you advanced information of the web pages for the router for your reference.

# Using Web-Based Manager

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

Connect to 19	2.168.1.1	
44	4/4	Å.
Wireless ADSL2+	Router	
User name:	😰 admin	*
Password:	•••••	
	Remember my password	

- Start your web browser and type 192.168.1.1, the private IP address of the ADSL Router, in the URL field.
- After connecting to the device, you will be prompted to enter username and password. By default, both the username 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 ADSL Router acts as a web server sending HTML pages/forms on your request. You can fill in these pages/forms and apply them to the ADSL Router.

# **Outline of Web Manager**

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

			×
DSL	Quick Start   Status   Adv	anced   Wireless	1 Management
			Language: English 💌
Connect to Internet	Connect to Internet	<b>connect</b> to Broadband.	
(Title)	Enter your Broadband use Internet Connection: Total Online Time: Broadband User Name Password	er name and password, th pppoe_8_35_1 0 secs	nen dick "Connect".
	Connect		
firmware: 3.61j ADSL2+: A2pB022c.d20d Wireless: 3.131.35.4	Current Version	× × · · · ·	Main Window

**Title**: The title of this management interface.

Main Including Quick Start, Status, Advanced, Wireless, and Management.

MainThe current workspace of the web manager, containing configurationWindow: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 router. And only after rebooting the router, 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.)



# **Quick Start**

The pages under the Quick Start menu provide user a quick way to set up the router. If you do not know much about the router, you can use the Quick Start pages to adjust basic settings to activate your router.

# **Connect to Internet**

This is a quick way to connect to the Internet by using PPPoE interface, please click **Connect to Internet** to open the web page.

Enter the user name and password (that you get from the ISP) for your ADSL router and click **Connect**.

The system will connect automatically, and then you can access the Internet.

### <u>Connect to Internet</u>

Your ADSL router is ready to connect to Broadband

Enter your Broadband user name and password, then click "Connect".			
Internet Connection:	pppoe_8_35_1		
Total Online Time:	0 secs		
Broadband User Name			
Password			
Connect			

# **Quick Setup**

The quick setup wizard will guide you to configure the ADSL router through some specific steps. Yet different connection interface will lead to different setting pages. Refer to the following pages for detailed information.

# Auto Scan Internet Connection (PVC):

If there is no any PVC configured in your ADSL router, you can check this item. Otherwise, please uncheck this box.

VPI (Virtual Path Identifier): Identifies the virtual path between endpoints in

an ATM network. The valid range is from 0 to 255. To enter the setting, please refer to the setting that the ISP offered.

### VCI (Virtual Channel Identifier):

Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols). To enter the setting, please refer to the setting that the ISP gave you.

After entering the VPI/VCI value, please click **Next** for the following step.

### Quick Setup

This Quick Setup will guide you through the steps necessary to configure your ADSL router. Select the check box below to scan the Internet connection automatically. It is recommended that there is no any PVC configured in your ADSL router before performing auto-scanning connection. Auto Scan Internet Connection (PVC)

Auto Scan Internet Connection (PVC)

### Configure Internet Connection -- ATM PVC

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



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

Next >

# **Connection Type**

The system provides several protocols for you to choose. Your ISP will offer you the most suitable settings of the protocol. Before you set this page, please refer to the protocol that your ISP offered.

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

For instance, PPP over Ethernet (PPPoE) is selected in this demonstrative figure.

Configure Inte	rnet Connection - Connection Type
Select the prot instructed you	ocol and encapsulation type with the ATM PVC that your ISP ha to use.
Protocol:	PPP over ATM (PPPoA)     PPP over Ethernet (PPPoE)
	O IP over ATM (IPoA)

Encapsulation Type: LLC/SNAP 🔽

🔘 Bridging

Configure Internet Connection - Connection Type

< Back Next >

# **PPP over ATM/ PPP over Ethernet**

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

According to the ISP's configuration on the server, you can choose PPPoE Select the protocol and encapsulation type with the ATM PVC that your ISP has or PPPoA modes.

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

instructed you to us	).	
Protocol:	<ul> <li>PPP over ATM (PPPoA)</li> <li>PPP over Ethernet (PPPoE)</li> <li>IP over ATM (IPoA)</li> <li>Bridging</li> </ul>	
Encapsulation Type:		
Configure Internet	_ < Back   Next >	J

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

Check Enable NAT if you need.

### MTU:

It means the maximum size of the packet that transmitted in the network. The packet of the data greater than the value set here will be divided into several packets for transmitting.

Type the value into the field of MTU. The default MTU value for PPPoE is 1492; while for PPPoA is 1500.

Click Next for the next procedure.

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

Obtain an IP address automatically

<ul> <li>Use the following IP</li> </ul>	address:
WAN IP Address:	0.0.0.0

🗹 Enable NAT

MTU: 1492 (default: 1492)

< Back Next >

### **PPP Username & PPP Password:**

Key in the username and password that you received from your ISP. (e.g., *askey4/askey4*)

### Always On:

Select this item to make the connection active all the time.

# **Dial on Demand:**

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

### Manually Connect:

Select this item to make a connection by pressing the <u>Connect</u> hyperlink on the Advanced Setup-Internet-Connections web page.

# On the **Configure LAN side Settings** page, you have to fill in the data requested.

### Primary IP Address & Subnet Mask:

Key in the information that offered by your ISP for the LAN connection.

# Configure the secondary IP Address and Subnet Mask:

Check this box to set up a secondary IP Address to connect to your router if they are not included in the range that DHCP server accepts. See the next figure for the secondary IP address and subnet mask.

# Secondary IP Address & Subnet Mask:

Key in the second IP address and the subnet mask received from the ISP for your LAN connection.

**MTU:** (refer to the WAN section) The default **MTU** value for **LAN side Settings** is 1500. You may modify it if necessary.

# **DHCP Server On:**

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

# Start IP Address & End IP Address: Enter the information needed.

### Lease Time:

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

### **DHCP Server Off:**

Check this item if DHCP service is not needed on the LAN.

### Configure Internet Connection - PPP User Name and Password

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

PPP User Name: PPP Password:	askey4	
Session established by:	Dial on Demand     Disconnect if no activity for 20     Manually Connect     Disconnect if no activity for 20	minutes minutes Back Next >

### Configure LAN side Settings

Enter the ADSL router IP address and subnet mask for LAN interface and then enable DHCP server on LAN interface to provide IP address settings for your computers.

Primary IP Address:	192.168.1.1		
Subnet Mask:	255.255.255.0		
Configure secondar	y IP address and	subnet mask	
MTU:	1500 (default	: 1500)	
OHCP Server On	Start IP:	192.168.1.2	
	End IP:	192.168.1.254	
	Lease Time:	1 days 0 ho	ours 0 minutes
O DHCP Server Off			
			< Back Next >

On this web page, the primary IP address and subnet mask will be shown on it. You can modify them if needed.

### Configure LAN side Settings

Enter the ADSL router IP address and subnet mask for LAN interface and then enable DHCP server on LAN interface to provide IP address settings for your computers.

Primary IP Address:	192.168.1.1	
Subnet Mask:	255.255.255.0	
Configure secondar	y IP address and	d subnet mask
Secondary IP Address:		
Subnet Mask:		
MTU:	1500 (default	:: 1500)
OHCP Server On	Start IP:	192.168.1.2
	End IP:	192.168.1.254
	Lease Time:	1 days 0 hours 0 minutes

DHCP Server Off

Key in all the necessary settings and click **Next** for the coming page. You can check the contents on the Summary page.

If you find anything incorrect, click Back to modify the settings.

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

This Internet Connection -- Summary

VPI / VCI	0/39
Connection Type	PPPoE LLC/SNAP, Dial on Demand, Idle Timer 20 mins, QoS On
NAT	Enabled
WAN IP Address	Automatically Assigned
Default Gateway	Automatically Assigned
DNS Server	Automatically Assigned
AN Configuration:	
Primary LAN IP	192.168.1.1 / 255.255.255.0
	0.0.0.0 / 255.255.255.255
Secondary LAN IP	
Secondary LAN IP DHCP Server	On 192.168.1.2 ~ 192.168.1.254

Now, the system will reboot to activate Reboot ADSL Router the new settings that you have set in this section.

Please wait for 2 minutes before restarting the router.

The ADSL router has been configured and is rebooting.

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

# **IP over ATM**

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

Protocol:

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

Choose IPoA and click Next.

### Configure Internet Connection - Connection Type

Select the protocol and encapsulation type with the ATM PVC that your ISP has instructed u to use

> O PPP over ATM (PPPoA) PPP over Ethernet (PPPoE) IP over ATM (IPoA) O Bridging

Encapsulation Type: LLC/SNAP 🔽

### < Back Next >

### None:

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

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

### WAN IP Address & WAN Subnet Mask:

If you choose Use the following IP address, you have to enter the IP address and subnet mask information received from the ISP for the WAN interface.

### **Obtain DNS server address** automatically:

Only when you select Obtain an IP address automatically that this option is available. You may click this button to allow the system to get DNS server address automatically.

## Use the following DNS server addresses:

Select this item to set the DNS server addresses manually, type the information provided by your ISP in the following Primary DNS and Secondary DNS server entries, e.g. 168.95.1.1 and 168.95.192.1.

Click Enable NAT if you want.

On the Configure LAN side Settings Configure LAN side Settings page, you have to fill in the data requested.

### Primary IP Address & Subnet Mask:

Key in the information that offered by your ISP for the LAN connection, e.g., 192.168.1.1 for IP address and 255.255.255.0 for subnet mask.

### MTU:

(Please refer to the PPPoA/ PPPoE section.) The default MTU setting here is 1500. You may modify it if necessary.

### Configure Internet Connection - WAN IP Settings

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

$\sim$			
0	Obtain an I	P address	automaticall

- O Use the following IP address:
- WAN IP Address: WAN Subnet Mask:
- Obtain DNS server address automatically Output the following DNS server addresses:
- Primary DNS server: 168.95.1.1 Secondary DNS server: 168.95.192.1

🗹 Enable NAT

< Back Next >

After setting up the WAN IP and DNS server information, click Next to open the following page.

Enter the ADSL router IP address and subnet mask for LAN interface and then enable DHCP server on LAN interface to provide IP address settings for your computers.

Primary IP Address:	192.168.1.1		
Subnet Mask:	255.255.255.0		
🗌 Configure secondar	y IP address and	l subnet mask	
MTU:	1500 (default	: 1500)	
OHCP Server On	Start IP:	192.168.1.2	
	End IP:	192.168.1.254	
	Lease Time:	1 days 0 k	ours 0 minutes
O DHCP Server Off			
			< Back Next >

### Configure the secondary IP Address and Subnet Mask for LAN interface:

Check this box to set up a secondary IP Address to connect to your router if they are not included in the range that DHCP server accepts. You have to key in the information received from your ISP for the LAN connection, e.g., the secondary IP is 10.11.80.81 and the mask is 255.255.255.248 in the example illustrated in the figure.

### **DHCP Server On:**

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

# Start IP Address & End IP Address:

Enter the information needed.

## Lease Time:

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

### **DHCP Server Off:**

Check this item if DHCP service is not needed on the LAN.

You can check the settings on the Summary page.

If you find anything incorrect, click Back to modify the settings.

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

And the following page will appear.

Now, the system will reboot to activate Reboot ADSL Router the new settings that you have set in this section.

Please wait for 2 minutes before restarting the router.

### Configure LAN side Settings

Enter the ADSL router IP address and subnet mask for LAN interface and then enable DHCP server on LAN interface to provide IP address settings for your computers.

Primary IP Address:	192.168.1.1	
Subnet Mask:	255.255.255.0	
Configure secondar	y IP address and su	ubnet mask
Secondary IP Address:	10.11.80.81	
Subnet Mask:	255.255.255.248	
MTU:	1500 (Default: 1	500)
OHCP Server On	Start IP:	192.168.1.2
	End IP:	192.168.1.254
	Lease Time:	1 days 0 hours 0 minutes
O DHCP Server Off		

< Back Next >

## Key in all the necessary settings. Click Next for the coming page.

### This Internet Connection -- Summary

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

VPI / VCI	0 / 32
Connection Type	IPoA LLC/SNAP, QoS On
NAT	Enabled
WAN IP Address	10.11.80.81
Default Gateway	0.0.0.0
DNS Server	168.95.1.1 ; 168.95.192.1
AN Configuration:	
Primary LAN IP	192.168.1.1 / 255.255.255.0
Secondary LAN IP	10.11.80.81 / 255.255.255.248
DHCP Server	On 192.168.1.2 ~ 192.168.1.254
DHCP Server	

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

< Back Finish

The ADSL router has been configured and is rebooting.

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

# Bridging

If the mode you choose is Bridging (or MER), please refer to the following information.

The bridging mode can configure your Configure Internet Connection - Connection Type router to send and receive packets between LAN and WAN interfaces. The WAN interface is ATM PVC: the LAN interface can be Ethernet, USB, or Wireless.

Choose Bridging and click Next.

### None:

If it is not necessary to set the WAN IP address, please click this button. In our example, we select this item.

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

WAN IP Address, WAN Subnet Mask, and Default Gateway: When choosing Use the following IP address, you have to key in the IP address, the subnet mask, and the default gateway provided by your ISP for the WAN interface.

While you choose to obtain the IP address automatically or use specific IP address, you have to decide whether to select Obtain DNS server address automatically or Use the following DNS server address and enter the information provided by you ISP.

Check Enable NAT if necessary.

Press Next to continue.

# Primary IP Address & Subnet Mask: Configure LAN side Settings

Key in the IP address and the subnet mask that provided by your ISP for LAN interface, e.g., 192.168.1.1 and 255.255.255.0, respectively.

MTU: Please refer to PPPoA/ PPPoE. MTU:

### **DHCP Server On:**

Check this item if DHCP service is needed on the LAN. The router will assign IP address and gateway address for each of your PCs. Enter the information for Start IP, End IP and Lease Time if you enable this function. The default value for lease time is one day.

### **DHCP Server Off:**

Check this item if DHCP service is not needed on the LAN; like our example.

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

Protocol:	PPP over ATM (PPPoA)
	PPP over Ethernet (PPPoE)
	🔘 IP over ATM (IPoA)
	💿 Bridging

Encapsulation	Type:	LLC/SNAP	~

### < Back Next >

Configure Internet Connection - WAN IP Setting

Enter	nformation	provided to	) you	i by your	· ISP t	o configure	the	WAN II	P settir	ıgs

💌 None	
🔘 Obtain an IP addres	s automatically
🔘 Use the following IP	address:
WAN IP Address:	
WAN Subnet Mask:	
Default Gateway:	

< Back Next >

### The default setting is none, while selecting Obtain an IP address automatically or Use the following **IP address**, the DNS setting appears, shown as the figure below.

Configure Internet Connection - WAN IP Setting

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

🔘 None	
<ul> <li>Obtain an IP address automatically</li> </ul>	
O Use the following IP address:	
WAN IP Address:	
WAN Subnet Mask:	
Default Gateway:	
<ul> <li>Obtain DNS server address automatically</li> </ul>	
O Use the following DNS server addresses:	
Primary DNS server:	
Secondary DNS server:	
💌 Enable NAT	
	< Back Next >

Enter the ADSL router IP address and subnet mask for LAN interface and then enable DHCP server on LAN interface to provide IP address settings for your computers.

Primary IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
<b>—</b> • •	

Configure secondary IP address and subnet masl

### 1500 (default: 1500)

O DHCP Server On	Start IP:	192.168.1.2
	End IP:	192.168.1.254
	Lease Time:	1 days 0 hours 0 minutes
DHCP Server Off		

< Back Next >

You can check the settings on the Summary page now.

If you find anything incorrect, click Back to modify the settings.

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

And the following page will appear.

Now, the system will reboot to activate Reboot ADSL Router the new settings that you have done in The ADSL router has been configured and is rebooting. this section.

Please wait for 2 minutes before restarting the router.

This Internet Connecti	on Summary
Make sure that the set	ings below match the settings provided by your ISP.
Internet (WAN) Confi	guration:
VPI / VCI	0/35
Connection Type	Bridge LLC/SNAP, QoS On
Connection Type	Bridge LLC/SNAP, QoS On
	Bridge LLC/SNAP, QoS On 192.168.1.1 / 255.255.255.0
LAN Configuration:	

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

# Status

# **Overview**

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

## **Device Information**

This information reflects the current status of your ADSL router.

System Up Time	00:00:06:17		
ADSL Speed (DS/US)	7616/832 Kbps		
LAN IP Address	192.168.1.1		
Default Gateway	10.11.95.233		
Primary DNS server	168.95.1.1		
Secondary DNS server	168.95.192.1		
Firmware Version	3.61j		
Boot Loader Version	1.0.37-6.8.4		
ADSL Driver Version	A2pB022c.d20d		
Wireless Driver Version	3.131.35.4.cpe1.0 (Wireless is enabled)		
Wireless BSSID	00:11:F5:8D:30:D5		
Ethernet MAC Address	00:11:F5:8D:30:D2		
USB MAC Address	00:11:F5:8D:30:D3		
Memory Size	4MB Flash / 16MB SDRAM		

# **ADSL Line**

This page shows all information for ADSL.

For knowing the quality of the ADSL connection, please click ADSL BER Test button to have advanced information.

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

### ADSL Line Status

Current ADSL line status is displayed as the below.

Line Mode	G.DMT	G.DMT Line State		Show Time	
Latency Type	Interleave	Line Up Tim	Line Up Time		
Line Coding	Trellis On	Line Up Cou	Line Up Count		
Statistics	Downstrea	Downstream		Upstream	
Line Rate	7616 Kbps	7616 Kbps			
Attainable Line Rate	11328 Kbps	11328 Kbps			
Noise Margin	22.2 dB	22.2 dB			
Line Attenuation	2.0 dB	2.0 dB			
Output Power	7.7 dBm		11.9 dBm		

More Information >>

ADSL BER Test

ADSL BER Test	🗿 http://192.168.1.1/berstart.tst?berState=0 - Microsoft 🔳 🔲 🔀				
This test determines the quality of the	ADSL BER Test - Start				
ADSL connection. It is done by transferring idle cells containing a known pattern and comparing the	The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.				
received data with this known pattern to check for errors.	Select the test duration below and click "Start".				
to check for errors.	Tested Time (sec): 20 💌				
	[Start] Close				
After selecting the test duration time	🗿 http://192.168.1.1/berrun.tst?berTime=20 - Microsof 🔳 🗖 🗙				
and click <b>Start</b> , the following dialog appears to tell you the test is running.	ADSL BER Test - Running				
You can stop the test by clicking Stop	The ADSL BER test is in progress. The connection speed is 7616 Kbps. The test will run for 20 seconds.				
or close this dialog window by pressing <b>Close</b> .	Click "Stop" to terminate the test.				
	Stop Close				
	V				
When the test is over, the result will be	🗿 http://192.168.1.1/berstop.tst - Microsoft Internet Ex 💽 🗖 🗙				
shown on the following dialog window for your reference. Click <b>Close</b> to	ADSL BER Test - Result				
close this window.	The ADSL BER test completed successfully.				
	Tested Time 20				
	Total Transferred Bits 137950464 Total Error Bits 0				
	Error Ratio 0.00e+00				
	Close				
	1				

# **Internet Connection**

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

# **Traffic Statistics**

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

You may click Reset to reset the amount.

### Internet Connection

Current Internet connections are listed below

PVC Name	<b>V</b> PI/VCI	Category	Protocol	NAT	QoS	WAN IP Address	Status / Online Time
pppoe_0_39_1	0/39	UBR	PPPoE LLC/SNAP	On	On	10.11.65.13	Up 00:00:43:40

### Traffic Statistics

The statistics of user data going through your ADSL router are listed below.

Interface	Received			Transmitted				
Internace	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
Ethernet	34307487	64762	0	0	38009659	62199	0	0
USB	0	0	0	0	0	0	0	0
Wireless	0	0	0	0	98738	644	0	0
WAN	30190656	47126	0	0	34306656	51247	0	0

Reset

# **DHCP** Table

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

### DHCP Table

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

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

# Wireless Clients

This table shows the MAC address for Wireless Clients Table all of the wireless LAN clients currently associated to your ADSL Router.

All of wireless LAN clients currently associated to your ADSL router are listed below.

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

MAC Address On-line Time

# **Routing Table**

This table shows the routing rules that Routing Table your router uses.

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

Destination	Netmask	Gateway	Interface	Metric
10.11.95.233	255.255.255.255	0.0.0.0	pppoe_0_39_1	0
192.168.1.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	10.11.95.233	pppoe_0_39_1	0

# **ARP** Table

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

### ARP Table

The IP-to-Physical address translation entries recorded in your ADSL router are listed below.

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

# 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.

Ho: Dor

### **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.

### LAN IP Address Configuration

Enter the ADSL router IP address and subnet mask for LAN interface.

Primary IP Address:	192.168.1.1	
Subnet Mask:	255.255.255.0	
Host Name:	RTA1025W	
Domain Name:	home	
🔲 Configure secondary	y IP address and subn	et mask

1500 (Default: 1500) MTU:

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

### Host Name:

List the host name of this device.

# Domain Name:

List the name of the domain.

### Configure the secondary IP Address and Subnet Mask:

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

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 for LAN configuration is 1500.

# Apply:

Click this button to activate the settings listed above.

### LAN IP Address Configuration

Enter the ADSL router IP address and subnet mask for LAN interface.

Primary IP Address:	192.168.1.1	
Subnet Mask:	255.255.255.0	
lost Name:	RTA1025W	
Domain Name:	home	
Configure secondary	/ IP address and subn	et mask.
Secondary IP Address:		
Subnet Mask:		
ATLI-	1500 (Default: 150)	ור

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

# Local Network – DHCP Server

This allows you to set DHCP server on LAN interface.

### **DHCP Server On:**

Check this item if DHCP service is needed on the LAN. The router 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.

### **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 router itself, you can relay to that specific server and enter the IP address of it, as *10.11.95.2* 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.

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.

### DHCP Server Configuration

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

<ul> <li>DHCP Server On</li> </ul>	Start IP:	192.168.1.2
	End IP:	192.168.1.254
	Lease Time:	1 days 0 hours 0 minutes
		Reserved IP Address List
🔿 Relay On	Relay to Server IP:	10.11.95.2

Server and Relay Off

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

### DHCP Server Configuration

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

O DHCP Server On	Start IP:	192.168.1.2
	End IP:	192.168.1.254
	Lease Time:	1 days 0 hours 0 minutes
		Reserved IP Address List
💿 Relay On	Relay to Server IP:	10.11.95.2
Server and Relay	/ Off	

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

http://192.168.1.1/viewdl	neprelist.html - Microsoft Internet Explo 🔳 🗖
Reserved IP Address L	ist
	ecific IP address for a certain PC by adding reen MAC address and IP address.
MAC Address	IP Address Delete
	Add Close
http://192.168.1.1/dhcpm	acfil.html - Microsoft Internet Explorer 📃 🗖
http://192.168.1.1/dhcpm Add a new reserved IP	
	address entry
Add a new reserved IP PC's MAC Address: (e.g.,00:90:96:01:2A:3f Assigned IP Address:	address entry
Add a new reserved IP PC's MAC Address: (e.g.,00:90:96:01:2A:3f Assigned IP Address:	address entr <b>y</b>
Add a new reserved IP PC's MAC Address: (e.g.,00:90:96:01:2A:3f Assigned IP Address:	address entr <b>y</b>
Add a new reserved IP PC's MAC Address: (e.g.,00:90:96:01:2A:3f Assigned IP Address:	address entr <b>y</b>
Add a new reserved IP PC's MAC Address: (e.g.,00:90:96:01:2A:3f Assigned IP Address:	address entr <b>y</b>

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.

http://192.168.1.1/viewdhcprelist.cgi?checkNum=7174&dhcpresli       Image: Comparison of the mapping entry between MAC address and IP address.					
MAC Address	IP Address	Delete			
00:90:96:01:2A:3B	192.168.1.2	Û			
	(Add	Close	I		
			~		

# Local Network – UPnP

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

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 ADSL Router.

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

UPnP Configuration

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 ADSL router.

🗹 Enable UPnP

Apply Cancel

# 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 this ADSL router. There are four Ethernet clients, one using USB, 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 router will

forward the multicast traffic to all hosts on all interfaces and consequently block and interrupt the traffic of USB and 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 Apply Cancel 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.

IGMP Snooping Configuration

With IGMP snooping, 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 ports which are bonded to the subscribed multicast groups.

Filtering out multicast packets which will be sent to your local network if no users play multimedia movies

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.

### IGMP Snooping Configuration

With IGMP snooping, 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 ports which are bonded to the subscribed multicast groups. Warning: To enable IGMP snooping, you must enable IGMP proxy first IGMP Snooping: Disabled O Enabled Apply Cancel

# Internet – Connections

To set WAN settings for each service, please open Advanced-Internet. This page allows you to edit, to remove, or to add WAN settings.

Internet Connection Configuration If you click the Connect hyperlink under the PVC Name item, the system Choose Add or Edit to configure Internet connection. Choose Finish to apply the changes and reboot the system will connect to WAN automatically. If the WAN connection is OK, you can check the detailed information directly.

You can add new PVC(s) by clicking the Add button, edit the settings for the present PVC by clicking ... in the Edit column, or delete the existing PVC by pressing in icon.



PVC Name	VPI/VCI	Category	Protocol	NAT	QoS	WAN IP Address	MTU	Edit
pppoe_0_39_1 Disconnect >>	0/39	UBR	PPPoE LLC/SNAP	On	On	Auto assigned	1492	<b>%</b> 0
The Internet connection is NOT active if PVC name is marked with (?). You need to click "Finish" to appl the changes and reboot the system for activating this PVC.								

Add Finish

### Adding a New One

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

### VPI (Virtual Path Identifier):

Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255. Please refer to the value that your ISP provides.

### VCI (Virtual Channel Identifier):

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

### Service Category:

It decides the size and rate for the packets of the data in different service type. There are five categories provided here for your selection, shown as the drop-down menu in the right column.

If you select UBR with PCR or CBR, you have to offer the value for the peak cell rate.

If you choose Non Realtime VBR, or Realtime VBR, you have to key in the value for the peak cell rate, sustainable cell rate, and maximum burst size.

As you can see in the right figure, the range for **Peak Cell Rate** is from 1 to 2500; the value for **Sustainable Cell** Rate ranges from 1 to 2499 and must be smaller than Peak Cell Rate, and the range for Maximum Burst Size is from 1 to 1000000.

### Configure Internet Connection -- ATM PVC

Please ent	ter VPI and VCI numbers for the Internet connection which is provided by your ISP.
VPI: 8	(0-255)
VCI: 35	(32-65535)

Service Category: UBR Without PCR 💌

< Back Next >

Configure Internet Connection -- ATM PVC

Please enter VPI and VCI numbers for the Internet connection which is provided by your ISP. VPI: 8 (0-255)

VCI: 35 (32-65535)



< Back Next >

### Configure Internet Connection -- ATM PVC

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

VPI: 8 (0-255) VCI: 35 (32-65535) Service Category: Non Realtime VBR 🛩 cell/s(1-2500) Peak Cell Rate: 0 Sus Rat

stainable Cell :e:	0	cell/s(1-2499)
kimum Burst Size:	0	cells(1-1000000)

Ma:

< Back Next >

After pressing **Next**, you will see the web page listed as the right one. Choose the protocol that you would like to use. (Here provides the example for **PPPoA**.)

Please refer to **Quick Setup** for more information if you don't know how to set the configuration.

You can check **Enable QoS** to improve performance for selected applications. More detailed information for QoS will be introduced in later instruction.

If you choose **PPPoE** (or **Bridging**), you will see the option for **802.1Q VLAN Tagging**.

# 802.1Q VLAN Tagging:

802.1Q-compliant switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN (and/or 802.1p priority) information can be inserted into an Ethernet frame. If a port has an 802.1Q-compliant device attached (such as another switch), these tagged frames can carry VLAN membership information between switches, thus letting a VLAN span multiple switches. However, it is important for network administrators to ensure ports with

non-802.1Q-compliant devices attached are configured to transmit untagged frames. Many NICs for PCs and printers are not 802.1Q-compliant. If they receive a tagged frame, they will not understand the VLAN tag and will drop the frame. Also, the maximum legal Ethernet frame size for tagged frames was increased in 802.1Q (and its companion, 802.3ac) from 1,518 to 1,522 bytes.

After checking **Enable 802.1Q VLAN Tagging**, you will have to enter a **VLAN ID**, as shown in the figure.

### VLAN ID:

The VLAN Identifier is a 12 bit field. It uniquely identifies the VLAN to which the frame belongs to and can have a value between 0 and 4095.

Click Next to continue.

### Configure Internet Connection - Connection Type

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

Protocol: 

PPP over ATM (PPPoA)
PPP over Ethernet (PPPoE)
IP over ATM (IPoA)
Bridging

Encapsulation Type: VC MUX 🛛 👻

### 🗹 Enable QoS

Enabling IP QoS for a PVC can improve performance for selected classes of applications. Please assign the priorities for various applications from the <u>Advanced...[Quality of Service</u> menu. Be aware that IP QoS also consumes system resources, the number of created PVCs will be reduced consequently.

< Back Next >

### Configure Internet Connection - Connection Type

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

rotocol:	🔘 PPP over ATM (PPPoA)
	PPP over Ethernet (PPPoE)
	🔘 IP over ATM (IPoA)
	A 1 1 1 1

🔘 Bridging

Encapsulation Type: LLC/SNAP 🔽

### 🗹 Enable QoS

Р

Enabling IP QoS for a PVC can improve performance for selected classes of applications. Please assign the priorities for various applications from the <u>Advanced. Quality of Service</u> menu. Be aware that IP QoS also consumes system resources, the number of created PVCs will be reduced consequently.

🗹 Enable 802.1Q VLAN Tagging

VLAN ID: 0 (range: 0 ~ 4095)

< Back Next >

Notice that **802.1Q VLAN Tagging** function can only be invoked under **PPPoE** and **Bridging** Mode; the system will not provide this option while setting **PPPoA** or **IPoA** mode. The **WAN IP settings** page will differ slightly according to the protocol that you choose. The graphic is the one that you will see if you choose the **PPPoE** mode in the previous step.

You can select **Enable NAT** or change the **MTU** value according to your needs.

### Add Default Route:

Check this item to add a default route.

The next figure following the WAN IP Settings in the PPPoE mode is shown at the right. You may refer to the **Quick Setup** for further information.

### Configure Internet Connection - WAN IP Settings

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

Obtain an IP address automatically     Use the following IP address:     WAN IP Address:     0.0.0.0	
✓ Enable NAT	
V Add Default Route	

< Back Next >

< Back Next >

< Back Next >

Configure Internet Connection - PPP User Name and Password In order to establish the Internet connection, please enter PPP user name and password that your ISP has provided.

PPP User Name :				
PPP Password:				
Session established by:	0 0	Always On Dial on Demand Disconnect if no activity for 20 Manually Connect Disconnect if no activity for 20		minutes
		< Ba	ick	Next >

If you choose **IP over ATM** from the **Connection Type** web page, you will get a web page as the figure.

You may refer to **Quick Start** – **Connection Type** – **IPoA** section for more information.

### Add Default Route:

Check this item to add a default IPoA route.

For example, after rebooting your router, the default route will be shown on the **Routing Table** under **Status** menu, you may check it.

If you choose **Bridging** from the **Connection Type** web page, you will get a web page as the figure listed at the right side.

Please refer to **Quick Setup** for more information.

After configuring the WAN IP Setting page, press Next, and then you will see the Summary page.

Check the information displayed here.

Enable this Internet Connection: Check the box to enable this internet connection or uncheck it to disable this setting. You may change this setting by press the Modify icon ...on the Advanced – Internet Connection Configuration page and click Next until the summary page is displayed.

### Configure Internet Connection - WAN IP Settings

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

None
 Obtain an IP address automatically
 Use the following IP address:
 WAN IP Address:
 10.11.95.233
 WAN Subnet Mask:
 255.255.255.248
 Obtain DNS server address automatically

Use the following DNS server addresses:
 Primary DNS server: 168.95.1.1

	Secondary DNS server:	
<b>~</b>	Enable NAT	
•	Add Default Route	

### <u>Routing Table</u>

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

Destination	Netmask	Gateway	Interface	Metric
10.3.95.233	255.255.255.255	0.0.0.0	pppoe_0_39_1	0
10.3.95.232	255.255.255.248	0.0.0.0	ipoa_0_32	0
192.168.1.0	255.255.255.0	0.0.0.0	br0	0
0.0.0.0	0.0.0.0	0.0.0.0	ipoa_0_32	1

### Configure Internet Connection - WAN IP Setting

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

None

Obtain an IP address automatically

Use the following IP address:
 WAN IP Address:

WAN Subnet Mask: Default Gateway:

### This Internet Connection -- Summary

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

🗹 Enable this Internet Connection

Internet (WAN) Confi	guration:	
VPI / VCI	0/38	
Service Category	UBR	
Connection Type	PPPoA VC MUX, Always On, QoS Or	n
NAT	Enabled	
WAN IP Address	Automatically Assigned	
Default Gateway	Automatically Assigned	
DNS Server	Automatically Assigned	
Click "Apply" to accept t Click "Back" to make an	nese settings. y modifications.	< Back Apply

# 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.

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.			

DNS Server Configuration				
If Enable Automatic Assigned DNS checkbox is selected, this router will accept the first received DNS assignment from the PPPDA, PPPDE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click "Apply" to save it.				
Enable Automatic Assigned DNS				
Primary DNS server: 168.95.1.1				
Secondary DNS server:				
Apply Cancel If changing from unselected Automatic Assigned DNS to selected Automatic Assigned DNS, You must reboot the router to get the automatic assigned DNS addresses.				

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 gueried, the system will send membership reports to the group.  $\triangleright$
- $\triangleright$ 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  $\triangleright$ will send a leave group membership report to the router's group.

IGMP Proxy Configuration

### Internet Connection:

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

### **IGMP Proxy Enabled:**

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

Enabling IGMP proxy function can allow the users on your local network to play the multimedia (video or audio) which sent from the servers on the Internet. Internet Connection IGMP Proxy Enabled pppoe\_0\_39\_1 **~** Apply Cancel

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

To invoke the IGMP Snooping function, the IGMP Proxy must be enabled first.

# Internet – ADSL

# Enable ADSL Port:

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

## 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.

### 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.

## Seamless Rate Adaptation:

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.

### ADSL Settings

🗹 Enable ADSL Port

Select the support of li	ne modes:	🗹 G.dmt	🗹 G.lite	🗹 T1.413
		ADSL2	READSL2	ADSL2+
		🔲 Annex M		
Capability Enabled:	🗹 Bitswap	[	Seamless R	ate Adaptatior

Apply Cancel

# **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.

### **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**.

### **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 subnet mask that you got from the ISP, type 0.0.0.0 or leave it blank.

### **Gateway IP Address:**

Click this button to forward packets to the specific gateway. Key in the gateway IP address that you want to use.

### WAN Interface:

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

# **Remove Static Route**

If you don't want the static route that you created, please click the in 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.

Add New Static Route

Static Route

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

Destination Network	(For default route, typ	e 0.0.0.0 or leave blank)
IP Address: Netmask:		]
Forward Packets to		
<ul> <li>● Gateway IP Address:</li> <li>● WAN Interface:</li> </ul>	pppoe_0_39_1 💌	]
< Back Apply		

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

Click Apply to view the routing result.



Static Route
Current static routes:
Destination Netmask Gateway WAN Interface Delete

Add

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

# 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 (Standa

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.

### **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.

### Dynamic Routing

You can enable RIP function on serveral interfaces of your ADSL router. Select the desired RIP version and operation mode, then tick the 'Enabled' checkbox to enable RIP when you click "Apply", or leave it unticked if you would like to disable RIP on those interfaces.

Interface	<b>RIP Version</b>	Operation Mode	Enabled
LAN	2 💌	Active 💌	
pppoe_0_39_1	Both 💌	Passive 🛩	

Apply Cancel

# 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.

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

After setting the virtual server, you should modify the filter rule about the port and service information which you set on the virtual server. Because the firewall protects the router by filter rule, you should update the filter rule after you set up the virtual server.

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).

### Add New Port Forwarding

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

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

### **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.

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.

### 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.

### From Internet Host IP Address:

Select the initial place for port forwarding. If you choose SINGLE, a box will appear for you to fill in the IP address for the specific host. And, if you choose SUBNET, the boxes for IP address and Netmask will appear for you to fill in the IP address and subnet mask for the specific subnet.

### Forward to Internal Host IP Address:

Key in the address for the host used as the destination that information will be forwarded to.

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



### Add New Port Forwarding Rule

Application Name:				
O Pre-defined:	Audio/Video	*	Camerades	*
🔘 User defined:				
From Internet Host IP	ALL	*		
Forward to Internal Host IP Address:				

### 

O Pre-defined:	Audio/Video	*	Media Player 7 🛛 💌
🔘 User defined:	Audio/Video Games Messaging/Conferencing Servers VPN		Gamerades GNUtella IstreamVideo2HP KaZaA Media Player 7
	Others		RealAudio RealPlayer 8 Plus SoutCast

### Add New Port Forwarding Rule



Forward to Internal Host IP Address:

By using the rules:								
Protocol	External Packet		Forward to Internal Host					
Protocol	Port Start	Port End	Port Start	Port End				
TCP 💌								
TCP 💌								
TCP 💌								

### < Back Apply

From Internet Host IP Address: Forward to Internal Host IP Address	ALL  ALL SINGLE SUBNET
From Internet Host IP Address:	SINGLE 🔽 IP Addr:
From Internet Host IP Address:	SUBNET VIP Addr:

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.

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 router 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.

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

The system provides 9 items for you to choose.

Application Name:				
Pre-defined:	Audio/Video	*	Media Player 7	*
🔘 User defined:				
From Internet Host IP	Address:	ALL	~	
Forward to Internal Host IP Address:		192.168	.1.200	

### < Back Apply

### 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	Exter	nal Packet		Internal Ho	Delete	
Application Name	IP Address	Protocol	Port	IP Address	Port	Delete
Media Player 7	ALL	TCP	1755	192.168.1.200	1755	
Media Player 7	ALL	UDP	70 - 7000	192.168.1.200	70 - 7000	

Select All

Add Delete

### Port Triggering

Port triggering funcion 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	Trig	ger	Ор	en	Delete
мррисации мате	Protocol	Port	Protocol	Port	Delete

Add

Application Name:	Pre-defined:	AIM Talk	*
	🔘 User defined:		

### < Back Apply</pre>

### Add New Port Triggering Rule

Application Name:	O Pre-defined:	AIM Talk	~
< Back Apply	O User defined:	AIM Talk Asheron's Call Calista IP Phone Delta Force (Client/Server) ICQ Napster Net2Phone Rainbow Six	
		Rogue Spear	

### Port Triggering

Port triggering funcion 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.

Protocol Port Protocol Port		Application Name	Trig	ger	Ор	en	Delete
	1	Application Name	Protocol	Port	Protocol	Port	Delete
AIM Talk TCP 4099 TCP 5090		AIM Talk	TCP	4099	TCP	5090	

Select All

Add Delete

## Or define by yourself by typing 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.

To close the function of DMZ Host,	
please click <b>Discarded</b> .	

To activate a DMZ host, please click **Forwarded to the DMZ host** radio button, and enter the IP Address of DMZ host.

 DMZ Host

 A DMZ host is a computer on your local network that can be accessed from the Internet regardless of port forwarding and firewall settings.

 Those IP packets from the Internet that do NOT belong to any applications configured in the port forwarding table will be:

 O Discarded

 O Forwarded to the DMZ host
 IP address of DMZ host:

Click Apply.

Apply Cancel

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.

### Dynamic DNS :

Dynamic DNS Configuration

Select **Enable** to enable DDNS; select **Disabled** to disable this function.

# **Dynamic DNS Provider:**

Choose a provider (*DynDNS.org, TZO.com, ChangeIP.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 connecting the Internet.

### User Name / Password :

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

### HostName.DomainName :

Key in the domain name or host name that you 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.

This page allows you to provide Internet users with a name (instead of an IP address) to access your virtual servers. This ADSL router supports dynamic DNS service provided by the provider "http://www.dyndns.ord", "http://www.tzo.com", 'http://www.changeip.com" or 'http://www.no-ip.com". Please register this service at these providers first. Dynamic DNS: 
Disabled 
Enabled
Dynamic DNS Provider:
DynDNS.org
User Name:
Password:
HostName.DomainName:
Status:

Apply Cancel

# Virtual Server – Static DNS

This page allows you to configure DNS mapping between Domain name and IP address for your local hosts. In case you want to access the local servers with domain names from the local network, you can configure the mapping information on the page.

Static DNS Configuration

### HostName.DomainName :

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

# IP Address :

Key in the IP address for the domain name to map.

Click **Apply** to upload your setting.

This page allows you to configure DNS mapping between name and IP address for your local hosts. In case if you want to access those local servers with name from local network, you can configure the mapping below.			
HostName.DomainName		IP Address	
RTA1025W.home	mapped to	192.168.1.1	
	mapped to		
		Mana Manaina XI.	

Apply Cancel

<u>More Mapping 🔉</u>
## NAT ALG Configuration

The need for IP address translation arises when a network's internal IP addresses cannot be used outside the network either for security reasons or because they are invalid for use outside the network. Use of NAT (Network Address Translation) devices allows local hosts on such private networks to transparently access the external global Internet and enables access to selective local hosts from the outside.

ALG (Application Level Gateway) is a security component that augments a firewall or NAT employed in a computer network. ALG allows legitimate application data to pass through the security checks of the firewall that would have otherwise restricted the traffic for not meeting its filter criteria. ALG application specific translation agents allow an application on a host in one address realm to connect to its counterpart running on a host in different realm transparently. An ALG may interact with NAT to set up state, use NAT state information, modify application specific payload and perform whatever else is necessary to get the application running across disparate address realms.

## Enable VPN ALG:

VPN ALG allows two or more simultaneous VPN connections through this router. The default setting 🥑 Enable SIP ALG for VPN ALG is enabled.

## Enable SIP ALG:

SIP ALG allows two or more simultaneous VoIP phone calls made by VoIP clients through this router. The default setting for SIP ALG is enabled.

Transparent use of SIP-based devices in a NAT scenario requires that modifications be made to the SIP messages. These modifications are performed by the ALG.

A **SIP ALG** provides functionality to allow VoIP traffic to pass both from the private to public and public to private side of the firewall when using Network Address Translation (NAT). The **SIP-ALG** inspects and modifies SIP traffic to allow SIP traffic to pass through the firewall so that person-to-person SIP sessions may be established.

Click **Apply** to upload your setting.

#### NAT ALG Configuration

Enable VPN ALG

- VPN ALG allows two or more simultaneous VPN connections through this router.
  - SIP ALG allows two or more simultaneous VoIP phone calls made by VoIP clients through this router.

Apply Cancel

## 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 configures the filter rule in the router to block or filter protocols and addresses. The systems behind the router usually have a direct access to the Internet; however some dangerous services such as NIS and NFS are usually blocked.

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

## Firewall – Bridge Filtering

on this device.

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.

Choose <b>Disabled</b> to disable the bridge filtering function. Click <b>Enabled</b> to monitor and block redundant packets.	packets with spe	cific proto	cols and M. Iction is of	ridge pagcket filterin AC addresses. Ily available for the C Enabled	e Internet connect	
To initiate the Bridge Filtering rules, select the <b>Enabled</b> radio button and click <b>Apply</b> .	packets with spe	; you to sp acific proto	cols and M	ridge pagcket filterin AC addresses. nly available for the	-	
Click <b>Add</b> to configure a new bridge filtering rule.	Bridge Filtering:	O Dis	abled	Enabled	Ap	ply Cancel
Note that the <b>Add</b> option is available only when there is a bridge mode PVC		internet onnection	Protocol	Source MAC addr	Dest MAC addr	Allow Delete

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 New Bridge Packet Filtering Rule         Those packets which are matched with the rule created below will be blocked.         Traffic Direction:       Outbound ♥ from local network to Internet         Internet Connection this filtering rule applies on:       ♥ br_0_35         Protocol:       PPPoE ♥         Source MAC Address:       (e.g., 00:90:96:01:2A:C3)         If the rule with source or destination MAC Address:       If the rule with source or destination mAC address is "00:00:00:00:00:00" or explicit of arefie without checking source or destination MAC address.
There are three options for traffic direction: <b>Outbound</b> means from local network to Internet; <b>Inbound</b> means from Internet to local network; <b>Bi-direction</b> includes both directions.	Cutbound Cutbound Inbound Bi-direction
The protocols that you can choose is listed as the right figure shows. Select one proper protocol for this bridge filtering rule.	Protocol: PPPoE  PPPoE IPv4 IPv4 IPv6 AppleTalk IPX NetBEUI IGMP
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 <b>Add</b> or <b>Delete</b> button to maintain the bridge filtering rules.	Bridge Filtering         This page allows you to specify the bridge pagcket filtering rules to block those redundant packets with specific protocols and MAC addresses.         Bridge packet filtering function is only available for the Internet connections of bridging mode.         Bridge Filtering:       Disabled       Enabled       Apply       Cancel         Traffic       Internet       Protocol       Source MAC addr       Dest MAC addr       Allow       Delete         Outbound       br_0_35       PPPoE       00:90:96:01:2a:3       00:00:00:00:00:00       Select All
<b>Firewall – IP Filtering</b> 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 <b>Disabled</b> to disable the firewall function. Click <b>Enabled</b> to	IP Filtering This page allows you to specify the IP packet filtering rules to prevent the services accessed from the Internet hosts or limit the Internet access for local hosts. IP Filtering:  Disabled  Enabled  Apply Cancel
To initiate the IP Filtering, please select the <b>Enabled</b> radio button and click <b>Apply</b> .	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.
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 Outbound traffic or Inbound traffic as the direction for filtering	IP Filtering: Disabled Enabled Apply Cancel Select the direction to filter packets: Outbound traffic Inbound traffic Protocol Source IP addr Dest IP addr Start End Allow Edit Add

packets.

To add a new Filtering rule, click Add.

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.

When you choose **User Defined** setting, you have to enter a port number in the "as" field.

#### Source/Destination IP address:

To specify IP address to allow or deny data transmission, please pull down the drop-down menu to choose a proper one.

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 New Outbound IP Filtering Rule

Allow Traffic	⊙ Yes	🔘 No
Protocol:	TCP	
Source IP address:	ALL 🔽	
Destination IP address:	ALL 🔽	
Port Range:	Start	End

< Back	Apply

Protocol:



#### Add New Outbound IP Filtering Rule

Allow Traffic	📀 Yes	🔘 No
Protocol:	User Defined 💌	as

#### Add New Outbound IP Filtering Rule

Allow Traffic	⊙ Yes	🔘 No
Protocol:	ТСР	
Source IP address:	ALL 💌	
Destination IP address:	ALL SINGLE SUBNET	
Port Range:	Start	End

< Back Apply</pre>

#### Add New Outbound IP Filtering Rule

Allow Traffic	⊙ Yes	🔘 No
Protocol:	TCP 💌	
Source IP address:	ALL 🖌	
Destination IP address:	ALL 🖌	
Port Range:	Start 0	End 65535

< Back Apply

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.

#### IP Filtering

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

IP Filtering: O Disabled O Enabled (Apply Cancel)						
Select the direction to filter packets: <ul> <li>Outbound traffic</li> <li>Inbound traffic</li> </ul>						
Protocol	Source IP addr	Dest IP addr	Port	Range	Allow	Fdit
PIULULUI	Source IP duur	Dest IP audi	Start	End	AIIUW	Eult
ТСР	ALL	ALL	0	65535	-	<b>%</b> . 🗊

#### IP Filtering

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

IP Filtering:	O Disabled	💿 Enabled			Apply	Cancel
Select the direction to filter packets: O Outbound traffic $\odot$ Inbound traffic						
Destacal	Course ID addr	Doct ID adde	Port F	Range	Allow	r dit
Protocol	Source IP addr	Dest IP addr	Port F Start	Range End	Allow	Edit

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
Р	recedenc	e	Т	ype of Se	ervice Fie	eld	

## 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
	Different	tiated Ser	vices Co	de 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 router.

## Quality of Service – Bridge QoS

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.

## **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 802.1p Priority.

## **Traffic Priority:**

There are three options – Low, Medium, and High that you can choose. The router will arrange the precedence for the traffic according to the traffic priority setting here.

As for the settings for the DSCP value and the WAN 802.1p value of the upstream packets, they will be seen on the WAN side.

## 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.

#### Bridge QoS

This page allows you to classify the upstream traffic (to the Internet) by assigning the transmission priority for various user data. Bridge QoS function prioritizes the data transmission based on layer 2 bridge packets.

		Traffic Priority	<b>Traffic Conditions</b>		
Traffic Name Priority		DiffServ Class	WAN 802.1p	LAN 802.1p	Delete
					Add

#### Add New Bridge QoS Traffic Rule

All of specified condi	tions in the traffic	rule must be satisfied for the rule to take effect.
Traffic Class Name:		
Traffic Conditions		
LAN 802.1p Priority:	0 🕶	
Assign Priority for I	this Traffic Rule	
Traffic Priority:	Low 🖌	
DiffServ Class (DSCP):	No Change 💌	The corresponding DSCP value in the IP header of the upstream packets will be overwritten by selected value
WAN 802.1p:	No Change 🔽	The WAN 802.1p value of the upstream packets can b overwritten by selected value.
< Back Apply		

Traffic Priority:



DiffServ Class (DSCP);	No Change 📘
(DUCP).	No Change
	BE - 0x00
	AF13 - 0x38
	AF12 - 0x28
	AF11 - 0x24
	CS1 - 0x20
	AF23 - 0x58
	AF22 - 0x48
	AF21 - 0x44
	CS2 - 0x40
	AE33 - 0x78
	AF32 - 0x68
	AF31 - 0x64
	CS3 - 0x60
	AF43 - 0x98
	AF42 - 0x88
	AF41 - 0x84
	CS4 - 0x80
	EF - 0xB8
	CS5 - 0xA0
	CS6 - 0xC0
	CS7 - 0xE0

## 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 – IP QoS**

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.

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

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:

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



Bridge QoS

This page allows you to classify the upstream traffic (to the Internet) by assigning the transmission priority for various user data. Bridge QoS function prioritizes the data transmission based on layer 2 bridge packets.

		Traffic Priority	Traffic Conditions		
raffic Name	Priority	DiffServ Class	WAN 802.1p	LAN 802.1p	Delete
sd I	Low	Be - 0×00	0	0	
:D	Low	Be - 0x00	0	o Select	

Add Delete

#### IP QoS

This page allows you to classify the upstream traffic (to the Internet) by assigning the transmission priority for various user data. IP QoS function prioritizes the data transmission based on layer 3 IP packets.

		THC FHOIL	-y			marine cu	maraons				
Traffic Name	Priority	DiffServ Class	WAN 802.1p	LAN Ports	Source MAC	Destination MAC	Protocol	Source IP Source Port	Dest IP Dest Port	Delete	
										Add	l

× 10 o hu

#### Add New IP QoS Traffic Rule

T (() D ) 11

All of specified conditions in t	ne tranic rule	must be :	satisfied for the	rule to take effect.
Traffic Class Name:				
Traffic Conditions LAN Ports which traffic come	from: 🗹	Ethernet	USB	Vireless
Source MAC Address:			MAC Mask:	
Destination MAC Address:			MAC Mask:	
Protocol:	TCP/UDP 💌			
Source IP Address:			Subnet Mask:	
Source Port (Start-End):	·	-		
Destination IP Address:			Subnet Mask:	
Destination Port(Start-End):		-		

#### Assign Priority for this Traffic Rule

Traffic Priority:	Low 🚩	
DiffServ Class (DSCP):	No Change 🔽	The corresponding DSCP value in the IP header of the upstream packets will be overwritten by selected value.
WAN 802.1p:	No Change 🔽	The WAN 802.1p value of the upstream packets can be overwritten by selected value.
< Back Apply		

Protocol:



## 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.: Destination Port(Start-End): 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.

## 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.



Destination IP Address:



#### Assign Priority for this Traffic Rule

Traffic Priority: Low

frame i nome, i		
DiffServ Class (DSCP):	No Change 🔽	The corresponding DSCP value in the IP header of the upstream packets will be overwritten by selected value.
WAN 802.1p:	No Change 🔽	The WAN 802.1p value of the upstream packets can be overwritten by selected value.

#### IP QoS

This page allows you to classify the upstream traffic (to the Internet) by assigning the transmission priority for various user data. IP QoS function prioritizes the data transmission based on layer 3 IP packets.

	Traffic Priority Traffic Conditions					Traffic Conditions				
Traffic Name	Priority	DiffServ Class	WAN 802.1p		Source MAC	Destination MAC	Protocol	Source IP Source Port	Dest IP Dest Port	Delete
А	Low	No Change	NO Chappe	Ethernet, USB, Wireless	All	All	TCP/UDP	All All	All 1-1024	
в	Medium	No Change	NO	Ethernet, USB, Wireless	All	All	TCP/UDP	All 201-8000	All All	
с	High	No Change	Chasses	Ethernet, USB, Wireless	All	АШ	TCP/UDP	192.168.1.0/ 255.255.255.0 All	All All	
D	High	No Change	Chasse	Ethernet, USB, Wireless	All	All	TCP/UDP	All	168.95.1.88 All	

Select All 📃 Add Delete



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.

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

## **Port Mapping**

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.

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 have two PVCs; they are pppoe\_0\_39\_1and br\_0\_35.

Click Add to create a new port mapping group.

Port Mapping Configuration

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

NOTE: DHCP server and all routing/firewall functions are only available at the Default

Virtual LAN Function on Ethernet:		💿 Disable	ed 🔘 Enabled	Apply Ca	incel
Group Name	Internet Connect	ions L	AN Ports		Edit
Default	pppoe_0_39_1	$\frown$	thernet, USB, Wire	less	
Derault	pppoe_0_39_1		thernet, USB, Wire	less	0

#### Port Mapping Configuration

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

NOTE: DHCP server and all routing/firewall functions are only available at the Default

Virtual LAN Func	tion on Ethernet:	O Disabled	Enabled	Apply	Cancel
Group Name	Internet Connec	tions	Ports	<u> </u>	Edit
Default	pppoe_0_39_1	Ether Ether Wirel	net.1, Ethernet net.3, Ethernet ess	.2, .4, U98,	
					Add

Port Mapping Configuration

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

NOTE: DHCP server and all routing/firewall functions are only available at the Default

Virtual LAN Functio	n on Ethernet:	🔿 Disal	bled (	Enabled	Apply	Cancel
Group Name Internet Connections		LAN Por	rts		Edit	
Default 🤇	pppoe_0_39_1, br_(	35		t.1, Ethernet.2 t.3, Ethernet.4 ;		

## 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 Ethernet, USB, wireless, etc.) will be displayed in the left side box. When you choose it and click Add, it will be transferred into the Grouped Interfaces at the right side box. Yet, if you want to remove the interface from the current group, it will be returned the current group, it will be returned back to the Default group (left side box) after you click Remove.

#### Add New Port Mapping Group

Available interfaces can be LAN ports or Internet connections of ATM PVC bridge mode.



Add

Now we are going to map USB, 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 USB, Wireless, and Ethernet1 to grouped interfaces. The four items are moved to the right box now.

When the setting is done, click **Apply**.

Now we can check the result of the

You may click to edit the created group, press in to delete it, or click Add

to create another group.

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 USB, Wireless, and Ethernet port1.

Add New Port Mapping Group

Available interfaces can be LAN ports or Internet connections of ATM PVC bridge mode

Group Name: bridge The group name must be unique.



Selected interfaces will be removed from their existing groups and added to the new group. If you remove one interface from current group, this interface will be returned back to the Default group.

#### Port Mapping Configuration

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

NOTE: DHCP server and all routing/firewall functions are only available at the Default group.

Virtual LAN Function on Ethernet: O Disabled O Enabled Apply Cancel						
Group Name	Internet Connect	ions	LAN P	orts		Edit
Default	pppoe_0_39_1		Etherr Etherr	iet.2, Ethernet.: iet.4	з,	
bridge	br_0_35		Ethern	iet.1, USB, Wire	less	<b>%</b> . 🕅
bridge	br_0_35		Etherr	iet.1, USB, Wire	less	<b>%</b> . (

Add



The following relationship figure illustrates the port mapping configuration.

Under this configuration, any devices that is connected to USB, 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 router as an Access Point. You may setup the settings for security, access control, and repeater features for this device.

## **Basic Settings**

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

#### **Enable Wireless Network:**

Click this check box to enable the wireless network function.

#### Wireless Basic Settings

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

# 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.

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.

## 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.

## 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.

Enable Wireless Network	
Wireless Main Network Name (SSID):	RTA1025W-8D30D5 ( Hide Wireless Main Network)
Wireless Guest Network Name (SSID):	( Hide Wireless Guest Network)
Channel:	11 💌 ( 🔲 Select Best Quality Channel Automatically)
Transmission Mode:	mixed mode 💌
Transmission Rate:	Auto 💌
Multicast Rate:	Auto 💌
Turbo Mode:	Oisabled
Wireless User Isolation:	Off 🗸

Apply Cancel

Transmission Mode: It decides the mode of data transmission. Choose the one that you want to use from the drop-down menu. There are 802.11b only, 802.11g only and Mixed Mode provided here.	Transmission Mode:	mixed mode mixed mode 802.11b only 802.11g only
<b>Transmission Rate:</b> 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 Mode: Transmission Rate:	Auto 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps Auto
transmission rate settings under <b>802.11b only</b> include 1, 2, 5.5, 11Mbps and Auto. The transmission rates for <b>802.11g</b> settings include 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps and Auto. As for <b>mixed</b> <b>mode</b> , only Auto is available.	Transmission Mode: Transmission Rate:	B02.11g only
	Transmission Mode: Transmission Rate:	Mixed mode V Auto V 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.	Multicast Rate:	Auto 💌
For example, you may select <i>802.11g</i> only as the <b>transmission mode</b> , and select high <b>multicast rate</b> like <i>54 Mbps</i> .		
<b>Turbo Mode:</b> When it is enabled, the data transmission will be faster for this router. Check <b>Enabled</b> to invoke this function for speeding up the transmission, or check <b>Disabled</b> to close this function.	Turbo Mode:	● Disabled ○ Enabled
Wireless User Isolation: To make the communication between the clients, please choose Off. To cut the communication between the clients, please choose On.	Wireless User Isolation:	Off V Off On
Click <b>Apply</b> 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 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:

Wireless Security

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

## Wireless Security:

The **Disabled** item offers you the less protection for wireless communication. If you choose **Disabled**, the Encryption Keys will not be shown on this page.

There are nine wireless security modes for you to select.



/ireless Security:	Disabled	~

Apply Cancel After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

Wireless Security:



## For 64-bit WEP/128-bit WEP



#### Protected by WEP only

#### 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.

#### Wireless Security

This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.

Select Wireless Network:	RTA1025W-8D30D5 🚩	
Wireless Security:	64-bit WEP	
Authentication Type: Op	en System 👻	
Encryption Keys		
Enter 5 ASCII characters	or 10 hexadecimal digits for 64-bit encryption keys.	
Format:	OHexadecimal digits (0-9,A-F,and a-f are valid)	
	<ul> <li>ASCII characters (any printable characters are valid)</li> </ul>	
Key1:		
Key2:		
Key3:		
Key4:		
Default Transmission Key:	1 💌	
Apply Cancel After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection		

#### Wireless Security

This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.

Select Wireless Network:	RTA1025W-8D30D5 🚩	
Wireless Security:	128-bit WEP	
Authentication Type: Op	oen System 💌	
Encryption Keys		
Enter 13 ASCII character	s or 26 hexadecimal digits for 128-bit encryption keys.	
Format:	OHexadecimal digits (0-9,A-F,and a-f are valid)	
	$\odot{\rm ASCII}$ characters (any printable characters are valid)	
Key1:		
Key2:		
КеуЗ:		
Key4:		
Default Transmission Key:	1 💌	
After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.		
Authentication Type: 🛛 Open System 🔽		
	Open System	

## 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

**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.

## 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 mode, the content you can type is 13 characters or 26 hexadecimal digits.

#### **Default Transmission Key:**

Select one of the network keys that you set on the Key boxes 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.

#### 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 RADIUSauthentication 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.

## 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.
- B02.1x client: a WLAN card supporting WEP.
- □ Authentication Mechanism.

#### Wireless Security

This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.

Select Wireless Network:	RTA1025W-8D30D5 💌
Wireless Security:	802.1x
RADIUS Server IP Address:	0.0.0.0
RADIUS UDP Port:	1812
RADIUS Shared Secret:	

Apply Cancel After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

#### For WPA (Wi-Fi Protected Access)

#### The WPA (WiFi-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.

#### Wireless Security

This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.

Select Wireless Network:	RTA1025W-8D30D5 💌	
Wireless Security:	WPA	۷
Data Encryption:	TKIP	
WPA Group Rekey Interval:	0 seconds	
RADIUS Server IP Address:	0.0.0.0	
RADIUS UDP Port:	1812	
RADIUS Shared Secret:		

Apply Cancel After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

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. On the other hand, the longer the rekey interval, the longer the delay for a new user to gain group access.

# 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.

#### 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.

#### Wireless Security

WPA Group Rekey

Interval

This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.

Select Wireless Network	: RTA1025W-8D30D5 💌
Wireless Security:	WPA-PSK
Data Encryption: TKI	P 💌
WPA Pre-Shared Key	
Enter the key to be betw digits	veen 8 and 63 ASCII characters, or 64 hexadecimal
Format:	○ Hexadecimal digits (0-9,A-F,and a-f are valid)
	<ul> <li>ASCII characters (any printable characters are valid)</li> </ul>
Pre-Shared Key:	

0

Apply Cancel After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

seconds

## For WPA-2; Mixed WPA2/WPA

#### 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.

#### Wireless Security

This page allow you to protect your wireless network by specifying WEP, 802.1x, WPA, or WPA2 wireless security. Before setting up security, ensure that your wireless adaptors support the same type of security. Most support WEP, but not all support WPA, WPA2, or 802.1x.

Select Wireless Network:	RTA1025W-8D30D5
Wireless Security:	WPA2
Data Encryption:	AES 💌
WPA2 Pre-authentication:	💿 Disabled 🛛 🔿 Enabled
Network Re-auth Interval:	36000 seconds
WPA Group Rekey Interval:	0 seconds
RADIUS Server IP Address:	0.0.0
RADIUS UDP Port:	1812
RADIUS Shared Secret:	

Apply Cancel After enabling security and clicking Apply, you will lose the connection with your wireless ADSL router. You should now set-up security on your wireless adapters in order to re-establish the connection.

This page lets you to specify the wireless adaptors that are allowed to connect to your ADSL router. Click "Apply" to configure the wireless access control mode.

On in Allow mode (Only those wireless adaptors listed in the access control table are allowed to connect to your ADSL router, others are denied.)
 On in Deny mode (Only those wireless adaptors listed in the access control table cannot connect to your ADSL router, others are allowed.)

## **Access Control**

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

Access Control:

Wireless MAC Access Control

💿 Off

#### 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.

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.

MAC Address of Wireless adaptor: Key in the MAC Address to be filtered. And click Apply.

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.

SS W	View Access Control List Apply Cancel
AC	<ul> <li>http://192.168.1.1/wlmacflt.cmd?action=view - Microsoft I</li> <li>Wireless Access Control List:</li> <li>MAC Address Delete</li> </ul>
ir on	Add Close
or: red.	http://192.168.1.1/vlmacfit.html - Microsoft Internet Expl Add a wireless adaptor to the control list MAC Address of wireless 00:90:96:01:02:03 adaptor: (e.g.,00:90:96:01:02:03) < Back Apply
ess	🗿 http://192.168.1.1/wlmacflt.cmd?action=add&wlFltMacAdd 📰 🗖
٩C	Wireless Access Control List: MAC Address Delete 00:90:96:01:02:03 m
Click II be	Add Close

## 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 AP, the repeater, 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 works as the repeater for AP-A, and thus client D and E may receive the signal smoothly.



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

#### **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 **SSID** and **WEP key**, so that they may work as repeater 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**.

The right figure shows an example 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 they can function as repeaters to extend the coverage area for each other.

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

#### Wireless Repeater

 This page allows you to configure wireless repeater feature (also known as Wireless Distribution System) for your wireless network. Click "Apply" to configure the wireless repeater options.

 AP Mode:

 Access Point and Wireless Repeater Function
 Wireless Repeater only

 Search Other Repeaters:

 Auto
 Manual
 Scan Now

CH SSID MAC Address Transmission Mode Select

#### Apply Cancel

Wireless Reneater

This page allows you to configure wireless repeater feature (also known as Wireless Distribution System) for your wireless network. Click "Apply" to configure the wireless repeater options.

AP Mode: 

 Access Point and Wireless Repeater Function
 Wireless Repeater only

Search Other Repeaters:	🔘 Auto	💿 Manual
MAC Address of Remote Wireless Repeaters:		(e.g.,00:90:96:01:02:03)

Apply Cancel

#### Wireless Repeater

This page allows you to configure wireless repeater feature (also known as Wireless Distribution System) for your wireless network. Click "Apply" to configure the wireless repeater options.

AP Mode: 

 Access Point and Wireless Repeater Function
 Wireless Repeater only

сн	SSID	MAC Address	Transmission Mode	Select
11	Broadcom	02:10:18:73:82:06	802.11g	
11	ALICE-WLAN	00:90:96:78:79:84	802.11g	
11	RTA1025W-000004	00:11:F5:F4:49:01	802.11g	
11	Malli	00:90:96:11:08:04	802.11b	
2	Askey-WLan	00:90:96:28:CC:72	802.11b	
З	roy	00:90:96:67:8E:99	802.11g	
1	AP61	00:03:7F:BE:F0:EF	802.11g	
6	linksys	00:90:00:00:00:C0	802.11g	

## Management

## **Diagnostics**

same page.

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.

Press Run Diagnostic Tests on the Diagnostic Tests page.

Diagnostic Tests				
This ADSL router is capable of testing your ADSL con	nection.			
Select the Internet Connection: pppoe_0_39_1 💌		Run Dia	gnostic Tests	
Diagnostic Tests				
This ADSL router is capable of testing your ADSL conr	nection.			
Select the Internet Connection: pppoe_0_39_1 💌		Run Dia	gnostic Tests	
Test the connection to your local network				
Test your Ethernet Connection:	PASS	Help		

DOWN Help

PASS Help

PASS <u>Help</u>

PASS Help

PASS Help

PASS Help

PASS Help

PASS Help

PASS Help

FAIL Help

FAIL Help

PASS Help

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

The Result would be shown on the

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.

#### Take the Help link of ADSL Synchronization for example.

It not only explains the situation for Pass and Fail, but offers the troubleshooting procedures for you to follow.

Press Back to return.

## Ping primary Domain Name Server: ADSL Synchronization Test

Test the connection to your ADSL service provider

Test ATM OAM F4 end-to-end ping:

Test the connection to your Internet service provider

Test your USB Connection:

Test your Wireless Connection:

Test ADSL Synchronization:

Test ATM OAM F5 segment ping: Test ATM OAM F5 end-to-end ping:

Test ATM OAM F4 segment ping:

Test PPP server connection:

Test authentication with ISP:

Test the assigned IP address:

Ping default gateway:

Pass: Indicates that the ADSL router has detected a ADSL signal from the telephone company.

Indicates that the ADSL router does not detect a signal from the telephone company's ADSL network. The ADSL LED will continue to flash green. Fail:

If the test fails, follow the troubleshooting procedures listed below and rerun the diagnostics tests

#### Troubleshootina

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

#### < Back

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

## Management Accounts

This page allows you to CHANGE the user name and password for accessing your ADSL Router.

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.

#### Admin Account

Admin account has unrestricted access to change and view configuration of your ADSL router.

User Name:	admin
New Password:	
Confirm New Password:	

Apply Cancel

#### User Account

ι

Ν

Using the user account can configure most common functions and view statistics of your ADSL router.

lser Name:	user
lew Password:	
onfirm New Password:	

Apply Cancel

## Management Control – From Remote

There are six interfaces for the remote access. Please choose from them if you want to enable the remote access control.

#### Select the Internet Connect:

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

#### Web Browser:

Check this box if you want to have remote control through HTTP. The default port number is 8080. Modify the port whenever you want.

#### Telnet:

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

## FTP:

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

## TFTP:

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

#### Secure Shell (SSH):

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

## Ping:

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

#### **Remote Management Control**

Enable remote access to let an expert, e.g. helpdesk, configure your ADSL router remotely.

Select the Internet Conn	ection: pppoe_0_39_1 🔽	
o allow remote access to your router via		
🗌 Web Browser		
Web server port on W	/AN interface: 8080	
Telnet	FTP	
TFTP	Secure Shell (SSH)	
PING		
If enabling remote acce all Internet hosts can pi	ss to your router via PING, ng to your router.	

Authorized Host IP Address List Apply Cancel

Authorized Host IP Address List: Decide whether all internet hosts can access your router or only authorized internet hosts can access. Click Apply to save your setting.

dress List	
nection: pppoe_0_39_1 💌	
an access your router	
ernet hosts can access your router	
Apply	Cancel
n	Idress List nnection: [pppo_0_39_1 v can access your router termet hosts can access your router Apply

## Management Control – From Local

You can allow local access to your router via the checked interfaces.

## Authorized Host IP Address List:

Refer to Remote Management Control.

Click **Apply** to activate your settings or click **Cancel** to retain the original settings.

#### Local Management Control

Enable local access to let an expert, e.g. helpdesk, configure your ADSL router from your local network.

To allow local access to your router via

🕑 Web Browser	FTP
🗹 Telnet	🔽 SSH
TFTP	

Authorized Host IP Address List Apply Cancel

## **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.



ACS: Auto-Configuration Server CPE: Customer Premise Equipment

Compliant with DSL's Forum's TR-069 Remote Management Specification, the ADSL Router 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 ADSL routers. By these provision value-added services, the ADSL Router 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.

## 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://10.11.95.124:8082/askey/ACSS erver without SSL or https://10.11.95.124:8443/askey/ACS Server with SSL.

## 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

### 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.

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

Trusted CA (Certificate Authority) Certificate and correct current time are used to identify the validation of the Certificate which is <u>sent from ACS during SS</u>L connection. You can import the Trusted CA Certificates through the <u>Trusted CA Certificates</u> window and enable the Internet time function from the <u>Management...trustermer Time menu</u>.

#### TR-069 Client Configuration

IR-069, a CPE WAN Management Protocol, allows the Auto-Configuration Server (ACS) to perform the auto-provisioning of settings, firmware updates, status and performance nontroning, and diagnostics to a collection of ADSL routers.

$\odot$ without SSL $\bigcirc$ with SSL	
http:// 10.11.95.124:8082/as	
0011F5-RTA1025W-8D30D2	Used to authenticate this device
••••	when making a connection to ACS
0011F5-RTA1025W-8D30D2	Used to authenticate an ACS making a Connection Request to
	this device
	http:// 10.11.95.124:8082/as 0011F5-RTA1025W-8D30D2 ••••• 0011F5-RTA1025W-8D30D2

Periodic Transmission of Inform Request: ODisabled 

Enabled

Transmission Interval of Inform Request: 300 seconds

Apply Cancel

#### TR-069 Client Configuration

TR-069, a CPE WAN Management Protocol, allows the Auto-Configuration Server (ACS) to perform the auto-provisioning of settings, firmware updates, status and performance monitoring, and diagnostics to a collection of AOSL routers.

Connect to ACS:	O without SSL 💿 with SSL	
ACS URL Address:	https:// 10.11.95.124:8443/as	
ACS User Name:	0011F5-RTA1025W-8D30D2	Used to authenticate this device
ACS Password:		when making a connection to ACS
Connection Request User Name:	0011F5-RTA1025W-8D30D2	Used to authenticate an ACS
Connection Request Password:		making a Connection Request to this device

sion of Inform Request: 🔘 Disabled 💿 Enabled

Transmission Interval of Inform Request: 300 seconds

#### Identify the Validation of Certificate from ACS:

Trusted CA (Certificate Authority) Cortificate and correct current time are used to identify the validation of the Certificate which is sent from ACS during SSL connection. You can import the Trusted CA Certificates through the <u>Trusted CA Certificates</u> window and enable the Internet time function from the <u>Management. Jinternet Time</u> monu.

Apply Cancel

Periodic Transmission of Inform Request: ODisabled 💿 Enabled Transmission Interval of Inform Request: 300 seconds

## Press Trusted CA Certificates 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.

#### Update Now:

time.

Set Time by (Time Server/ 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 via time server 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 Cancel

## 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.

#### Internet Time

Click this button to refresh the current To synchronize your router with other network devices, you can set its time manually or with an Internet time server.

Current time:	2006/01/01, 01:39 Update Now
Set Time by:	🔘 Time Server 💿 Manua
Time:	Year 2006 Month 1 Day 1
nine.	Hour 1 Minute 39
Time Zone:	(GMT+08:00) Taipei 💌
Apply Ca	ncel
Internet Tim	e
	ze your router with other network devices, you can set its time with an Internet time server.
Current time	2006/01/01_01-39

Current time:	2006/01/01, 01:39 Opuate Now
Set Time by:	📀 Time Server 🔘 Manual
Primary Time Server:	time.windows.com 👻
Secondary Time Server:	time.nist.gov 💌
Time Zone:	(GMT+08:00) Taipei 💌

## 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.

## **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.

System Loa

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

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

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

View System Log Configure System Log

#### 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

> Debugging 🗸 Error

Local

Oisabled O Enabled

×

¥

Log:
Log Level:
Display Level:
Mode:
Apply Cancel

Log Level:



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:

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 for a programmer or example, 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.

Display Level:



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:

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.

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

- 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.)
- Set the **Mode** as *Both*, key in the 3. Server IP Address as 10.11.95.2, Disp and leave the Server UDP Port as the default value 514.
- 4. Press Apply to invoke the settings.

Mode:	Local	~
	Local	
	Remote	
	Both	
Mode:	Remote	*

Server UDP Port:

System Log Configuration	
This dialog allows you to configure System Log setting	

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 ontions

Log:	🔘 Disabled 🛛 💿 Enabled
Log Level:	Debugging 🖌
Display Level:	Error 💌
Mode:	Both 💌
Server IP Address:	10.11.95.2
Server UDP Port:	514
Apply Cancel	

×

#### Viewing System Log – Remote Side (Server) To view the system log on the Log

To view the system log on the Log Server (10.11.95.2), a log viewing tool must be installed.

- 1. Download the <u>Kiwi Syslog</u> <u>Daemon</u> from <u>Kiwi Enterprises</u>.
  - Kiwi Syslog Daemon is a freeware Syslog Daemon for Windows. It receives, logs, displays and forwards Syslog messages from hosts such as routers, switches, and any other syslog enabled device. You can choose other logger tools; here, we use Kiwi for example.

Download the tool from the Kiwi Enterprises website.

	Quality networking tools	at affordable pric
iwi Sysla	g Daemon	Version 7
opyright 19	96-2004 Kiwi Enterprises	
Registere	d to	
Name:		
Company:		
E-Mail:		
Serial:		
Edition:	Freeware	

- 2. Install the Kiwi Syslog server software on the PC (10.11.95.2).
- 3. Open the **Kiwi Syslog Daemon** application. You will get to a screen shown as follows.

07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:30:	1:22     User.Deb       1:22     User.Deb       1:22     User.Deb       1:21     User.Aler       1:15     User.Aler       1:12     User.Aler	10.11.65.12           10.11.65.12           10.11.65.12           10.11.65.12           10.11.95.4           10.11.95.4           10.11.95.4           10.11.95.4	igmp[944]: iptables -t filter -I FORWARD 1 -i ppp_0_39_1 -d 224.0.0.22 -j DROP 2>/dev/null
07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:	1:22         User.Deb           1:21         User.Aler           1:15         User.Aler           1:12         User.Aler           1:12         User.Aler           1:12         User.Aler           1:12         User.Aler	g 10.11.65.12 g 10.11.65.12 10.11.95.4 10.11.95.4 10.11.95.4 10.11.95.4	igmp[344]: iptables + filter -1 FORWARD 1 -i ppp_0_39_1 - d 224.0.0.22 -i DROP 2>/dev/null         igmp[342]: iptables + filter -D FORWARD -i ppp_0_39_1 - d 224.0.0.22 -i DROP 2>/dev/null         igmp[342]: iptables + filter -D FORWARD -i ppp_0_39_1 - d 224.0.0.22 -i DROP 2>/dev/null         kernet: Intrusion -> Ni=joa 0 33 0UT=b0 SRC=201.239.176.0 DST=211.21.179.146         LEN-48 T05=0x00 PREC=0x00 TTL=109 ID=3333 DF PR0T0=TCP SPT=4733         DPT=4899 WIND0W=65535 RES=0x00 SYN URGP=0         kernet: Intrusion -> Ni=joa 0 33 0UT=br0 SRC=201.239.170.60 DST=211.21.179.146         LEN-48 T05=0x00 PREC=0x00 TTL=109 ID=32976.60 F PR0T0=TCP SPT=4733         DPT=4899 WIND0W=65535 RES=0x00 SYN URGP=0         kernet: Intrusion > Ni=joa 0 33 0UT=b0 SRC=201.239.170.60 DST=211.21.179.146         LEN-48 T05=0x00 PREC=0x00 TTL=109 ID=32976.06 DST=211.21.179.146         LEN-48 T05=0x00 PREC=0x00 TTL=109 ID=32972 DF PR0T0=TCP SPT=4733         DPT=4899 WIND0W=65535 RES=0x00 SYN URGP=0         kernet: Intrusion > Ni=joa 0.3 0UT=b0 SRC=61.222 198.226 DST=61.222.223.189         LEN-48 T0S=0x00 PREC=0x00 TTL=118 ID=58236 DF PR0T0=TCP SPT=4268         DPT=489 WIND0W=64240 RES=0x00 SYN URGP=0         kernet: Intrusion > Ni=joa 0 30 UT=M SRC=61.63.03:00:00:00:00:00:00:00:SRC=61.64.235.203
07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:32:	1:22 User.Deb 1:21 User.Aler 1:15 User.Aler 1:12 User.Aler 1:12 User.Aler 0:00 User.Aler	g 10.11.65.12 10.11.95.4 10.11.95.4 10.11.95.4 10.11.95.4 10.11.95.6	igmp[942]:         ipubles 1         filter -D FORWARD -i ppp. 0.33_1 -d 224.0.0.22 -i DROP 22/dev/null           kernel:         Intrusion -> IN-ipa 0.33 0UT-br0 SRC-201.239.170.60 DST=211.21.179.146           LEN-48 T0S-0x00 PREC-0x00 TTL-109 ID-33333 DF PR0T0-TCP SPT=4733           DPT-4899 WIND0W=65535 RES-0x00 SYN URGP=0           kernel:         Intrusion -> IN-ipa 0.33 0UT-br0 SRC-201.239.170.60 DST=211.21.179.146           LEN-48 T0S-0x00 PREC-0x00 TTL-109 ID-32376 DF PR0T0-TCP SPT=4733           DPT-4899 WIND0W=65535 RES-0x00 SYN URGP=0           kernel:         Intrusion -> IN-ipa 0.33 0UT-br0 SRC-201.239.170.60 DST=211.21.179.146           LEN-48 T0S-0x00 PREC-0x00 TTL-109 ID-32775 DF PR0T0-TCP SPT=4733           DPT-4899 WIND0W=65535 RES-0x00 SYN URGP=0           kernel:           kernel:           Intrusion -> IN-ipa 0.33 0UT-br0 SRC-61.222 198.226 DST=61.222.223.189           LEN-48 T0S-0x00 PREC-0x00 TTL-118 ID-58236 DF PR0T0-TCP SPT=4268           DPT-133 WIND0W=65230 RES-0x00 SYN URGP=0           kernel:           kernel:           DPT-139 WIND0W=65230 RES-0x00 SYN URGP=0           kernel:           kernel:           DPT-139 WIND0W=65230 RES-0x00 SYN URGP=0           kernel:           kernel:           DPT-139 WIND0W=65200 REC-0x00 TTL-118 ID-58236 DF PR0T0-TCP SPT=4268           DPT-139 WIND0W=65200 REC-0x00 SYN UR
07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:31:           07-19-2006         10:30:           07-19-2006         10:30:           07-19-2006         10:30:	1:21 User.Aler 1:15 User.Aler 1:12 User.Aler 0:00 User.Aler	10.11.95.4 10.11.95.4 10.11.95.4 10.11.95.6	kernel: Intrusion > Nimipa 0 33 0UT=br0 SRC=201.239 170.60 DST=211.21.179.146           LEN=48 T0S=0x00 PREC=0x00 TTL=109 ID=33333 DF PR0T0=TCP SPT=4733           DPT=4899 WINDOW=65535 RES=0x00 SYN URGP=0           kernel: Intrusion > IN=ipa 0 33 0UT=br0 SRC=201.239.170.60 DST=211.21.179.146           LEN=48 T0S=0x00 PRC=0x00 TTL=109 ID=3278 DF PR0T0=TCP SPT=4733           DPT=4899 WINDOW=65535 RES=0x00 SYN URGP=0           kernel: Intrusion > IN=ipa 0 33 0UT=br0 SRC=201.239.170.60 DST=211.21.179.146           LEN=48 T0S=0x00 PREC=0x00 TTL=109 ID=32772 DF PR0T0=TCP SPT=4733           DPT=4899 WINDOW=65535 RES=0x00 SYN URGP=0           kernel: Intrusion > Ni=ipa 0 33 0UT=br0 SRC=1222 198.226 DST=61.222.233.189           LEN=48 T0S=0x00 PREC=0x00 TTL=118 ID=58236 DF PR0T0=TCP SPT=4268           DPT=139 WINDOW=64240 RES=0x00 SYN URGP=0           kernel: Intrusion > Ni=ipa 0 33 0UT=br0 SRC=61.222 198.226 DST=61.222.233.189           LEN=48 T0S=0x00 PREC=0x00 TTL=118 ID=58236 DF PR0T0=TCP SPT=4268           DPT=139 WINDOW=64240 RES=0x00 SYN URGP=0           kernel: Intrusion > Ni=ipa 0 33 0UT= MAC=aa:aa:03:00:00:00:00:00:00:00:SRC=61.64.235.203
07-19-2006 10:31: 07-19-2006 10:30: 07-19-2006 10:29:	1:12 User.Aler D:00 User.Aler	10.11.95.4	LEN=48 T0S=0x00 PREC=0x00 TTL=109 ID=32976 DF         PR0T0=TCP SPT=4733           DPT=4899 WIND0W=65535 RES=0x00 SYN URGP=0         Remel: Intrusion > IN=ipa 0 33 0UT=br0 SRC=201.239.170.60 DST=211.21.179.146           LEN=48 T0S=0x00 PREC=0x00 TTL=109 ID=32772 DF         PR0T0=TCP SPT=4733           DPT=4899 WIND0W=65535 RES=0x00 SYN URGP=0         Remel: Intrusion > IN=ipa 0, 34 0UT=br0 SRC=61.222.198.226 DST=61.222.23.189           LEN=48 T0S=0x00 PREC=0x00 TTL=118 ID=58236 DF         PR0T0=TCP SPT=4268           DPT=139 WIND0W=664240 RES=0x00 SYN URGP=0 I         1           Remel: Intrusion > IN=ipa 0, 33 0UT= MAC=aa:aa:03:00:00:00:00:00:00:08:00 SRC=61.64.235.203         1
07-19-2006 10:30: 07-19-2006 10:29:	D:00 User.Aler	10.11.95.6	LEN-48 T05-0x00 PREC=0x00 TTL=109 ID=32772 DF         PR0T0=TCP SPT=4733           DPT=4899 WIND0W=65535 RES=0x00 SYN URGP=0         Remel: Intrusion >> Ni=jaa_0_34 0UT=br0 SRC=61.222.198.226 DST=61.222.223.189           LEN-48 T05=0x00 PREC=0x00 TTL=118 ID=58236 DF         PR0T0=TCP SPT=4268           DPT=139 WIND0W=64240 RES=0x00 SYN URGP=01         1           Remel: Intrusion >> Ni=jaa_0_33 0UT= MAC=aa:aa:03:00:00:00:00:00:00:00 SRC=61.64.235.203         1
07-19-2006 10:29:			LEN-48 T05-0x00 PREC=0x00 TTL=118 ID=58236 DF PR0T0=TCP SPT=4268 DPT=139 WINDOW=64240 RES=0x00 SYN URGP=0 1 kernet: Intrusion -> IN=ipa 0 33 0UT= MAC=aa:aa:03:00:00:00:00:00:00 SRC=61.64.235.203
	9:10 User.Aler	10.11.95.4	
07-19-2006 10:26:			SPT=3168 DPT=16881 WINDOW=16384 RES=0x00 SYN URGP=0
	6:59 User.Deb	ıg 10.11.65.12	igmp[805]: iptables -t filter -l FORWARD 1 -i ppp_0_39_1 -d 239.255.255.250 -j ACCEPT 2>/dev/null
07-19-2006 10:26:	6:59 User.Deb	g 10.11.65.12	igmp[803]: iptables -t filter -D FORWARD -i ppp_0_39_1 -d 239.255.255.250 -j ACCEPT 2>/dev/null
07-19-2006 10:26:	6:58 User.Deb	g 10.11.65.12	igmp[770]: iptables -D FORWARD -i ppp_0_39_1 -d 239.255.255.250 -j DROP 2>/dev/null
07-19-2006 10:26:	6:56 User.Deb	ıg 10.11.65.12	syslog: sntp -s time.windows.com -s time.nist.gov -t "Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna'
07-19-2006 10:26:	6:56 User.Deb	ıg 10.11.65.12	syslog: kill -1 418
07-19-2006 10:26:			
07-19-2006 10:26		and the second	
		e 10.11.65.12	
07-19-2006 10:26:			
07-19-2006 10:26:	6:55 User.Deb	ıg 10.11.65.12	syslog: kill -SIGTERM 174

The **Date** and **Time** record the logging time. The **Priority** field shows the log level, the **Hostname** exhibits the position of the host, and the **Message** column displays the process the description of it—before the colon is the name of the process and after the colon is the alpharetion for that process.

after the colon is the elaboration for that process.

For example, message 1 shows *alert* level information which is a kernel process containing detailed intrusion information; message 2 displays *notice* level information which is an IGMP process exhibiting that the IGMP function had been started.

## Viewing System Log – Local Side (ADSL Router)

For viewing the system log on local side, click the **View System Log** button on the webpage for system log configuration.

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

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

View System Log Configure System Log

The system log record on the router will be displayed on a screen shown as below.

System Log Refresh Close				
Date/Time	Facility	Severity	Message	3
2006/07/19 04:27:40	daemon	crit	pppd[517]: Received valid IP address from server. Connection UP.	
2006/07/19 04:27:40	daemon	crit	pppd[517]: PPP LCP UP.	
2006/07/19 04:27:38	daemon	crit	pppd[517]: PPP session established.	
2006/07/19 04:27:38	daemon	crit	pppd[517]: PPP server detected.	
2006/07/19 04:27:32	user	crit	kernel: ADSL link up, fast, us=832, ds=8000	
2006/07/19 04:27:32	user	crit	kernel: ADSL G.992 message exchange	
2006/07/19 04:27:28	user	crit	kernel: ADSL G.992 channel analysis	
2006/07/19 04:27:25	user	crit	kernel: ADSL G.992 started	
2006/07/19 <b>4</b> 04:27:21	user	crit	kernel: ADSL G.994 training	
2006/07/19 04:27:21	user	crit	kernel: eth0 Link UP.	
2006/07/19 04:27:21	syslog	emerg	BCM63XX started: BusyBox v1.00 (2006.07.17- 12:38+0000)	

The **Date/Time** records the logging time, and the Facility field distinguishes different classes of system log message. The **Severity** field shows the log level, and the **Message** column displays the process and the description of it—the name of the process appears before the colon and the elaboration for that process after the colon.

For example, message 3 shows *critical* level information which is a *pppd* (PPP daemon) process showing that a valid IP address had been received from server, and connection is up; message 4 is a kernel process belonging to *critical* level information which reveals that the Ethernet 0 link is up.

You can press Refresh to update the log files or press Close to close the window.

Note that the earlier messages may be automatically replaced by the updated information when the buffer is overflowed on the router.

Backup Config	
To backup your settings of the router, you can use <b>Backup Config</b> web page to save the configuration.	Backup Configuration Use to save your ADSL router's current settings into the computer. Backup
	Restore Configuration Use to reset your ADSL router with settings previously saved on the computer. Backup File: Browse
Click <b>Backup</b> button and the warning window will be prompted. Click <b>OK</b> to	Microsoft Internet Explorer
continue the backup procedure.	The router's configuration is going to be saved to your computer. Please don't turn off this router !
The system will ask your command about the next procedure. Click <b>Save</b>	File Download
to backup.	Name: backupsettings.xml Type: XML Document From: 192.168.1.1
	Dpen Save Cancel
	While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u>
You may change the file name and choose a place to save the backup file.	Save As       Save As     ? X       Save in:     backup       We backup settings       More Recent       Desktop
	My Documents
	File name:         backupsettings         Save           My Network         Save as type:         XML Document         Cancel
And when you want to restore the settings in the future, simply open <b>Backup Config</b> web page and use <b>Browse</b> button to locate the file.	Choose file    Look in   bockup  bocku
	My Computer

After opening the backup file, click **Restore**.

#### Backup Configuration

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

E	Back	up	]	
_				

#### **Restore Configuration**

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

Backup File:	D:\backup\backupsettings.xml	Browse

Restore

## **Update Firmware**

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

Note: Router must not turn off during firmware updates.

## **Reset Router**

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

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

#### Update Firmware

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

 Current Firmware Version:
 3.61j



#### Reset Router

This page allows you to restart your ADSL router after changing settings that require rebooting. It also allows you to reset all settings to factory default settings if you have problems with your current configuration.

🔲 Reset to factory default settings

Reboot After clicking "Reboot", please wait for 2 minutes to let the system reboot.

#### Restore Factory Default Settings

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

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

## UPnP for XP

Universal plug and play (UPnP) is 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.

Windows Components Wizard

You can add or remove components of Windows XP

Windows Components

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.
- 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 ADSL2+ Router) for UPnP function.



- 6. Double click on the icon, and the ADSL router will open another web page via the port for UPnP function. The IE address will be directed to the configuration main webpage as shown in the graphic.
- 7. 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 do not renew IP addresses.

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

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

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

## **Problems with WAN**

You cannot access the Internet.

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

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

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

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 Upgrading

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:	Browse

Update Firmware

Action: Setup you PC with a static IP address, such as 192.168.1.2, and then access the router's web page by entering <u>http://192.168.1.1</u>. 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.

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

#### **DHCP (Dynamic Host Configuration Protocol)**

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

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

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

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

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

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

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

#### NAT (Network Address Translation) IP Address

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

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

For example, the ADSL Router is assigned with the public IP address of 168.111.2.1. With NAT enabled, it creates a Virtual LAN. Each PC on the Virtual LAN is assigned with a private IP address with default value of 192.168.2.2 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, metasignaling channel or a generic broadcast signaling channel. Your ISP should supply you with the values.

# **Appendix A: Specifications**

Interface	One RJ-11 port for ADSL connection
Interlace	
	• Four RJ-45 ports for IEEE 802.3/802.3u 10/100 Base-T
	auto-sensing and auto-crossover Ethernet connection
	<ul> <li>One USB client port compliant to USB v1.1</li> </ul>
	<ul> <li>On-board wireless LAN module for IEEE 802.11g (2.4</li> </ul>
	GHz) wireless LAN connection
	• One hidden button for restoration of factory default
	settings
Regulatory Approvals	EMC: FCC part 15 Class B, CE
and Compliance	Telecom: FCC part 68
	Safety: UL, CB, LVD
Power Requirement	Power Adaptor: Input 120±10 or 230±10 VAC;
and Operation	Output 12 VAC, 1A
Environment	Power Consumption: less than 10 Watt
Requirement	Ambient Temperature: 0 to 40°C (32 to 96°F)
	Relative Humidity: 20% to 90% (non-condensing)
Physical	PCB: 152 mm x 113 mm
T TrySical	
	Housing: 190mm(L) x 130mm(W) x 40mm(H)
	Weight: 350g

# Appendix B: Client Setup for 802.1x, WPA, and WPA-PSK

### **Retreiving Client Certificate**

 $\diamond$  This step is only required if you intend to authenticate with EAP/TLS.

While there are many ways you may receive a certificate from your Certificate Authority, the example here is to show you how to retrieve your certificate from a Microsoft Certificate Services server via its easy web interface.

- 1. Please connect the client to a network that doesn't require port authentictaion.
- Open up Microsoft Explorer, connect to your CA via the url http://yourserver/certsrv (see your local administrator if it has been changed from the default).

For example, if the Microsoft Certificate Service server uses the IP address 192.168.0.2, then we have to key in <u>http://192.168.0.2/certsrv</u> on the url box.

3. You will be asked to log in, use your domain credentials. (e.g., *ABC*)



Connect to 192	.168.0.2
R	
Connecting to 192	.168.0.2
<u>U</u> ser name:	🖸 ABC 💽 💽
Password:	*****
1	Remember my password

4. Make sure that **Request a** certificate is selected, and click Next.



5. Select User Certificate, then Next.

6. Click **Submit** in the following step.

7. You may retrieve your certificate by clicking **Install this** certificate.

	soft Internet Exp	lorer	
File Edit View Favorites Tools Help			<b></b>
🌀 Back 🝷 🕥 - 💽 🗟 🏠 🔎	🕽 Search   trav	orites 🛛 💽 Med	ia 🚱 🂙
Address 🕘 http://192.168.0.2/certsrv/certfnsh.	asp	~	🔁 Go Links 🌺
Microsoft Certificate Services Wirele	ssCA		Home
Certificate Issued			
The certificate you requested was i	issued to you.		
Install this certificate			
			1000
Done		🥥 Interne	et .:
a Done		🌍 Interne	et 🤢
Done Root Certificate Store		🌍 Interne	et 🥫
	rtificate to the Root		at
Root Certificate Store Do you want to ADD the following ce Subject : WirelessCA, Systems, Wire		Store?	×
Root Certificate Store Do you want to ADD the following ce Subject : WirelessCA, Systems, Wire Issuer : Self Issued Time Validity : Thursday, October 11	eless Widgets, Colleg , 2001 through Satu	Store? Je Park, MD, US, Irday, October 1	ca@yourdomain.tld
Root Certificate Store Do you want to ADD the following ce Subject : WirelessCA, Systems, Wire Issuer : Self Issued Time Validity : Thursday, October 11 Serial Number : 7667/4800 863756A: Thumphrit (sha) : PEGC3F50 A863	eless Widgets, Colleg , 2001 through Satu 3 4F77E081 551337( 3678E 79C055A8 51)	Store? Je Park, MD, US, rday, October 1 27 217043 BE7A0CB	ca@yourdomain.tld 1, 2003
Root Certificate Store  Do you want to ADD the following ce Subject : WirelessCA, Systems, Wire Issuer : Self Issue Time Validiy : Thursday, October 11 Serial Number : 76:FASD0 68375A2	eless Widgets, Colleg , 2001 through Satu 3 4F77E081 551337( 3678E 79C055A8 51)	Store? Je Park, MD, US, rday, October 1 27 217043 BE7A0CB	ca@yourdomain.tld 1, 2003

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

#### **Enabling 802.1x Authentication and Security**

- 1. Click **Run** from the **Start** menu. Type *services.msc* and click **OK**.
- 2. Scroll to the bottom of the list. Double click on the **Wireless Zero Configuration** service and verify that it is set to *Automatic* and that it is *Started*. Click **OK** to continue.
- 3. Click the **Start** button, select **Control Panel**, then **Network Connections.**
- Right click on your wireless network card and select Properties. Click on the Wireless Networks tab.
- 5. Click **Add** to continue.

Services						X
File Action View	Help					
← → 💽 🗗	🗟 🗟 🙎 🕨 🖬 🗉 🖦					
🖏 Services (Local)	Services (Local)					
	Wireless Zero Configuration	Name A	Description	Status	Startup Type	
	Stop the service Restart the service Description: Provides automatic configuration for the 802.11 adapters	Windows Image Ac Windows Installer Windows Managem Windows Managem Windows Media Con Windows Media Con Windows Media Con Windows Time	Provides s Serves sha Monitors th Maintains d	Started	Manual Manual Automatic Manual Manual Automatic Automatic	
		Wireless Zero Confi WWI Performance A Workstation			Automatic Manual Automatic	• •
	Extended Standard /					

🕹 wireless Properties 🛛 🕐 🔀
General Wireless Networks Advanced
✓ Use Windows to configure my wireless network settings
Available networks:
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.
View Wireless Networks
Preferred networks: Automatically connect to available networks in the order listed below:
Move up Move down
Add Remove Properties
Learn about <u>setting up wireless network</u> Advanced
OK Cancel

- 6. Select the **Association** Tab, and enter the SSID of the AP. (e.g., *Please*)
- 7. Set *Open* as the **Network Authentication** from the drop down menu, and *WEP* for **Data encryption**.
- 8. Click **OK**, and then select the **Authentication Tab**.

Wireless network proper	ties 🔹 🤉 🔀
Association Authentication	Connection
Network name (SSID):	Please
-Wireless network key	
This network requires a ke	ey for the following:
Network Authentication:	Open 🔽
Data encryption:	WEP 💌
Network key:	
Confirm network key:	
Key index (advanced):	1 () me automatically
This is a computer-to-con access points are not use	nputer (ad hoc) network; wireless ed
	OK Cancel

- 9. Ensure that Enable network access control using IEEE 802.1X is selected, and Smart Card or other Certificate is selected from the EAP type.
- 10. Click **Properties** under **EAP** type.

Wireless ne	twork proper	ties		? 🗙
Association	Authentication	Connection		
	option to provide iernet networks.	authenticated	d network access for	
💌 Enable I	EEE 802.1x auth	nentication for	this network	
EAP type:	Smart Card or c	ther Certificat	e	~
	icate as guest wł		Propert uter information is av omputer information is	ailable
			OK Ca	incel

11. You can choose whether to use one of your certificates you have loaded on the computer, or use a smart card for access.

> In our example, Use a certificate on this computer option is chose and Use simple certificate selection (Recommended) is checked.

- 12. Check the Validate server certificate check box if server certificate validation is required.
- 13. In the **Trusted Root Certification Authorities** field, check the check box beside the name of the certificate authority from which the server certificate was downloaded. (e.g., *askey.savd.tw*)

Note that if you leave all check boxes unchecked, you will be prompted to accept a connection to the root certification authority during the authentication process.

Smart Card or other Certificate Properties 🛛 🔹 💽
When connecting:
O Use my smart card
<ul> <li>Use a certificate on this computer</li> </ul>
Use simple certificate selection (Recommended)
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
ABA.ECOM Root CA
🖾 askey.savd.tw
Autoridad Certificadora de la Asociacion Nacional del Notaria
Autoridad Certificadora del Colegio Nacional de Correduria Pu
Baltimore EZ by DST
Belgacom E-Trust Primary CA
C&W HKT SecureNet CA Class A
C&W HKT SecureNet CA Class B
View Certificate
Use a different user name for the connection
OK Cancel

14. Click **OK** twice to close the dialogs until return to **Wireless Networks** tab of **wireless properties**. Now we can see the wireless network which we have just set up being displayed on the **Prefered networks**.



15. Click **OK** to save your settings. The configuration is complete

#### **Enabling WPA Authentication and Security**

- The first four steps are the same as the setting for 802.1x authentication, please refer to the previous part.
- 5. Select the **Association** Tab, and enter the SSID of the AP. (e.g., *Please*)
- 6. Choose *WPA* from the drop down menu for the **Network Authentication**, and *TKIP* for **Data encryption**.
- 7. Click **OK**, and then select the **Authentication Tab**.

- 8. The Enable network access control using IEEE 802.1X is selected by default, and Protected EAP (PEAP) is selected from the EAP type.
- 9. Click **Properties** under **EAP type**.

Wireless network prop	erties 🛛 🛛 🛛 🔀
Association Authenticatio	n Connection
Network name (SSID):	Please
Wireless network key-	
This network requires a	key for the following:
Network Authentication	n: 🛛 🔽 💌
Data encryption:	TKIP
Network key:	
Confirm network key:	
Key index (advanced):	1
The key is provided	for me automatically
This is a computer-to-o access points are not	computer (ad hoc) network; wireless used
	OK Cancel
and the second se	
Vireless network prop	erties ? 🔀
Vireless network prop Association Authenticatio	
Association Authenticatio	n Connection de authenticated network access for
Association Authenticatio Select this option to provi wireless Ethernet network	n Connection de authenticated network access for
Association Authenticatio Select this option to provi wireless Ethernet network	Connection  de authenticated network access for s.  uthentication for this network
Association Authenticatio Select this option to provi wireless Ethernet network	Connection  de authenticated network access for s.  uthentication for this network
Association Authenticatio Select this option to provi wireless Ethernet network C Enable IEEE 802.1x a EAP type: Protected EA	Connection de authenticated network access for s. uthentication for this network P(PEAP)
Association Authenticatio Select this option to provi wireless Ethernet network C Enable IEEE 802.1x a EAP type: Protected EA	n Connection de authenticated network access for s. uthentication for this network AP (PEAP)
Association Authenticatio Select this option to provi wireless Ethernet network Enable IEEE 802.1 x a EAP type: Protected EA Authenticate as computed Authenticate as guest	n Connection de authenticated network access for s. uthentication for this network AP (PEAP) Properties uter when computer information is available
Select this option to provi wireless Ethernet network C Enable IEEE 802.1x a EAP type: Protected E/	Connection  de authenticated network access for s.  uthentication for this network  AP (PEAP)  Properties  uter when computer information is available
Association Authenticatio Select this option to provi wireless Ethernet network Enable IEEE 802.1 x a EAP type: Protected EA Authenticate as computed Authenticate as guest	n Connection de authenticated network access for s. uthentication for this network AP (PEAP) Properties uter when computer information is available
Association Authenticatio Select this option to provi wireless Ethernet network C Enable IEEE 802.1 x a EAP type: Protected EA	Connection  de authenticated network access for s.  uthentication for this network  AP (PEAP)  Properties  uter when computer information is available

- 10. Choose Use a certificate on this computer option and select Use simple certificate selection (Recommended).
- 11. Check the Validate server certificate check box if server certificate validation is required
- 12. In the **Trusted Root Certification Authorities** field, check the check box beside the name of the certificate authority from which the server certificate was downloaded. (e.g., *askey.savd.tw*) Note that if you leave all check

boxes unchecked, you will be prompted to accept a connection to the root certification authority during the authentication process.

- 13. Click **OK** three times to close the dialogs and save all the settings until return to **Network Connections.**
- 14. Now the configuration for WPA authentication is completed. And you may start to use the wireless device.

When connecting: Use my smart card Use a certificate on this computer Use simple certificate selection (Recommended)
Validate server certificate
Trusted Root Certification Authorities:         ABA.ECOM Root CA         Image: Saved two         Autoridad Certificadora de la Asociacion Nacional del Notaria         Autoridad Certificadora del Colegio Nacional de Correduria Pu         Baltimore EZ by DST         Belgacom E-Trust Primary CA         C&W HKT SecureNet CA Class A         C&W HKT SecureNet CA Class B
View Certificate
Use a different user name for the connection
Network Connections           File         Edit         View         Favorities         Tools         Advanced         Help           Image: Section of the sectio

#### **Enabling WPA-PSK Authentication and Security**

- 1. Click the **Start** button, select **Control Panel**, then **Network Connections.**
- 2. Right click on your wireless network card and select **Properties**. Click on the **Wireless Networks** tab.
- 3. Click Add to continue.

General Wireless Networks Advanced
Use Windows to configure my wireless network settings
Available networks:
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.
View Wireless Networks
Preferred networks: Automatically connect to available networks in the order listed below:
Move up Move down
Add Remove Properties
Learn about <u>setting up wireless network</u> Advanced
OK Cancel
Wireless network properties
Association Authentication Connection
Association Authentication Connection
Association Authentication Connection Network name (SSID): Please
Association Authentication Connection          Network name (SSID):       Please         Wireless network key
Association Authentication Connection Network name (SSID): Please Wireless network key This network requires a key for the following:
Association Authentication Connection          Network name (SSID):       Please         Wireless network key         This network requires a key for the following:         Network Authentication:         WPA-PSK
Association Authentication Connection Network name (SSID): Please Wireless network key This network requires a key for the following: Network Authentication: WPA-PSK V Data encryption: TKIP
Association Authentication Connection Network name (SSID): Please Wireless network key This network requires a key for the following: Network Authentication: WPA-PSK V Data encryption: TKIP V Network key:
Association Authentication Connection Network name (SSID): Please Wireless network key This network requires a key for the following: Network Authentication: WPA-PSK V Data encryption: TKIP V Network key: •••••••
Association Authentication Connection Network name (SSID): Please Wireless network key This network requires a key for the following: Network Authentication: WPA-PSK Data encryption: TKIP Network key: Confirm network key: Key index (advanced): 1

22

- 4. Select the **Association** Tab, and enter the SSID of the AP. (e.g., *Please*)
- 5. Choose WPA-PSK for the Network Authentication and *TKIP* for Data encryption.
- 6. Enter **Network key** twice to access the AP.
- 7. Click **OK** to save the settings and return to the **Wireless Networks** tab on **Wireless Properties**.

8. The Network with WPA-PSK authentication has been set up, and is displayed in the preferred networks field.

	🕂 wireless Properties 🔹 ? 🗙
ł	General Wireless Networks Advanced
	✓ Use Windows to configure my wireless network settings
	Available networks: To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.
	View Wireless Networks
	Preferred networks: Automatically connect to available networks in the order listed below:
	Please (Automatic) Move up
	Add Remove Properties
	Learn about setting up wireless network Advanced
	OK Cancel
	( <sup>(p)</sup> wireless is now connected Connected to: Please Signal Strength: Low
	🚬 🔊 😣 👔 😓 10:38

9. Now the configuration for WPA-PSK authentication is completed.