DSLR-2000N

802.11n WLAN ADSL2+ Router

User’s Manual

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

·Onboard airplanes, or

·In an explosive environment, or

·In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not exclickly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

FCC statement

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

PART 68 statement

This equipment complies with Part 68 of FCC Rules and the requirements adopted by the ACTA.. On the bass unit of this equipment is a label that contains, among other information, a product identifier in the format **US: CAMDL01BDSLR2000N.** If requested, this number must be provided to the telephone company. The REN for this product is part of the product identifier that has the format **US: CAMDL01BDSLR2000N.** The digits represented by 01 are the REN without a decimal point.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. If advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact the following address and phone number for information on obtaining service or repairs:

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Company: TRENDNET, Inc.
Address: 20675 Manhattan Place, Torrance, CA 90501, USA
Tel: 310-961-5500

CE statement

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN60950-1: 2006

Safety of Information Technology Equipment

EN 50385: 2002

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1 (2006-10)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1 (2008-04)

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V1.3.2 (2008-04)

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems , 5 GHz high performance RLAN equipment and 5,8GHz Broadband Data Transmitting Systems.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

cs Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

CE0560

TABLE OF CONTENT

ABOUT THIS GUIDE

Congratulations on your purchase of this 300Mbps Wireless G 2/2+ ADSL Modem Router. This integrated access device combines ADSL modem, Internet gateway functions with wireless LAN and Fast Ethernet switch. It provides a complete solution for Internet surfing and office resource sharing, and it is easy to configure and operate for every user.

Purpose

This manual discusses how to install the IEEE 300Mbps Wireless N 2/2+ ADSL Modem Router.

Terms/Usage

In this guide, the term "the WLAN ADSL Router" refers to your 300Mbps Wireless N 2/2+ ADSL Modem Router.

Overview of this User's Guide

Introduction. Describes the 300Mbps Wireless N 2/2+ ADSL Modem Router and its features.

Unpacking and Setup. Helps you get started with the basic installation of the 300Mbps Wireless N 2/2+ ADSL Modem Router.

Identifying External Components. Describes the front panel, rear panel and LED indicators of the 300Mbps Wireless N 2/2+ ADSL Modem Router.

Connecting the WLAN ADSL Router. Tells how you can connect the 300Mbps Wireless N 2/2+ ADSL Modem Router.

Technical Specifications. Lists the technical (general, physical and environmental, performance and Routers settings) specifications of the 300Mbps Wireless N 2/2+ ADSL Modem Router.

INTRODUCTION

The 300Mbps Wireless N ADSL 2/2+ Modem Router is an all-in-one modem and wireless g router.

No need to buy a separate modem and router. This sleek device provides an ADSL 2/2+ modem, wireless g router and 4-port switch, all in a single product.

Quickly install this device to surf the Internet, download files, play games and talk Online. Advanced wireless encryption, a double firewall and a wireless on/off switch protect your valuable data. Wi-Fi Protected Setup (WPS) allows users to securely synchronize WPS supported wireless peripheral devices at the touch of a button.

Applications:

Broadband Internet access:

Several computers can share one high-speed broadband connection through wireless or wired (WLAN, LAN and WAN-Internet).

Resource sharing:

Share resources such as printers, scanners and other peripherals.

File sharing:

Exchange data, messages, and distribute files thus making good use of hard disk space.

Online gaming:

Through the local area network, online gaming and e-commerce services can be easily setup.

Firewall:

A built-in firewall function — for security and anti-hacking systems.

Supported Features:

- ◆ Compliant with ADSL G.dmt (G.992.1), G.lite (G.992.2) standards and
- ◆ Compliant with ADSL2 G.dmt.bis (G.992.3) & ADSL2+ G.992.5 standards
- ◆ Up to 24Mbps downstream, 1.2Mbps upstream with ADSL2+ service
- ◆ IEEE 802.11b/g/n Infrastructure operating modes
- ◆ Supports TR069 remote management, Web based configuration and Command Line Interface (CLI) via Telnet
- ◆ Supports NAT, DHCP
- ◆ Supports VLAN and QoS
- ◆ Supports up to 8 PVCs
- ◆ Supports 64/128-bit WEP, WPA/WPA2 and WPA-PSK/WPA2-PSK
- ◆ Supports Wi-Fi Protected Setup (WPS) for easy connection

Wireless Performance Considerations

There are a number of factors that can impact the range of wireless devices.

1. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose.
2. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
3. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
4. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter’s site survey tool to determine the best antenna orientation for your wireless devices.
5. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.
6. Any device operating on the 2.4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone’s base station as far away as possible from your wireless devices.

If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points. The use of higher gain antennas may also provide the necessary coverage depending on the environment.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the 300Mbps Wireless N 2/2+ ADSL Modem Router.

Unpacking

Open the box of the WLAN ADSL Router and carefully unpack it. The box should contain the following items:

- 300Mbps Wireless N 2/2+ ADSL Modem Router
- CD-Rom (User's Guide)
- External power adapter
- 1 1.5m (5ft) Cat.5 Ethernet Cable
- 1 RJ-11 (ADSL) cable

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

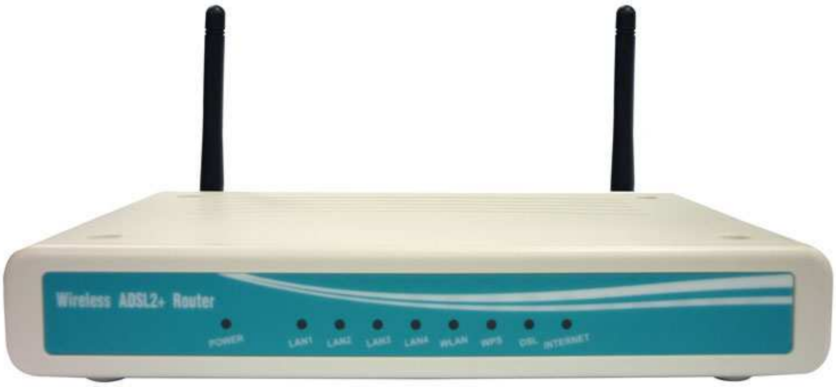
The setup of the WLAN ADSL Router can be performed properly using the following methods:

- The power outlet should be within 1.82 meters (6 feet) of the Broadband Router.
- Visually inspect the DC power jack and make sure that it is fully secured to the power adapter.
- Make sure that there is proper heat dissipation and adequate ventilation around the WLAN ADSL Router. Do not place heavy objects on the WLAN ADSL Router.
- Fix the direction of the antenna. Try to place the WLAN ADSL Router in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.

HARDWARE INSTALLATION

Front Panel

The figure below shows the front panel of the IEEE 802.11b/g/n Wireless ADSL Router.



Front Panel

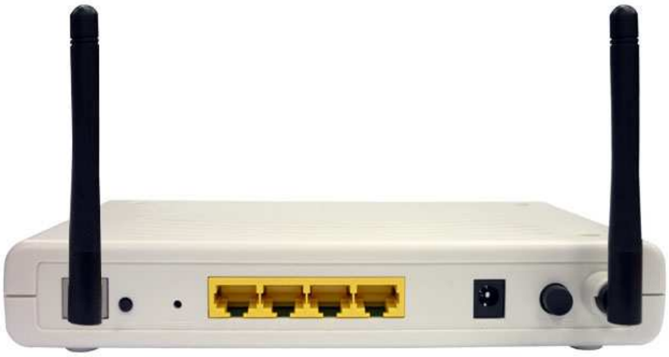
LED Indicators

LED	Color	State	Description
Power	Green	Solid on	Power on, normal operation.
	Red	Solid on	Power on, self-test failed, indicating device malfunction.
	Off		Power off.
DSL	Green	Blinking	Pending ADSL line synchronization.
		Solid on	ADSL line synchronized.
Internet	Green	Blinking	Internet activity.
		Solid on	Internet connectivity, no activity.
	Red	Solid on	Internet connection setup failed.
	Off		No Internet connection.
LAN 1~4	Green	Blinking	Ethernet activity.
		Solid on	Ethernet connection, no activity.
	Off		No Ethernet connection.
WLAN	Green	Blinking	Wireless activity.
		Solid on	Wireless connection, no activity.
	Off		Wireless disabled.

WPS	Green	Blinking	WPS in progress.
		Solid on	WPS success.
	Red	Solid on	WPS fail.
	Off		WPS disabled.

Rear Panel

The figure below shows the rear panel of the IEEE 802.11b/g/n Wireless ADSL Router.



Rear Panel

Antenna

One 2dBi gain antenna for wireless connection.

LAN (1-4)

Four RJ-45 10/100Mbps Auto-MDIX ports for connecting to either 10Mbps or 100Mbps Ethernet connections.

DSL (ADSL Port)

Connect to an active telephone line (RJ-11).

DC IN

Receptor for the supplied power adapter.

ON/OFF (On/Off Switch)

Press this button to turn the unit on or off.

WPS Button

Press to enable Wi-Fi Protected Setup.

RESET

Holding the Reset button for 5 seconds restores the WLAN ADSL Router to its original factory default settings.

Hardware connections

Connecting the WLAN ADSL Router

1. Connect ADSL Cable

   Connect the supplied RJ-11 ADSL cable from to the DSL port on the Wireless ADSL Router (the RJ11 connector) to the ADSL terminator provided by your phone company.

2. Connect LAN Cables

   Use standard LAN cables to connect PCs to the LAN ports on the Wireless ADSL Router.

3. Connect Power

   Connect the supplied power adapter to the Wireless ADSL Router. Use only the power adapter provided. Using a different one may cause hardware damage.

Check the installation

The LEDs on the WLAN ADSL Router are clearly visible and the status of the network link can be seen instantly:

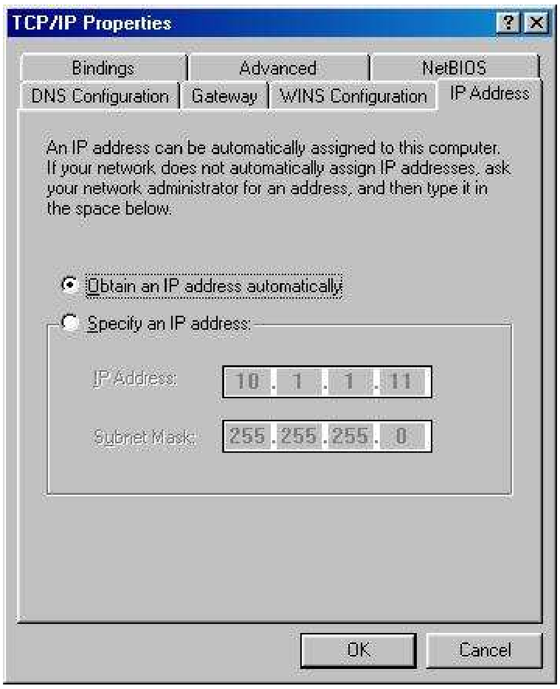
1. With the power source on, once the device is connected to the phone line and PCs, the Power, LAN, WLAN and DSL, INETRNET LEDs of the WLAN ADSL Router will light up indicating a normal status.
2. When the ADSL line is connected the DSL LED will light up.
3. When the Internet is connected the INTERNET LED will light up. (Need to configuration)

PC NETWORK TCP/IP SETTING

The network TCP/IP settings differ based on the computer's operating system (Win95/98/ME/NT/2000/XP/Vista) and are as follows.

Windows 95/98/ME

1. Click on the "**Network neighborhood**" icon found on the desktop.
2. Click the right mouse button and a context menu will be show.
3. Select "**Properties**" to enter the TCP/IP setting screen.
4. Select "**Obtain an IP address automatically**" on the "**IP address**" field.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

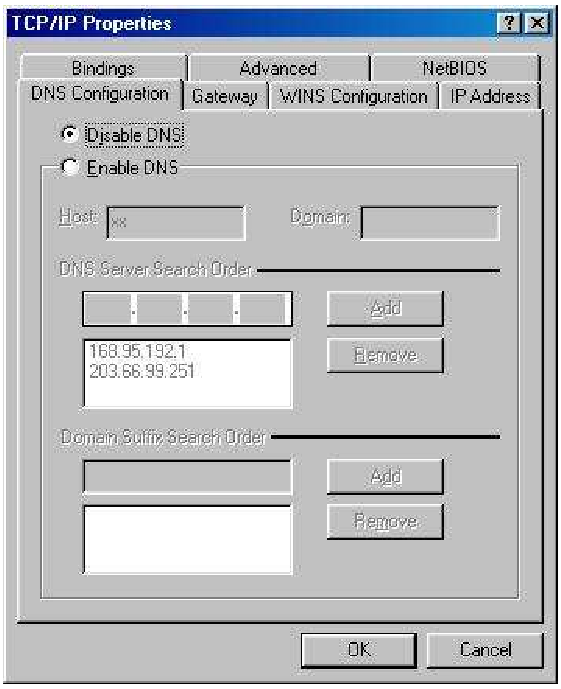
● Obtain an IP address automatically

○ Specify an IP address:

IP Address: 10 . 1 . 1 . 11

Subnet Mask: 255 . 255 . 255 . 0

5. Select "**Disable DNS**" in the "**DNS**" field.



● Disable DNS

○ Enable DNS

Host: xx

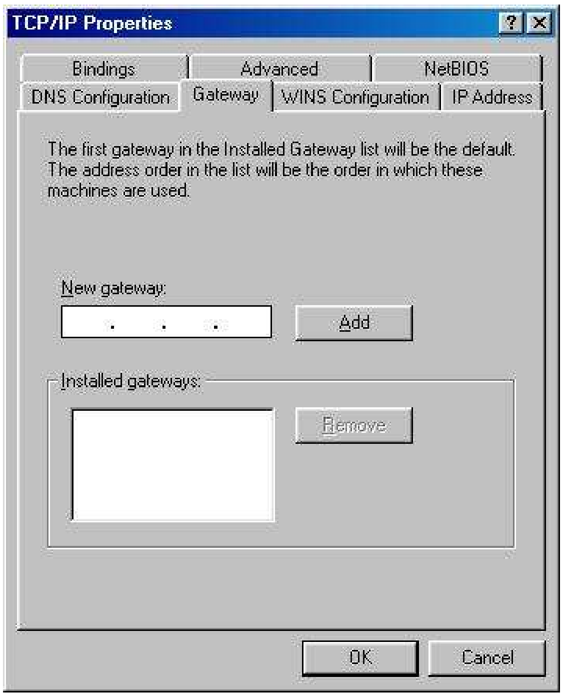
Domain:

DNS Server Search Order

168.95.192.1
203.66.99.251

Domain Suffix Search Order

6. Select “**None**” for the “**Gateway address**” field.



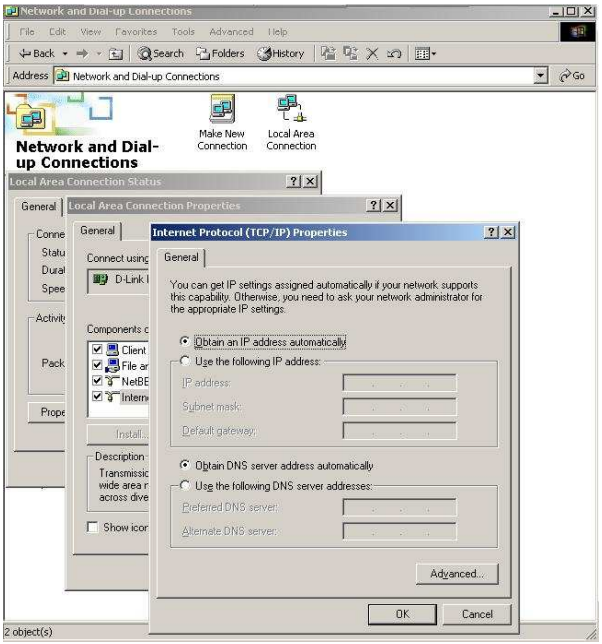
TCP/IP Properties

The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

Windows 2000

Double click on the “**My Computer**” icon on the desktop. When “**My Computer**” window opens, open the “**Control Panel**” and then open the “**Network dialup connection**” applet. Double click on the “Local area network connection” icon. Select “Properties” to enter the TCP/IP setting window.

1. In the “**Local area network status**” window, click on “**Properties**.”
2. In the “**Local area network connection**” window, first select TCP/IP setting and then select “**Properties**.”
3. Set both “**IP address**” and “**DNS**” to **Automatic configuration**.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

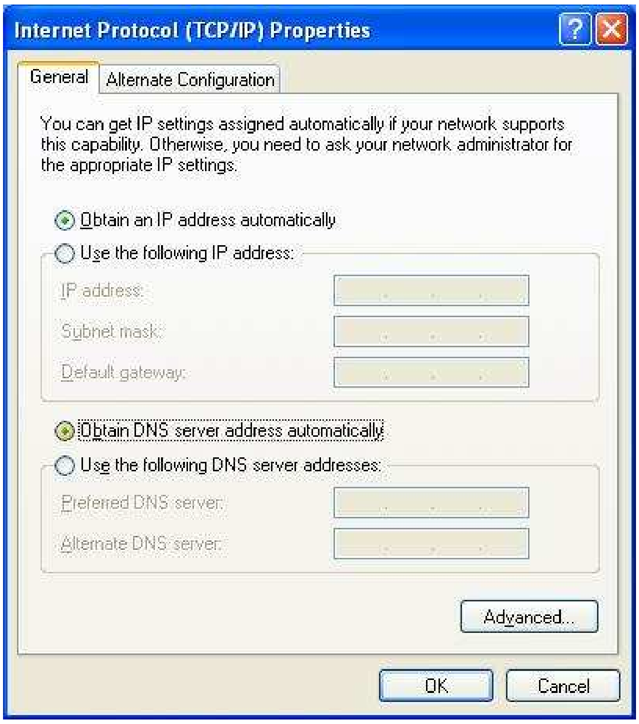
Preferred DNS server:

Alternate DNS server:

Windows XP / Vista

Point the cursor and click the right button on the "My Network Place" icon. Select "properties" to enter the TCP/IP setting window.

1. Set "**IP address**" to "**Obtain an IP address automatically**."
2. Set "**DNS**" to "**Obtain DNS server address automatically**."



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

CONFIGURATION

First make sure that the network connections are functioning normally.

This WLAN Router can be configured using Internet Explorer 5.0 or newer web browser versions.

Login to the WLAN ADSL Router through Wireless LAN

Before configuring the WLAN ADSL Router through WLAN, make sure that the SSID, Channel and the WEP is set properly.

The default setting of the WLAN ADSL Router that you will use:

- ✓ SSID: ADSL_Modem/Router
- ✓ Channel: Auto
- ✓ 802.11 Mode: 802.11b+g+n mixed mode
- ✓ Security: disable
- ✓ IP Address: 192.168.1.1
- ✓ VPI/VCI for ATM: 5/35
- ✓ ADSL Line mode: Auto-detect

Login to the WLAN ADSL Router

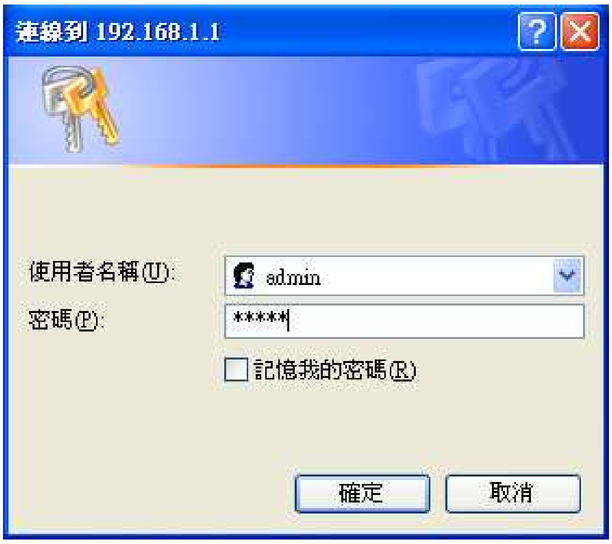
Before you configure this device, note that when the WLAN ADSL Router, make sure the host PC must be set on the **IP subnet** that can be accessed by the xDSL/Cable modem. For example, when the default network address of the xDSL/Cable modem Ethernet interface is 192.168.1.x, then the host PC should be set at 192.168.1.xxx (where xxx is a number between 2 and 254), and the default subnet mask is 255.255.255.0.

Using the Web Browser

1. Open Internet Explorer 6.0 or above Internet browser.
2. Enter IP address ***http://192.168.1.1*** (the factory-default IP address setting) to the URL web address location.

http://192.168.1.1/

3. When the following dialog box appears, enter the user name and password to login to the main configuration window, the default username and password is "***admin***".



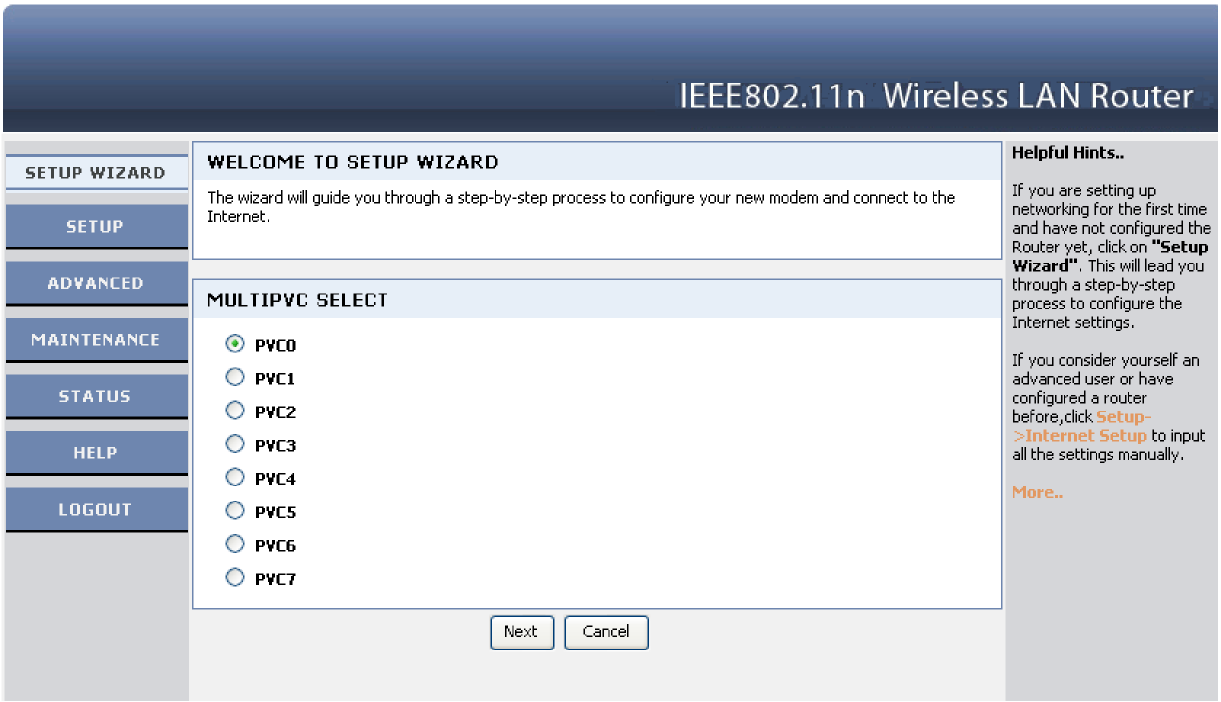
連線到 192.168.1.1

使用者名稱(U): admin

密碼(P): *****

□ 記憶我的密碼(R)

After entering the user name and password, the main page comes up, the screen will display the SETUP WIZARD status.



IEEE802.11n Wireless LAN Router

WELCOME TO SETUP WIZARD

The wizard will guide you through a step-by-step process to configure your new modem and connect to the Internet.

MULTIPVC SELECT

● PVC0
○ PVC1
○ PVC2
○ PVC3
○ PVC4
○ PVC5
○ PVC6
○ PVC7

Helpful Hints..

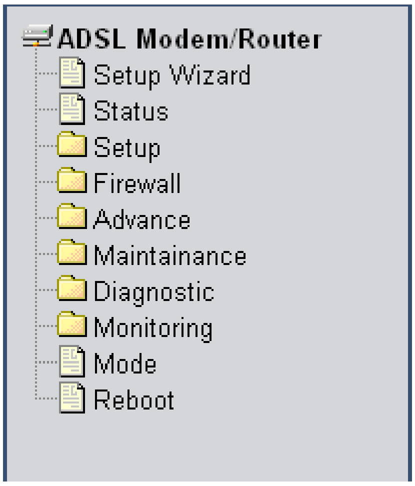
If you are setting up networking for the first time and have not configured the Router yet, click on **"Setup Wizard"**. This will lead you through a step-by-step process to configure the Internet settings.

If you consider yourself an advanced user or have configured a router before,click **Setup->Internet Setup** to input all the settings manually.

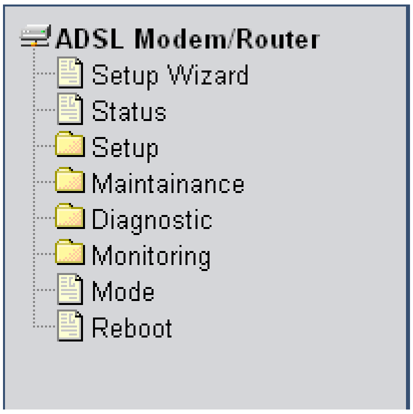
More..

Configuration Menu

When the main page appears, find the Configuration menu in the left side of the screen. Click on the setup item that you want to configure. There are ten options: Setup Wizard, Status, Setup, Firewall (form router mode only), Advance (form router mode only), Maintenance, Diagnostic, Monitoring, Mode and Reboot as shown in the Configuration Menu screen.



Configure menu on Router mode



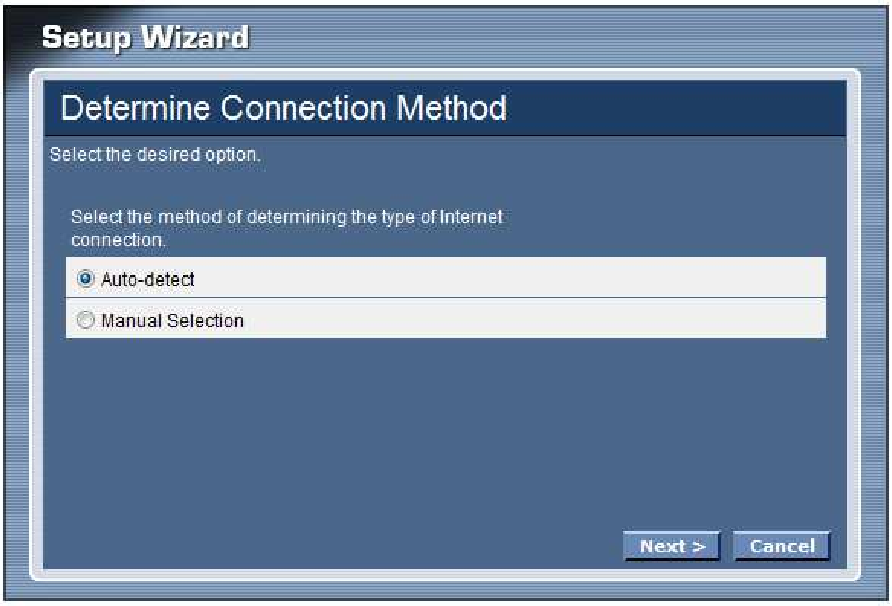
Configure menu on Modem mode

SETUP WIZARD

Setup wizard is provided as part of the web configuration utility. User can simply follow the step-by-step process to get the WLAN ADSL Router configuration ready by clicking on` the “Wizard” button on the function menu. The following screen will appear.

Step 1: Determine Connection Method

Choose “Auto-detect” for auto detect the Internet connection method or “Manual Selection” for manually configure the ADSL setting.



Setup Wizard

Determine Connection Method

Select the desired option.

Select the method of determining the type of Internet connection.

● Auto-detect
○ Manual Selection

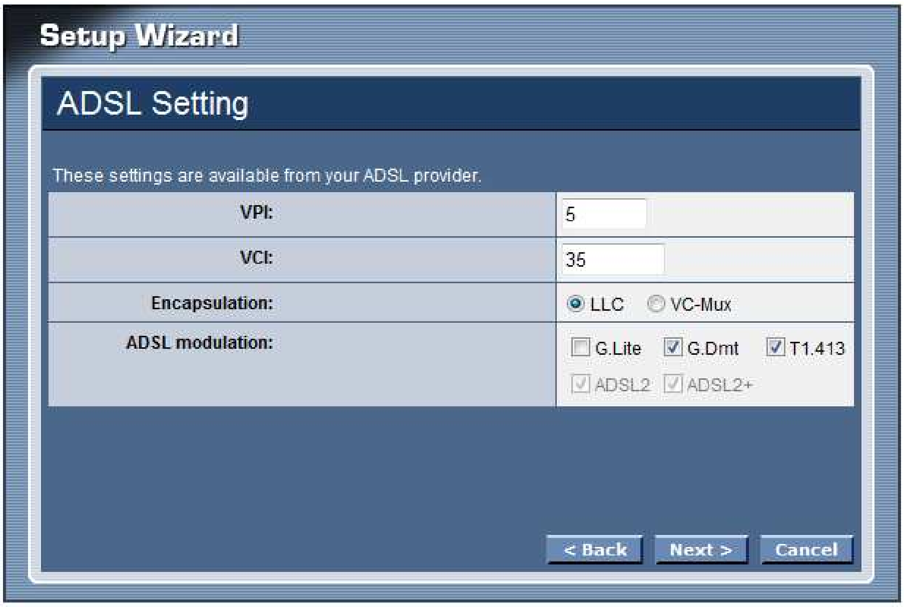
Auto-detect

Selected the “Auto-detect” then click “Next” button, the wizard will automatically detect the first usable PVC and automatically detect PPPoE, PPPoA, and Bridge Protocol (with DHCP Server available)

Manual Selection

Selected the “Manual Selection” then click “Next” button, the wizard will setting the Internet connection manually.

Step 2: ADSL Setting



ADSL Setting

These settings are available from your ADSL provider.

VPI:	5
VCI:	35
Encapsulation:	● LLC ○ VC-Mux
ADSL modulation:	□ G.Lite ☑ G.Dmt ☑ T1.413 ☑ ADSL2 ☑ ADSL2+

VPI: Enter the VPI value provided by ISP

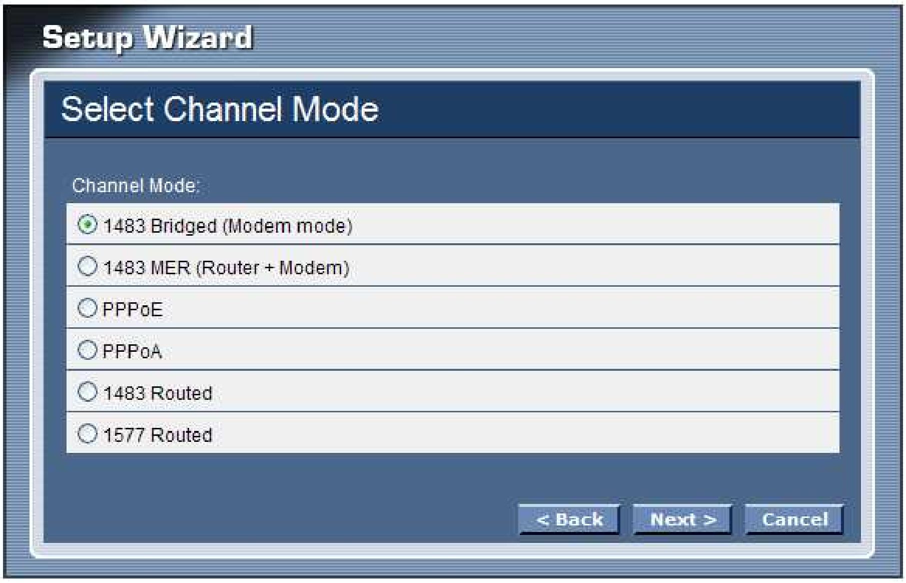
VCI: Enter the VCI value provided by ISP

Encapsulation: Select the encapsulation type for LLC or VC-Mux

ADSL modulation: Select the ADSL modulation type defined by your ISP

Step 3: Select Channel Mode

Select the type of network protocol for 1483 Bridged, 1483 MER, PPPoE, PPPoA or 1483 Routed.



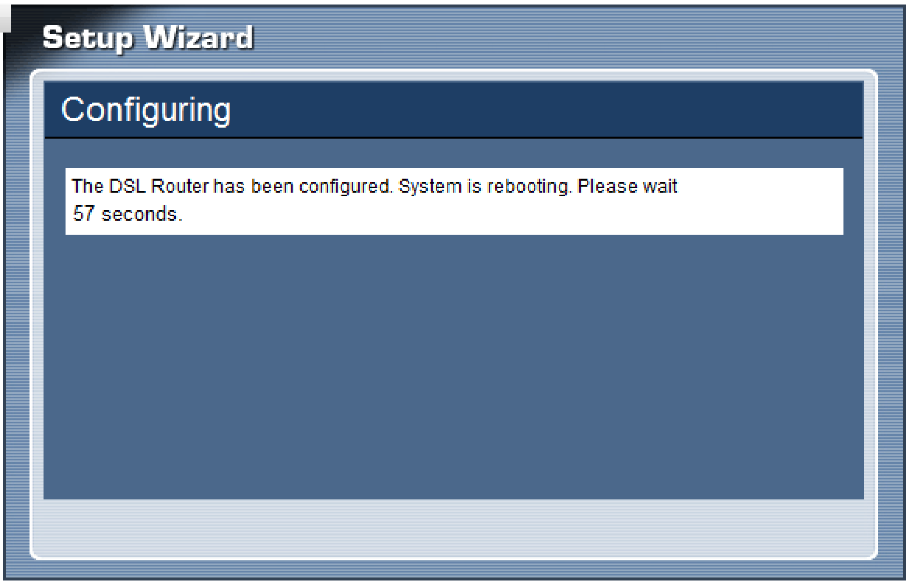
Select Channel Mode

Channel Mode:

- ● 1483 Bridged (Modem mode)
- ○ 1483 MER (Router + Modem)
- ○ PPPoE
- ○ PPPoA
- ○ 1483 Routed
- ○ 1577 Routed

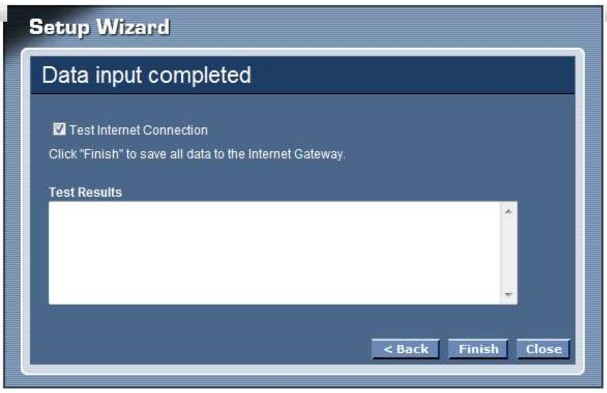
1483 Bridged

Selected the 1483 Bridged mode then click next button, the WLAN ADSL Router will save configuration and reboot the WLAN ADSL Router.



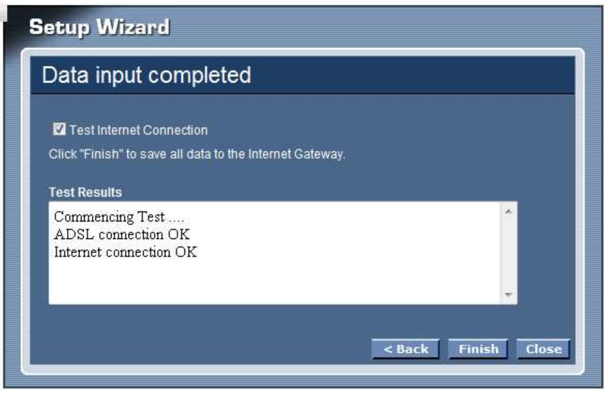
The DSL Router has been configured. System is rebooting. Please wait 57 seconds.

When rebooted the WLAN ADSL Router, enabled the "Test Internet Connection" then click finish button for test Internet connection; click close button close the setup wizard.



☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.



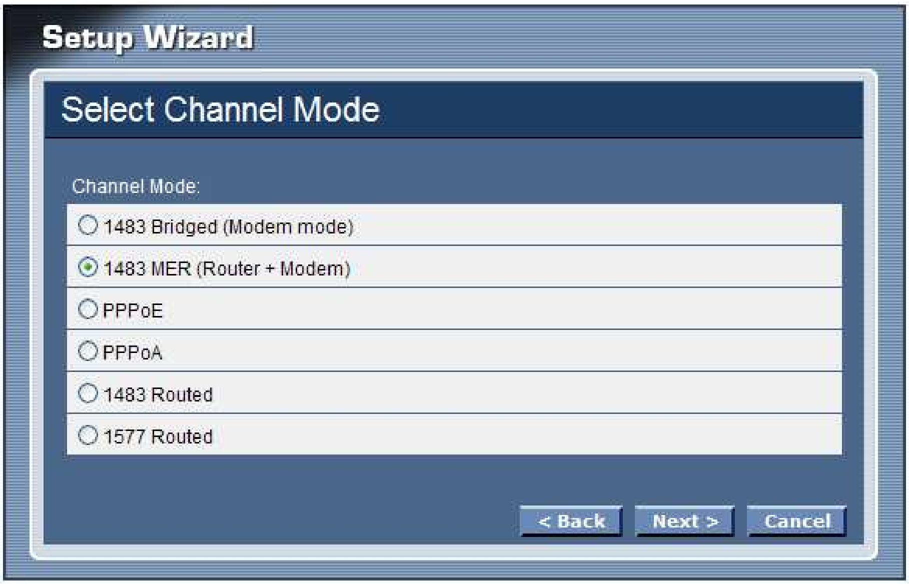
☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

```
Commencing Test ....
ADSL connection OK
Internet connection OK
```

1483 MER

Selected the 1483 MER mode then click next button, continuing the WAN IP setting.

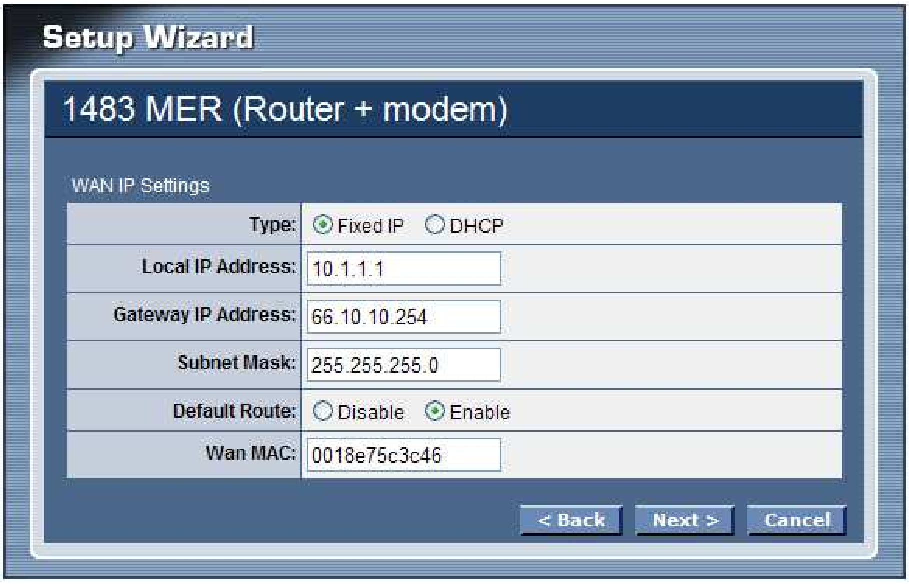


Select Channel Mode

Channel Mode:

- ○ 1483 Bridged (Modem mode)
- ● 1483 MER (Router + Modem)
- ○ PPPoE
- ○ PPPoA
- ○ 1483 Routed
- ○ 1577 Routed

Select whether user wants to specify an IP address manually, or want DHCP to obtain an IP address automatically.



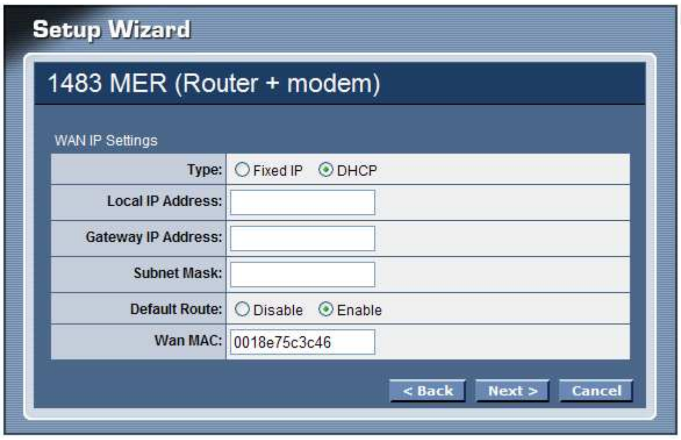
1483 MER (Router + modem)

WAN IP Settings

Type:	● Fixed IP ○ DHCP
Local IP Address:	10.1.1.1
Gateway IP Address:	66.10.10.254
Subnet Mask:	255.255.255.0
Default Route:	○ Disable ● Enable
Wan MAC:	0018e75c3c46

If selected to 1483 MER mode with DHCP, the follows step will going on:

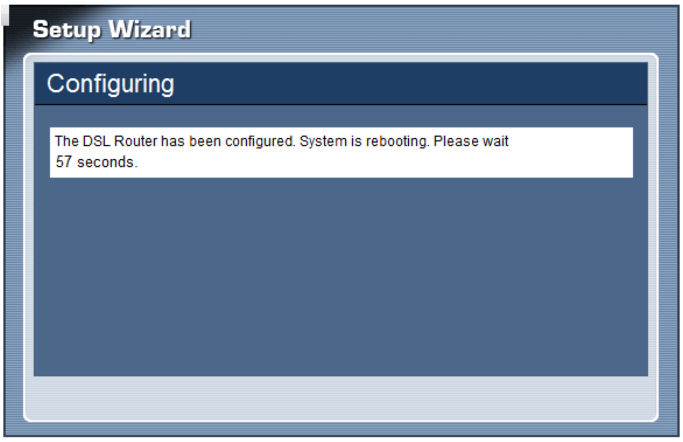
Click next button to save configuration and reboot the WLAN ADSL Router



1483 MER (Router + modem)

WAN IP Settings

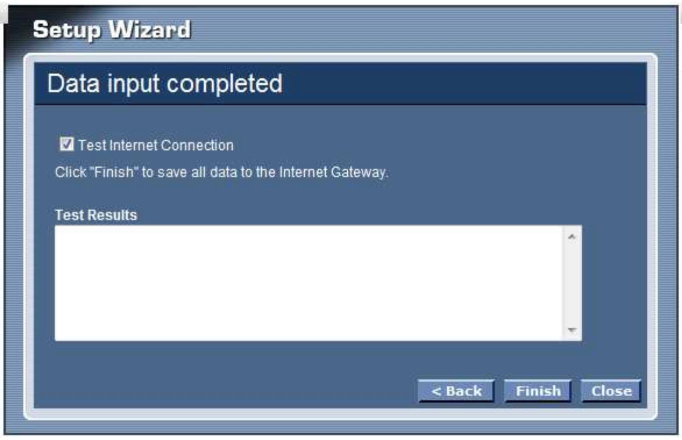
Type:	○ Fixed IP ● DHCP
Local IP Address:	
Gateway IP Address:	
Subnet Mask:	
Default Route:	○ Disable ● Enable
Wan MAC:	0018e75c3c46



Configuring

The DSL Router has been configured. System is rebooting. Please wait 57 seconds.

When rebooted the WLAN ADSL Router, enabled the "Test Internet Connection" then click finish button for test Internet connection; click close button close the setup wizard.

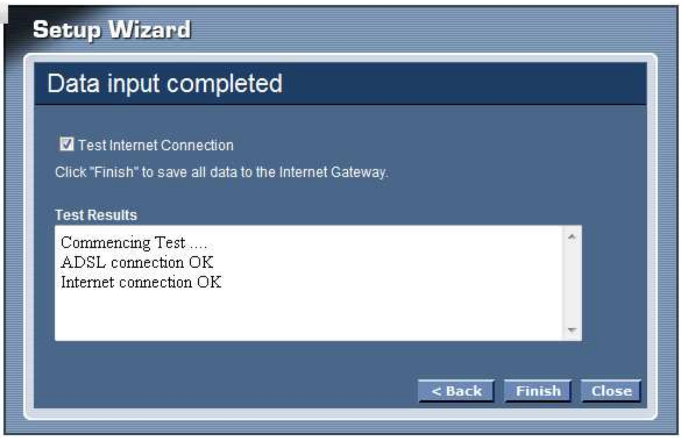


Data input completed

☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

Test Results



Data input completed

☑ Test Internet Connection

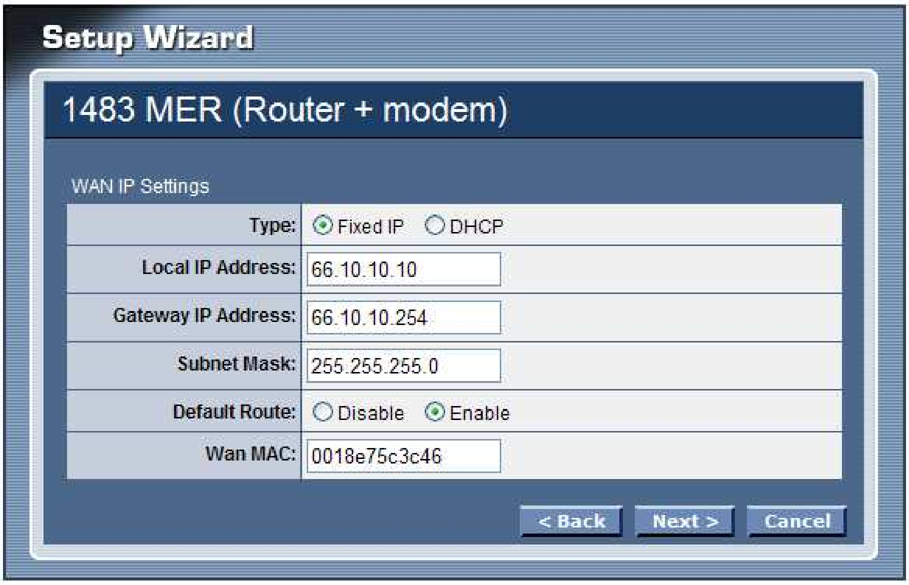
Click "Finish" to save all data to the Internet Gateway.

Test Results

```
Commencing Test ....
ADSL connection OK
Internet connection OK
```

If selected to 1483 MER mode with Fixed IP, the follows step will going on:

Enter the Local IP Address, Gateway IP Address, Subnet Mask and Wan MAC (if need to specify the other Wan MAC address) in the text boxes, click next button to continue the DNS server setting.

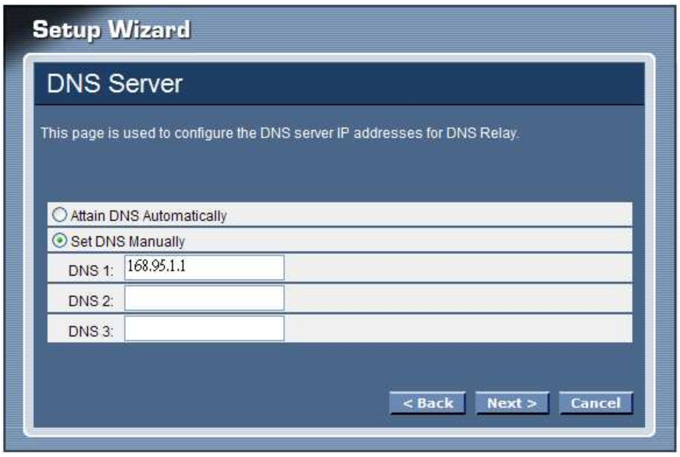


1483 MER (Router + modem)

WAN IP Settings

Type:	● Fixed IP ○ DHCP
Local IP Address:	66.10.10.10
Gateway IP Address:	66.10.10.254
Subnet Mask:	255.255.255.0
Default Route:	○ Disable ● Enable
Wan MAC:	0018e75c3c46

Setting the DNS server assigned by DHCP or manually, click next button to save configuration and reboot the WLAN ADSL Router



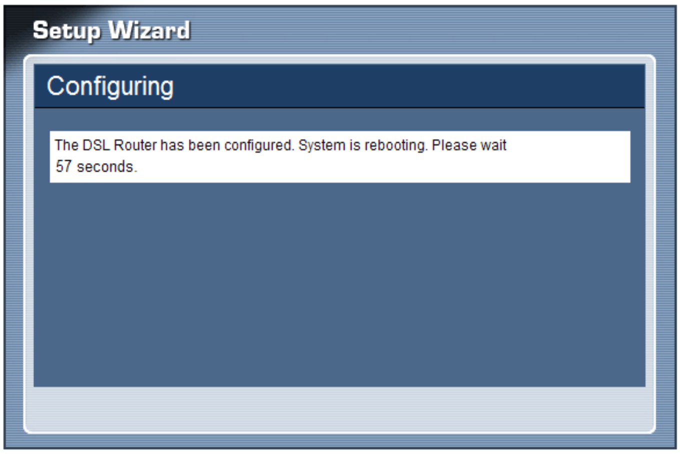
DNS Server

This page is used to configure the DNS server IP addresses for DNS Relay.

○ Attain DNS Automatically

● Set DNS Manually

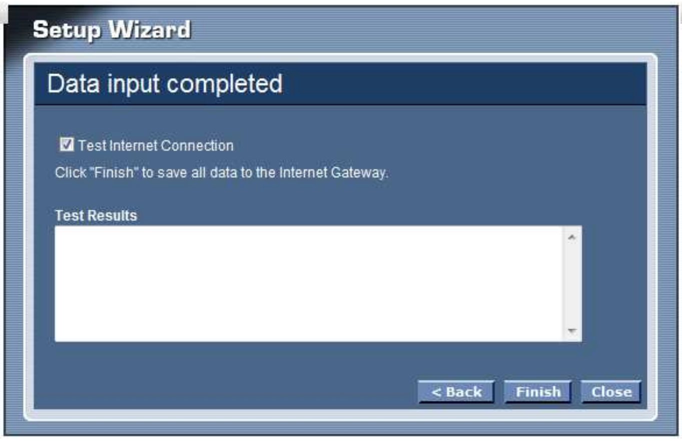
DNS 1:	168.95.1.1
DNS 2:	
DNS 3:	



Configuring

The DSL Router has been configured. System is rebooting. Please wait 57 seconds.

When rebooted the WLAN ADSL Router, enabled the "Test Internet Connection" then click finish button for test Internet connection; click close button close the setup wizard.

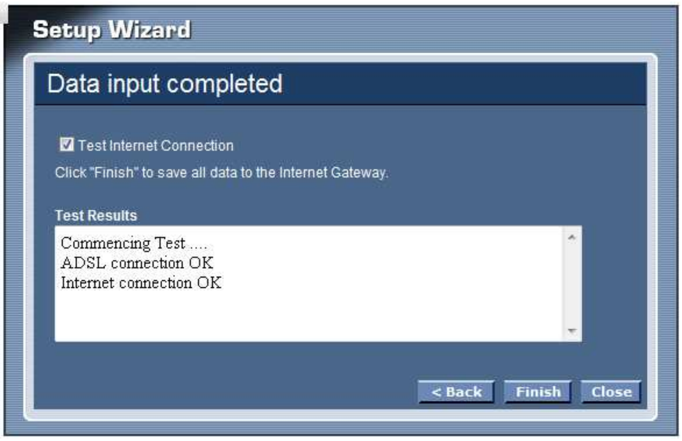


Data input completed

☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

Test Results



Data input completed

☑ Test Internet Connection

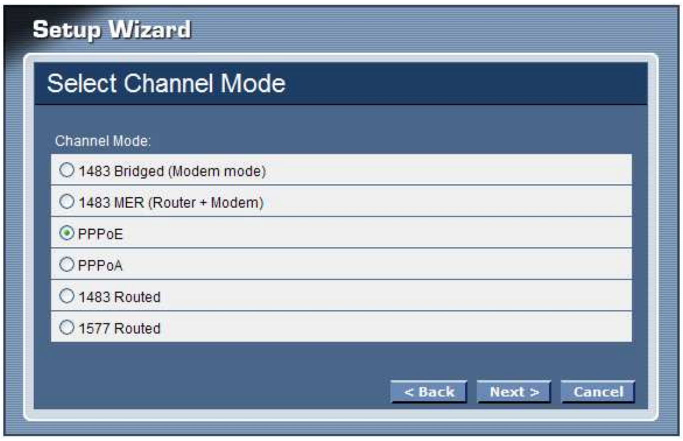
Click "Finish" to save all data to the Internet Gateway.

Test Results

```
Commencing Test ....
ADSL connection OK
Internet connection OK
```

PPPoE/PPPoA

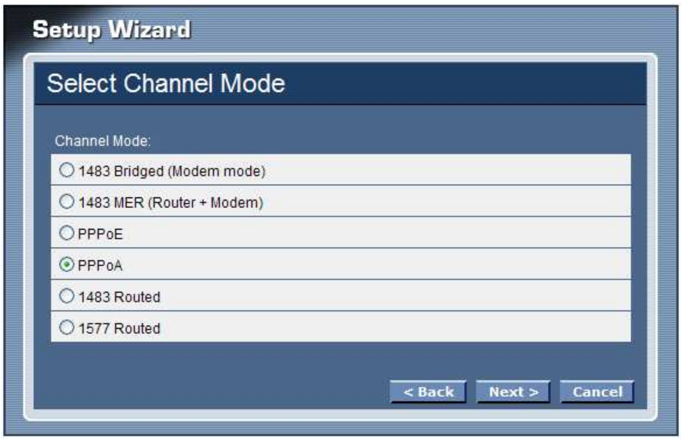
Selected the PPPoE or PPPoA mode then click next button, continue the account setting.



Select Channel Mode

Channel Mode:

○ 1483 Bridged (Modem mode)
○ 1483 MER (Router + Modem)
● PPPoE
○ PPPoA
○ 1483 Routed
○ 1577 Routed



Select Channel Mode

Channel Mode:

○ 1483 Bridged (Modem mode)
○ 1483 MER (Router + Modem)
○ PPPoE
● PPPoA
○ 1483 Routed
○ 1577 Routed

User Name: Enter the username provided by ISP.

Password: Enter the password provided by ISP

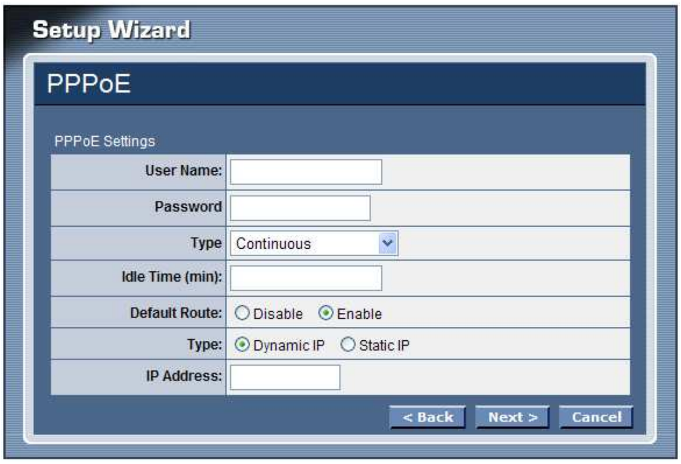
Type: Select the connection type for *Continuous* Connecting, *Connect on Demand* or *Manual* connecting.

Idle Time: Enter the idle time for Connect on Daemon, when no Internet access during the idle time, the ADSL connection will auto disconnect.

Default Route: Setting the default router function disable or enable.

Type: Select the IP address assign by DHCP or manually setting.

IP Address: Enter the IP address provided by your ISP when the Type is selected by Static IP.

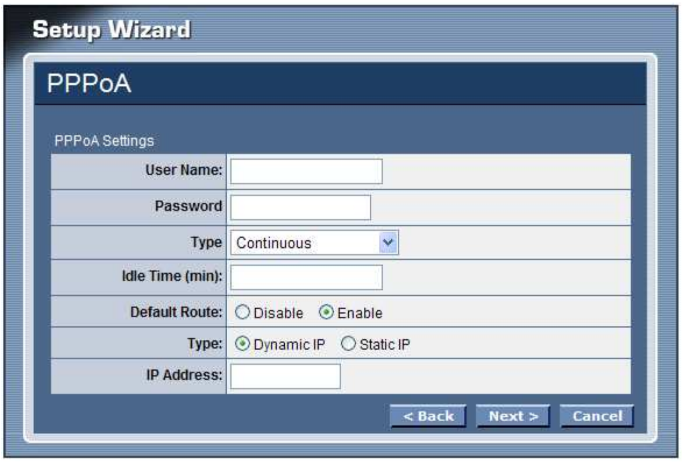


Setup Wizard

PPPoE

PPPoE Settings

User Name:	
Password	
Type	Continuous
Idle Time (min):	
Default Route:	○ Disable ● Enable
Type:	● Dynamic IP ○ Static IP
IP Address:	



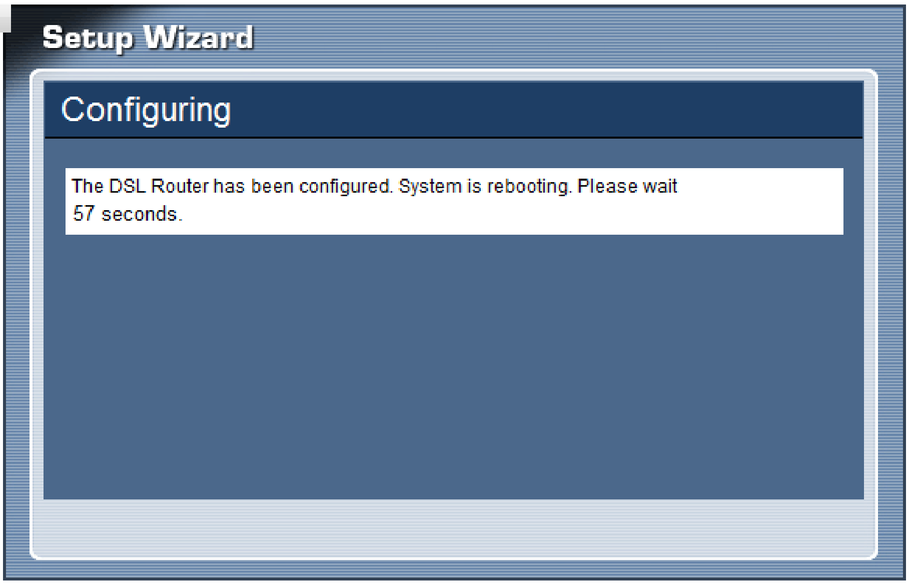
Setup Wizard

PPPoA

PPPoA Settings

User Name:	
Password	
Type	Continuous
Idle Time (min):	
Default Route:	○ Disable ● Enable
Type:	● Dynamic IP ○ Static IP
IP Address:	

Click next button to save configuration and reboot the WLAN ADSL Router

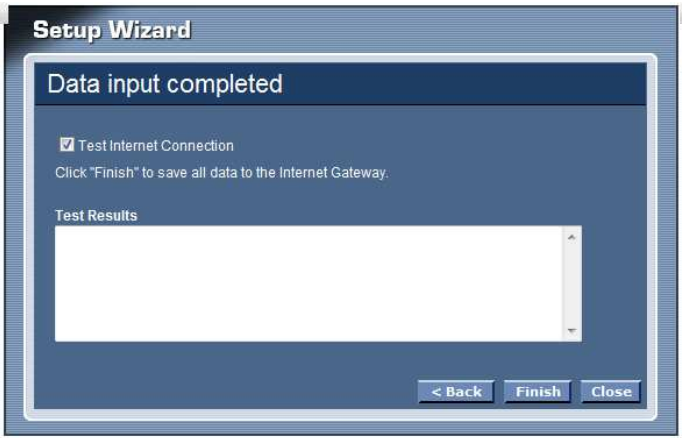


Setup Wizard

Configuring

The DSL Router has been configured. System is rebooting. Please wait 57 seconds.

When rebooted the WLAN ADSL Router, enabled the “Test Internet Connection” then click finish button for test Internet connection; click close button close the setup wizard.

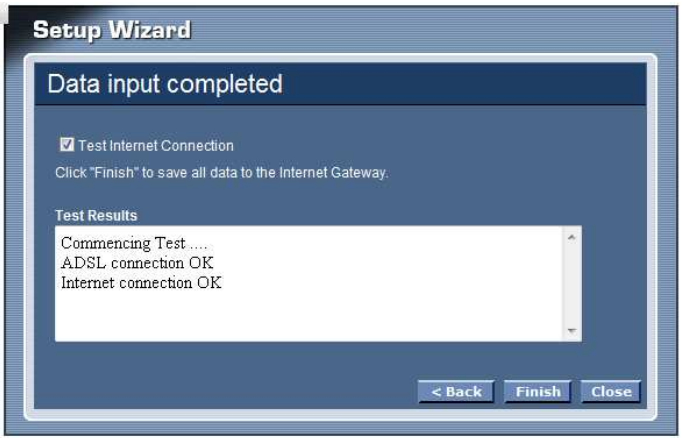

Setup Wizard

Data input completed

☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

Test Results


Setup Wizard

Data input completed

☑ Test Internet Connection

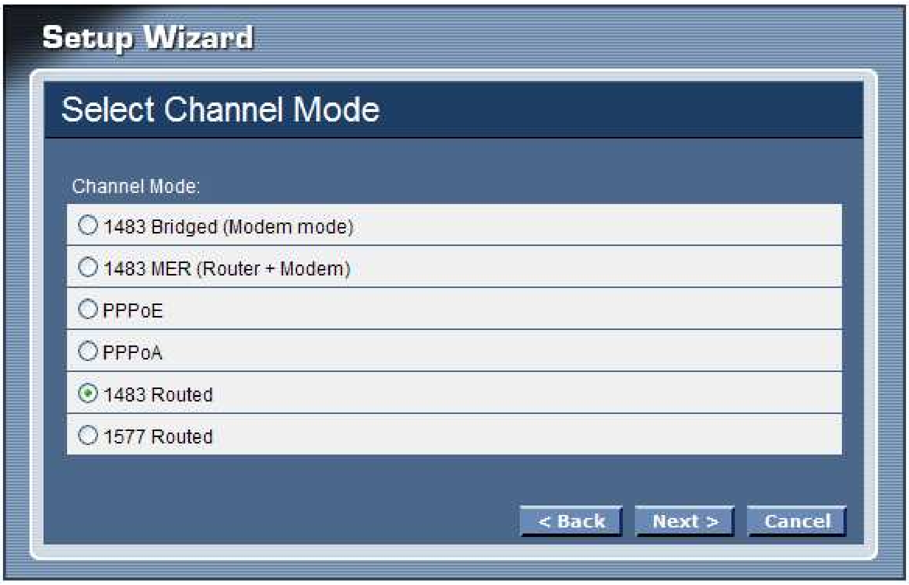
Click "Finish" to save all data to the Internet Gateway.

Test Results

```
Commencing Test ....
ADSL connection OK
Internet connection OK
```

1483 Routed

Selected the 1483 Routed mode then click next button, continuing the WAN IP setting.


Setup Wizard

Select Channel Mode

Channel Mode:

- ○ 1483 Bridged (Modem mode)
- ○ 1483 MER (Router + Modem)
- ○ PPPoE
- ○ PPPoA
- ● 1483 Routed
- ○ 1577 Routed

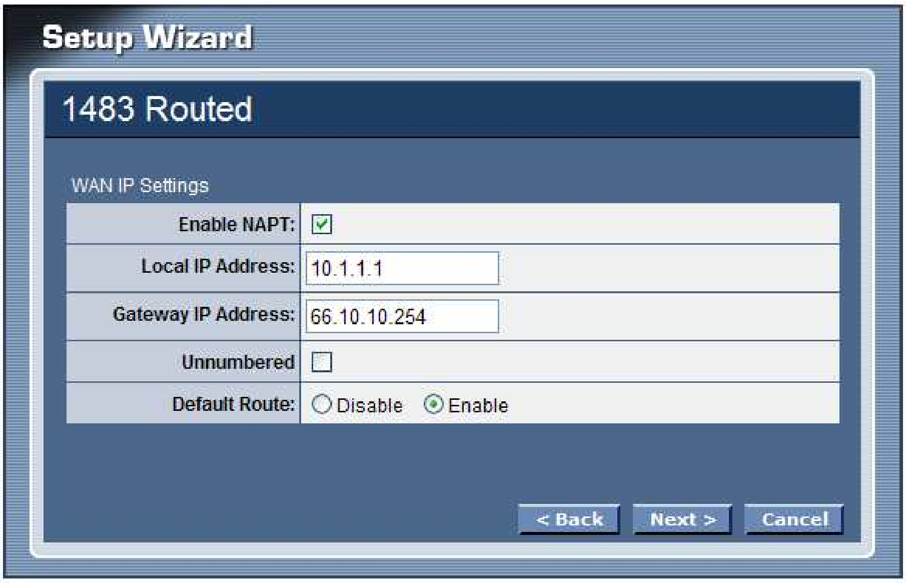
NAPT: Checked to enable the NAPT on the WLAN ADSL Router.

Local IP Address : Enter local IP address provided by ISP

Gateway IP Address : Enter gateway IP address provided by ISP

Unnumbered: Checked to enable the IP unnumbered on the WLAN ADSL Router.

Default Route: Setting the default router function disable or enable.



Setup Wizard

1483 Routed

WAN IP Settings

Enable NAPT: ☑

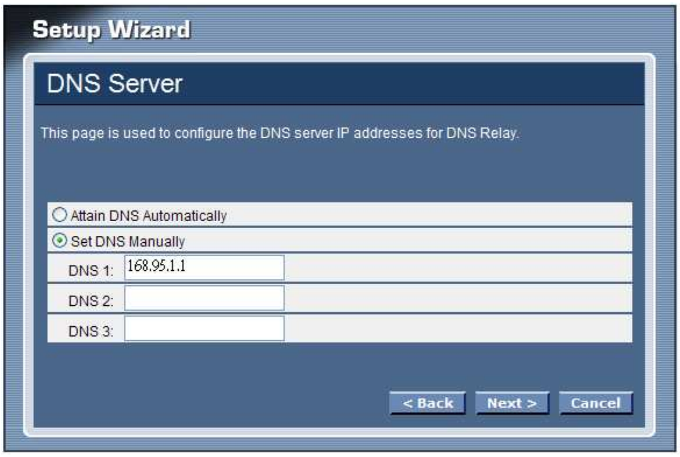
Local IP Address: 10.1.1.1

Gateway IP Address: 66.10.10.254

Unnumbered □

Default Route: ○ Disable ● Enable

Setting the DNS server assigned by DHCP or manually, click next button to save configuration and reboot the WLAN ADSL Router.



Setup Wizard

DNS Server

This page is used to configure the DNS server IP addresses for DNS Relay.

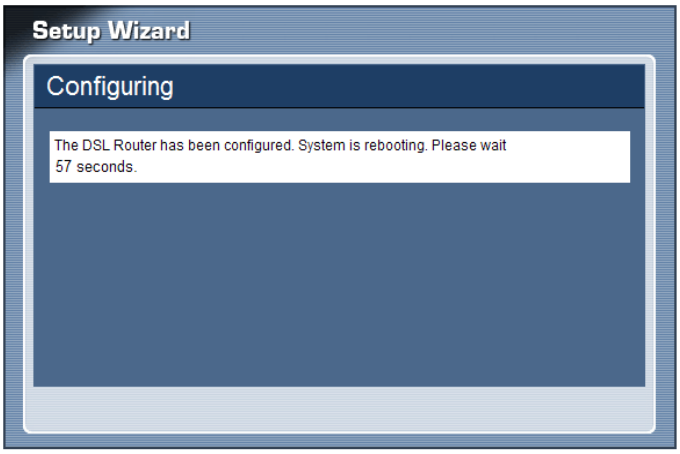
○ Attain DNS Automatically

● Set DNS Manually

DNS 1: 168.95.1.1

DNS 2:

DNS 3:



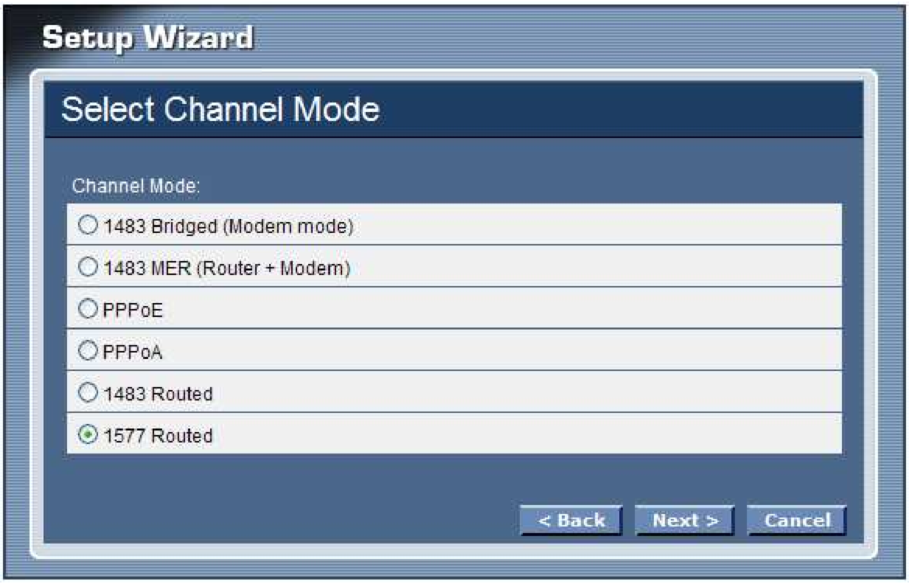
Setup Wizard

Configuring

The DSL Router has been configured. System is rebooting. Please wait 57 seconds.

1577 Routed

Selected the 1577 Routed mode then click next button, continuing the WAN IP setting.



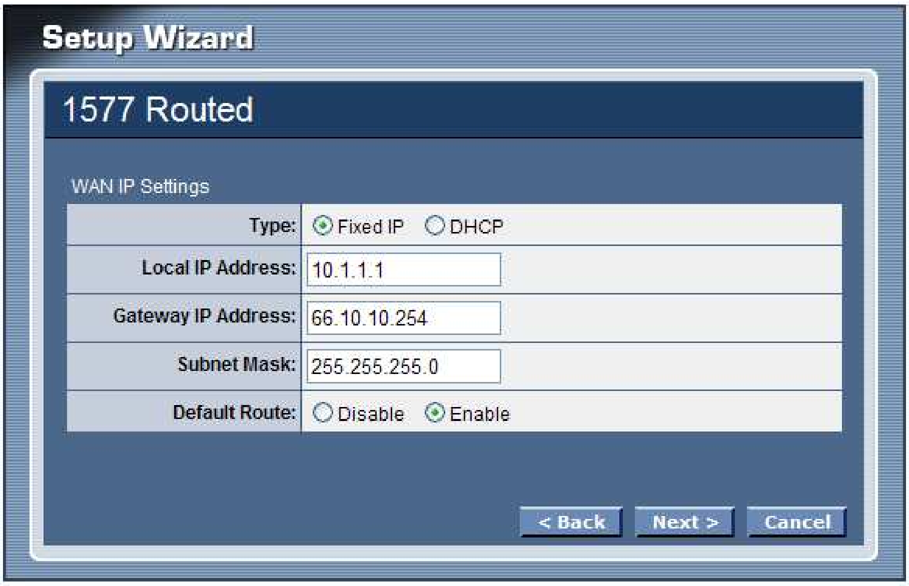
Setup Wizard

Select Channel Mode

Channel Mode:

- ○ 1483 Bridged (Modem mode)
- ○ 1483 MER (Router + Modem)
- ○ PPPoE
- ○ PPPoA
- ○ 1483 Routed
- ● 1577 Routed

Select whether user wants to specify an IP address manually, or want DHCP to obtain an IP address automatically.



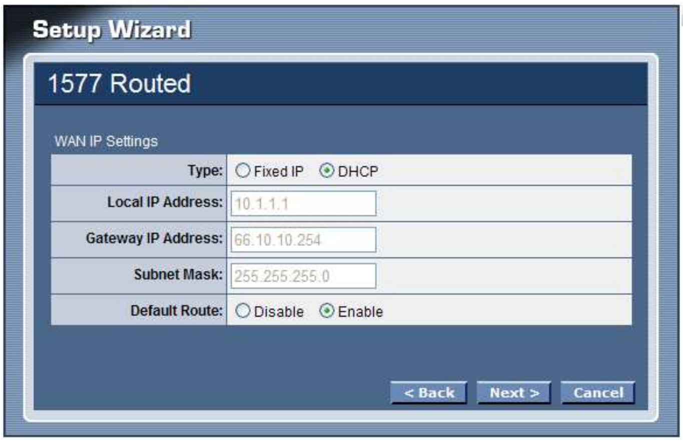
Setup Wizard

1577 Routed

WAN IP Settings

Type:	● Fixed IP ○ DHCP
Local IP Address:	10.1.1.1
Gateway IP Address:	66.10.10.254
Subnet Mask:	255.255.255.0
Default Route:	○ Disable ● Enable

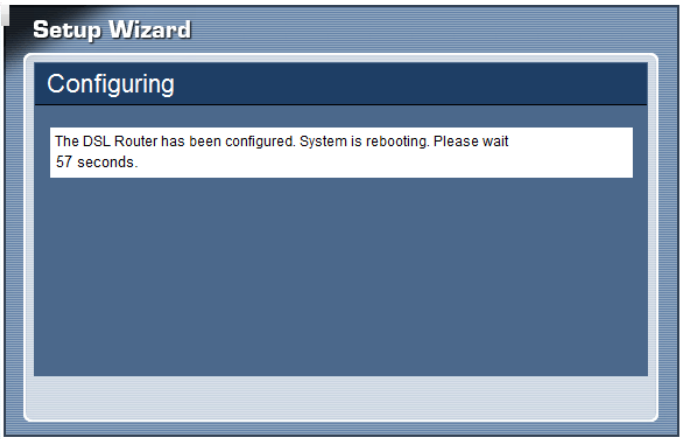
If selected to 1577 Routed mode with DHCP, the follows step will going on:
Click next button to save configuration and reboot the WLAN ADSL Router



1577 Routed

WAN IP Settings

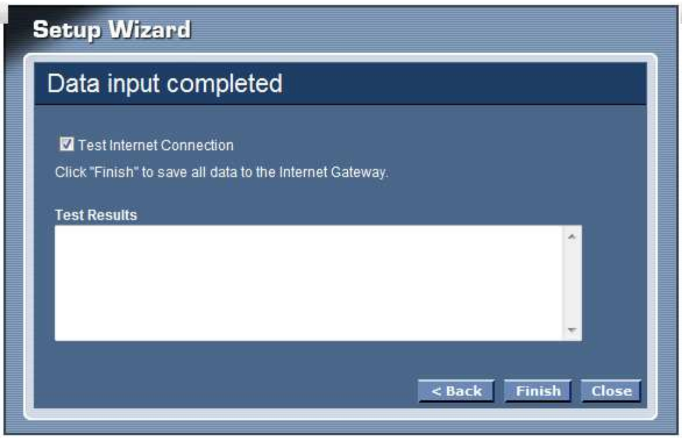
Type:	○ Fixed IP ● DHCP
Local IP Address:	10.1.1.1
Gateway IP Address:	66.10.10.254
Subnet Mask:	255.255.255.0
Default Route:	○ Disable ● Enable



Configuring

The DSL Router has been configured. System is rebooting. Please wait
57 seconds.

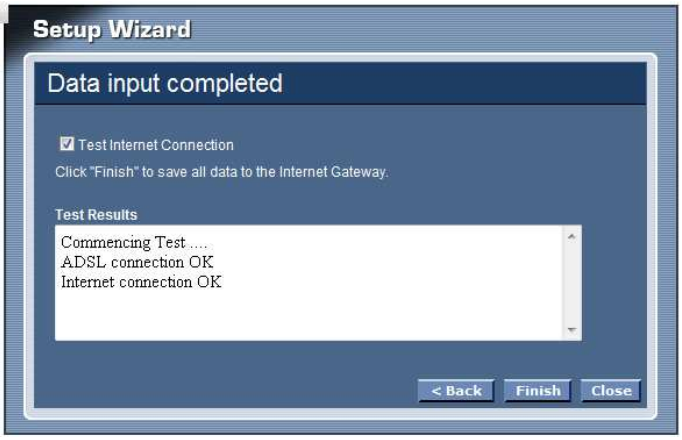
When rebooted the WLAN ADSL Router, enabled the "Test Internet Connection" then click finish button for test Internet connection; click close button close the setup wizard.



Data input completed

☑ Test Internet Connection
Click "Finish" to save all data to the Internet Gateway.

Test Results



Data input completed

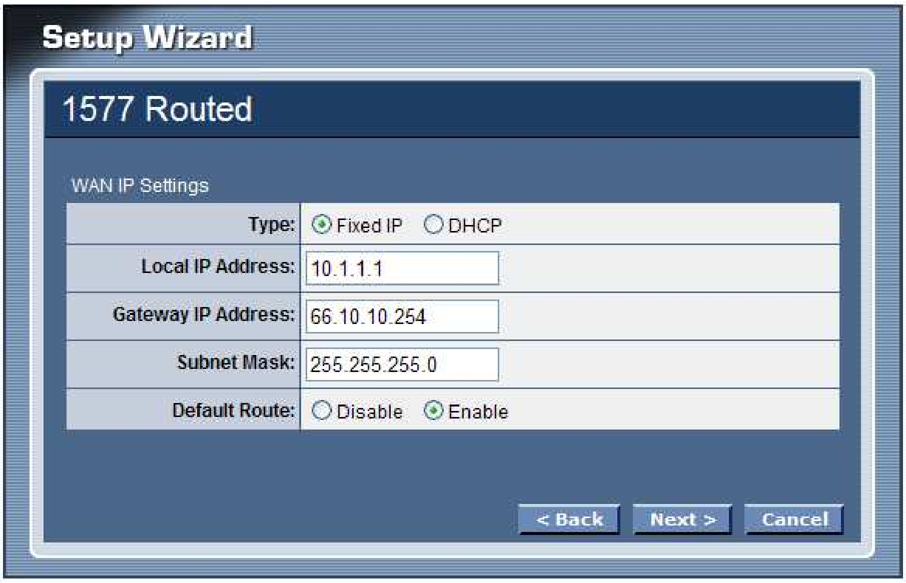
☑ Test Internet Connection
Click "Finish" to save all data to the Internet Gateway.

Test Results

```
Commencing Test ....
ADSL connection OK
Internet connection OK
```

If selected to 1577 Routed mode with Fixed IP, the follows step will going on:

Enter the Local IP Address, Gateway IP Address, Subnet Mask and Wan MAC (if need to specify the other Wan MAC address) in the text boxes, click next button to continue the DNS server setting.

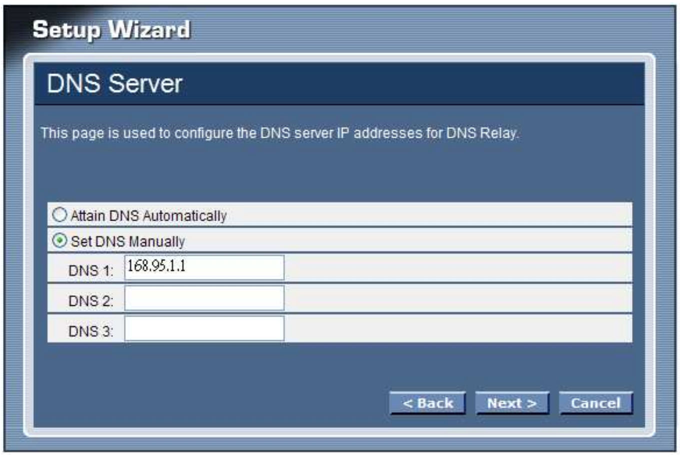

Setup Wizard

1577 Routed

WAN IP Settings

Type:	● Fixed IP ○ DHCP
Local IP Address:	10.1.1.1
Gateway IP Address:	66.10.10.254
Subnet Mask:	255.255.255.0
Default Route:	○ Disable ● Enable

Setting the DNS server assigned by DHCP or manually, click next button to save configuration and reboot the WLAN ADSL Router


Setup Wizard

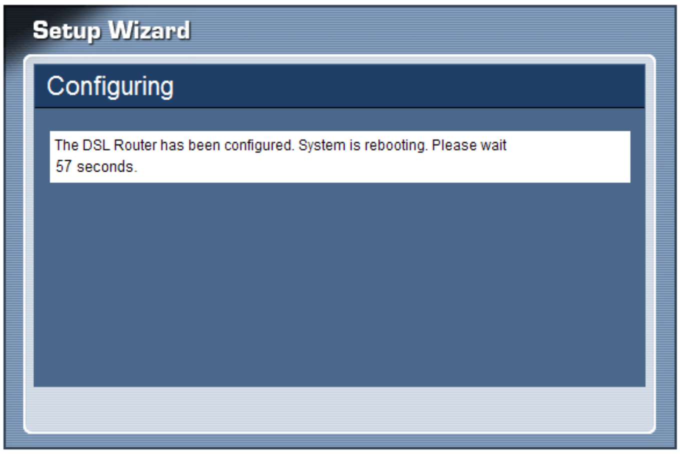
DNS Server

This page is used to configure the DNS server IP addresses for DNS Relay.

○ Attain DNS Automatically

● Set DNS Manually

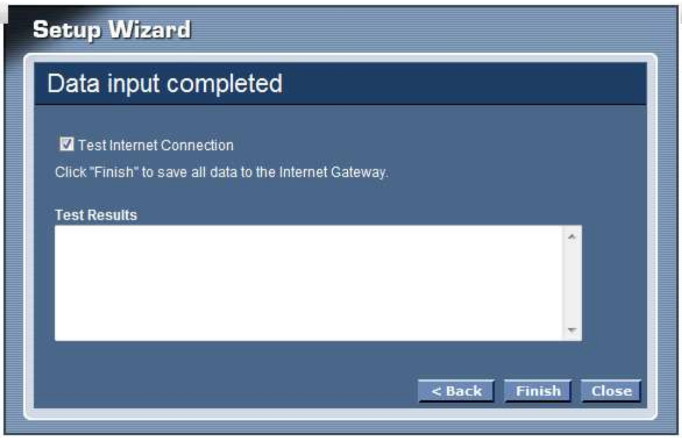
DNS 1:	168.95.1.1
DNS 2:	
DNS 3:	


Setup Wizard

Configuring

The DSL Router has been configured. System is rebooting. Please wait 57 seconds.

When rebooted the WLAN ADSL Router, enabled the “Test Internet Connection” then click finish button for test Internet connection; click close button close the setup wizard.



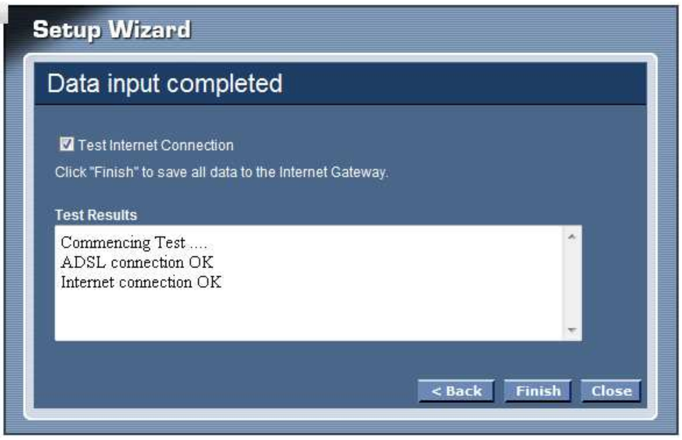
Setup Wizard

Data input completed

☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

Test Results



Setup Wizard

Data input completed

☑ Test Internet Connection

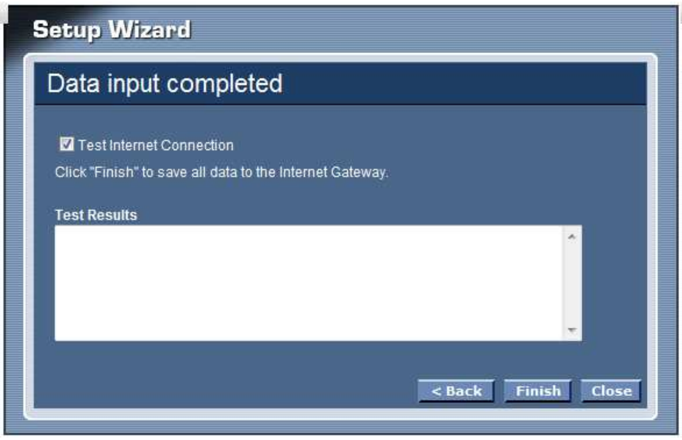
Click "Finish" to save all data to the Internet Gateway.

Test Results

```
Commencing Test ....
ADSL connection OK
Internet connection OK
```

Step 4: Completed the Setup Wizard

When rebooted the WLAN ADSL Router, enabled the “Test Internet Connection” then click finish button for test Internet connection; click close button close the setup wizard.



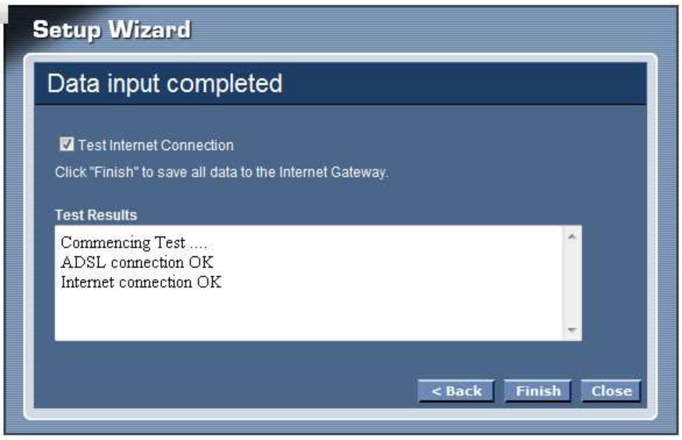
Setup Wizard

Data input completed

☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

Test Results



Setup Wizard

Data input completed

☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

Test Results

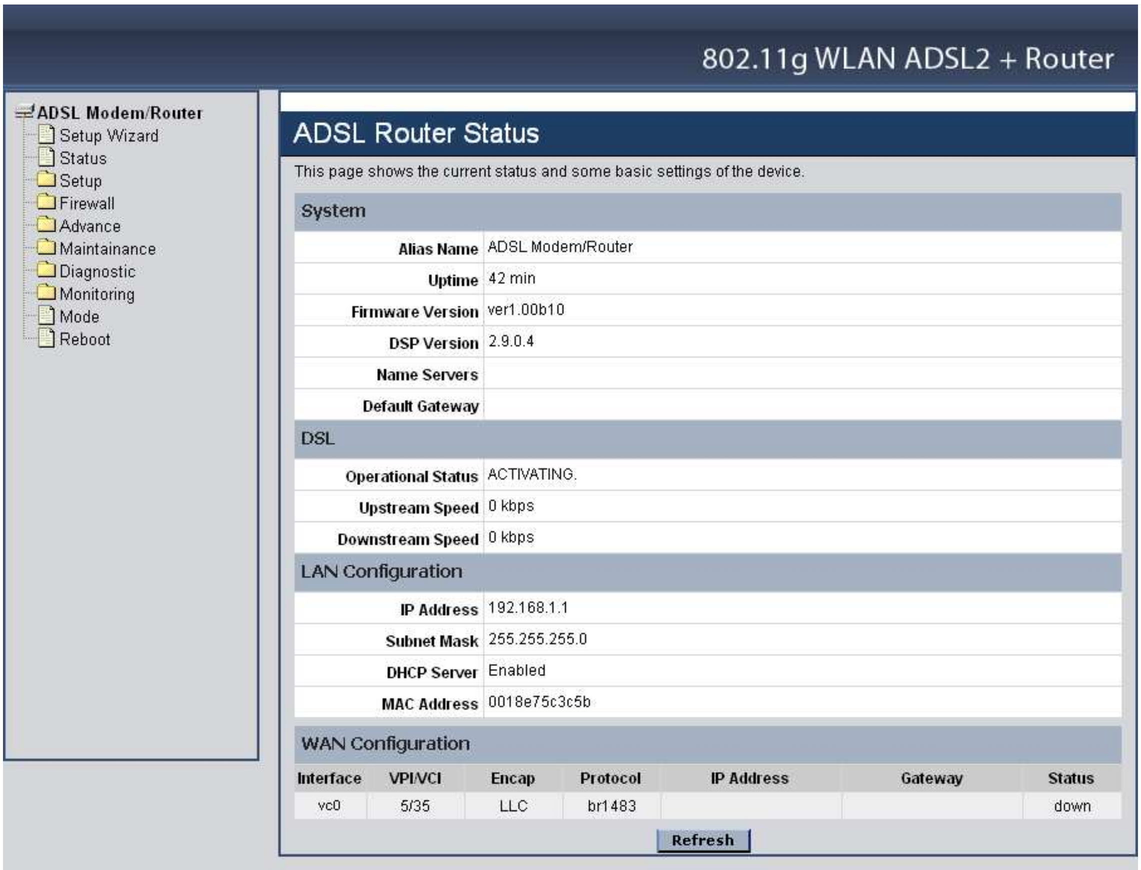
```
Commencing Test ....
ADSL connection OK
Internet connection OK
```

MANUAL SETINGS

Find that there are ten items, including Setup Wizard, Status, Setup, Firewall (form router mode only), Advance (form router mode only), Maintenance, Diagnostic, Monitoring, Mode and Reboot in Setup menu.

Status

This page displays the WLAN ADSL Router current status and settings. Click the “Refresh” button to update the status.



ADSL Router Status

This page shows the current status and some basic settings of the device.

System	
Alias Name	ADSL Modem/Router
Uptime	42 min
Firmware Version	ver1.00b10
DSP Version	2.9.0.4
Name Servers	
Default Gateway	
DSL	
Operational Status	ACTIVATING.
Upstream Speed	0 kbps
Downstream Speed	0 kbps
LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	0018e75c3c5b

WAN Configuration

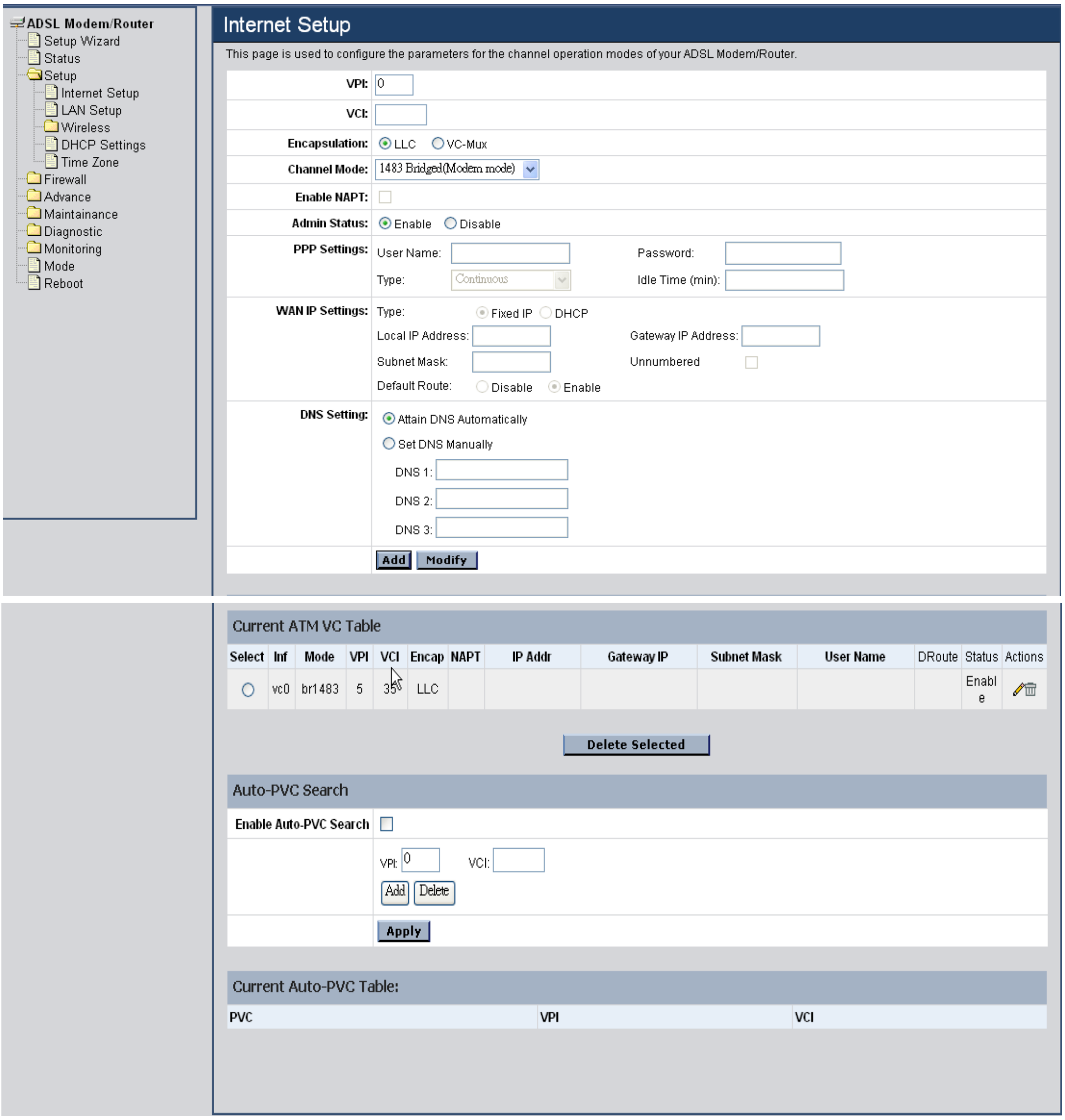
Interface	VPI/VCI	Encap	Protocol	IP Address	Gateway	Status
vc0	5/35	LLC	br1483			down

Setup

The section enables users to configure the Internet (ADSL), LAN, Wireless, DHCP and Time Zone setting.

Internet Setup

The WLAN ADSL Router comes with 8 ATM Permanent Virtual Channels (PVCs) at the most. There are mainly three operations for each of the PVC channels: add, delete and modify. And there are several channel modes to be selected for each PVC channel. For each of the channel modes, the setting is quite different accordingly.



Internet Setup

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router.

VPI:	0
VCI:	
Encapsulation:	● LLC ○ VC-Mux
Channel Mode:	1483 Bridged(Modem mode)
Enable NAPT:	□
Admin Status:	● Enable ○ Disable
PPP Settings:	User Name: Password: Type: Continuous Idle Time (min):
WAN IP Settings:	Type: ● Fixed IP ○ DHCP Local IP Address: Gateway IP Address: Subnet Mask: Unnumbered □ Default Route: ○ Disable ● Enable
DNS Setting:	● Attain DNS Automatically ○ Set DNS Manually DNS 1: DNS 2: DNS 3:
	Add Modify

Current ATM VC Table

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IP Addr	Gateway IP	Subnet Mask	User Name	DRoute	Status	Actions
○	vc0	br1483	5	35	LLC							Enable	

Delete Selected

Auto-PVC Search

Enable Auto-PVC Search	□
	VPI: 0 VCI: Add Delete
	Apply

Current Auto-PVC Table:

PVC	VPI	VCI

VPI: Virtual Path Identifier. Enter the VPI value provided by ISP.

VCI: Virtual Channel Identifier. Ethernet the VCI value provided by ISP.

Encapsulation: Select the encapsulation type LLC or VC-Mux produced by your ISP.

Channel Mode: Select the channel mode for 1483 Bridged, 1483 MER, PPPoE, PPPoA, 1483 Routed or 1577 Routed provide by ISP.

Enable NAPT: Checked to enable the NAPT function on the WLAN ADSL Router.

Admin Status: Enable or disable the ATM VC setting when adding to the ATM VC Table.

PPP Settings: When the channel mode selected by PPPoE or PPPoA.

User Name: Enter the user name provide by ISP.

Password: Enter the user name provide by ISP.

Type: Select the connection type for “Continuous”, “Connect on Daemon” or “Manual” connect.

Idle Time: Enter the idle time for Connect on Daemon, when no Internet access during the idle time, the ADSL connection will auto disconnect.

WAN IP Settings:

Type: Select whether user wants to specify an IP address manually, or want DHCP to obtain an IP address automatically. When Fixed IP is selected, type the Local IP Address, Gateway IP Address and Subnet Mask in the text boxes. User’s ISP will provide with this information.

Unnumbered: Checked to enable the IP unnumbered on the WLAN ADSL Router.

Default Route: Setting the default router function disable or enable.

WAN MAC: Enter the specified WAN MAC address provided by your ISP

DNS Setting:

Attain DNS Automatically: Select this item if you want to use the DNS servers obtained by the WAN interface via the auto-configuration mechanism.

Set DNS Manually: Select this item to configure up to three DNS IP addresses.

DNS 1~3: Ethernet the IP address of the DNS server.

Add Button: Click add button to add the new VC setting to the ATM VC Table.

Modify Button: Selected on of VC setting from the Current ATM VC Table then click the Modify button to save the modified VC setting.

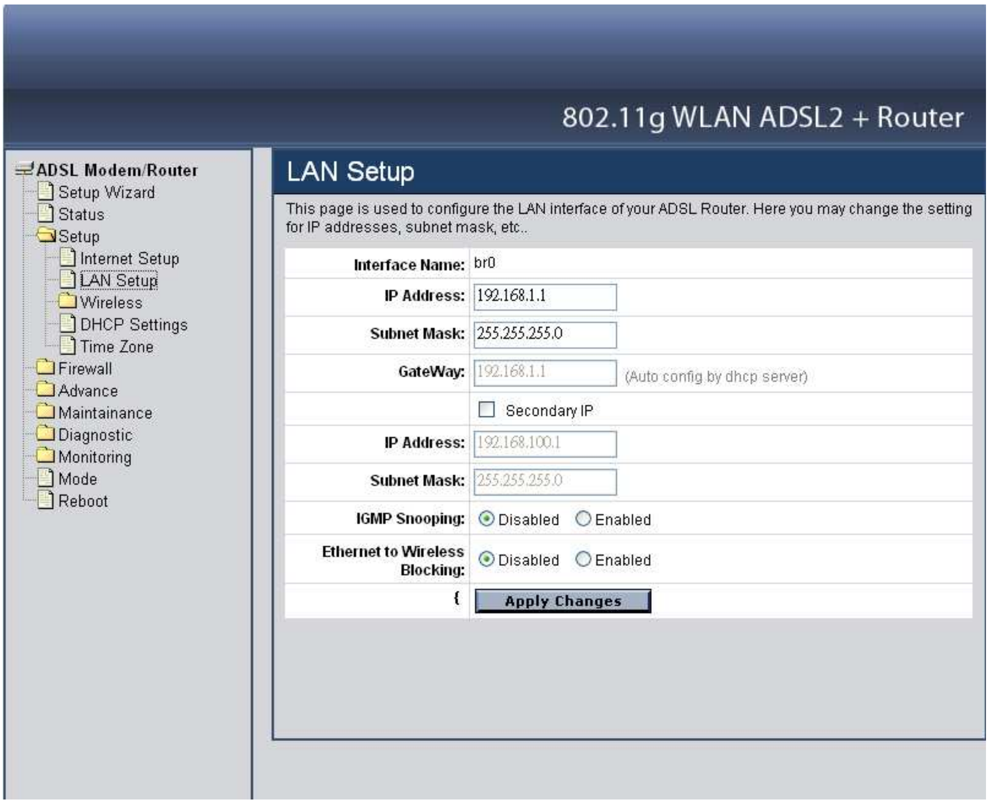
Current ATM VC Table: Shows all of the ATM VC settings in the table.

Auto-PVC Search: Enable the Auto-PVC Search or add new PVC setting manually.

Current Auto-PVC Table: Shows all of the Auto-PVC settings in the table.

LAN Setup

This screen enables users to set up the WLAN ADSL Router WAN connection, specify the IP address for the WAN, add DNS numbers, and enter the MAC address.



LAN Setup

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresses, subnet mask, etc..

Interface Name:	br0
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
GateWay:	192.168.1.1 (Auto config by dhcp server)
	□ Secondary IP
IP Address:	192.168.100.1
Subnet Mask:	255.255.255.0
IGMP Snooping:	● Disabled ○ Enabled
Ethernet to Wireless Blocking:	● Disabled ○ Enabled
{	Apply Changes

IP Address: This is the IP address of the router. The default IP address is 192.168.1.1.

Subnet Mask: Type the subnet mask for the router in the text box. The default subnet mask is 255.255.255.0.

Secondary IP: Checked to enable the secondary IP address setting on the LAN.

IP Address: The secondary IP address setting of the LAN.

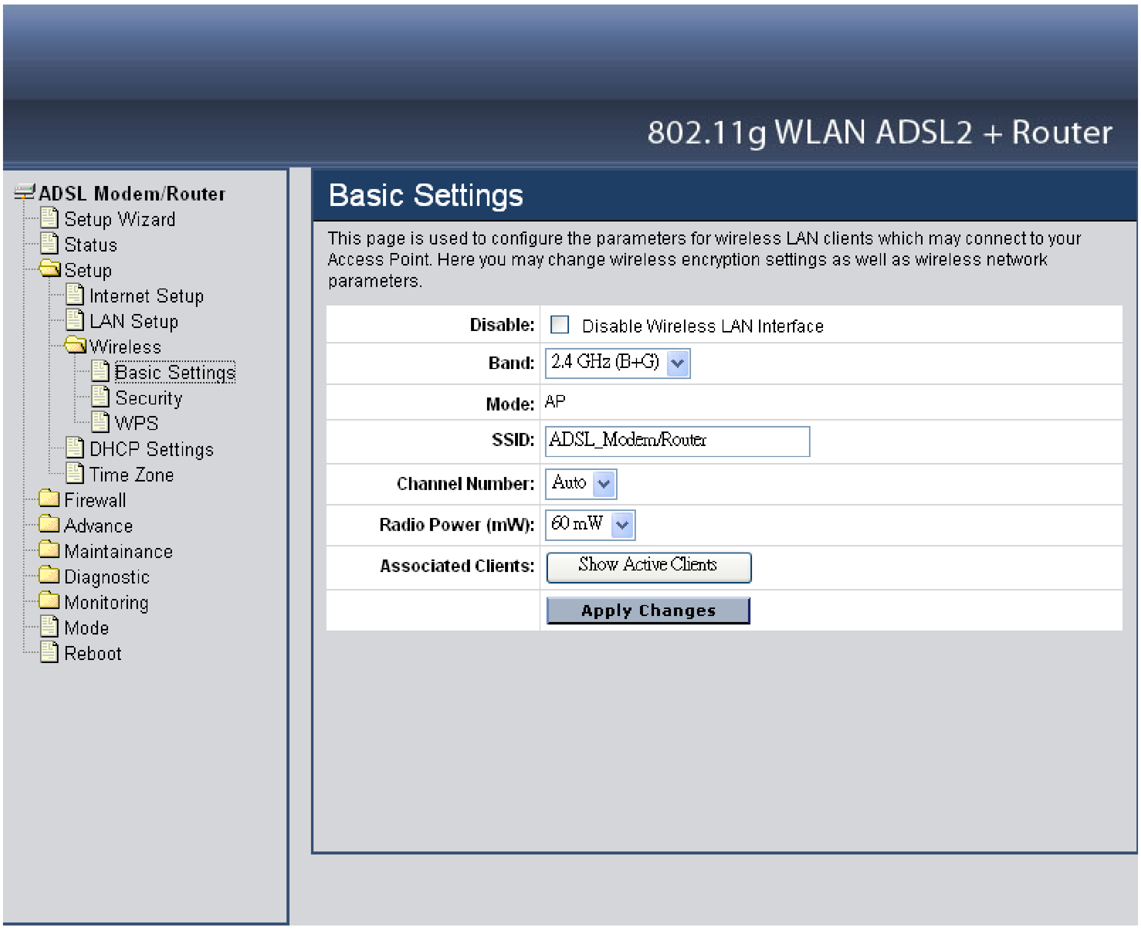
Subnet Mask: The secondary Subnet Mask setting of the LAN.

IGMP Snooping: Enable/disable the IGMP snooping function for the multiple bridged LAN ports.

Ethernet to Wireless Blocking: When enabled the Ethernet to Wireless Blocking, all of Ethernet users can’t communicate with WLAN users.

Wireless

This section enables users to configuration the wireless communications parameters for the WLAN ADSL Router.



Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable:	□ Disable Wireless LAN Interface
Band:	2.4 GHz (B+G)
Mode:	AP
SSID:	ADSL_Modem/Router
Channel Number:	Auto
Radio Power (mW):	60 mW
Associated Clients:	Show Active Clients

Basic Settings

This page allow user to enable and disable the wireless LAN function, create a SSID, and select the channel for wireless communications.

Disable: Checked to disable the wireless function of the WLAN ADSL Router.

Band: Select one of the following:

- **2.4Ghz (B+G)** - Selected if you are allowing both 802.11b and 802.11g wireless clients connect to the WLAN ADSL Router at the same time.
- **2.4Ghz (B)** - Selected if you are allowing the 802.11b wireless clients connect to the WLAN ADSL Router only.
- **2.4Ghz (G)** - Selected if you are allowing the 802.11g wireless clients connect to the WLAN ADSL Router only.

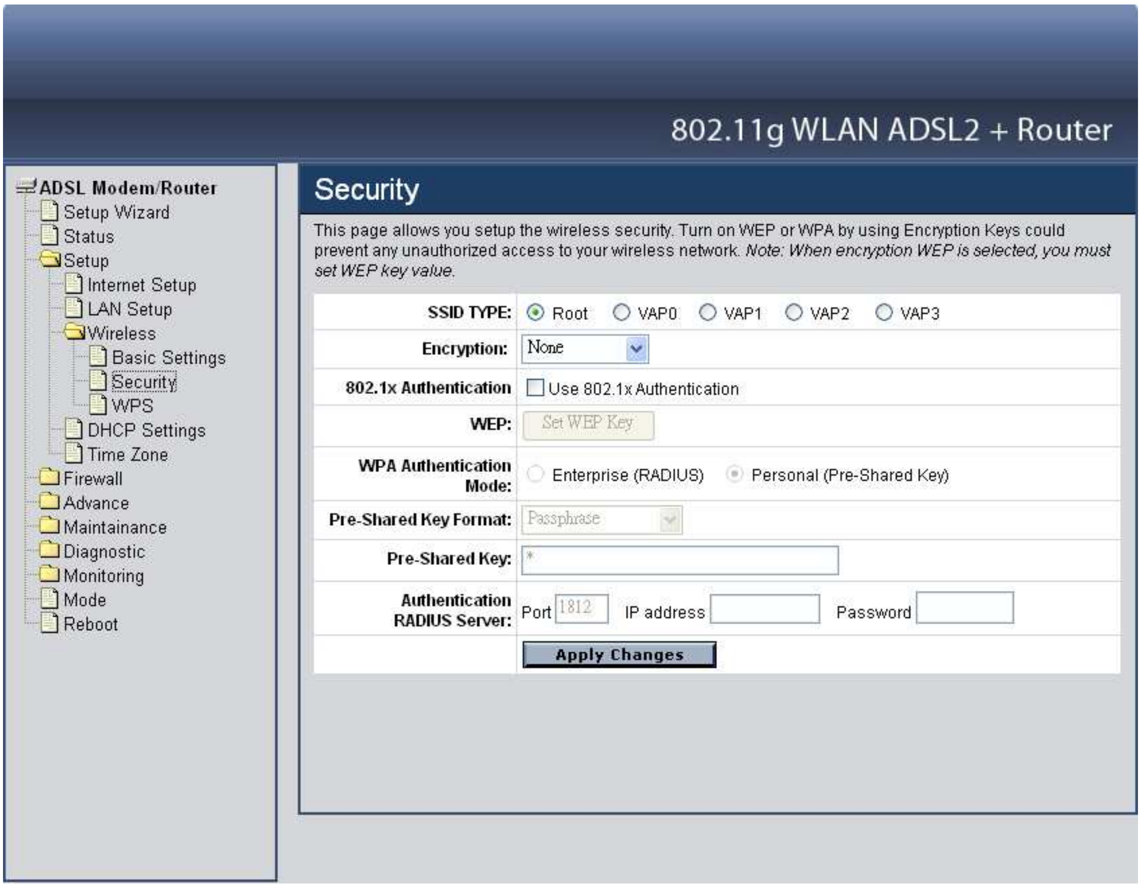
SSID: Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the WLAN ADSL Router.

Channel: Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the WLAN ADSL Router.

Radio Power (mW): The maximum output power for wireless LAN: 15mW, 30mW or 60mW.

Associated Clients: Click the “Show Active Client” button displays the information of connected wireless clients.

Security



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network. *Note: When encryption WEP is selected, you must set WEP key value.*

SSID TYPE:	● Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3
Encryption:	None
802.1x Authentication	□ Use 802.1x Authentication
WEP:	Set WEP Key
WPA Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	*
Authentication RADIUS Server:	Port 1812 IP address Password
	Apply Changes

SSID TYPE: The WLAN ADSL Router supports up to four multiple SSID feature (Multiple Virtual AP), select which AP (Root AP, VAP0~VAP3) will configure the security setting.

Encryption: There are 4 types of security to be selected. To secure your WLAN, it’s strongly recommended to enable this feature.

WEP: Make sure that all wireless devices on your network are using the same encryption level and key. Click Set WEP Key button to set the encryption key.

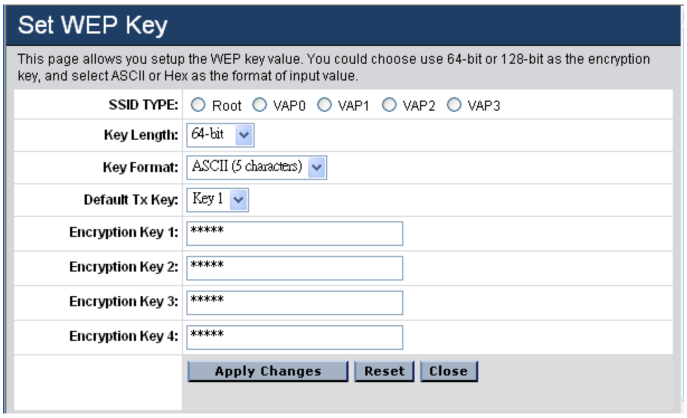
WPA (TKIP): WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilized a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

WPA2 (AES): WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilized a symmetric 128-bit block data encryption.

WAP2 Mixed: The AP supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.

802.1x Authentication: Checked to enable the 802.1x authentication. This option is selectable only when the “Encryption” is selected to either None or WEP. If the “Encryption” is WEP, you need to further select the WEP key length to be either WEP 64bits or WEP 128bits.

WEP: Click the “Set WEP Key” button to setting WEP key when the “Encryption” is selected to “WEP”.



Set WEP Key

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

SSID TYPE:	○ Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3
Key Length:	64-bit
Key Format:	ASCII (5 characters)
Default Tx Key:	Key 1
Encryption Key 1:	*****
Encryption Key 2:	*****
Encryption Key 3:	*****
Encryption Key 4:	*****

SSID TYPE: The WLAN ADSL Router supports up to four multiple SSID feature (Multiple Virtual AP), select which AP (Root AP, VAP0~VAP3) will setting the WEP key.

Key Length: Select the level of encryption from the drop-down list 64 and 128-bit encryption.

Key Format: Select the key format from the drop-down list HEX or ASCII.

Default TX Key: Select which encryption key 1~4 will be use to default TX key.

Encryption Key 1 ~ 4: Enables users to create up to 4 different WEP keys, manually enter a set of values for each key.

WPA Authentication Mode: There are 2 types of authentication mode for WPA.

Enterprise (RADIUS): WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Please refer to “Authentication RADIUS Server” setting below for RADIUS setting.

Personal (Pre-Shared Key): Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the “Pre-Shared Key Format” and “Pre-Shared Key” setting respectively. Please refer to “Pre-Shared Key Format” and “Pre-Shared Key” setting below.

Pre-Shared Key Format:

Passphrase: Select this to enter the Pre-Shared Key secret as user-friendly textual secret.

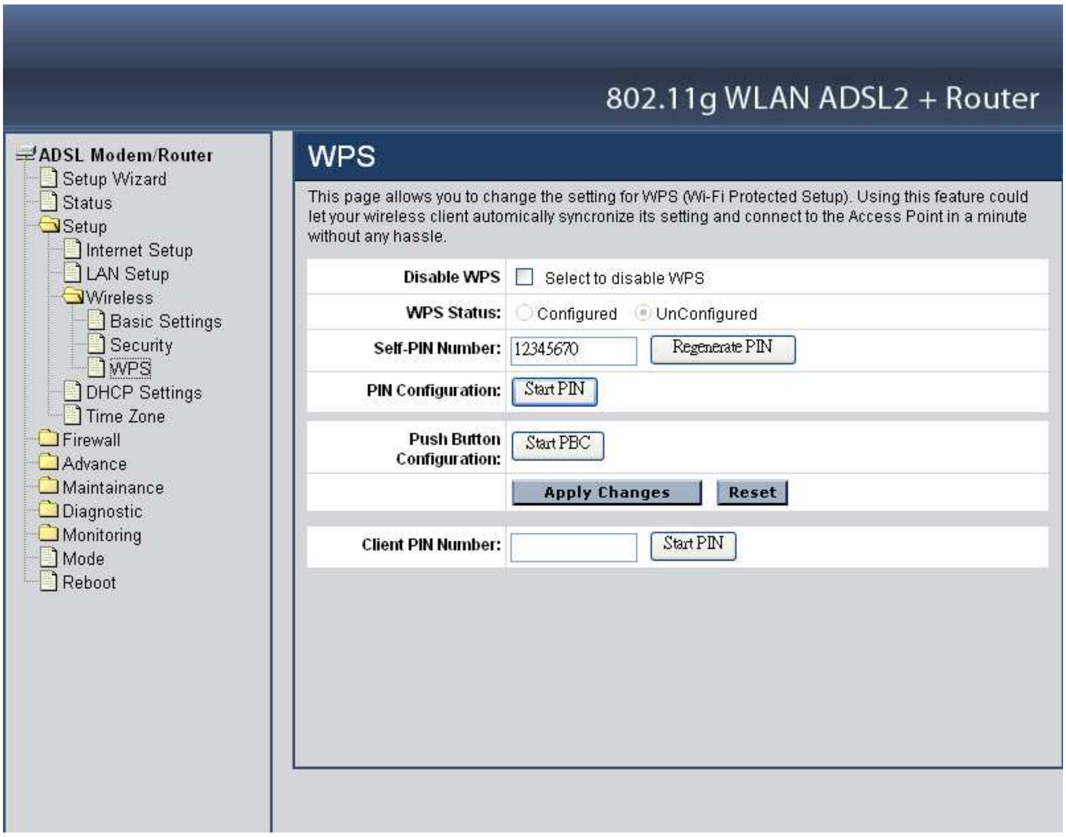
Hex (64 characters): Select this to enter the Pre-Shared Key secret as hexadecimal secret.

Pre-Shared Key: Specify the shared secret used by this Pre-Shared Key. If the “Pre-Shared Key Format” is specified as Passphrase, then it indicates a passphrase of 8 to 63 bytes long; or if the “Pre-Shared Key Format” is specified as Passphrase, then it indicates a 64-hexadecimal number.

Authentication RADIUS Server: If the WPA-RADIUS is selected at “WPA Authentication Mode”, the port (default is 1812), IP address and password of external RADIUS server are specified here.

WPS

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, The Wi-Fi Protected Setup (WPS) is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management. The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network. This device supports Push Button method and PIN method for WPS. The following sub-paragraphs will describe the function of each item. The webpage is as below. Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, The Wi-Fi Protected Setup (WPS) is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management. The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network. This device supports Push Button method and PIN method for WPS. The following sub-paragraphs will describe the function of each item. The webpage is as below.



WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

Disable WPS	☐ Select to disable WPS
WPS Status:	○ Configured ● UnConfigured
Self-PIN Number:	12345670 Regenerate PIN
PIN Configuration:	Start PIN
Push Button Configuration:	Start PBC
	Apply Changes Reset
Client PIN Number:	Start PIN

Disable WPS: Checked to disable the Wi-Fi protected Setup.

WPS Status: When the WLAN ADSL Router settings are factory default (out of box), it is set to open security and un-configured state. “WPS Status” will display it as “UnConfigured”. If it already shows “Configured”, some registrars such as Vista WCN will not configure AP. Users will need to go to the “Backup/Restore” page and click “Reset” to reload factory default settings.

Self-PIN Number: The “Self-PIN Number” is AP’s PIN. Whenever users want to change AP’s PIN, they could click “Regenerate PIN” and then click “Apply Changes”. Moreover, if users want to make their own PIN, they could enter four-digit PIN without checksum and then click “Apply Changes”. However, this would not be recommended since the registrar side needs to be supported with four-digit PIN.

PIN Configuration: Click the “Start PIN” button to start the PIN method of WPS.

Push Button Configuration: Click the “Start PBC” button to start the push btton method of WPS.

Client PIN Number: It is only used when users want their station to join AP’s network. The length of PIN is limited to four or eight numeric digits. If users enter eight-digit PIN with checksum error, there will be a warning message popping up. If users insist on this PIN, AP will take it.

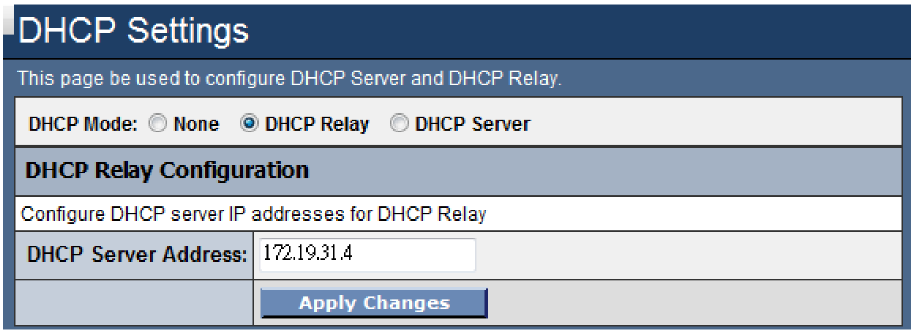
DHCP Settings

You can configure your WLAN ADSL Router to use the Dynamic Host Configuration Protocol (DHCP). This section provides DHCP instructions for implementing it on your network by selecting the role of DHCP protocol that this device wants to play.

DHCP Mode: There are two different DHCP roles that this device can act as: DHCP Server and DHCP Relay. When acting as DHCP server, you can setup the server parameters at the below DHCP Server setting; while acting as DHCP Relay, you can setup the relay at the below DHCP Relay setting. Otherwise, selected the None to disable the DHCP service.

DHCP Relay

Some ISPs perform the DHCP server function for their customers' home/small office network. In this case, you can configure this device to act as a DHCP relay agent. When a host on your network requests Internet access, the device contacts your ISP to obtain the IP configuration, and then forward that information to the host. You should set the DHCP mode after you configure the DHCP relay.


DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

DHCP Mode: ○ None ● DHCP Relay ○ DHCP Server

DHCP Relay Configuration

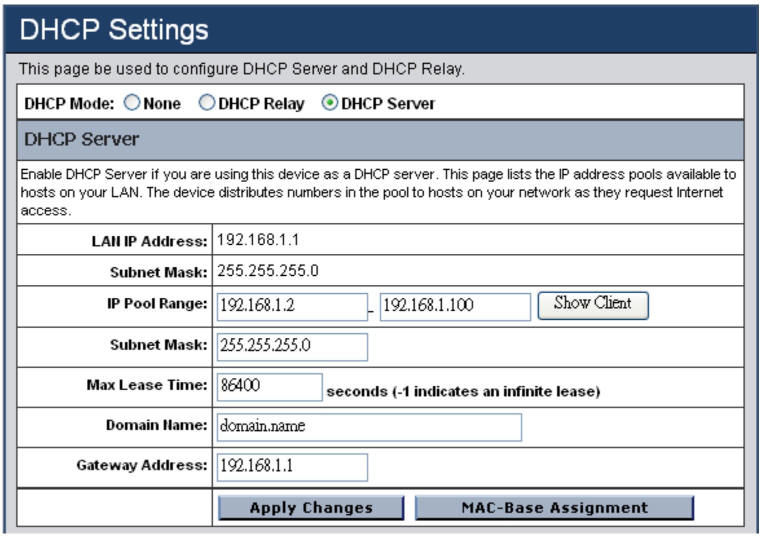
Configure DHCP server IP addresses for DHCP Relay

DHCP Server Address: 172.19.31.4

DHCP Server Address: Specify the IP address of your ISP's DHCP server. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

DHCP Server

By default, the device is configured as a DHCP server, with a predefined IP address pool of 192.168.10.2 through 192.168.10.100 (subnet mask 255.255.255.0).



DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

DHCP Mode: ○ None ○ DHCP Relay ● DHCP Server

DHCP Server

Enable DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IP Pool Range:	192.168.1.2 - 192.168.1.100 Show Client
Subnet Mask:	255.255.255.0
Max Lease Time:	86400 seconds (-1 indicates an infinite lease)
Domain Name:	domain.name
Gateway Address:	192.168.1.1

IP Pool Range: Specify the lowest and highest addresses in the pool.

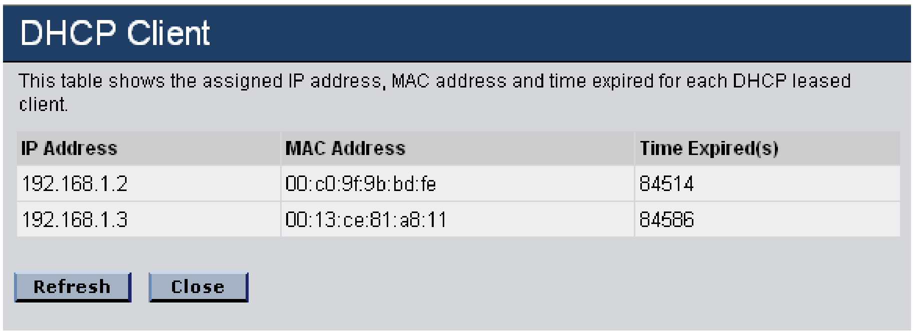
Subnet Mask: Specify the subnet mask value.

Max Lease Time: The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 86400 seconds (1 day). The value –1 stands for the infinite lease.

Domain Name: A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.

Gateway Address: Specify the gateway IP address.

Show Client: When click the “Show Client” button, all dynamic DHCP client computers are listed in the new window and providing the IP address, MAC address and Time Expired of the client.

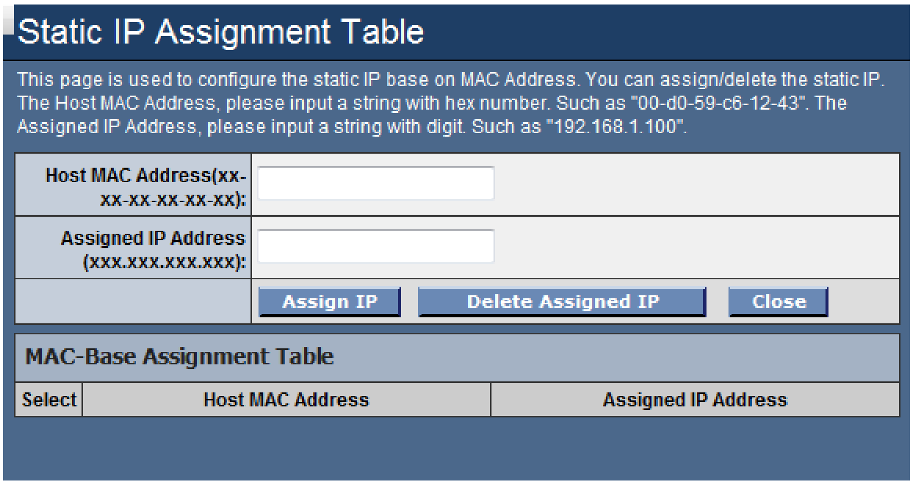


DHCP Client

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
192.168.1.2	00:c0:9f:9b:bd:fe	84514
192.168.1.3	00:13:ce:81:a8:11	84586

MAC-Base Assignment: Click the “MAC-Base Assignment” button to configure the static IP base on MAC Address. You can assign/delete the static IP. The Host MAC Address, please input a string with hex number. Such as "00-d0-59-c6-12-43". The Assigned IP Address, please input a string with digit. Such as "192.168.10.100". Click “Assign IP” button to add the static DHCP setting to the MAC-Base Assignment Table.



Static IP Assignment Table

This page is used to configure the static IP base on MAC Address. You can assign/delete the static IP. The Host MAC Address, please input a string with hex number. Such as "00-d0-59-c6-12-43". The Assigned IP Address, please input a string with digit. Such as "192.168.1.100".

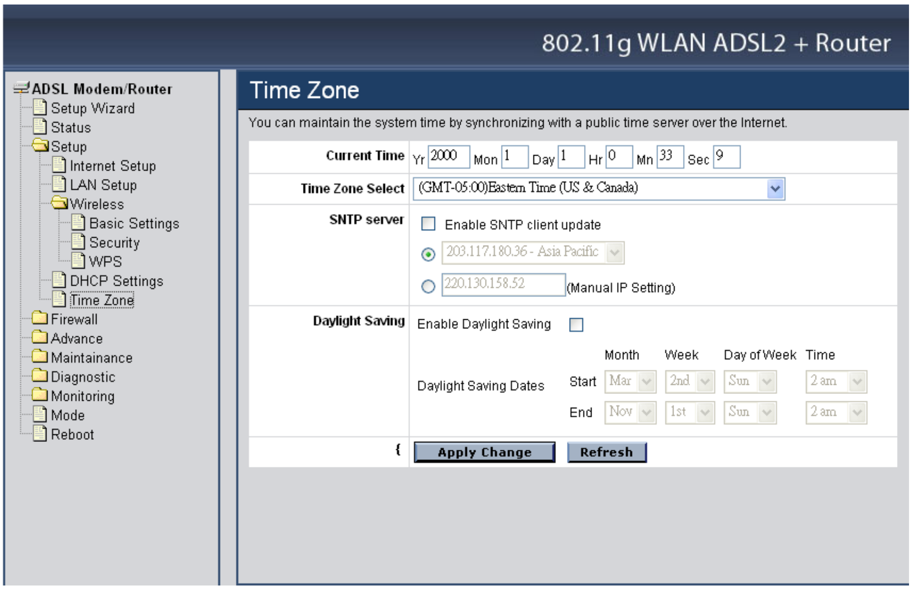
Host MAC Address(xx-xx-xx-xx-xx-xx):	
Assigned IP Address (xxx.xxx.xxx.xxx):	

MAC-Base Assignment Table

Select	Host MAC Address	Assigned IP Address

Time Zone

Simple Network Timing Protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. The WLAN ADSL Router supports SNTP client functionality in compliance with IETF RFC2030. SNTP client functioning in daemon mode which issues sending client requests to the configured SNTP server addresses periodically can configure the system clock in the WLAN ADSL Router.



Time Zone

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time: Yr 2000 Mon 1 Day 1 Hr 0 Mn 33 Sec 9

Time Zone Select: (GMT-05:00)Eastern Time (US & Canada)

SNTP server: □ Enable SNTP client update
● 203.117.180.36 - Asia Pacific
○ 220.130.158.52 (Manual IP Setting)

Daylight Saving: Enable Daylight Saving □

Daylight Saving Dates

	Month	Week	Day of Week	Time
Start	Mar	2nd	Sun	2 am
End	Nov	1st	Sun	2 am

Current Time: The current time of the specified time zone. You can set the current time by yourself or configured by SNTP.

Time Zone Select: The time zone in which the WLAN ADSL Router resides.

Enable SNTP client update: Enable the SNTP client to update the system clock.

SNTP server: The IP address or the host name of the SNTP server. You can select from the list or set it manually.

Daylight Saving: Checked to enable daylight saving time. When enabled, select the start and end date for daylight saving time.

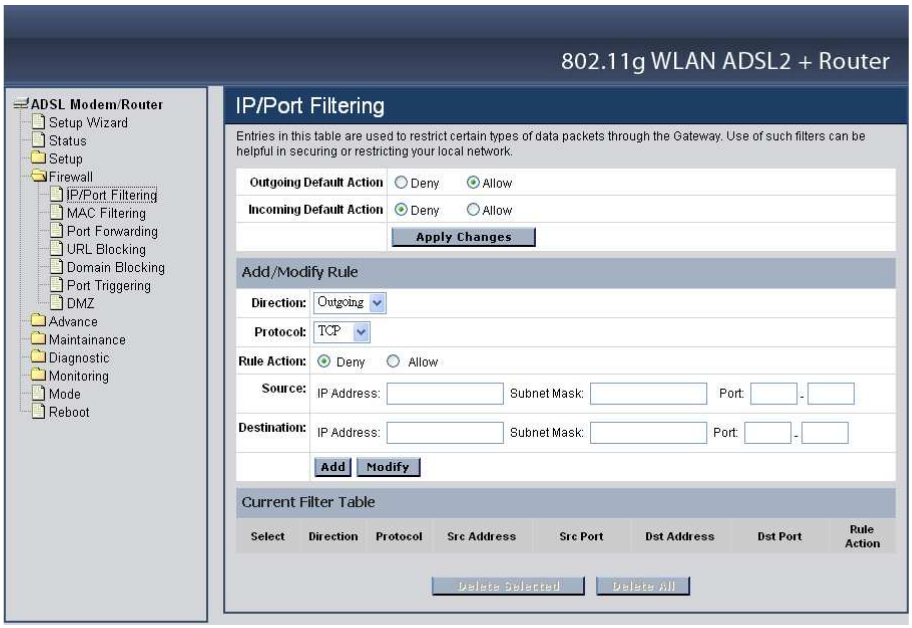
Firewall – Used only on Router mode settings

The Firewall setting is for the WLAN ADSL Router is configured on Router mode only. Please refer the **Mode** setting in page 79.

Firewall contains several features that are used to deny or allow traffic from passing through the device.

IP/Port Filtering

The IP/Port filtering feature allows you to deny/allow specific services or applications in the forwarding path.



Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Action ○ Deny ● Allow

Incoming Default Action ● Deny ○ Allow

Direction: Outgoing

Protocol: TCP

Rule Action: ● Deny ○ Allow

Source: IP Address: Subnet Mask: Port: -

Destination: IP Address: Subnet Mask: Port: -

Select	Direction	Protocol	Src Address	Src Port	Dst Address	Dst Port	Rule Action

Outgoing Default Action: Specify the default action on the LAN to WAN forwarding path.

Incoming Default Action: Specify the default action on the WAN to LAN forwarding path.

Add/Modify Rule

Add or modify the IP/Port filtering rule.

Direction: Select the traffic forwarding direction “Outgoing” or “Incoming”.

Protocol: Select the protocol type for TCP, UDP or ICMP.

Rule Action: Deny or allow traffic when matching this rule.

Source: The source IP address, Subnet Mask and Port range assigned to the traffic on which filtering is applied.

Destination: The destination IP address, Subnet Mask and Port range assigned to the traffic on which filtering is applied.

Add: Click the “Add” button to save the rule entry to the configuration.

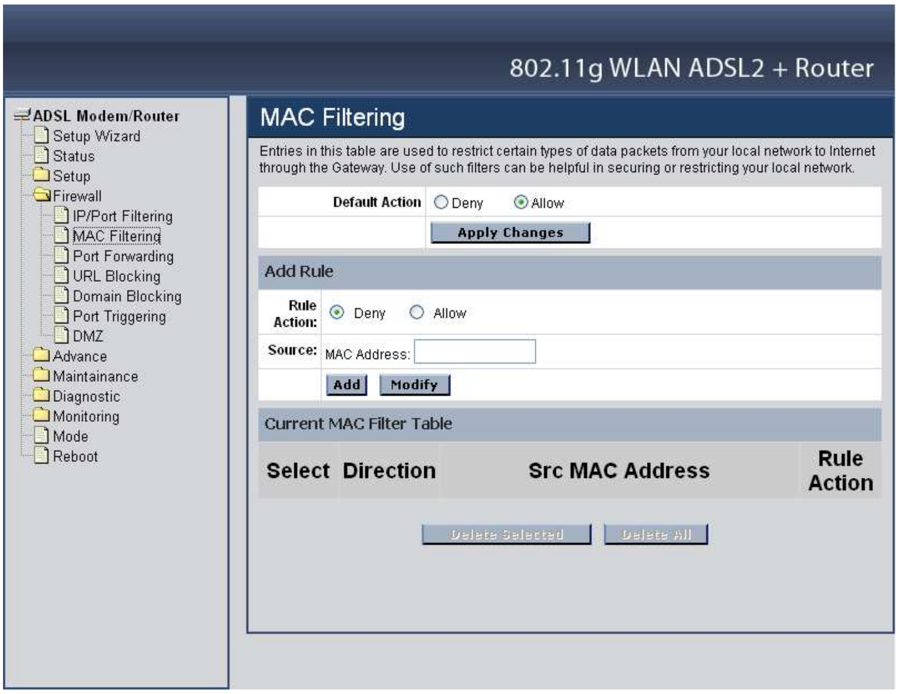
Modify: Click the “Modify” button to modify the selected rule form the Current Filter Table.

Delete Selected: Click the “Delete Selected” button to delete the selected rule from Current Filter Table.

Delete All: Click the “Delete All” button to delete the all of rule in the Current Filter Table.

MAC Filtering

The MAC filtering feature allows you to define rules to allow or deny frames through the device based on source MAC address, and traffic direction.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Default Action ○ Deny ● Allow

Add Rule

Rule Action: ● Deny ○ Allow

Source: MAC Address:

Current MAC Filter Table

Select	Direction	Src MAC Address	Rule Action

Default Action: Specify the default action on the LAN to WAN forwarding path.

Add/Modify Rule

Add or modify the MAC filtering rule.

Rule Action: Deny or allow traffic when matching this rule.

Source: The source MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don’t care.

Add: Click the “Add” button to save the rule entry to the configuration.

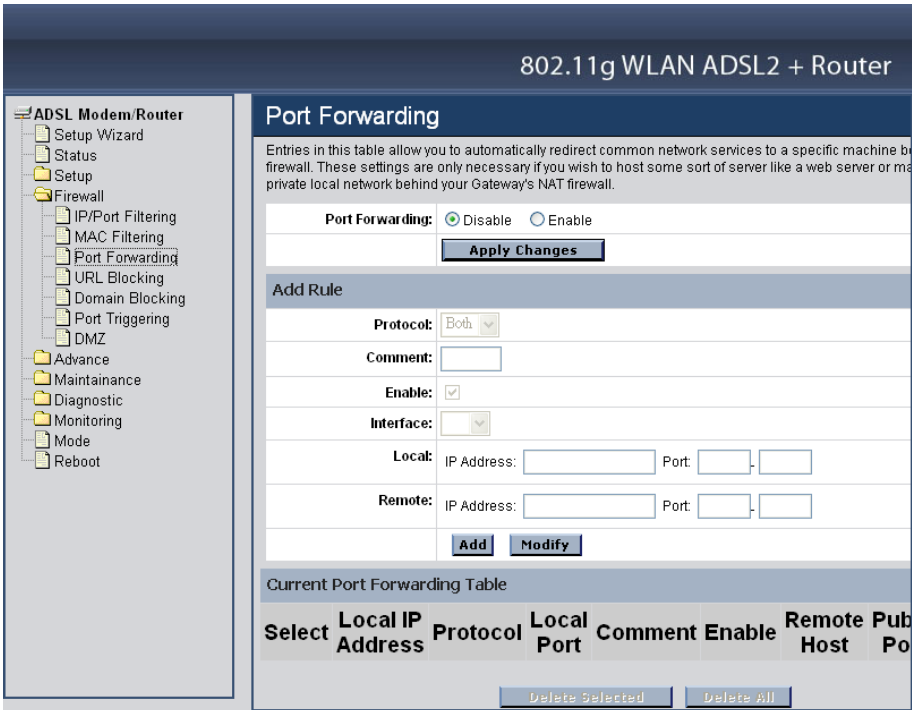
Modify: Click the “Modify” button to modify the selected rule form the Current MAC Filter Table.

Delete Selected: Click the “Delete Selected” button to delete the selected rule from Current MAC Filter Table.

Delete All: Click the “Delete All” button to delete the all of rule in the Current MAC Filter Table.

Port Forwarding

Firewall keeps unwanted traffic from the Internet away from your LAN computers. Add a Port Forwarding entry will create a tunnel through your firewall so that the computers on the Internet can communicate to one of the computers on your LAN on a single port.



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine b
firewall. These settings are only necessary if you wish to host some sort of server like a web server or ma
private local network behind your Gateway's NAT firewall.

Port Forwarding: ● Disable ○ Enable

Add Rule

Protocol:	Both
Comment:	
Enable:	☑
Interface:	
Local:	IP Address: Port: -
Remote:	IP Address: Port: -

Current Port Forwarding Table

Select	Local IP Address	Protocol	Local Port	Comment	Enable	Remote Host	Pub Po

Port Forwarding: Select to enable or disable the port forwarding feature.

Add/Modify Rule

Add or modify the Port Forwarding rule.

Protocol: Select the protocol type for TCP, UDP or Both (TCP and UTP).

Enable: Check to enable this rule.

Interface: Select the WAN interface on which the port-forwarding rule is to be applied.

Local: The local IP address and Port range assigned to the traffic on which filtering is applied.

Destination: The remote IP address and Port range assigned to the traffic on which filtering is applied.

Add: Click the “Add” button to save the rule entry to the configuration.

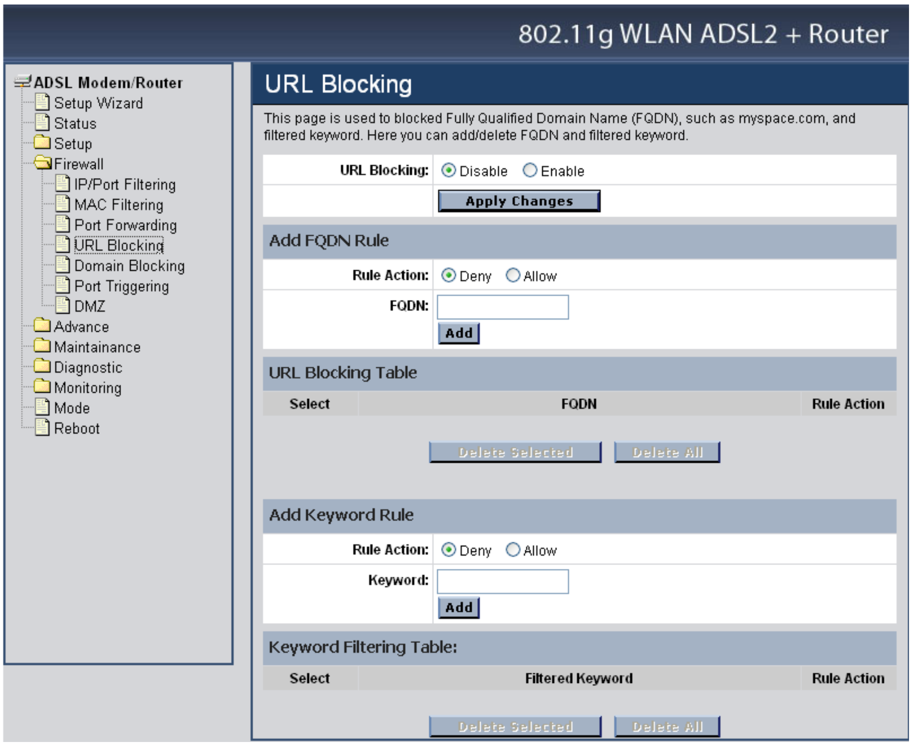
Modify: Click the “Modify” button to modify the selected rule form the Current Port Forwarding Table.

Delete Selected: Click the “Delete Selected” button to delete the selected rule from Current Port Forwarding Table.

Delete All: Click the “Delete All” button to delete the all of rule in the Current Port Forwarding Table.

URL Blocking

The URL Blocking is the web filtering solution. The firewall includes the ability to block access to specific web URLs based on string matches. This can allow large numbers of URLs to be blocked by specifying only a FQDN (such as tw.yahoo.com). The URL Blocking enforce a Web usage policy to control content downloaded from, and uploaded to, the Web.



URL Blocking

This page is used to blocked Fully Qualified Domain Name (FQDN), such as myspace.com, and filtered keyword. Here you can add/delete FQDN and filtered keyword.

URL Blocking: ● Disable ○ Enable

Apply Changes

Add FQDN Rule

Rule Action: ● Deny ○ Allow

FQDN:

Add

URL Blocking Table

Select	FQDN	Rule Action

Delete Selected Delete All

Add Keyword Rule

Rule Action: ● Deny ○ Allow

Keyword:

Add

Keyword Filtering Table:

Select	Filtered Keyword	Rule Action

Delete Selected Delete All

URL Blocking: Select to enable or disable the URL blocking feature.

Add FQDN Rule

Rule Action: Deny or allow traffic when matching this rule.

FQDN: A fully qualified domain name (or FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely, such as tw.yahoo.com. The FQDN will be blocked to access.

Add: Click the “Add” button to save the rule entry to the configuration.

Delete Selected: Click the “Delete Selected” button to delete the selected rule from URL Blocking Table.

Delete All: Click the “Delete All” button to delete the all of rule in the URL Blocking Table.

Add Keyword Rule

Rule Action: Deny or allow traffic when matching this rule.

Keyword: The filtered keyword such as yahoo. If the URL includes this keyword, the URL will be blocked to access.

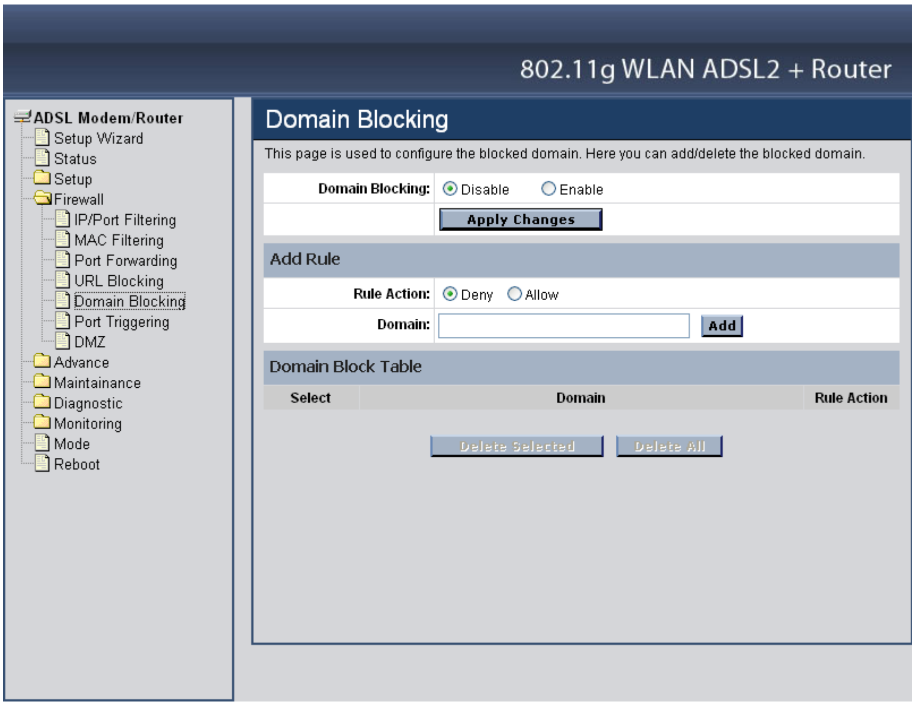
Add: Click the “Add” button to save the rule entry to the configuration.

Delete Selected: Click the “Delete Selected” button to delete the selected rule from Keyword Filtering Table.

Delete All: Click the “Delete All” button to delete the all of rule in the Keyword Filtering Table.

Domain Blocking

The firewall includes the ability to block access to specific domain based on string matches. For example, if the URL of Taiwan Yahoo web site is “tw.yahoo.com” and you enter “yahoo.com”, the firewall will block all the DNS queries with “yahoo.com” string. So the Host will be blocked to access all the URLs belong to “yahoo.com” domain. That means you can protect your computer, your house, your office and anything else that uses DNS from being able to service domains that you don’t want to load.



Domain Blocking

This page is used to configure the blocked domain. Here you can add/delete the blocked domain.

Domain Blocking: ● Disable ○ Enable

Apply Changes

Add Rule

Rule Action: ● Deny ○ Allow

Domain:

Add

Domain Block Table

Select	Domain	Rule Action

Delete Selected Delete All

Domain Blocking: Select to enable or disable the Domain blocking feature.

Add Rule

Rule Action: Deny or allow traffic when matching this rule.

Domain: Enter the blocked domain.

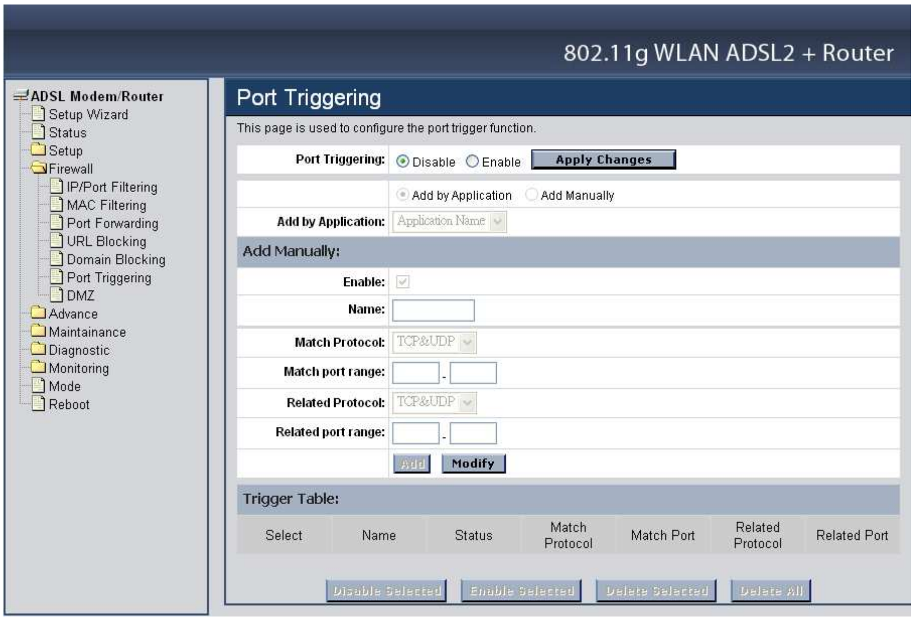
Add: Click the "Add" button to save the rule entry to the configuration.

Delete Selected: Click the "Delete Selected" button to delete the selected rule from Domain Block Table.

Delete All: Click the "Delete All" button to delete the all of rule in the Domain Blocking Table.

Port Triggering

The Port Triggering enables users to specify special applications, such as games which require multiple connections that are blocked by NAT.



Port Triggering

This page is used to configure the port trigger function.

Port Triggering: ● Disable ○ Enable

● Add by Application ○ Add Manually

Add by Application: Application Name

Add Manually:

Enable: ☑

Name:

Match Protocol: TCP&UDP

Match port range: -

Related Protocol: TCP&UDP

Related port range: -

Trigger Table:

Select	Name	Status	Match Protocol	Match Port	Related Protocol	Related Port

Port Triggering: Select to enable or disable the Port Triggering feature.

Add by Application

Add by Application: Select pre-define the application rule from list then click "Add" button to add the selected application rule.

Add by Manually

Enable: Check to enable this rule.

Name: Enter a descriptive name for the application rule.

Match Protocol: Select the outgoing protocol type for TCP, UDP or TCP&UTP.

Match port range: Enter the outgoing port range that can be used to access the application in the text boxes.

Related Protocol: Select the incoming protocol type for TCP, UDP or TCP&UTP.

Related port range: Enter the incoming port range that can be used to access the application in the text boxes.

Add: Click the “Add” button to save the rule entry to the configuration.

Modify: Click the “Modify” button to modify the selected rule form the Trigger Table.

Delete Selected: Click the “Delete Selected” button to delete the selected rule from Trigger Table.

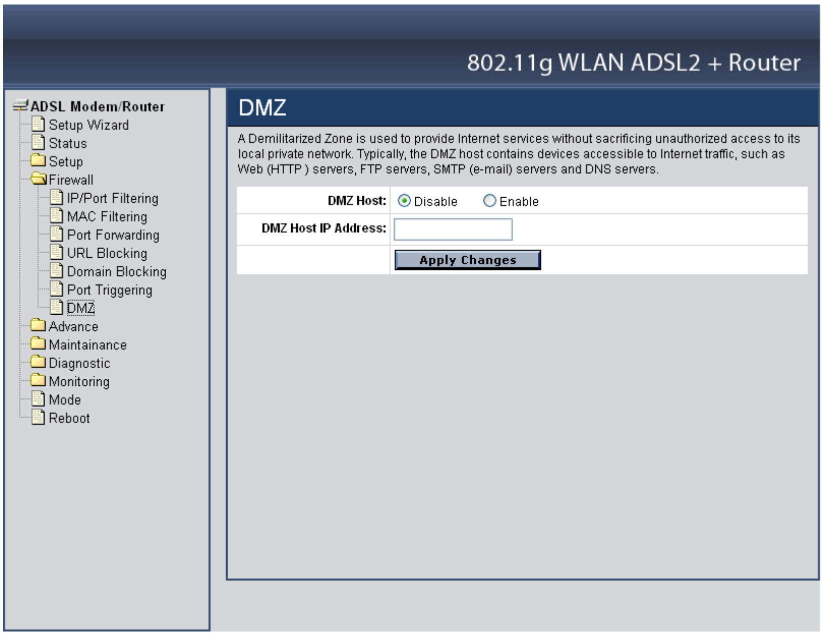
Delete All: Click the “Delete All” button to delete the all of rule in the Trigger Table.

Disable Selected: Click the “Disable Selected” button to disable the selected rule from Trigger Table.

Enable Selected: Click the “Enable Selected” button to Enable the selected rule from Trigger Table.

DMZ

A DMZ (Demilitarized Zone) allows a single computer on your LAN to expose ALL of its ports to the Internet. Enter the IP address of that computer as a DMZ (Demilitarized Zone) host with unrestricted Internet access. When doing this, the DMZ host is no longer behind the firewall.



DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ Host: ● Disable ○ Enable

DMZ Host IP Address:

DMZ Host: Select to enable or disable the DMZ feature.

DMZ Host IP Address: Enter a IP address of the local host. This feature sets a local host to be exposed to the Internet

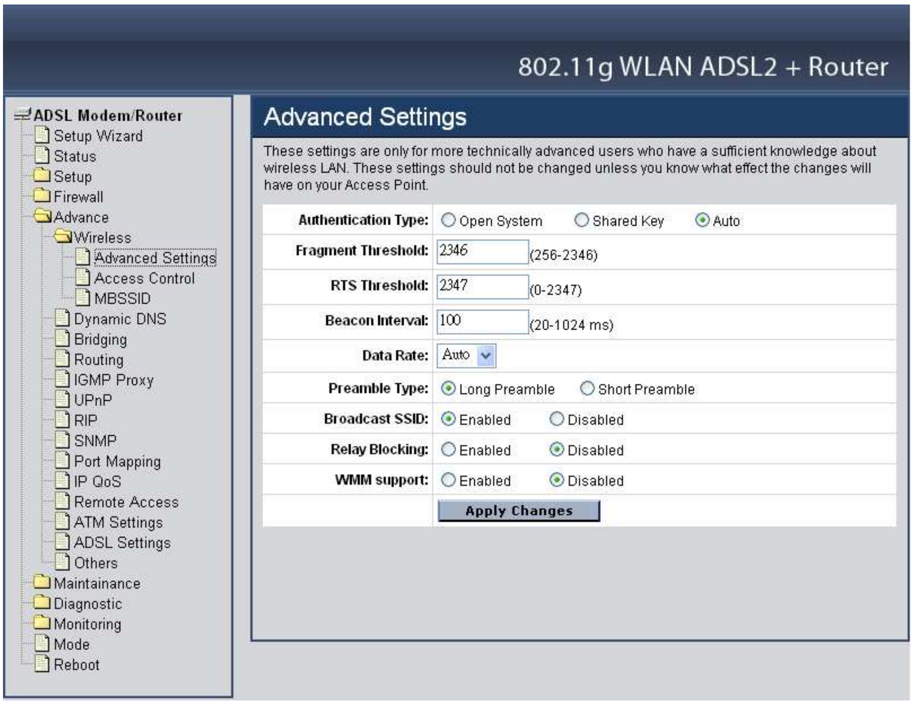
Advance – Used only on Router mode settings

The Advance setting is for the WLAN ADSL Router is configured on Router mode only. Please refer the **Mode** setting in page 79.

Wireless

Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your WLAN ADSL Router.



Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
Relay Blocking:	○ Enabled ● Disabled
WMM support:	○ Enabled ● Disabled
	Apply Changes

Authentication Type: Open System: Open System authentication is not required to be successful while a client may decline to authenticate with any particular other client. **Shared Key:** Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear. Requiring the use of the WEP privacy mechanism. **Auto:** Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill client’s requirement.

Fragment Threshold: This value should remain at its default setting of 2000. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increases the “Fragment Threshold” value within the value range of 256 to 2346. Setting this value too low may result in poor network performance. Only minor modifications of this value are recommended. The default is 2346.

RTS Threshold: This value should remain at its default setting of 2000. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset “RTS threshold” size, the RTS/CTS mechanism will not be enabled. The ADSL modem (or AP) sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The default is 2347.

Beacon Interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1024. A beacon is a packet broadcast by the ADSL modem (or AP) to synchronize the wireless network. The default is 100.

Data Rate: The rate of data transmission should be set depending on the speed of your wireless network. You should select from a range of transmission speeds, or you can select Auto to have the WLAN ADSL Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client. The default setting is Auto.

Preamble Type: The Preamble Type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the AP and mobile wireless stations. Make sure to select the appropriate preamble type. Note that high network traffic areas should use the short preamble type. CRC is a common technique for detecting data transmission errors.

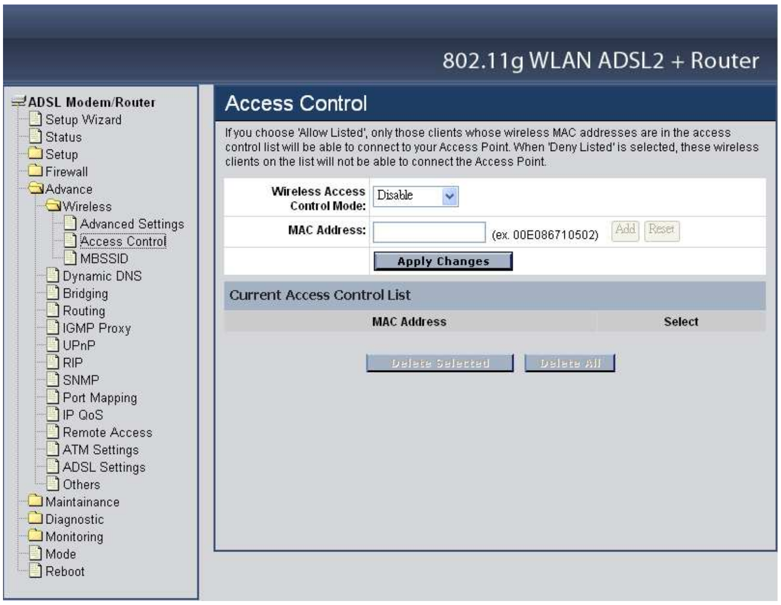
Broadcast SSID: Select to enable or disable the Broadcast SSID feature. If this option is enabled, the device will automatically transmit their network name (SSID) into open air at regular interval. This feature is intended to allow clients to dynamically discover and roam between WLANs; if this option is disabled, the device will hide its SSID. When this is done, the station cannot directly discover its WLAN and MUST be configure with the SSID. Note that in a home Wi-Fi network, roaming is largely unnecessary and the SSID broadcast feature serves no useful purpose. You should disable this feature to improve the security of your WLAN.

Relay Blocking: Select to enable or disable the Relay Blocking feature. When Relay Blocking is enabled, wireless clients will not be able to directly access other wireless clients.

WMM support: Select to enable or disable the WMM (Wi-FI Multimedia) QoS feature.

Access Control

This feature allows administrator to have access control by enter MAC address of client stations. When Enable this function, MAC address can be added into access control list and only those clients whose wireless MAC address are in the access control list will be able to connect to your WLAN ADSL Router.



Access Control

If you choose 'Allow Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

MAC Address: (ex. 00E086710502) Add Reset

Current Access Control List

MAC Address	Select

Wireless Access Control Mode:

Disable: Disable the wireless ACL feature;

Allow Listed: When this option is selected, no wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device);

Deny Listed: When this option is selected, all wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device).

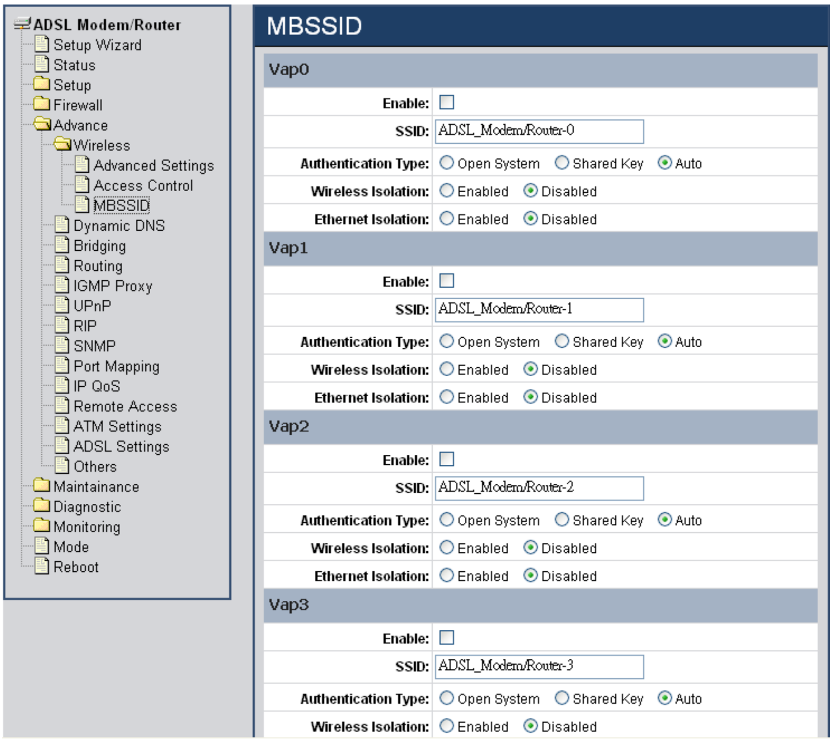
MAC Address: Enter client MAC address and click “Add” button to add client MAC address into current access control list.

Delete Selected: Click the “Delete Selected” button to delete the selected rule from Current Access Control List.

Delete All: Click the “Delete All” button to delete the all of rule in the Current Access Control List.

MBSSID

The WLAN ADSL Router supports up to four virtual AP (Vap0~Vap3) setting allows wireless users connect up to the WLAN ADSL Router through up to four different WLAN SSID and security settings.



MBSSID

Vap0

Enable: □
SSID: ADSL_Modem/Router-0
Authentication Type: ○ Open System ○ Shared Key ● Auto
Wireless Isolation: ○ Enabled ● Disabled
Ethernet Isolation: ○ Enabled ● Disabled

Vap1

Enable: □
SSID: ADSL_Modem/Router-1
Authentication Type: ○ Open System ○ Shared Key ● Auto
Wireless Isolation: ○ Enabled ● Disabled
Ethernet Isolation: ○ Enabled ● Disabled

Vap2

Enable: □
SSID: ADSL_Modem/Router-2
Authentication Type: ○ Open System ○ Shared Key ● Auto
Wireless Isolation: ○ Enabled ● Disabled
Ethernet Isolation: ○ Enabled ● Disabled

Vap3

Enable: □
SSID: ADSL_Modem/Router-3
Authentication Type: ○ Open System ○ Shared Key ● Auto
Wireless Isolation: ○ Enabled ● Disabled

Enable: Enable or disable the Vap (Virtual AP) setting.

SSID: Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the WLAN ADSL Router.

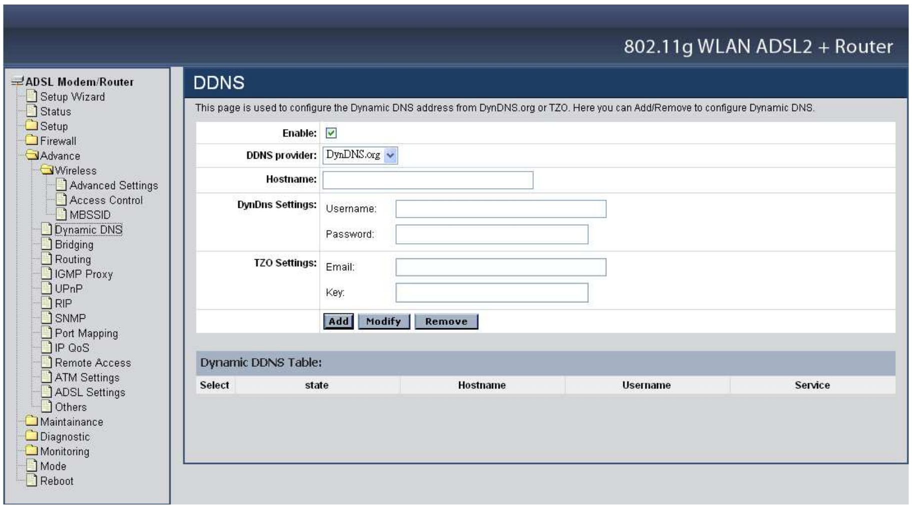
Authentication Type: Open System: Open System authentication is not required to be successful while a client may decline to authenticate with any particular other client. **Shared Key:** Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear. Requiring the use of the WEP privacy mechanism. **Auto:** Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill client’s requirement.

Wireless Isolation: Select to enable or disable the Wireless Isolation feature. When Wireless Isolation is enabled, wireless clients will not be able to access to the other wireless clients.

Ethernet Isolation: Select to enable or disable the Ethernet Isolation feature. When Ethernet Isolation is enabled, wireless clients will not be able to access to the Ethernet clients.

Dynamic DNS

Each time your device connects to the Internet, your ISP assigns a different IP address to your device. In order for you or other users to access your device from the WAN-side, you need to manually track the IP that is currently used. The Dynamic DNS feature allows you to register your device with a DNS server and access your device each time using the same host name. The Dynamic DNS page allows you to enable/disable the Dynamic DNS feature.



DDNS

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

Enable: ☑

DDNS provider: DynDNS.org

Hostname:

DynDns Settings: Username: Password:

TZO Settings: Email: Key:

Dynamic DDNS Table:

Select	state	Hostname	Username	Service

Enable: Checked to enable this registration account for the DNS server.

DDNS Provider: There are two DDNS providers to be selected in order to register your device with: DynDNS and TZO. A charge may occur depends on the service you select.

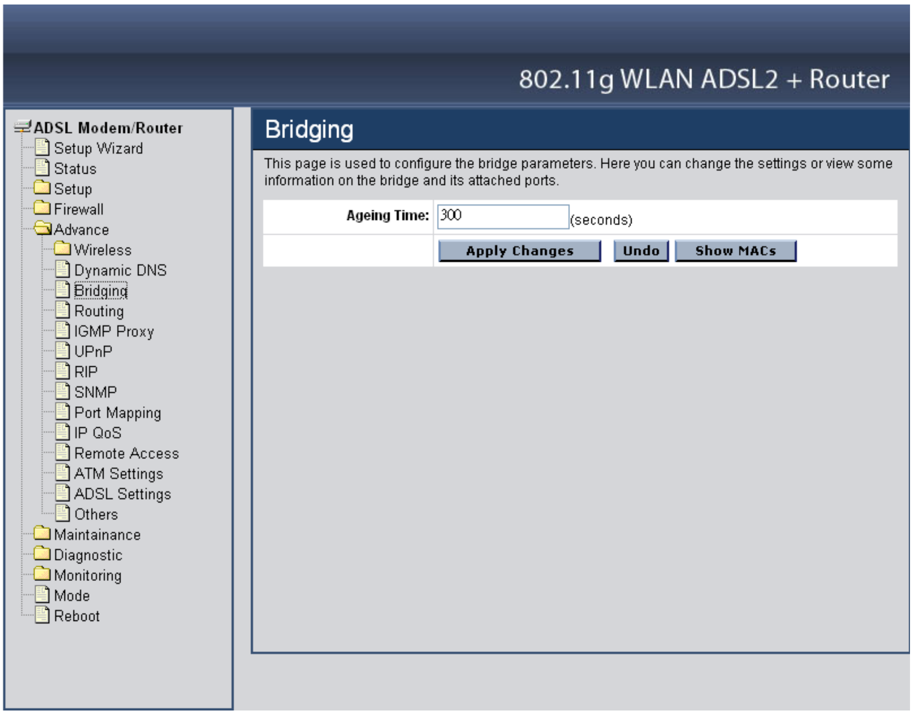
Hostname: Domain name to be registered with the DDNS server.

DynDns Settings: Enter the username and password for your registered DynDNS account.

TZO Settings: Enter the email address and key for your registered TZO account.

Bridging

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.



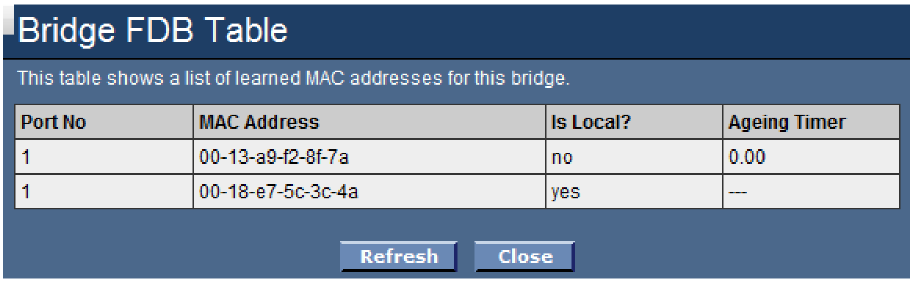
Bridging

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Ageing Time: 300 (seconds)

Aging Time: Set the Ethernet address ageing time, in seconds. After [Ageing Time] seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from Forwarding DataBase (fdb).

Show MACs: Click the “Show MACs” button to list MAC address in forwarding DataBase(fdb).



Bridge FDB Table

This table shows a list of learned MAC addresses for this bridge.

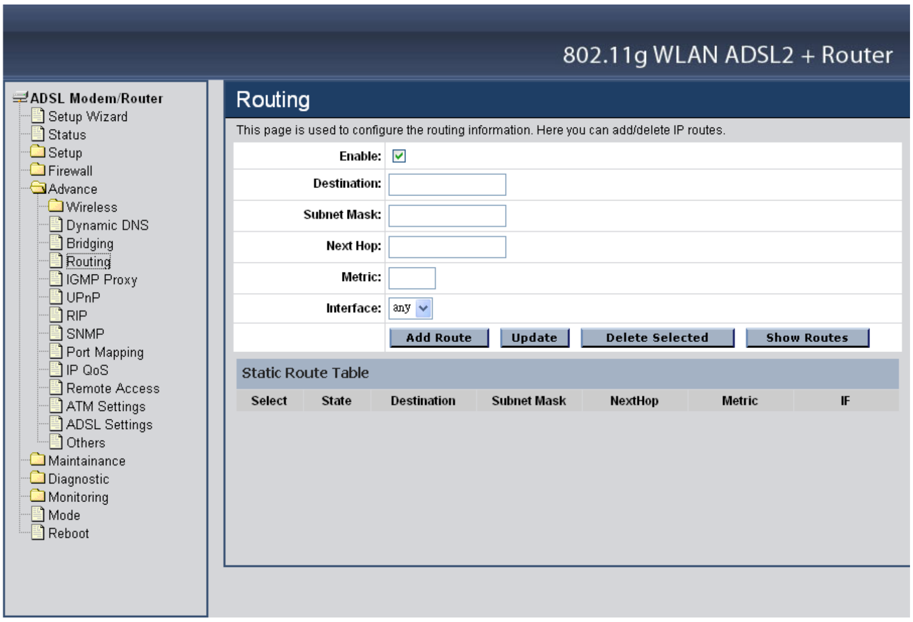
Port No	MAC Address	Is Local?	Ageing Timer
1	00-13-a9-f2-8f-7a	no	0.00
1	00-18-e7-5c-3c-4a	yes	---

Routing

The Routing page enables you to define specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the WLAN ADSL Router provide the most appropriate path for all your Internet traffic.

- On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the WLAN ADSL Router. Your LAN hosts know their default gateway either because you assigned it to them when you modified your TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.
- On the WLAN ADSL Router itself, a default gateway is defined to direct all outbound Internet traffic to a route at your ISP. The default gateway is assigned either automatically by your ISP whenever the device negotiates an Internet access, or manually by user to setup through the configuration.

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.



Routing

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:	☑
Destination:	
Subnet Mask:	
Next Hop:	
Metric:	
Interface:	any

Static Route Table

Select	State	Destination	Subnet Mask	NextHop	Metric	IF

Enable: Checked to enable the selected route or route to be added.

Destination: The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).

Subnet Mask: The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.

Next Hop: The IP address of the next hop through which traffic will flow towards the destination subnet.

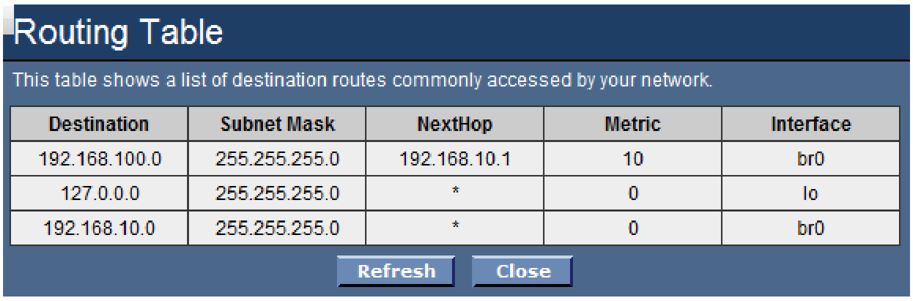
Metric: Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.

Interface: The WAN interface to which a static routing subnet is to be applied.

Add Router: Click the "Add Router" button to add a user-defined destination route.

Update: Click the "Update" button to modify the selected rule form the Static Route Table.

Show Routes: Click the "Show Routes" to display the routing table of the WLAN ADSL Router.



Routing Table

This table shows a list of destination routes commonly accessed by your network.

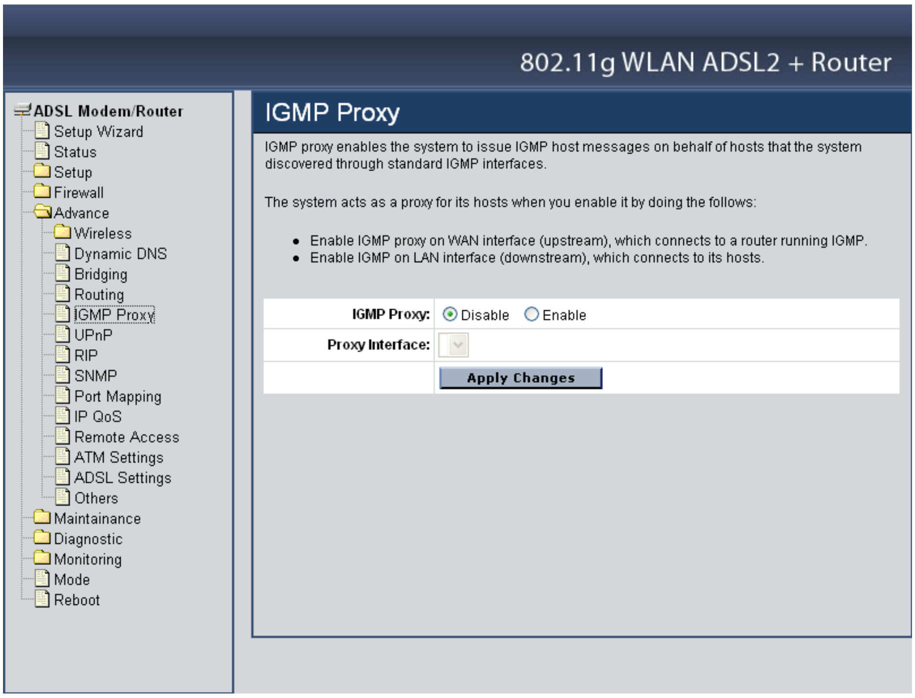
Destination	Subnet Mask	NextHop	Metric	Interface
192.168.100.0	255.255.255.0	192.168.10.1	10	br0
127.0.0.0	255.255.255.0	*	0	lo
192.168.10.0	255.255.255.0	*	0	br0

IGMP Proxy

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces.

The system acts as a proxy for its hosts when you enable it by doing the follows:

- Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
- Enable IGMP on LAN interface (downstream), which connects to its hosts.



IGMP Proxy

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces.

The system acts as a proxy for its hosts when you enable it by doing the follows:

- Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
- Enable IGMP on LAN interface (downstream), which connects to its hosts.

IGMP Proxy: ● Disable ○ Enable

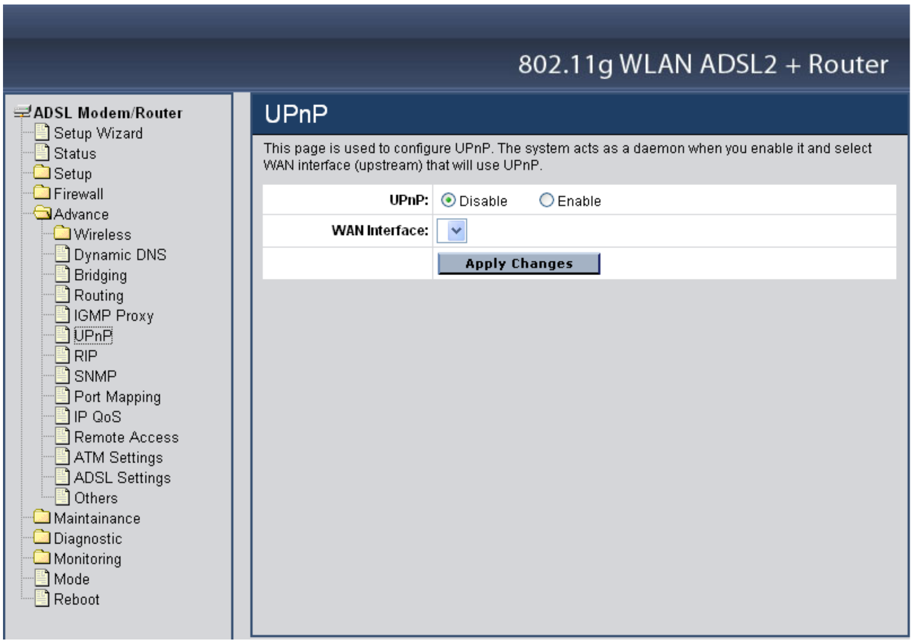
Proxy Interface:

IGMP Proxy: Select to enable or disable the IGMP proxy feature on the WLAN ADSL Router.

Proxy Interface: The upstream WAN interface is selected here.

UPnP

The WLAN ADSL Router supports a control point for Universal Plug and Play (UPnP) version 1.0, and supports two key features: NAT Traversal and Device Identification. This feature requires one active WAN interface. In addition, the host should support this feature. In the presence of multiple WAN interfaces, select an interface on which the incoming traffic is present. With NAT Traversal, when an UPnP command is received to open ports in NAT, the application translates the request into system commands to open the ports in NAT and the firewall. The interface to open the ports on is given to UPnP when it starts up and is part of the configuration of the application. For Device Identification, the application will send a description of the WLAN ADSL Router as a control point back to the host making the request.



UPnP

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

UPnP: ● Disable ○ Enable

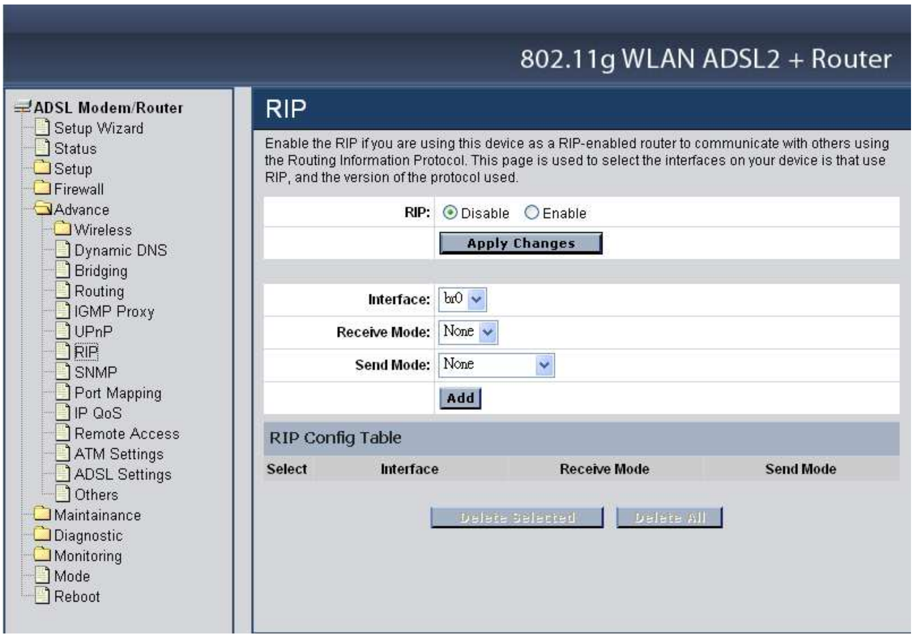
WAN Interface:

UPnP: Select to enable or disable the UPnP feature on the WLAN ADSL Router.

WAN Interface: Select WAN interface that will use UPnP from the drop-down lists.

RIP

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device is that use RIP, and the version of the protocol used.



RIP

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your device is that use RIP, and the version of the protocol used.

RIP: ● Disable ○ Enable

Interface: br0

Receive Mode: None

Send Mode: None

RIP Config Table

Select	Interface	Receive Mode	Send Mode

RIP: Select to enable or disable the RIP feature on the WLAN ADSL Router.

Receive Mode: Select which RIP version to be used for RIP listening, RIP1, RIP2 or Both (RIP1+RIP2), Selected None to disable the RIP listening.

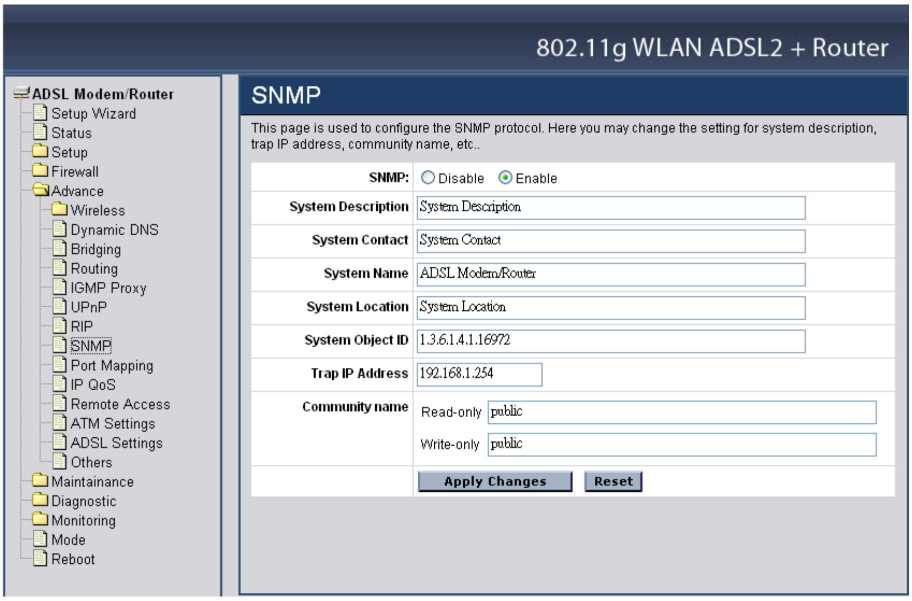
Send Mode: Select which RIP version to be used for RIP sending, RIP1, RIP2 or Both (RIP1+RIP2), Selected None to disable the RIP sending.

Delete Selected: Click the “Delete Selected” button to delete the selected RIP config from RIP Config Table.

Delete All: Click the “Delete All” button to delete the all of rule in the RIP config from RIP Config Table.

SNMP

Simple Network Management Protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The DSL device can be managed locally or remotely by SNMP protocol.



SNMP

This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap IP address, community name, etc..

SNMP:	○ Disable ● Enable
System Description	System Description
System Contact	System Contact
System Name	ADSL Modem/Router
System Location	System Location
System Object ID	1.3.6.1.4.1.16972
Trap IP Address	192.168.1.254
Community name	Read-only public Write-only public

SNMP: Enable or Disable the SNMP feature on the WLAN ADSL Router.

System Description: System description of the WLAN ADSL Router.

System Contact: Contact person and/or contact information for the WLAN ADSL Router.

System Name: An administratively assigned name for the WLAN ADSL Router.

System Location: The physical location of the WLAN ADSL Router.

System Object ID: Vendor Object Identifier. The vendor’s authoritative identification of the network management subsystem contained in the entity.

Trap IP Address: Destination IP address of the SNMP trap.

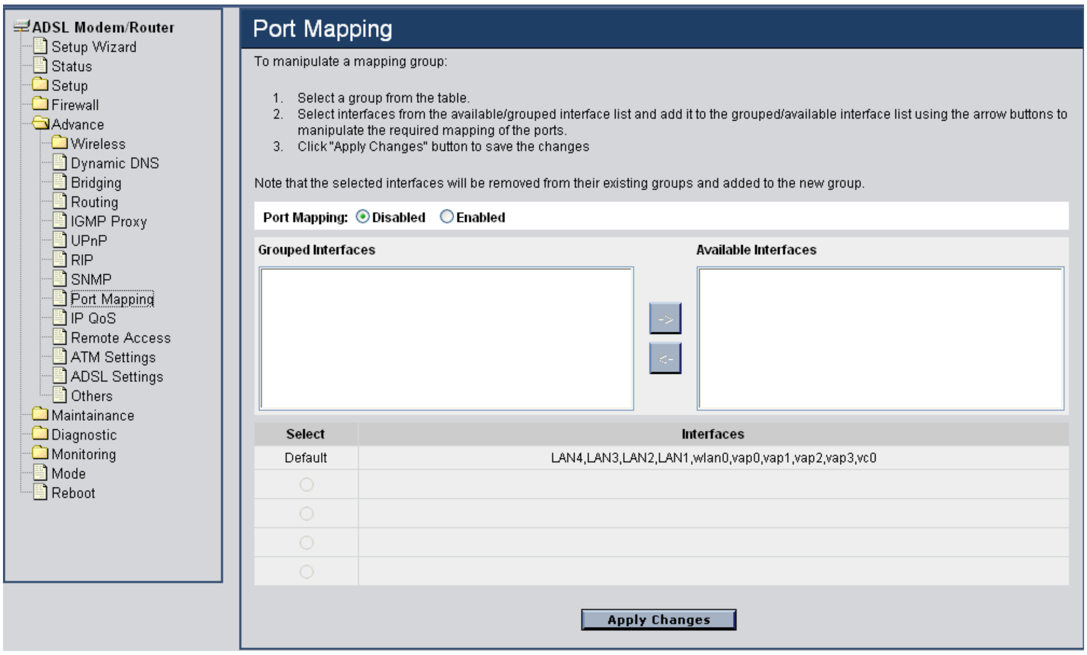
Community name:

Read-only: Name of the read-only community. This read-only community allows read operation to all objects in the MIB.

Write-only: Name of the write-only community. This write-only community allows write operation to the objects defines as read-writable in the MIB.

Port Mapping

The WLAN ADSL Router provides multiple interface groups. Up to five interface groups are supported including one default group. The LAN and WAN interfaces could be included. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the WLAN ADSL Router can isolate traffic from group to group for some application. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any group but only one group.



Port Mapping

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes

Note that the selected interfaces will be removed from their existing groups and added to the new group.

Port Mapping: ● Disabled ○ Enabled

Grouped Interfaces | Available Interfaces

Select	Interfaces
Default	LAN4,LAN3,LAN2,LAN1,wlan0,vap0,vap1,vap2,vap3,vc0
○	
○	
○	
○	

Port Mapping: Select to enable or disable the interface group feature. If disabled, all interfaces belong to the default group.

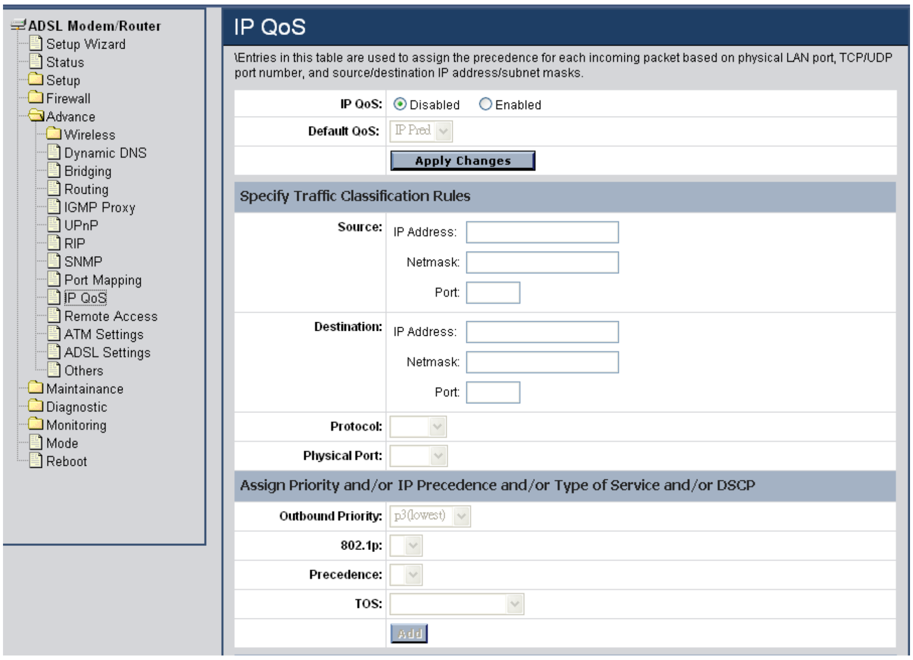
<u>Interface Group</u>

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click “Apply Changes” button to save the changes.

IP QoS

The WLAN ADSL Router provides a control mechanism that can provide different priority to different users or data flows. The QoS is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: Traffic Classification and Action. The Traffic Classification enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The Action enables you to assign the strictly priority level for and mark some fields in the packet that matches the Traffic Classification rule. You can configure any or all field as needed in these two QoS blocks for a QoS rule.



IP QoS

\Entries in this table are used to assign the precedence for each incoming packet based on physical LAN port, TCP/UDP port number, and source/destination IP address/subnet masks.

IP QoS: ● Disabled ○ Enabled

Default QoS: IP Pred

Specify Traffic Classification Rules

Source: IP Address: Netmask: Port:

Destination: IP Address: Netmask: Port:

Protocol:

Physical Port:

Assign Priority and/or IP Precedence and/or Type of Service and/or DSCP

Outbound Priority: p3(lowest)

802.1p:

Precedence:

TOS:

IP QoS: Select to enable or disable the IP QoS function.

Default QoS: Select the QoS method IP Pred or 802.1p from list.

Source: The IP address, subnet mask and port number of the traffic source.

Destination: The IP address, subnet mask and port number of the traffic destination.

Protocol: The selections are TCP, UDP, ICMP and the blank for none. This field is required if the source port or destination port has been entered.

Physical Port: The incoming ports. The selections include LAN ports, wireless port, and the blank for not applicable.

Outbound Priority: The priority level for the traffic that matches this classification rule. The possible selections are (in the descending priority): p0, p1, p2, p3.

802.1p: Select this field to mark the 3-bit user-priority field in the 802.1p header of the packet that match this classification rule. Note that this 802.1p marking is workable on a given PVC channel only if the VLAN tag is enabled in this PVC channel.

Precedence: Select this field to mark the IP precedence bits in the packet that match this classification rule.

TOS: Select this field to mark the IP TOS bits in the packet that match this classification rule.

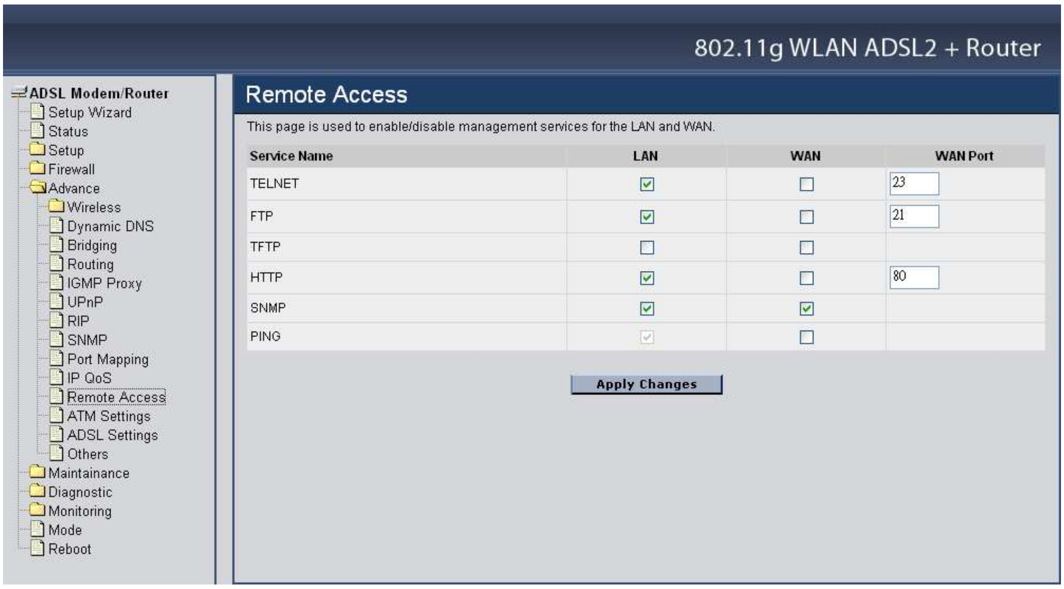
Add: Click to add the QoS rule to the UP QoS Rules.

Delete Selected: Click the "Delete Selected" button to delete the selected QoS rule from the IP QoS Rules.

Delete All: Click the "Delete All" button to delete the all of rule in the IP QoS Rules.

Remote Access

The Remote Access function can secure remote host access to your DSL device from LAN and WLAN interfaces for some services provided by the DSL device.



Remote Access

This page is used to enable/disable management services for the LAN and WAN.

Service Name	LAN	WAN	WAN Port
TELNET	☑	□	23
FTP	☑	□	21
TFTP	□	□	
HTTP	☑	□	80
SNMP	☑	☑	
PING	☑	□	

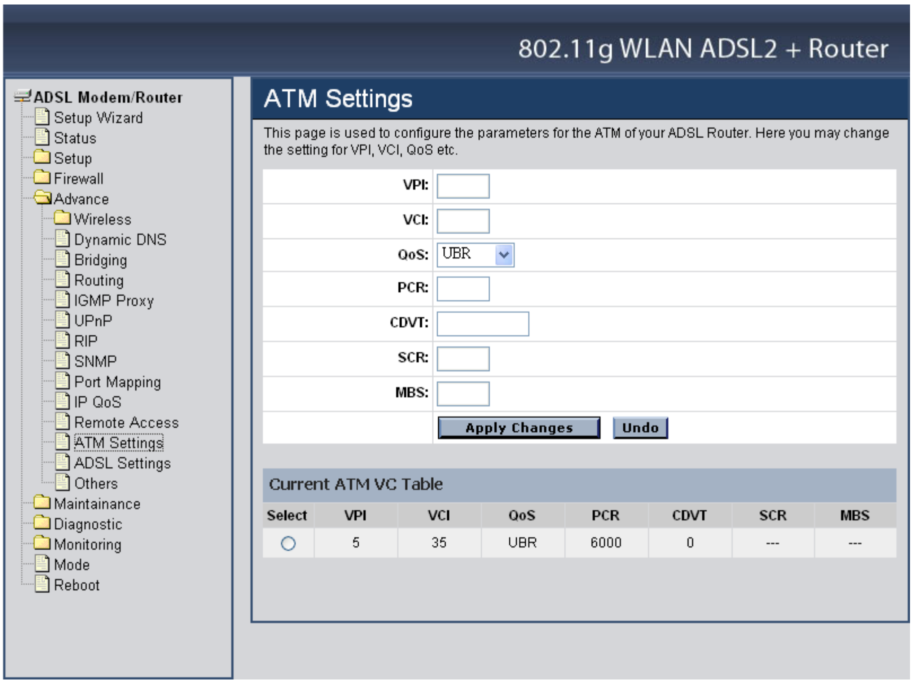
LAN: Checked the services on the LAN column to allows the services access from LAN side.

WAN: Checked the services on the WAN column to allows the services access from WAN side.

WAN Port: This field allows the user to specify the port of the corresponding service. Take the HTTP service for example; when it is changed to 8080, the HTTP server address for the WAN side is http://dsl_addr:8080, where the dsl_addr is the WAN side IP address of the WLAN ADSL Router.

ATM Settings

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for VPI, VCI, QoS etc.



ATM Settings

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for VPI, VCI, QoS etc.

VPI:

VCI:

QoS: UBR

PCR:

CDVT:

SCR:

MBS:

Current ATM VC Table

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
○	5	35	UBR	6000	0	---	---

VPI: Virtual Path Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table.

VCI: Virtual Channel Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through to the ATM switch.

QoS: Quality of Server, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The four QoS options are:

- **UBR (Unspecified Bit Rate):** When UBR is selected, the SCR and MBS fields are disabled.
- **CBR (Constant Bit Rate):** When CBR is selected, the SCR and MBS fields are disabled.
- **nrt-VBR (non-real-time Variable Bit Rate):** When nrt-VBR is selected, the SCR and MBS fields are enabled.
- **rt-VBR (real-time Variable Bit Rate):** When rt-VBR is selected, the SCR and MBS fields are enabled.

PCR: Peak Cell Rate, measured in cells/sec., is the cell rate which the source may never exceed.

CDVT: Cell Delay Variation Tolerance, is a QoS parameter in ATM network for managing traffic that is specified when a connection is set up. In CBR transmissions, CDVT determines the level of jitter that is tolerable for the data samples taken by the PCR.

SCR: Sustained Cell Rate, measured in cells/sec., is the average cell rate over the duration of the connection.

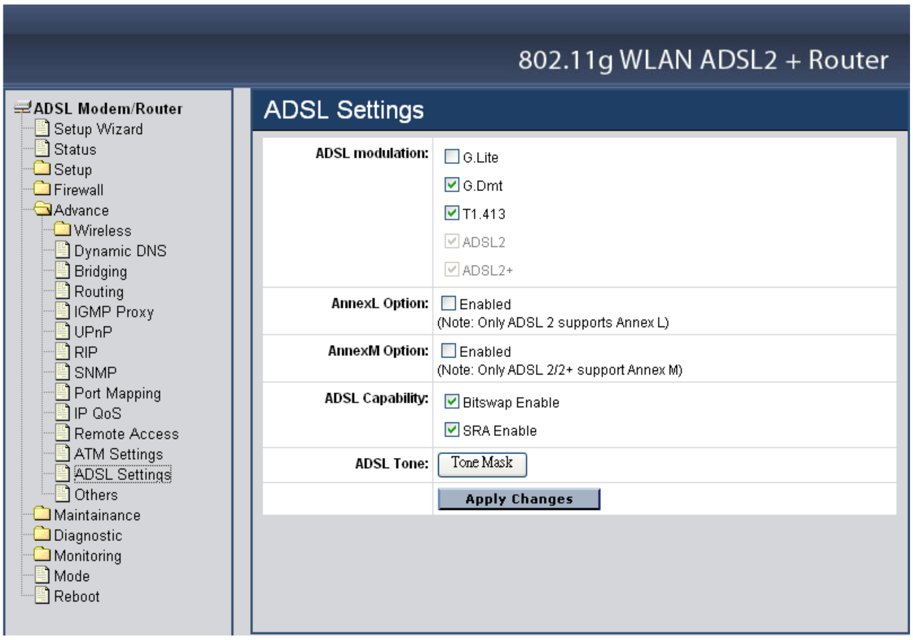
MBS: Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.

Apply Changes: Click to set new PVC QoS mode for the selected PVC. New parameters will take effect after save into flash memory and reboot the system.

Undo: Discard your settings.

ADSL Settings

The ADSL setting page allows you to select any combination of DSL training modes.



ADSL Settings

ADSL modulation: □ G.Lite
☑ G.Dmt
☑ T1.413
☑ ADSL2
☑ ADSL2+

AnnexL Option: □ Enabled
(Note: Only ADSL 2 supports Annex L)

AnnexM Option: □ Enabled
(Note: Only ADSL 2/2+ support Annex M)

ADSL Capability: ☑ Bitswap Enable
☑ SRA Enable

ADSL Tone: Tone Mask

ADSL modulation: Choose preferred xDSL standard protocols, defined by ISP.

G.lite: G.992.2 Annex A

G.dmt: G.992.1 Annex A

T1.413: T1.413 issue #2

ADSL2: G.992.3 Annex A

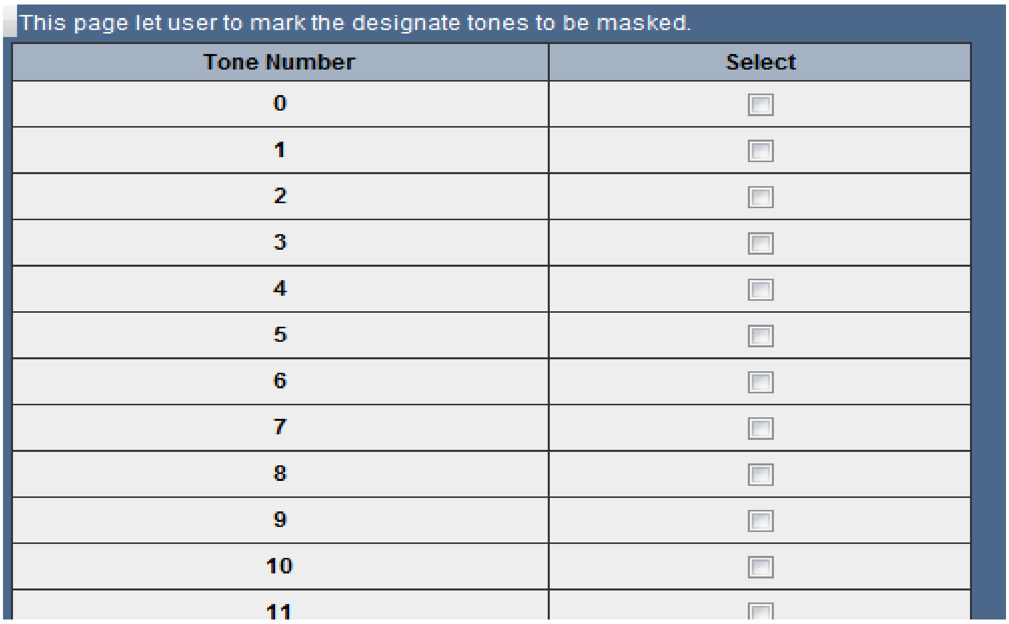
ADSL2+: G.992.5 Annex A

AnnexL Option: Checked to Enable the ADSL2/ADSL2+ Annex L capability.

AnnexM Option: Checked to Enable the ADSL2/ADSL2+ Annex M capability.

ADSL Capability: Checked to enable the bitswap capability or SRA capability.

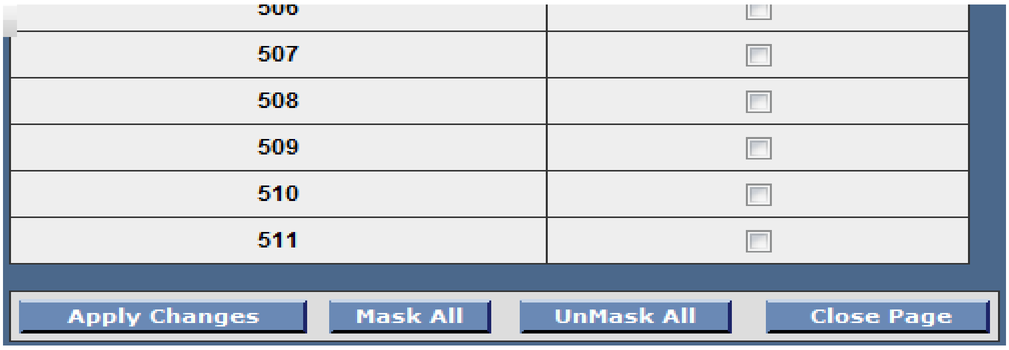
ADSL Tone: Click the "ADSL Tone" button to choose tones to be masked. Masked tones will not carry any data.



This page let user to mark the designate tones to be masked.

Tone Number	Select
0	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐
9	☐
10	☐
11	☐

:



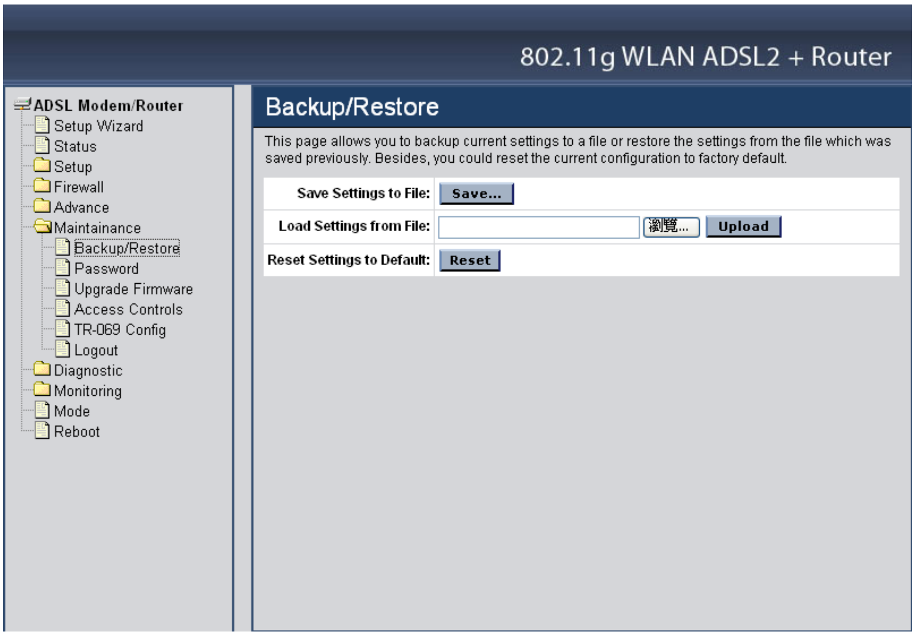
506	☐
507	☐
508	☐
509	☐
510	☐
511	☐

Apply Changes: Click to save the setting to the configuration and the modem will be retrained.

Maintainance

Backup/Restore

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.



Backup/Restore

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:	Save...
Load Settings from File:	瀏覽... Upload
Reset Settings to Default:	Reset

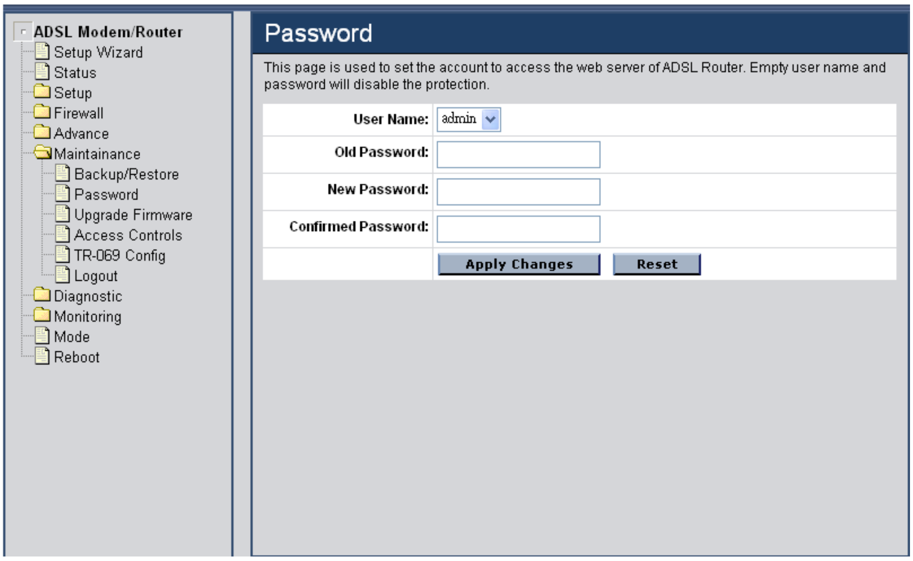
Save Setting to File: Click the “Save Setting to File” button to save current settings of the WLAN ADSL Router to local computer.

Load Setting from File: Click the “Browse” button and selected a saved setting file from file browse window then click “Upload” button to loading the saved setting to the WLAN ADSL Router.

Reset Settings to Default: Click the “Reset” button to reset the settings to factory default settings.

Password

The first time you log into the WLAN ADSL Router, you use the default password. There are two-level logins: ***admin*** and ***user***. The admin and user password configuration allows you to change the password for administrator and user.



Password

This page is used to set the account to access the web server of ADSL Router. Empty user name and password will disable the protection.

User Name:	admin
Old Password:	
New Password:	
Confirmed Password:	

User Name: Selection of user levels are: admin and user.

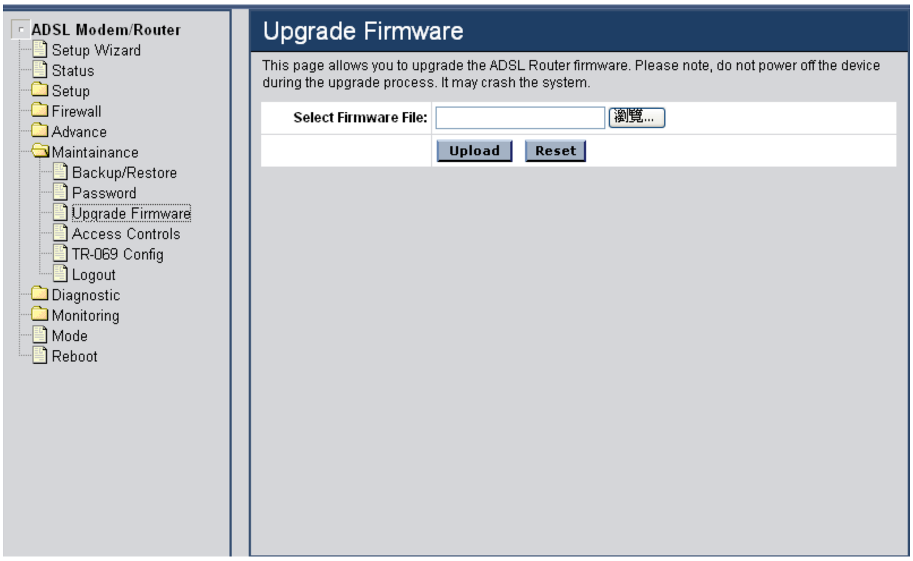
Old Password: Enter the old password for this selected login.

New Password: Enter the new password here.

Confirmed Password: Enter the new password here again to confirm.

Upgrade Firmware

This page allows you to upgrade the WLAN ADSL Router firmware. Please note, do not power off the device during the upgrade process. It may crash the system.



This page allows you to upgrade the ADSL Router firmware. Please note, do not power off the device during the upgrade process. It may crash the system.

Select Firmware File:

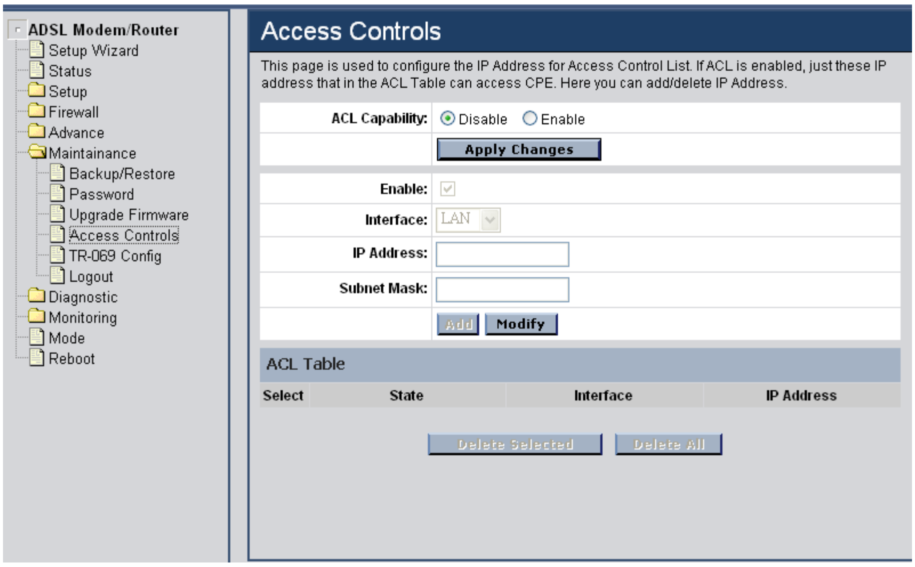
To upgrade the firmware for the DSL device:

- Click the Browse button to select the firmware file.
- Confirm your selection.
- Click the Upload button to start upgrading.

IMPORTANT! Do not turn off your DSL device or click the Reset button while this procedure is in progress.

Access Controls

The Access Control List (ACL) is a list of permissions attached to the WLAN ADSL Router. The list specifies who is allowed to access this device. If ACL is enabled, all hosts cannot access this device except for the hosts with IP address in the ACL table.



Access Controls

This page is used to configure the IP Address for Access Control List. If ACL is enabled, just these IP address that in the ACL Table can access CPE. Here you can add/delete IP Address.

ACL Capability: ● Disable ○ Enable

Enable: ☑

Interface: LAN

IP Address:

Subnet Mask:

ACL Table

Select	State	Interface	IP Address

ACL Capability: Enable or Disable the SNMP feature on the WLAN ADSL Router.

Enable: Checked to enable the selected route or route to be added.

Interface: Select the interface domain: LAN or WAN.

IP Address: Enter the IP address that allow access to this device.

Subnet Mask: Type the subnet mask in the text box.

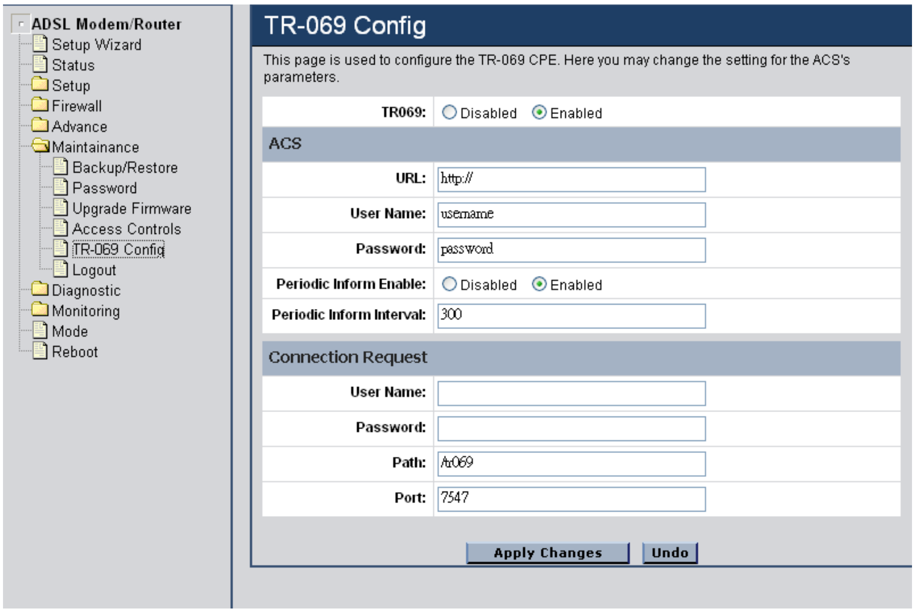
Add: Click to add the ACL rule to the ACL table.

Modify: Click the “Modify” button to modify the selected rule form the ACL Table.

Delete Selected: Click the “Delete Selected” button to delete the selected rule from ACL Table.

Delete All: Click the “Delete All” button to delete the all of rule in the ACL Table.

TR-069 is a protocol for communication between a CPE and Auto-Configuration Server (ACS). The CPE TR-069 configuration should be well defined to be able to communicate with the remote ACS.



TR-069 Config

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

TR069:	○ Disabled ● Enabled
ACS	
URL:	http://
User Name:	username
Password:	password
Periodic Inform Enable:	○ Disabled ● Enabled
Periodic Inform Interval:	300
Connection Request	
User Name:	
Password:	
Path:	/tr069
Port:	7547

TR069: Enable or Disable the TR-069 feature on the WLAN ADSL Router.

ACS

URL: Enter the ACS URL here.

User Name: The username the WLAN ADSL Router should use when connecting to the ACS.

Password: The password the WLAN ADSL Router should use when connecting to the ACS.

Periodic Inform Enable: When this field is enabled, the WLAN ADSL Router will send an Inform RPC to the ACS server at the system startup, and will continue to send it periodically at an interval defined in Periodic Inform Interval field; When this field is disabled, the WLAN ADSL Router will only send Inform RPC to the ACS server once at the system startup.

Periodic Inform Interval: Time interval in second to send Inform RPC.

Connection Request

User Name: The username the remote ACS should use when connecting to this device.

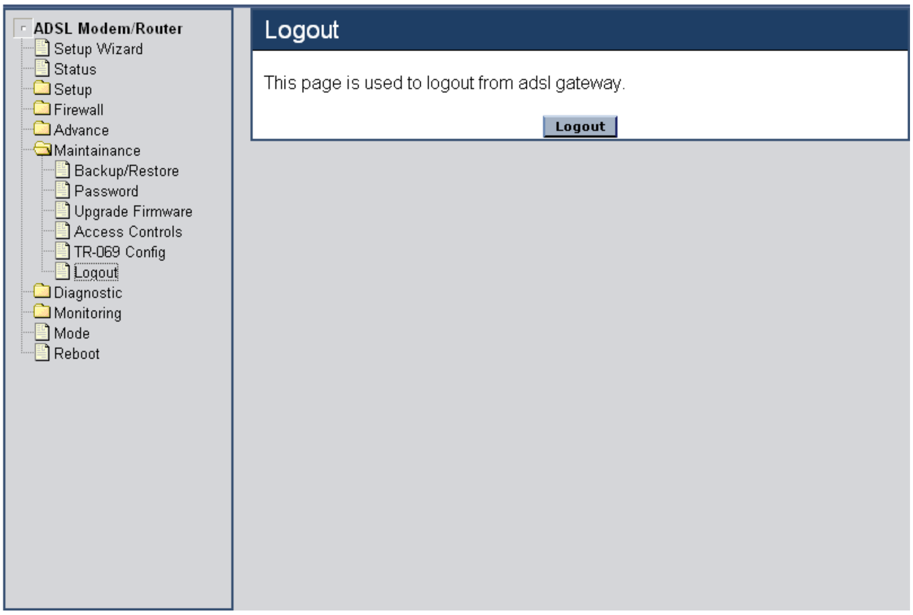
Password: The password the remote ACS should use when connecting to this device.

Path: The path of the device ConnectionRequestURL. The device ConnectionRequestURL should be configured based on the Device_IP, Path and Port as follows: http://Device_IP:Port/Path.

Port: The port of the device ConnectionRequestURL.

Logout

This page is used to logout from ADSL gateway.



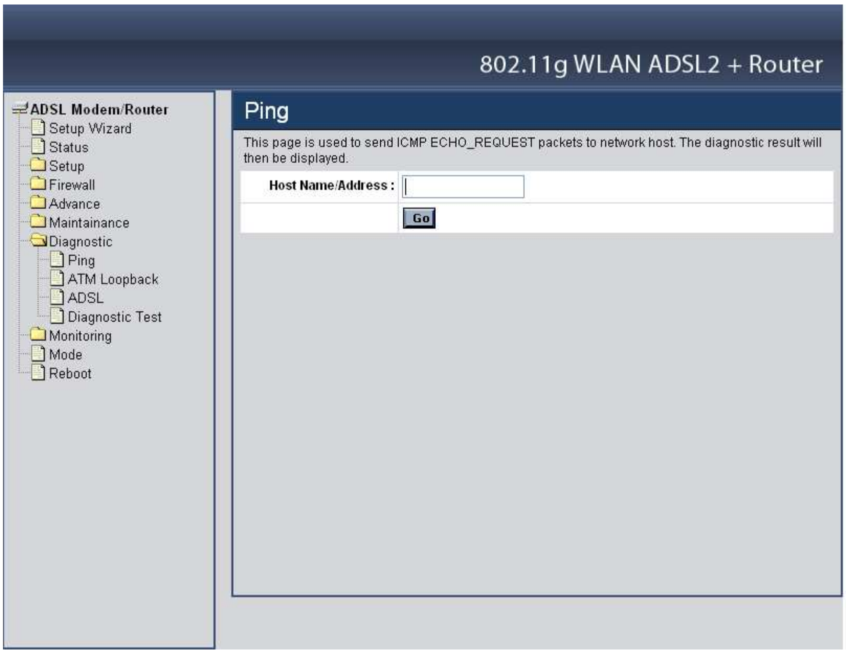
This page is used to logout from adsl gateway.

Click the “Logout” button to logout from the WLAN ADSL Router.

Diagnostic

Ping

Once you have your WLAN ADSL Router configured, it is a good idea to make sure you can ping the network. A ping command sends a message to the host you specify. If the host receives the message, it sends messages in reply. To use it, you must know the IP address of the host you are trying to communicate with and enter the IP address in the Host Address field. Click "Go" button to start the ping command, the ping result will then be shown in this page.

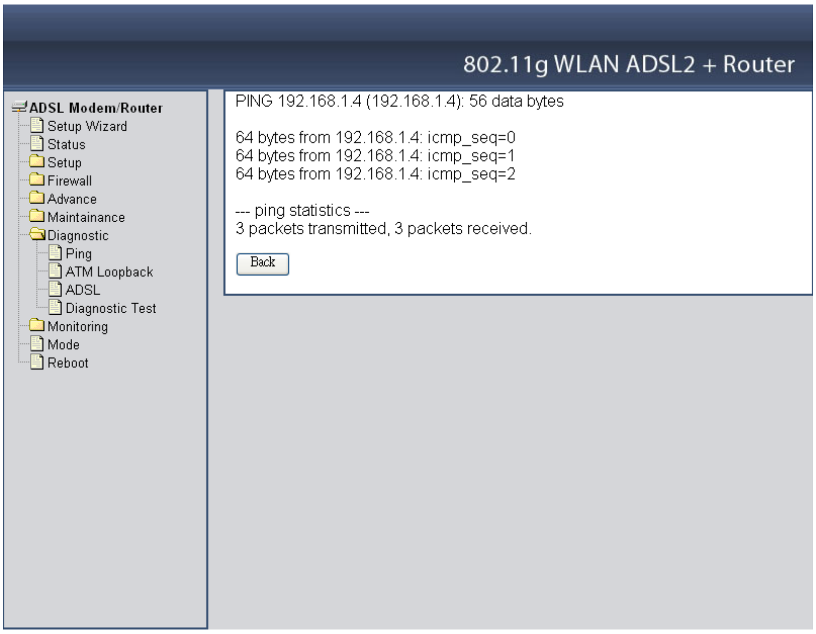


Ping

This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.

Host Name/Address :

Go: Click "Go" button to start the ping command, the ping result will then be shown in this page.



```
PING 192.168.1.4 (192.168.1.4): 56 data bytes

64 bytes from 192.168.1.4: icmp_seq=0
64 bytes from 192.168.1.4: icmp_seq=1
64 bytes from 192.168.1.4: icmp_seq=2

--- ping statistics ---
3 packets transmitted, 3 packets received.
```

ATM Loopback

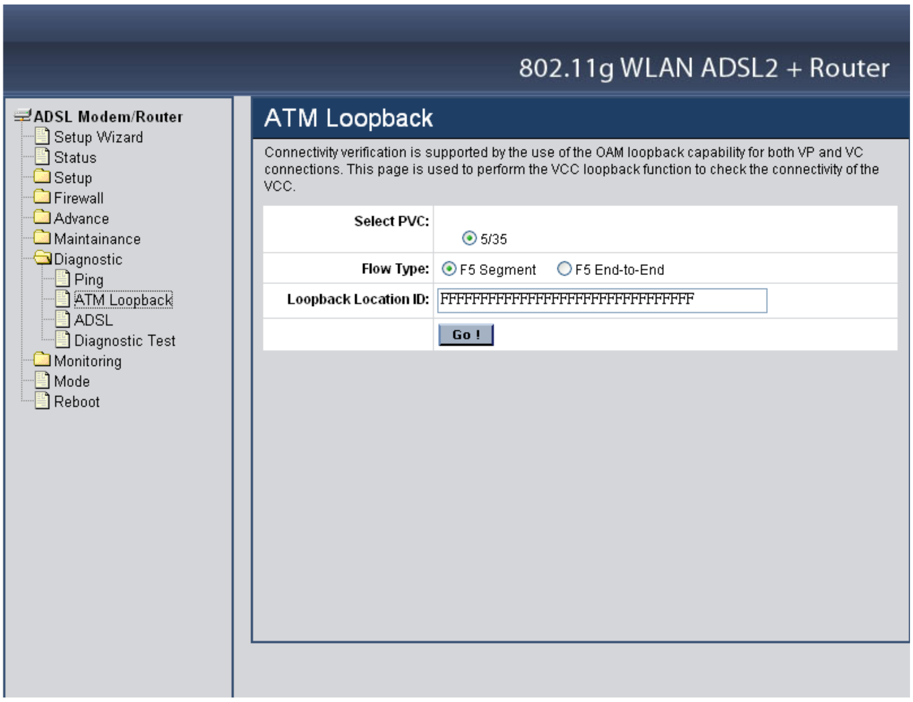
In order to isolate the ATM interface problems, you can use ATM OAM loopback cells to verify connectivity between VP/VC endpoints, as well as segment endpoints within the VP/VC. ATM uses F4 and F5 cell flows as follows:

- **F4:** used in VPs.
- **F5:** used in VCs.

An ATM connection consists of a group of points. This OAM implementation provides management for the following points:

- **Connection endpoint:** the end of a VP/VC connection where the ATM cell are terminated.
- **Segment endpoint:** the end of a connection segment.

This page allows you to use ATM ping, which generates F5 segment and end-to-end loop-back cells to test the reach ability of a segment endpoint or a connection endpoint.



ATM Loopback

Connectivity verification is supported by the use of the OAM loopback capability for both VP and VC connections. This page is used to perform the VCC loopback function to check the connectivity of the VCC.

Select PVC: ● 5/35

Flow Type: ● F5 Segment ○ F5 End-to-End

Loopback Location ID: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

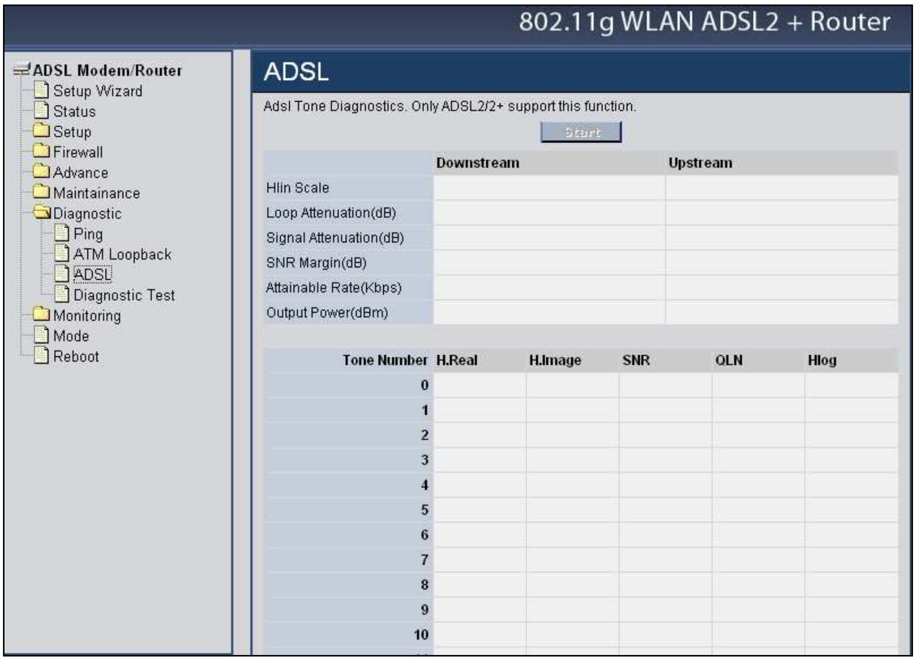
Select PVC: Select the PVC channel you want to do the loop-back diagnostic.

Flow Type: The ATM OAM flow type. The selection can be F5 Segment or F5 End-to-End.

Loopback Location ID: The loop-back location ID field of the loop-back cell. The default value is all 1s (ones) to indicate the endpoint of the segment or connection.

ADSL

This page shows the ADSL diagnostic result. Click “Start” button to start the ADSL diagnostic.



ADSL

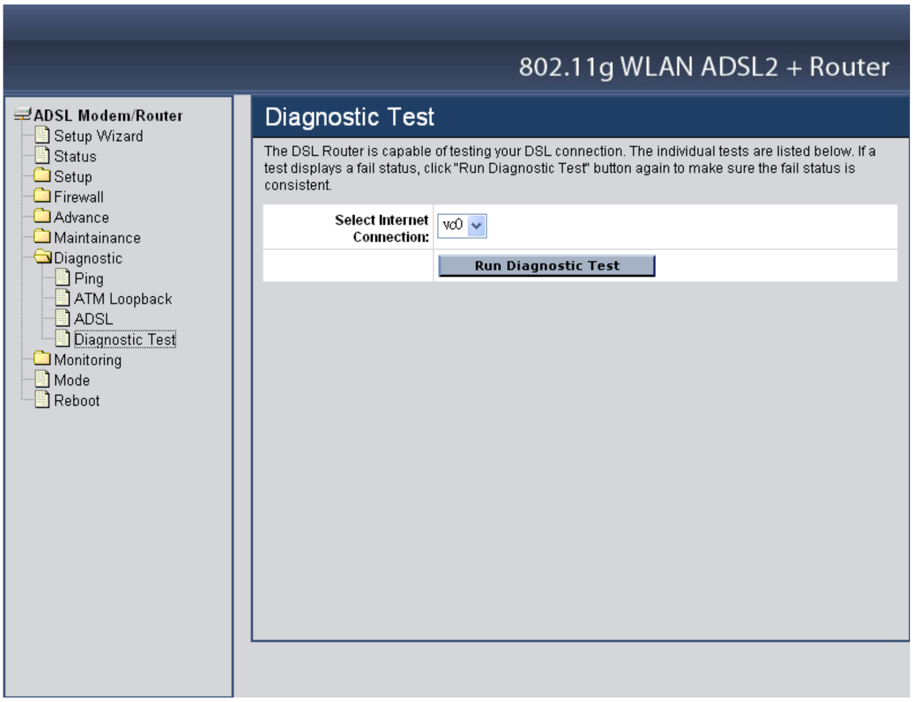
Adsl Tone Diagnostics. Only ADSL2/2+ support this function.

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Diagnostic Test

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.



Diagnostic Test

The DSL Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.

Select Internet Connection: vc0

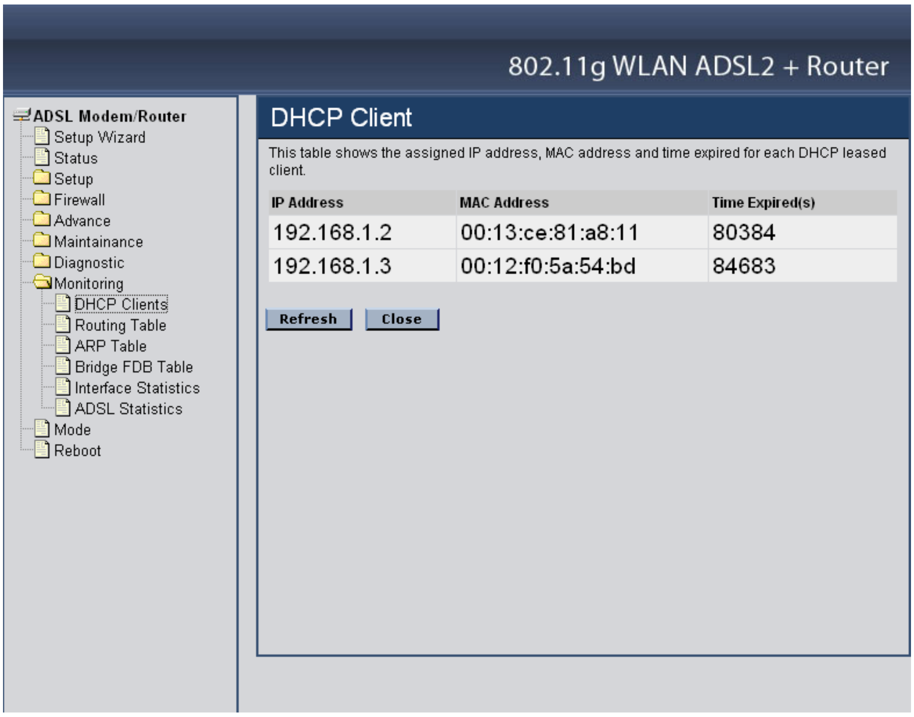
Select Internet Connection: The available WAN side interfaces are listed. You have to select one for the WAN side diagnostic.

Run Diagnostic Test: Click the "Run Diagnostic Test" button to start the diagnostic test.

Monitoring

DHCP Clients

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.



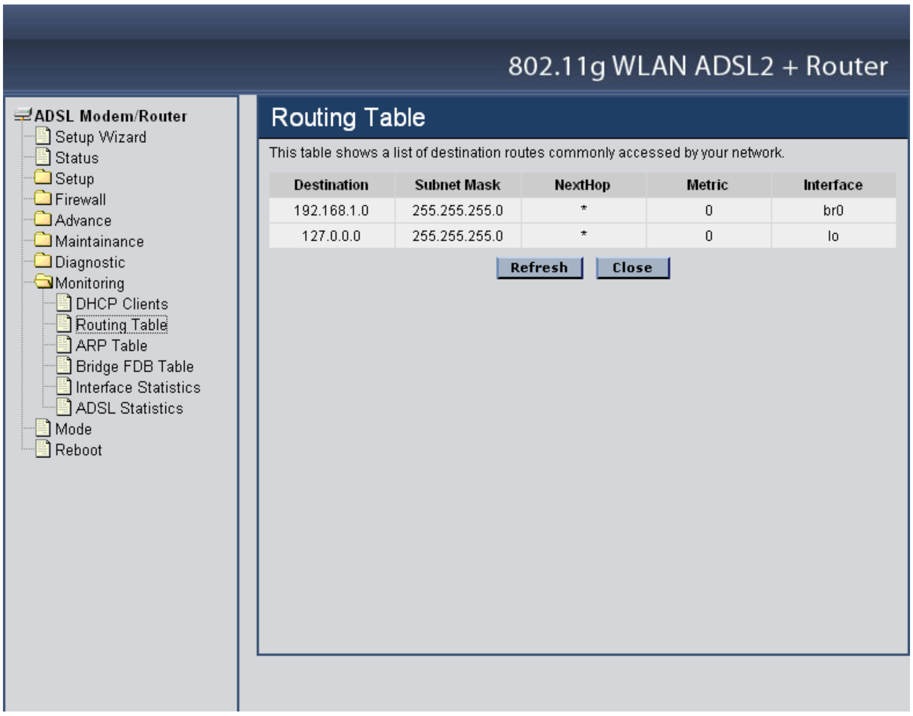
DHCP Client

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
192.168.1.2	00:13:ce:81:a8:11	80384
192.168.1.3	00:12:f0:5a:54:bd	84683

Routing Table

This table shows a list of destination routes commonly accessed by your network.



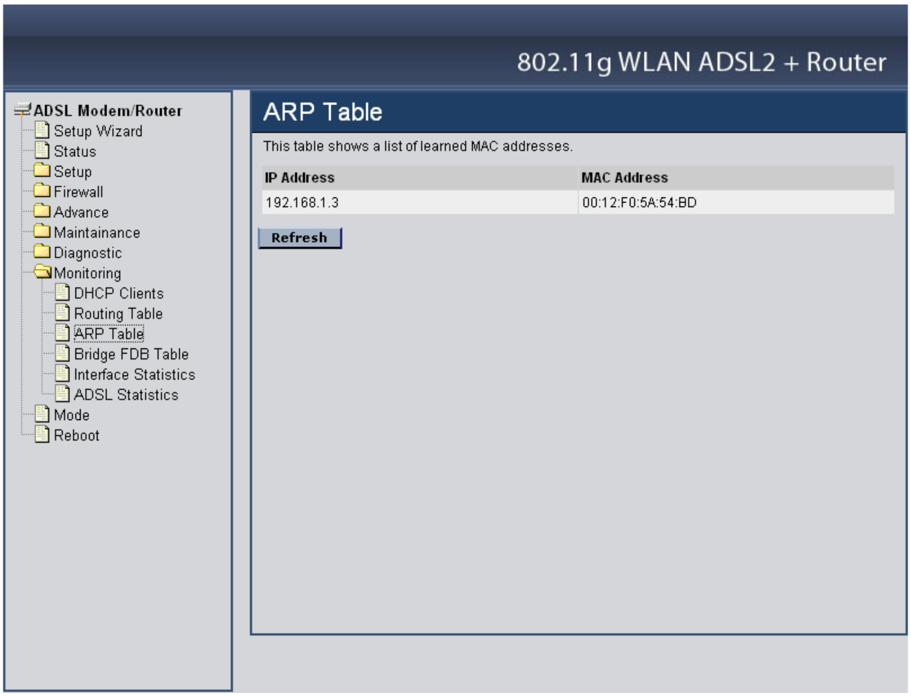
Routing Table

This table shows a list of destination routes commonly accessed by your network.

Destination	Subnet Mask	NextHop	Metric	Interface
192.168.1.0	255.255.255.0	*	0	br0
127.0.0.0	255.255.255.0	*	0	lo

ARP Table

This table shows a list of learned MAC addresses.



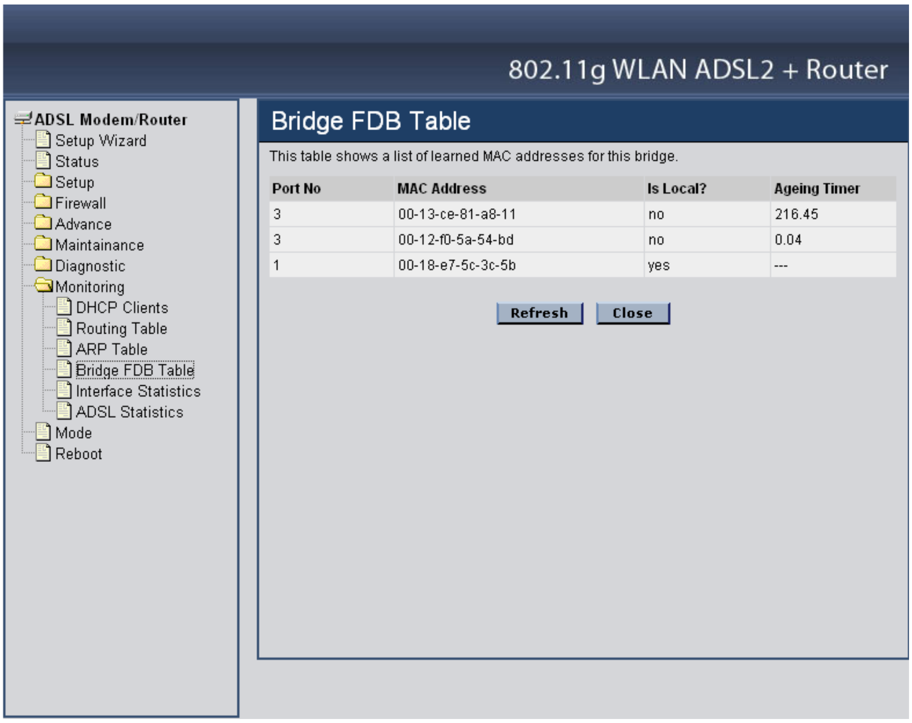
ARP Table

This table shows a list of learned MAC addresses.

IP Address	MAC Address
192.168.1.3	00:12:F0:5A:54:BD

Bridge FDB Table

This table shows a list of learned MAC addresses for this bridge.



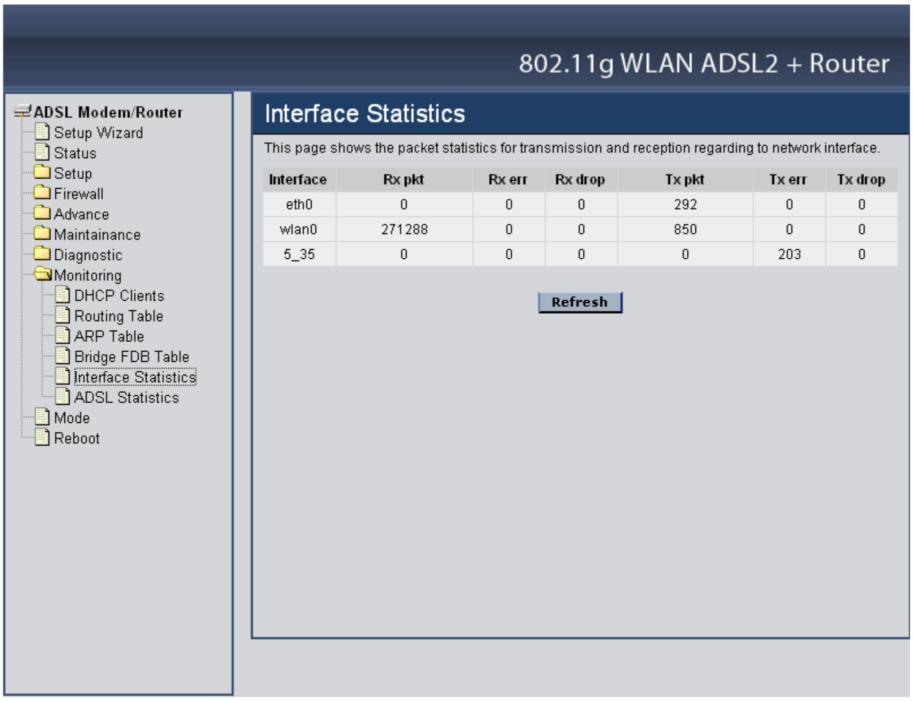
Bridge FDB Table

This table shows a list of learned MAC addresses for this bridge.

Port No	MAC Address	Is Local?	Ageing Timer
3	00-13-ce-81-a8-11	no	216.45
3	00-12-f0-5a-54-bd	no	0.04
1	00-18-e7-5c-3c-5b	yes	---

Interface Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.



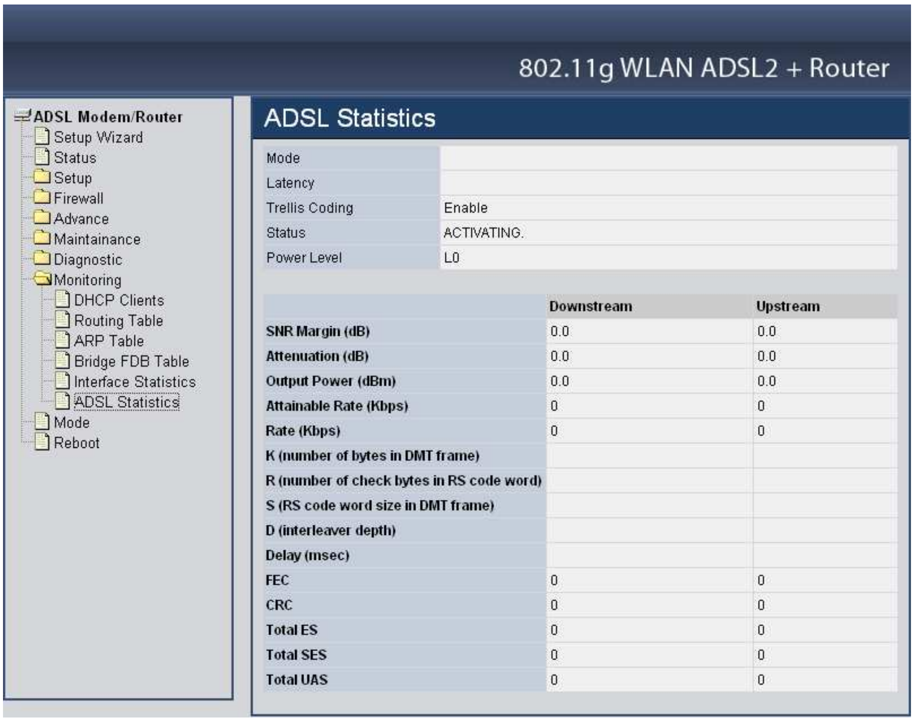
Interface Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0	0	0	0	292	0	0
wlan0	271288	0	0	850	0	0
5_35	0	0	0	0	203	0

ADSL Statistics

This page shows the packet statistics for transmission and reception regarding to the ADSL.



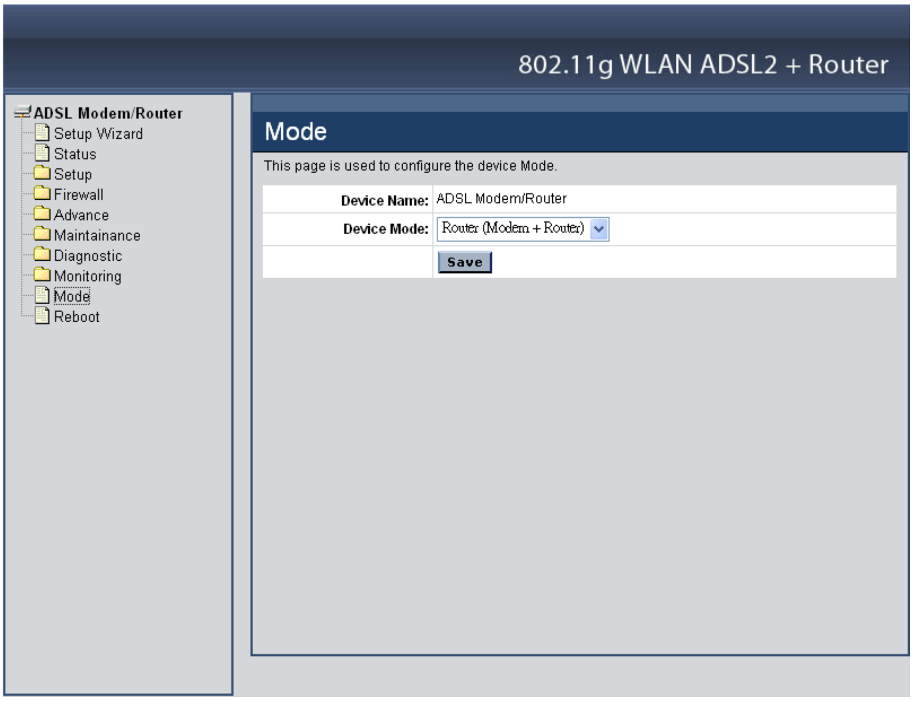
ADSL Statistics

Mode	
Latency	
Trellis Coding	Enable
Status	ACTIVATING.
Power Level	L0

	Downstream	Upstream
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power (dBm)	0.0	0.0
Attainable Rate (Kbps)	0	0
Rate (Kbps)	0	0
K (number of bytes in DMT frame)		
R (number of check bytes in RS code word)		
S (RS code word size in DMT frame)		
D (interleaver depth)		
Delay (msec)		
FEC	0	0
CRC	0	0
Total ES	0	0
Total SES	0	0
Total UAS	0	0

Mode

This page explains configuration and operation when in "Router" or "Modem" mode.



Mode

This page is used to configure the device Mode.

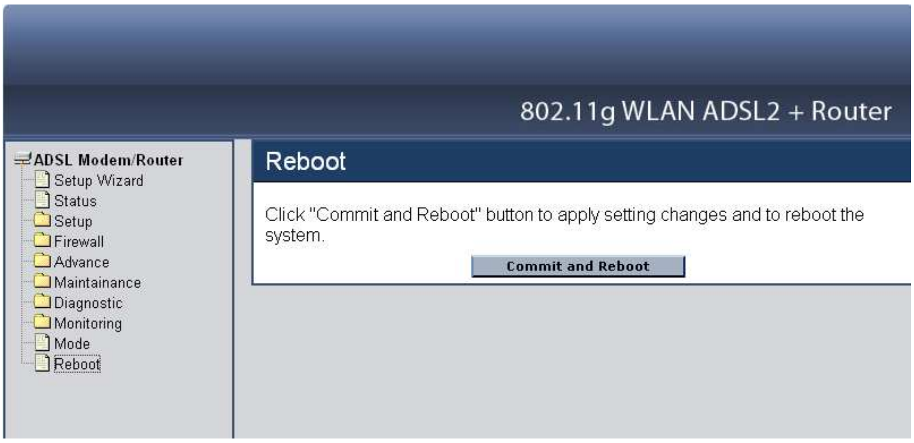
Device Name:	ADSL Modem/Router
Device Mode:	Router (Modem + Router)

Device Mode: There are two modes available on the Mode screen.

- **Router:** Both the ADSL Modem and the Router features are operational. In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users.
- **Modem:** Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.

Reboot

Click "Commit and Reboot" button to apply setting changes and to reboot the WLAN ADSL Router.



Click "Commit and Reboot" button to apply setting changes and to reboot the system.

TECHNICAL SPECIFICATIONS

General	
Standards	Compliant with ADSL standards: ANSI T1.413 Issue2, G.992.1 (G.dmt, Annex A), G.992.2 (G.lite) Compliant with ADSL2 standard: G.992.3 (G.dmt.bis) Compliant with ADSL2+ standard: G.992.5 Annex A IEEE 802.11b & 802.11g Wireless LAN IEEE 802.3u 10/100Base TX Fast Ethernet
Protocol	WLAN: CSMA/CA ATM & PPP: VC and LLC Multiplexing, Bridged/Routed Ethernet over ATM (RFC1483/2684), Classical IP over ATM(RFC-1577), OAM F4/F5 loop-back, PPP over ATM (RFC2364), PPP over Ethernet (RFC2516), ATM TrafficShaping QoS(UBR, CBR, rt-VBR, nrt-VBR) LAN/WAN Network: TCP/IP, NAT, HTTP, DHCP Server/Relay/Client, DDNS, DNS Proxy
Radio Technology	DSSS/OFDM
Data Transfer Rate	802.11n mode: up to 300Mbps (auto sense) 802.11g mode: up to 54Mbps (auto sense) 802.11b mode: up to 11Mbps (auto sense) Ethernet: 10Mbps (half duplex), 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half duplex), 200Mbps (full- duplex)
Receiver Sensitivity	802.11n: -63dBm typical @ 300Mbps 802.11g: -70dBm typical @ 54Mbps 802.11b: -85dBm typical @ 11Mbps
TX Power	802.11b: 21.1dBm typical 802.11g: 24.2dBm typical 802.11n: 26.1dBm typical
Network Cables	10BASE-T: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA- 568 100-ohm STP (100 m) 100BASE-TX: 2-pair UTP Cat. 5 (100 m), EIA/TIA-568 100-ohm STP (100 m)
Frequency Range	2412 ~ 2484 MHz ISM band
Modulation Schemes	DBPSK/DQPSK/CCK/OFDM
Security	64/128-bits WEP Encryption; WPA, WPA-PSK, WPA2, WPA2-PSK, WPS
Management	Web based Configuration, Command Line Interface (CLI) via Telnet, TR-069 Remote Management, SNMP Support

Channels	1~11 Channels (FCC) 1~13 Channels (ETSI)
Number of Ports	LAN: 4 x 10/100Mbps Auto-MDIX Fast Ethernet port WAN: 1 x RJ11Port

Physical and Environmental	
DC inputs	12VDC 1A
Power Consumption	7.38watts (max)
Temperature	Operating: 0^{o}C ~ 40^{o} C, Storage: -10^{o} ~ 70^{o} C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	195 x 120 x 30mm
EMI:	FCC part 15, FCC part 68, CE