4 Port 11g Wireless ADSL2/2+ Router

User Manual

For Annex A/B

Contents

1 System Overview 5

1.1 General Description 5
1.2 Specifications 6
1.2.1 ADSL Standard Compliance 6
1.2.2 ATM and PPP Protocols 6
1.2.3 Network Protocols & Features 6
1.2.4 Bridging 7
1.2.5 IEEE 802.11g Wireless Standards 7
1.2.6 Management 7
1.2.7 Ethernet Standards 7
1.3 Scope 8
1.4 Audience 9
1.5 Document Structure 10
1.6 System Requirement 11
1.7 Packet Contents 12

2 Knowing The 4 Ports 11g Wireless ADSL2/2+ Router 13

2.1 Front Panel: 13
2.2 Back Panel: 14
2.3 Side Panel: 15
2.4 Connection Mechanism: 16

3 Software Configuration 18

3.1 Setup Wizard 20
3.2 LAN Configuration 24
3.3 Wireless Configuration 25
3.3.1 Basic Setting 25
3.3.2 Advanced Settings 27
3.3.3 Security 30
3.3.4 Access Control 32
3.3.5 WDS 34
3.3.6 MBSSID 36
3.4 WAN Configuration 38

3.4.1 Channel Configuration 38
3.4.2 ATM Setting 40
3.4.3 ADSL Setting 42
3.5 Services Configuration 44
3.5.1 DHCP Mode 44
3.5.2 DHCP Server Configuration 45
3.5.3 DHCP Relay Configuration 46
3.5.4 DNS Configuration 47
3.5.4.1 DNS Server 47
3.5.4.2 Dynamic DNS 48
3.5.5 Firewall Configuration 50
3.5.5.1 IP/Port Filtering 50
3.5.5.2 MAC Filtering 52
3.5.5.3 Port Forwarding 54
3.5.5.4 URL Blocking 56
3.5.5.5 DMZ 58
3.5.6 IGMP Proxy Configuration 59
3.5.7 UPnP Configuration 61
3.5.8 RIP Configuration 63
3.6 Advance Configuration 65
3.6.1 Bridging 65
3.6.2 Routing 66
3.6.3 SNMP Configuration 68
3.6.4 Port Mapping 70
3.6.5 IP QoS 72
3.6.6 Remote Access 74
3.6.7 Other Advanced Configuration 75
3.7 Diagnostic 77
3.7.1 Ping 77
3.7.2 ATM Loopback 78
3.7.3 ADSL 79
3.7.4 Diagnostic Test 80
3.8 Admin 81
3.8.1 Commit/Reboot 81
3.8.2 Backup/Restore 82
3.8.3 System Log 83
3.8.4 Password 84
3.8.5 Upgrade Firmware 85

3.8.6 ACL 86
3.8.7 Time Zone 87
3.9 Statistics 88
3.9.1 Interfaces 88
3.9.2 ADSL 89

Appendix A: Protocol Stacks 90

Appendix B: Frequently Asked Questions 95

Appendix C: Troubleshooting Guide 97

Appendix D: Glossary 100

1 System Overview

1.1 General Description

Congratulations on your purchase of this outstanding 4-Ports 11g Wireless ADSL2/2+ Router. This device is an IEEE 802.11g Wireless and 4 Port Switch built-in ADSL 2/2+ Router that allows ADSL/ADSL2/ADSL2+ connectivity while providing Wireless LAN capabilities for residential, industries and SOHO environments. Wireless-G or the so-called 11g is the upcoming 54Mbps wireless networking standard that's almost 5 times faster than the widely deployed Wireless-B or the so-called 11b products found in homes, businesses, and public wireless hotspots around the world.

ADSL2/2+ is a transmission technology used to carry user data over a single twisted-pair line between the Central Office and the Customer Premises. The downstream data rates can go up to 24 Mbps and the upstream data rates can go up to 1Mbps with length reach up to 22Kft for ADSL2/2+ connection and 54Mbps transfer data rate for the 11g connection. This device allows ADSL2/2+ connectivity while providing Wireless LAN capabilities for home or office users. This asymmetric nature lends itself to applications such as Internet access and video delivery. With minimum setup, you can install and use the router within minutes.

1.2 Specifications

1.2.1 ADSL Standard Compliance

- Full rate ANSI T1.413 Issue2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant.
- ITU G.992.3, ITU G.992.5 and READSL2 ADSL2/2+ standards compliant.
- Support ADSL2/2+ Annex L and Annex M features.
- Downstream and Upstream data rates up to 24Mbps and 1Mbps.
- Reach length up to 22Kft.

1.2.2 ATM and PPP Protocols

- Support ATM AAL0, AAL2 & AAL5.
- Support OAM F4/F5 loop back.
- Support up to 8PVCs.
- Multiple Protocols over AAL5 (RFC 2684 / RFC 1483).
- Support Bridged and Routed Ethernet Encapsulation.
- Support VC and LLC based Multiplexing.
- Support PPPoA (RFC 2364) standard.
- Support PPPoE (RFC 2516) standard.
- Support UBR, CBR, rt-VBR and nrt-VBR Traffic shaping QoS.

1.2.3 Network Protocols & Features

- IP Routing – RIPv1 and RIPv2.
- Support Static Routing.
- Support DHCP Server, Relay and Client.
- Support DNS Relay.
- Support SNMP functionality.
- Support IP QoS features.
- Support IGMP functionality
- Support IP Filter and MAC Filter functionality
- URL Blocking features supported.
- Support Port Forwarding features.
- Support Port Triggering features.
- Support DMZ functionality.
- Support VPN Pass-Through.
- Built-in Diagnostic Tools.

- Built-in Firewall features.

1.2.4 Bridging

- Support IEEE 802.1d Transparent Bridging.
- Support WAN Bridge functionality.
- Support MAC Learning Address features.

1.2.5 IEEE 802.11g Wireless Standards

- IEEE 802.11b/g standards compliant.
- Support data rates up to 54Mbps (Auto-Rate Capable).
- Support OFDM (64QAM, 16QAM, QPSK, BPSK) and DSSS (DBPSK, DQPSK, CCK) modulation.
- Conforms to Wireless Ethernet Compatibility Alliance (WECA) Wireless Fidelity (Wi-Fi) Standard.
- Support WEP/WPA/WPA2/802.1X Encryption for data security.
- Support Wireless Access Control functionality.
- Support WDS features.
- Support 2.412GHZ ~ 2.484GHz frequency ranges.

1.2.6 Management

- Web-based Configuration / Management.
- Support FTP/TFTP/Telnet Management / Configuration.
- Support Remote Access Management / Configuration.
- Firmware upgrade and Reset to default via Web management.
- Restore factory default setting via Web or hardware reset button.
- WAN and LAN connection statistics.
- Support Password Authentication.
- Device System Log.

1.2.7 Ethernet Standards

- Built-in 4 Ports 10/100Mbps Ethernet Switch which compliant with IEEE 802.3x standards
- Automatic MDI/MDI-X crossover for 100 BASE-TX and 10 BASE-T ports.
- Auto-negotiation and speed-auto-sensing support.
- Port based VLAN supported in any combination.

1.3 Scope

This document provides the descriptions and usages for the 4 Ports 11g Wireless ADSL2/2+ Router's Web pages that are used in the configuration and setting process. Both basic and advanced descriptions and concepts are discussed. To help the reader understand more about these Web pages, some questions and answers (Q&A) are appended after the definition of each Web page along with the appendices at the end of the guide.

1.4 Audience

This document is prepared for use by those customers who purchase the 4 Ports 11g Wireless ADSL2/2+ Router and using the provided or embedded firmware. It assumes the reader has a basic knowledge of ADSL/ADSL2/ADSL2+, Wireless and networking.

1.5 Document Structure

Chapter 1: Introduction, provides a brief introduction to the product and user guide.

Chapter 2: Knowing The 4 Ports 11g Wireless ADSL2/2+ Router, provides device specifications and hardware connection mechanism.

Chapter 3: Setting Up TCP/IP In Windows, provides Windows system Network's configurations.

Chapter 4: Device Administration, describes the pages found under the Admin menu. These pages allow the user to view, change, edit, update, and save the 4 Ports 11g Wireless ADSL2/2+ Router's configurations or settings.

Appendix A: Router Terms, provides an introduction to basic Router Terms.

Appendix B: Frequently Asked Questions, is a compilation of useful questions regarding the 4Ports 11g Wireless ADSL2/2+ Router.

Appendix C: Troubleshooting Guide, is a compilation of questions and answers relating to common problems dealing with Windows networking and the 4 Ports 11g Wireless ADSL2/2+ Router Configurations.

Appendix D: Glossary, provides definitions of terms and acronyms of this 4 Ports 11g Wireless ADSL2/2+ Router.

1.6 System Requirement

Check and confirm that your system confirm the following minimum requirements:

- Personal computer (PC/Notebook).
- Pentium III compatible processor and above.
- Ethernet LAN card or IEEE 802.11b or IEEE 802.11g Wireless adaptor installed with TCP/IP protocol.
- USB Port (Optional)
- 64 MB RAM or more.
- 50 MB of free disk space (Minimum).
- Internet Browser.
- CD-ROM Drive.

1.7 Packet Contents

The 4 Ports 11g Wireless ADSL2/2+ Router package contains the following items:

- One 4 Ports 11g Wireless ADSL2/2+ Router
- One Power Adapter
- One RJ-11 ADSL Cable
- One CAT-5 Ethernet Cable
- One CD-ROM (Driver / Manual / Quick Setup Guide)

If any of the above items are damaged or missing, please contact your dealer immediately.

2 Knowing The 4 Ports 11g Wireless ADSL2/2+ Router

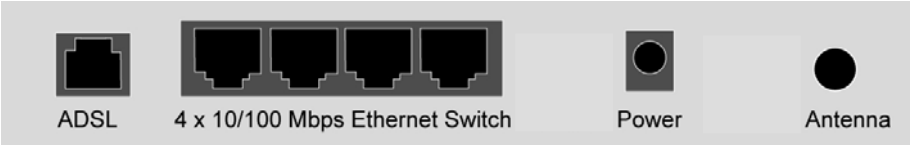
2.1 Front Panel:

The 4 Ports 11g Wireless ADSL2/2+ Router's LEDs indicators display information about the device's status.

PWR	Lights up when 4 Ports 11g Wireless ADSL2/2+ Router is powered on.
WL ACT	Lights up when Wireless system is ready.
	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is sending/receiving data.
1	Blinking when Port 1 of this 4 Ports 11g Wireless ADSL2/2+ Router is Sending or Receiving data.
2	Blinking when Port 2 of this 4 Ports 11g Wireless ADSL2/2+ Router is Sending or Receiving data.
3	Blinking when Port 3 of this 4 Ports 11g Wireless ADSL2/2+ Router is Sending or Receiving data.
4	Blinking when Port 4 of this 4 Ports 11g Wireless ADSL2/2+ Router is Sending or Receiving data.
ADSL	Lights up when a successful ADSL2/2+ connection is established.
	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is sending/receiving data.
PPP	Lights up when a PPP connection is established.

2.2 Back Panel:

The back panel of the 4 Ports 11g Wireless ADSL2/2+ Router contains ADSL, Ethernet Switches, Reset, Power Adapter connection and 2.4GHz Dipole Antenna connector.



ADSL	Port for connecting to the ADSL2/2+ Service Provider.
Ports 1~4	Four 10/100Mbps Ethernet Ports for connecting to the network devices
Power	Power adapter connector.
Antenna	2.4GHz Dipole Antenna.

All the Ethernet port of the 4 Ports 11g Wireless ADSL2/2+ Router supports auto-crossover capability.

2.3 Side Panel:

RESET Button:
Reboot & Restore the 4 Ports 11g Wireless ADSL2/2+ Router to factory defaults.

Reboot and Resetting Factory Defaults:

The reboot and restore to factory defaults feature will set the device to its factory default configuration by resetting the 4 Ports 11g Wireless ADSL2/2+ Router.

To **Reboot** the 1-Port ADSL 2/2+ Router :

Ensure that the device is powered on. Press the Reset button for **2~5** seconds to reboot the device.

To **Reset** the 1-Port ADSL 2/2+ Router **to default setting**:

- Ensure that the device is powered on.
- Press the Reset button for **5~15** seconds and release. The LED indicators will turns OFF and ON again indicates that the reset is in progress. Do not power off the device during the reset process.
- Reset is completed when the LED indicator return to steady green. The default settings are now restored.

2.4 Connection Mechanism:

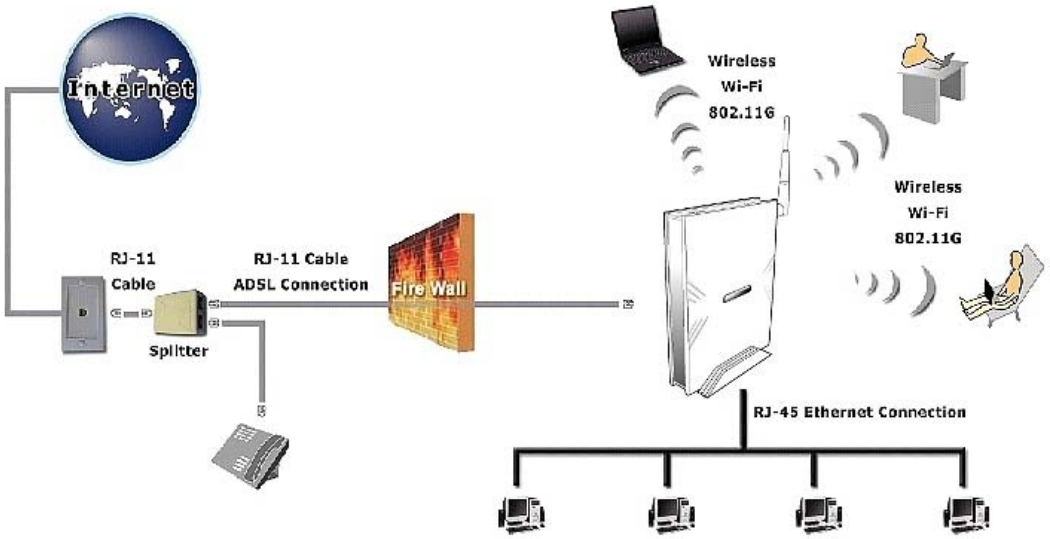
This section describes the hardware connection mechanism of 4 Ports 11g Wireless ADSL2/2+ Router on your Local Area Network (LAN) connected to the Internet, how to configure your 4 Ports 11g Wireless ADSL2/2+ Router for Internet access or how to manually configure your Internet connection.

You need to prepare the following items before you can establish an Internet connection through your 4 Ports 11g Wireless ADSL2/2+ Router:

1. A computer/notebook which must have an installed Ethernet Adaptor and an Ethernet Cable, or
2. A computer/notebook which have Wireless-b or Wireless-g wireless adaptor properly installed.
3. ADSL/ADSL2/ADSL2+ service account and configuration information provided by your Internet Service Provider (ISP). You will need one or more of the following configuration parameters to connect your 4 Ports 11g Wireless ADSL2/2+ Router to the Internet:

    a. VPI/VCI parameters
    b. Multiplexing Method or Protocol Type or Encapsulation Type
    c. Host and Domain Names
    d. ISP Login Name and Password
    e. ISP Domain Name Server (DNS) Address
    f. Fixed or Static IP Address.

Figure below shows the overall hardware connection mechanism of your 4 Ports 11g Wireless ADSL2/2+ Router.



Following are the steps to properly connect your 4 Ports 11g Wireless ADSL2/2+ Router:

1. Turn off your computer/notebook.
2. Connect the ADSL port of your 4 Ports 11g Wireless ADSL2/2+ Router to the wall jack of the ADSL/ADSL2/ADSL2+ Line with a RJ-11 cable.
3. Connect the Ethernet cable (RJ-45) from your 4 Ports 11g Wireless ADSL2/2+ Router (Switch) to the Ethernet Adaptor in your computer.
4. Connect the Power adaptor to the 4 Ports 11g Wireless ADSL2/2+ Router and plug it into a Power outlet.

The Power light will lit after turning on the 4 Ports 11g Wireless ADSL2/2+ Router.
Auto and self-diagnostic process will turn the LED indicators ON and OFF during the process.

Use the Power Adaptor exclusively in combination with the equipment supplied and do not use any other kind of power adaptor for the equipment.

5. Turn on your computer.
6. Refer to the next section to setup or configure your system's Network Adaptor.

3 Software Configuration

The DSL device is an ADSL wireless router. When you power on the device, the system will boot up and connect to ADSL automatically. The system provides a PVC for bridge test by default. The default configurations for the system are listed below.

- LAN IP address: 192.168.1.1, NetMask:255.255.255.0
- UART setting: 115200bps, 8 bits, no parity, 1 stop bit, no flow control.
- VPI/VCI for ATM: 0/35.
- ADSL Line mode: Auto-detect.

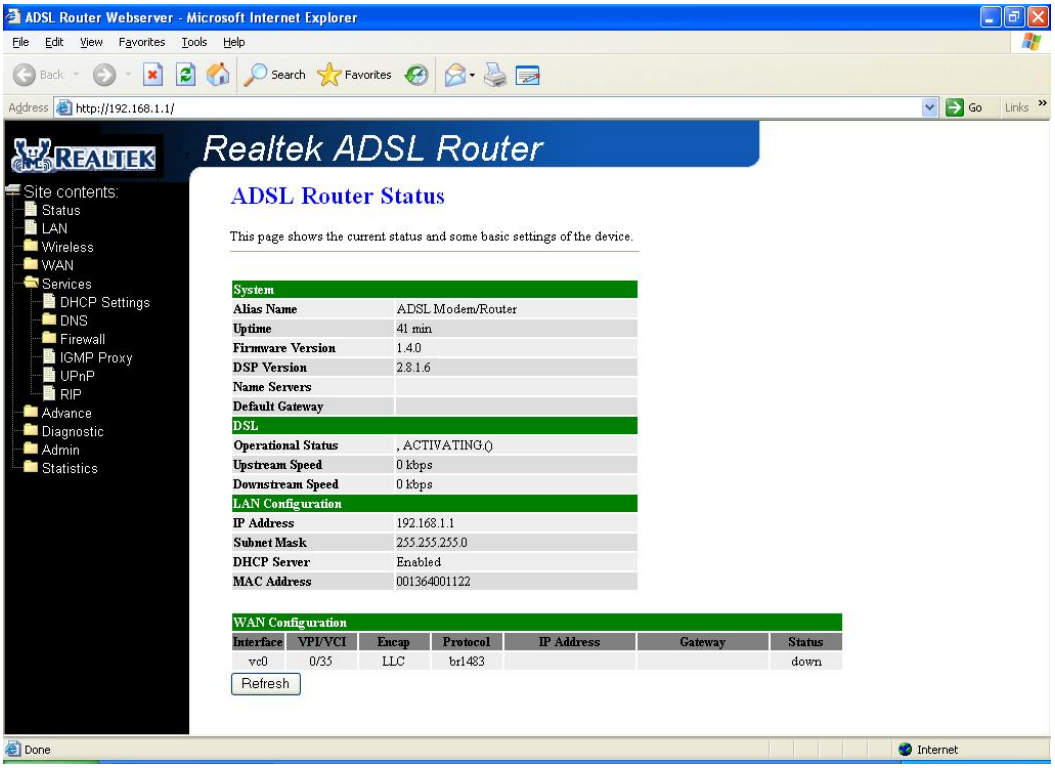
User can change settings via web browser. The following sections describe the set up procedures. Please set your PC's Ethernet port as follow:

- IP address: 192.168.1.XXX
- NetMask:255.255.255.0

Access the Web Console:

- Start your web browser.
- Type the Ethernet IP address of the modem/router on the address bar of the browser. Default IP address is 192.168.1.1.
- The **Enter Network Password** dialog box appears. Type the user name and password and then click OK. Default admin user name/password is "**admin/admin**".

Once you have connected to ADSL router. You will see the status page.



This page displays the ADSL modem/router's current status and settings. This information is read-only except for the PPPoE/PPPoA channel for which user can connect/disconnect the channel on demand. Click the "Refresh" button to update the status

Function buttons in this page:

Connect / **Disonnect**

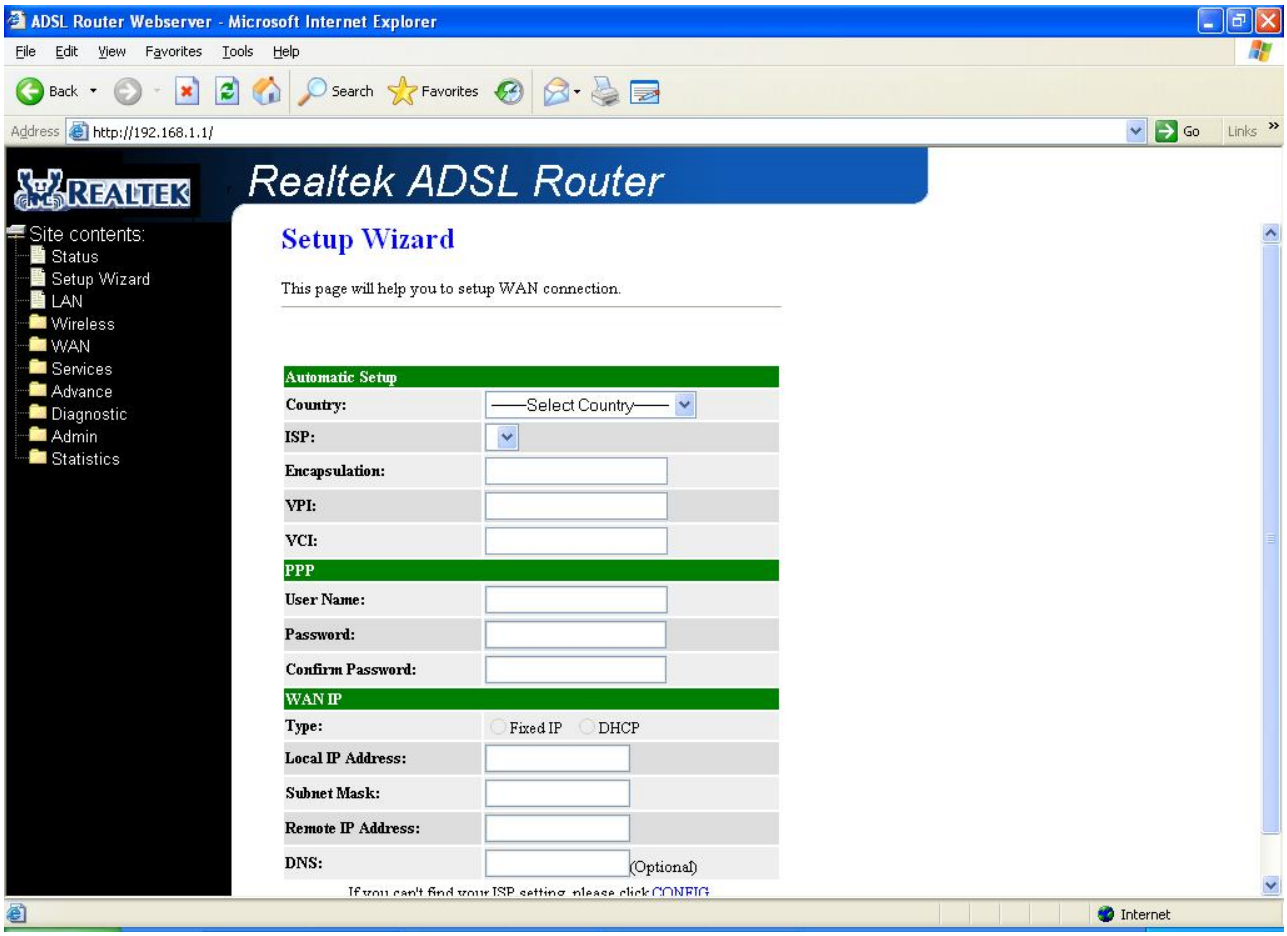
The two buttons take effect only when PVC is configured as PPPoE/PPPoA mode. Click Connect/Disconnect button to connect/disconnect the PPP dial up link.

.

3.1 Setup Wizard

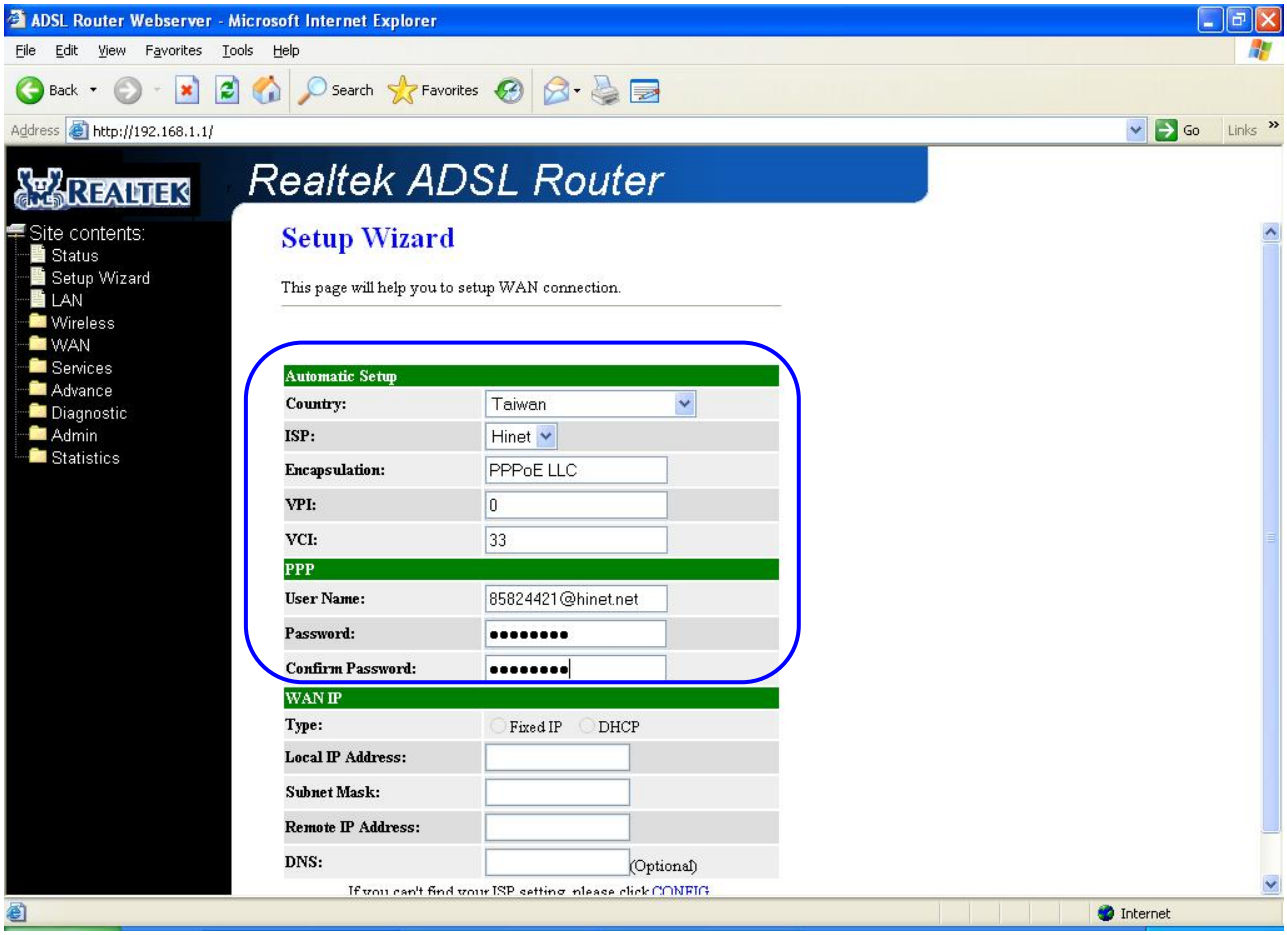
The **Setup Wizard** is a presetting wizard which meant to help you install the 4-Ports 11g Wireless ADSL2/2+ Router quickly and easily.

Click on **"Setup Wizard"** and the following screen will pop-up:



Follow the description below to complete your first time installation.

Select your country from the **Country** list and the ADSL service provider from the **ISP** List (If there are more than two ISP in your country) and note the **"Encapsulation"** type and **"VPI & VCI"** setting.



Click "CONFIG" if you can't find any available parameters from the presetting country list.
Check your ISP immediately for the setting/configuration details.

- For countries with the following **Encapsulation** type, you will enter in to set PPP Username and Password window as shown below:
  - ☑ **PPPoA VC-Mux**
  - ☑ **PPPoA LLC**
  - ☑ **PPPoE VC-Mux**
  - ☑ **PPPoE LLC**

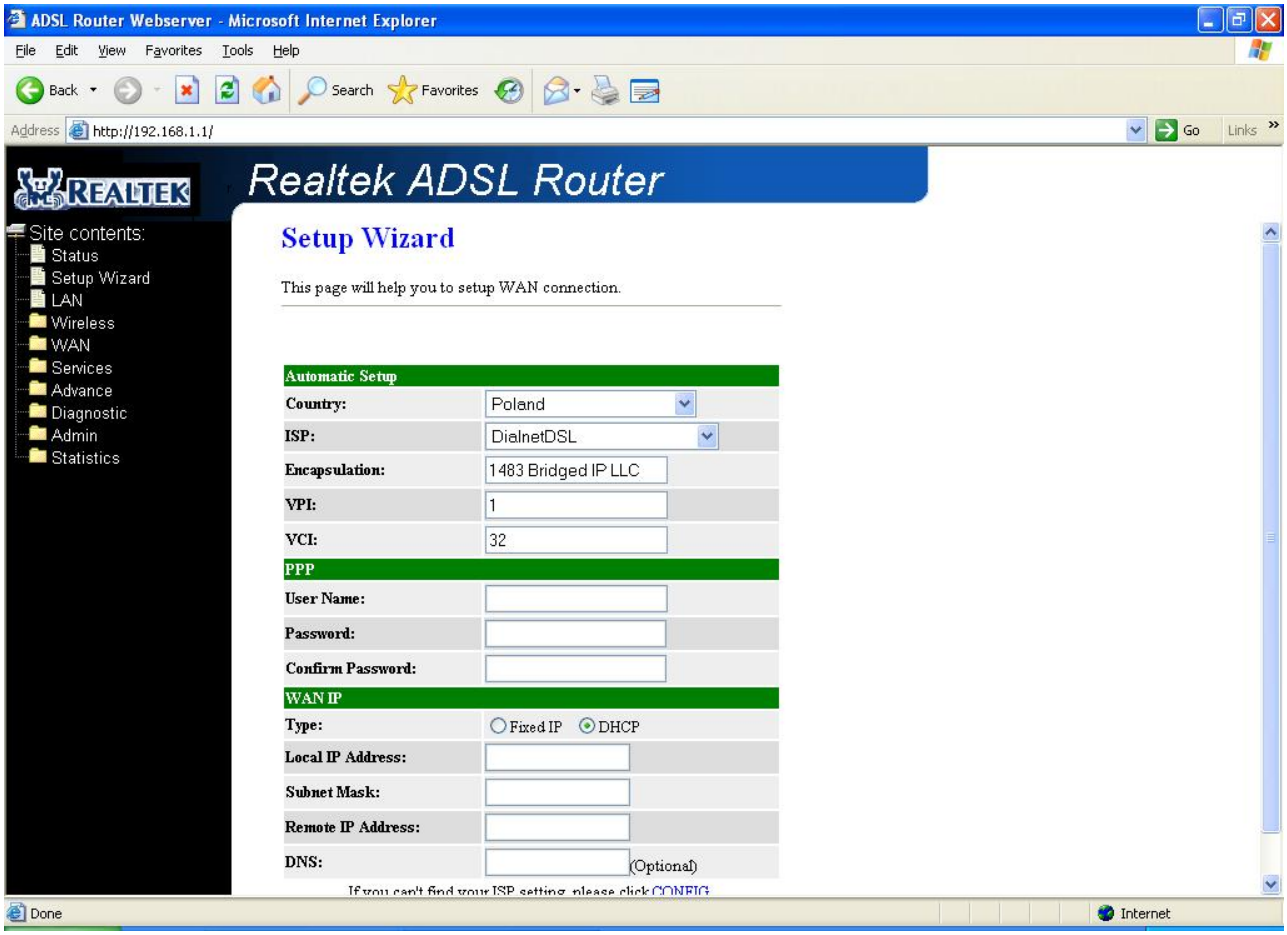
Manually enter your **"Username"** and **"Password"** which will be provided by your Service Provider (ISP). Click **"Save"** after setup. The following window display indicates the save setting process.

◆ For countries with the following **"Encapsulation"**, you need to type in all the information that your ISP provides for this protocol:

- ☑ **1483 Routed IP VC-Mux**
- ☑ **1483 Routed IP LLC**
- ☑ **1483 Bridged IP VC-Mux**
- ☑ **1483 Bridged IP LLC**

In this current window, you will find **TWO** different **Connection Type**:

- **Fixed IP** : Click the radio button to enable **Fixed IP** option then Manually enter the **"IP Address"**, **"Mask"**, **"Default Gateway"** and **"DNS"** which will be provided by your ISP. Just click the **"Save"** button to confirm your setting.
- **DHCP** : When DHCP mode is selected, nothing to be filled under this mode. Just click the **"Save"** button to confirm your setting.



- Static IP Address: **This is the static IP Address given by the ISP.**

Range for IP Address is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.

- Subnet Mask: **This is the subnet mask provided by the ISP.**

Range for Subnet Mask is x.x.x.x, where 0 ≦ x ≦ 255.

- Remote IP Address: **This is your gateway IP address.**

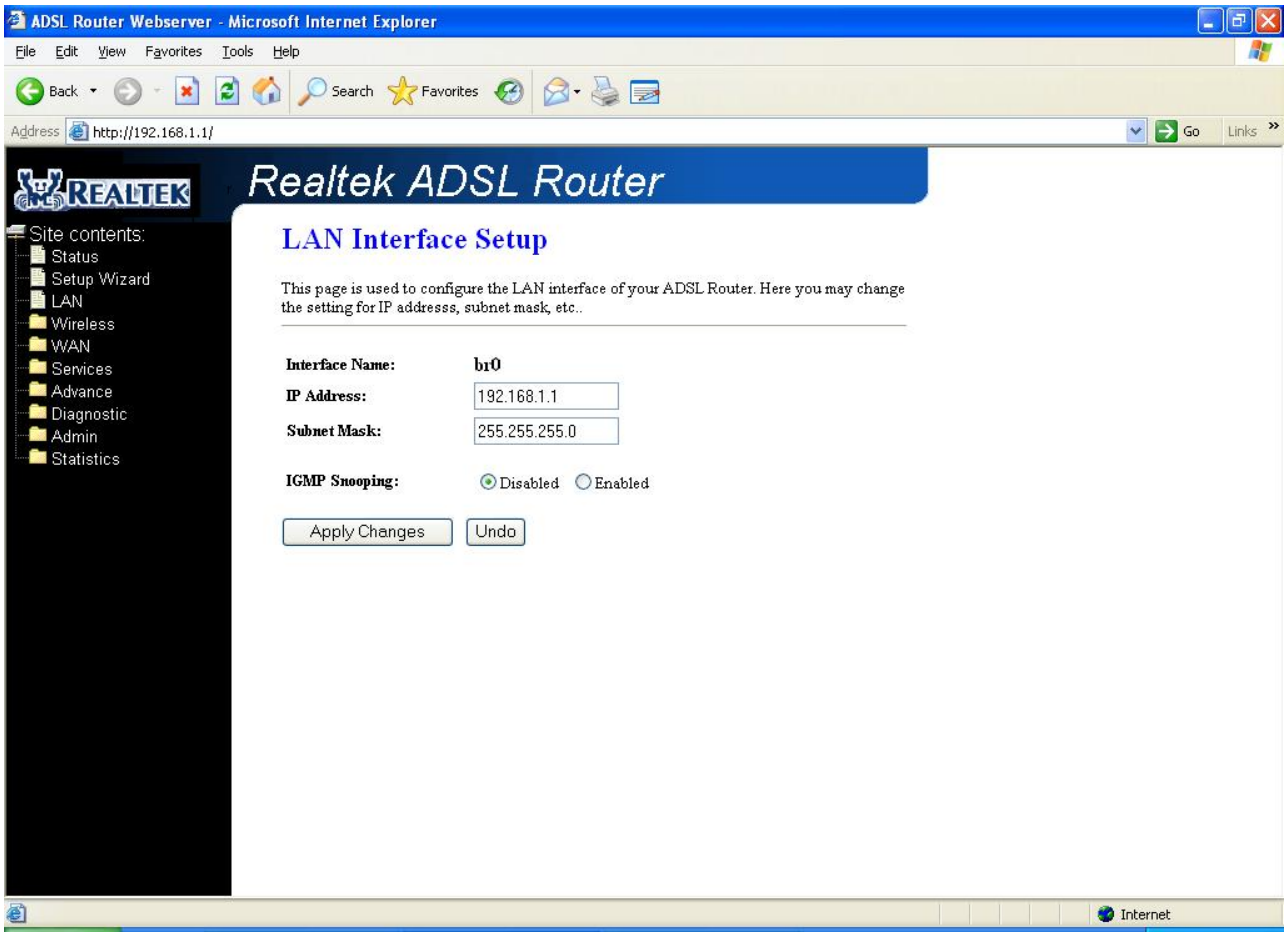
  Range for Gateway is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.

- DNS: **This is the DNS address specify by the user or ISP. Check your ISP for setting detail.**

  Range for DNS Address is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.

3.2 LAN Configuration

This page shows the current setting of LAN interface. You can set IP address, subnet mask, and IGMP Snooping for LAN interface in this page.



Fields in this page:

Field	Description
IP Address	The IP address your LAN hosts use to identify the device's LAN port.
Subnet Mask	LAN subnet mask.
IGMP Snooping	Enable/disable the IGMP snooping function for the multiple bridged LAN ports.

Function buttons in this page:

Apply Changes

Click to save the setting to the configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

Undo

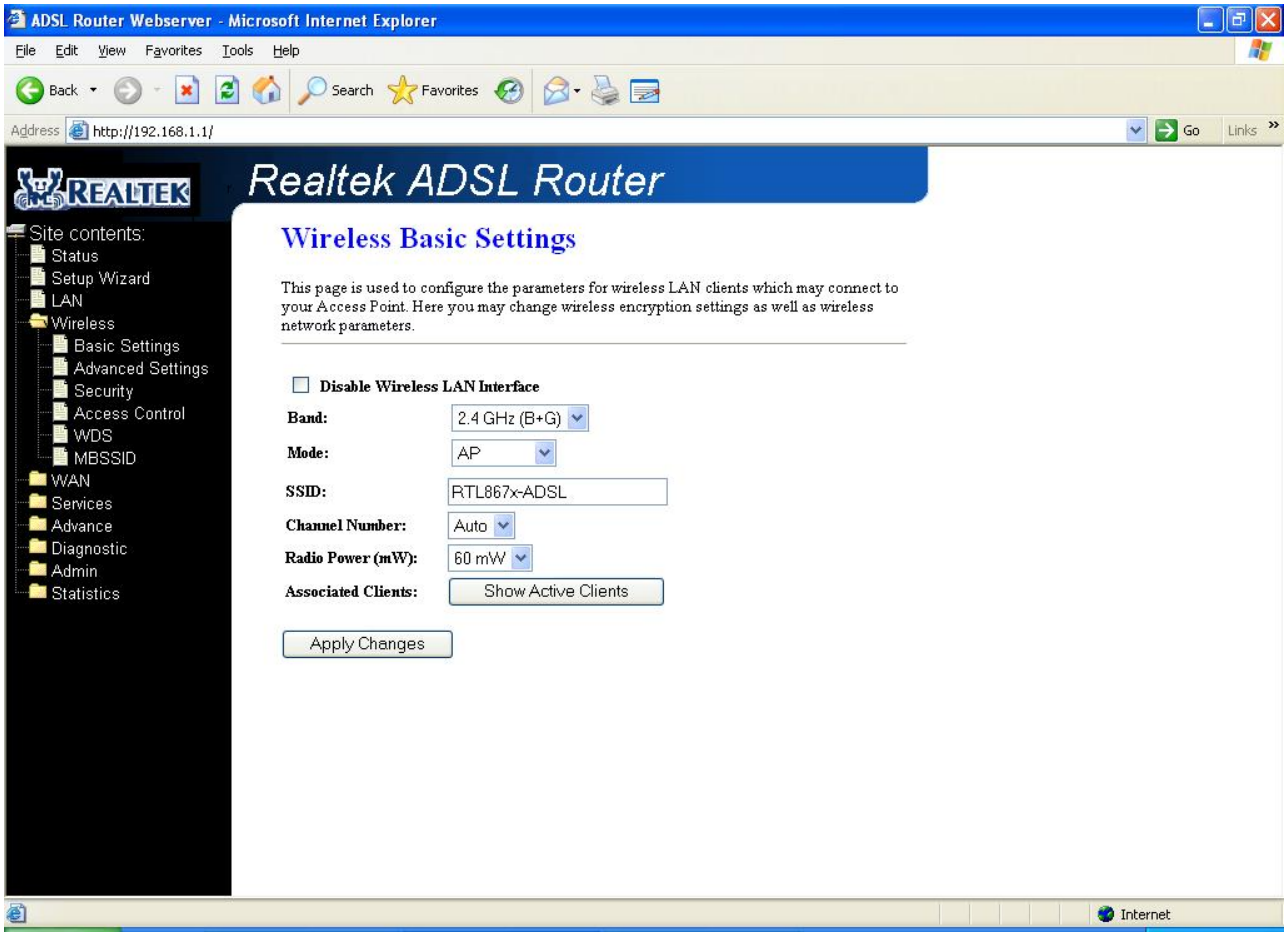
Discard your changes.

3.3 Wireless Configuration

This section provides the wireless network settings for your WLAN interface. The wireless interface enables the wireless AP function for ADSL modem.

3.3.1 Basic Setting

This page contains all of the wireless basic settings. Most users will be able to configure the wireless portion and get it working properly using the setting on this screen.



Fields in this page:

Field	Description
Disable Wireless LAN Interface	Check it to disable the wireless function for ADSL modem.
Band	Select the appropriate band from the list provided to correspond with your network setting.
Mode	The selections are: AP or AP+WDS.
SSID	The Service Set Identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. The mobile wireless

	stations shall select the same SSID to be able to communicate with your ADSL modem (or AP).
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference.
Radio Power (mW)	The maximum output power: 15mW, 30mW or 60mW.

Function buttons in this page:

Associated Clients

Click it will show the clients currently associated with the ADSL modem as below.

Apply Changes

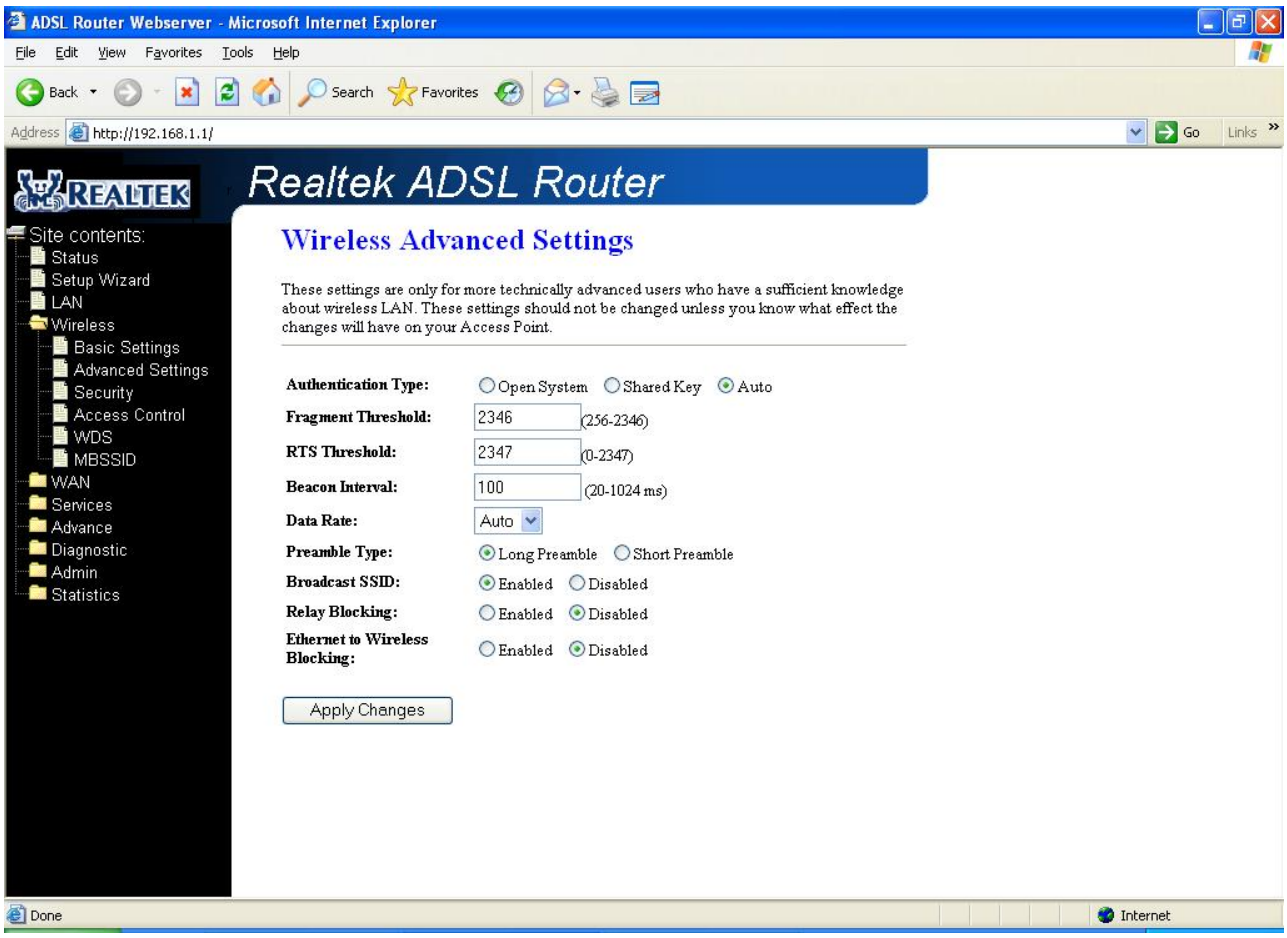
Change the settings. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

Reset

Discard your changes and reload all settings from flash memory.

3.3.2 Advanced Settings

This page allows advanced users who have sufficient knowledge of wireless LAN. These setting shall not be changed unless you know exactly what will happen for the changes you made on your DSL device.



Fields in this page:

Field	Description
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 2346. 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.
RTS Threshold	This value should remain at its default setting of 2347. 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.
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 ADSL modem (or AP) 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	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	When **Relay Blocking** is enabled, wireless clients will not be able to directly access other wireless clients.
Ethernet to Wireless Blocking	When enabled, traffic between Ethernet and wireless interfaces are not allowed.

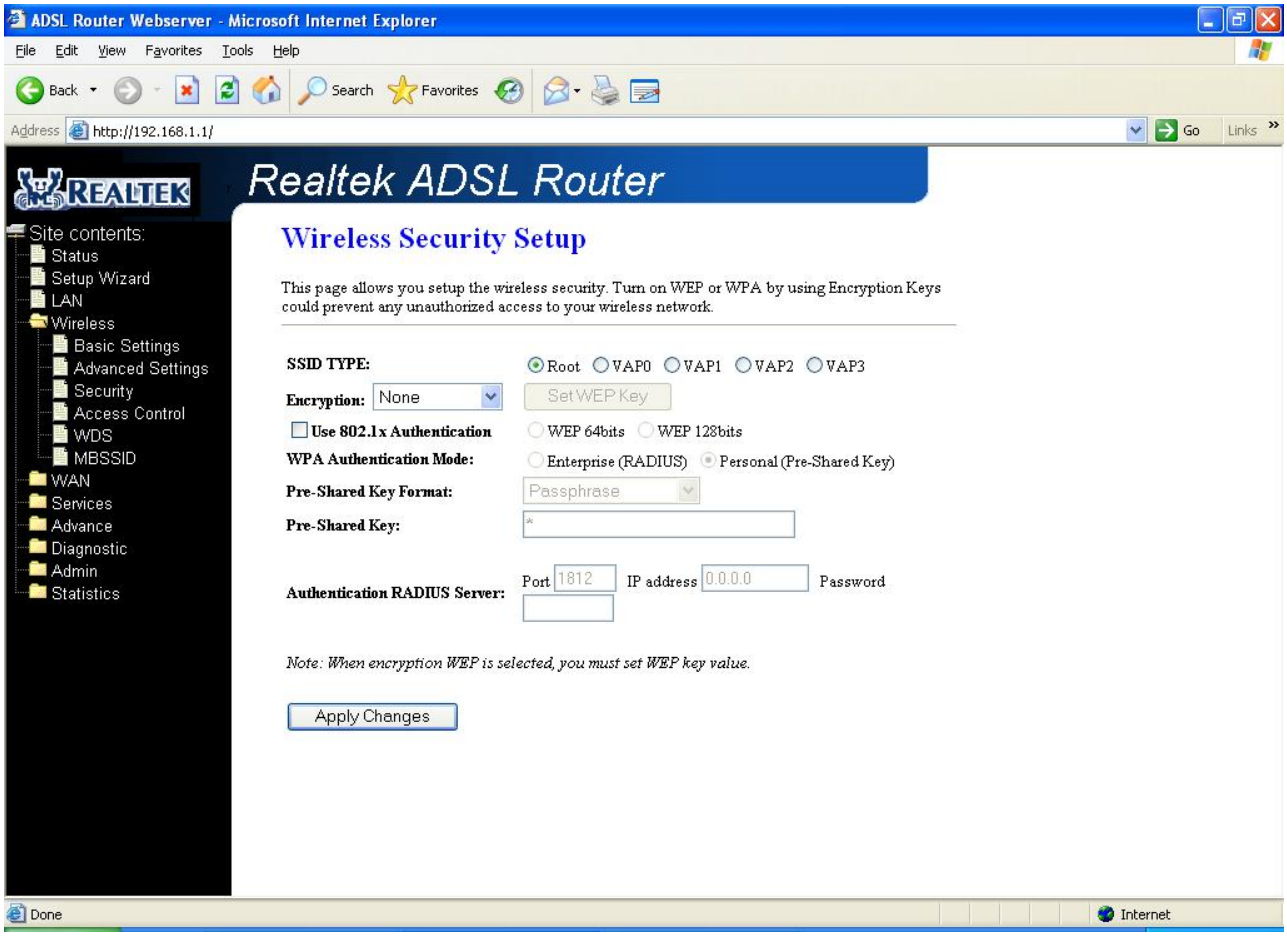
Function buttons in this page:

Apply Changes

Change the settings. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

3.3.3 Security

This screen allows you to setup the wireless security. Turn on WEP or WPA by using encryption keys could prevent any unauthorized access to your WLAN.



Fields in this page:

Field	Description
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.

Use 802.1x Authentication	Check it to enable 802.1x authentication. This option is selectable only when the "Encryption" is choose 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.*
WPA Authentication Mode	There are 2 types of authentication mode for WPA. **WPA-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. The WPA algorithm is selected between TKIP and AES, please refer to "WPA cipher Suite" below. **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.

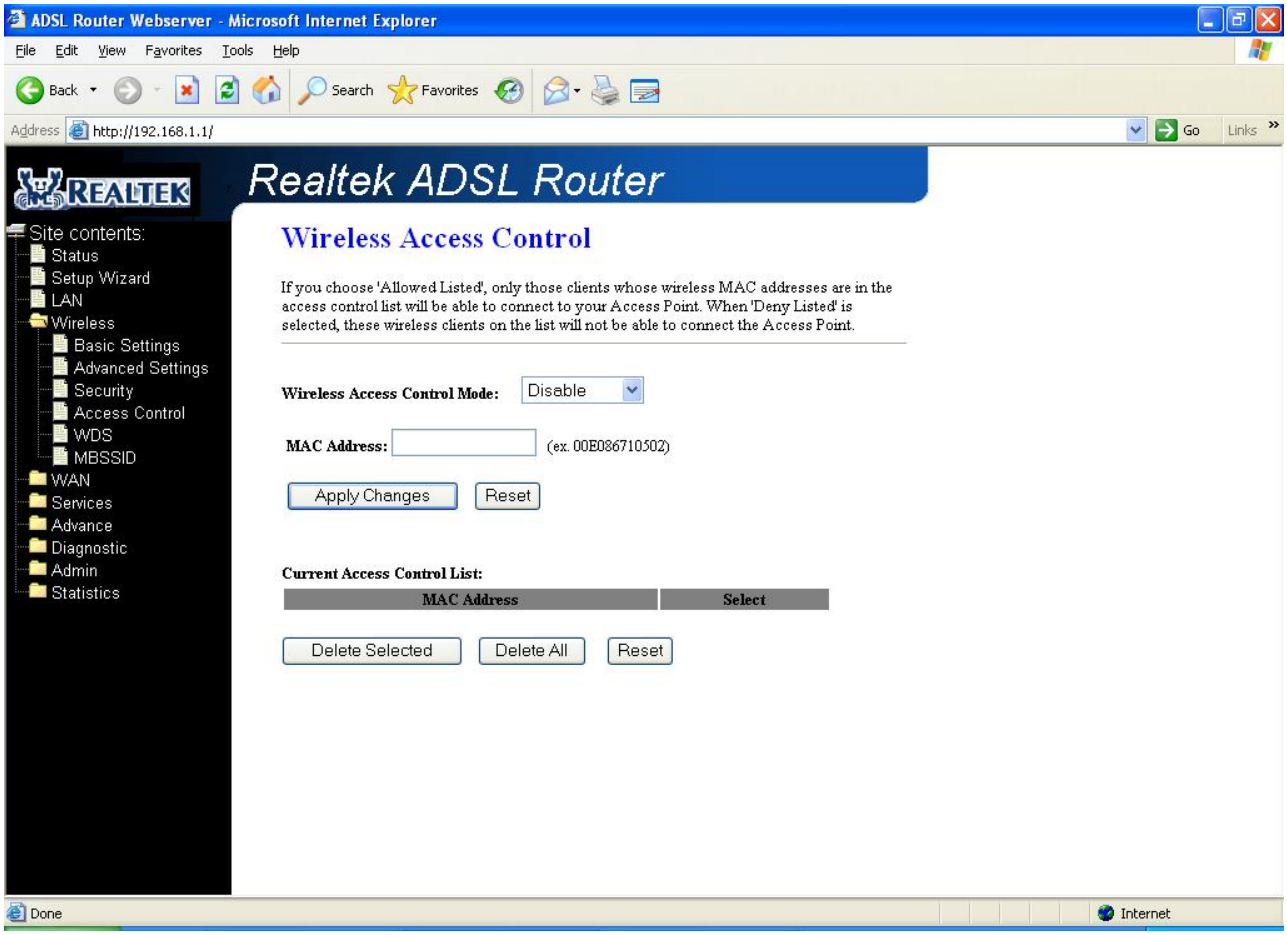
Function buttons in this page:

Apply Changes

Change the settings. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

3.3.4 Access Control

This page 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 DSL device (or AP).



Fields in this page:

Field	Description
Wireless Access Control Mode	The Selections are: **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 press “Apply Changes” button to add client MAC address into current access control list.

Function buttons for the setting block:

Apply Changes

Click to add this entry into the Current Access Control List.The Current Access Control List lists the client MAC addresses. Any wireless client with its MAC address listed in this access control list will be able to connect to the device. You can select the entries at the Select column and apply to the following function buttons.

Function buttons for the **Current Access Control List**:

Delete Selected

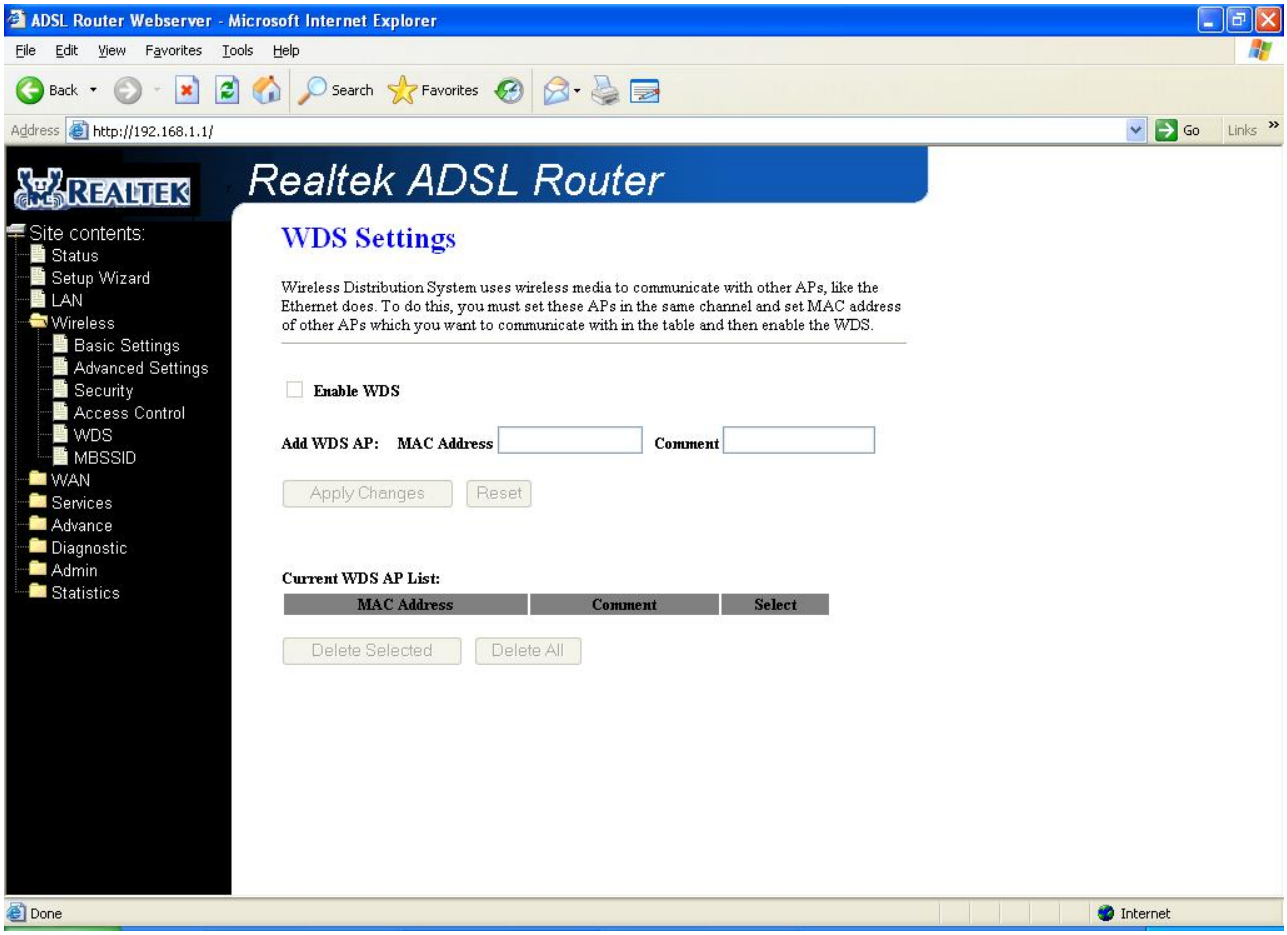
Delete the selected entries from the list.

Delete All

Flush the list.

3.3.5 WDS

Wireless Distribution System (WDS) is a system that interconnects BSS to build a premise wide network. The DSL device supports the WDS protocol, which allows a point to point link to be established between two APs. Only if you select AP+WDS mode on the Basic Settings page, this WDS page can be configured.



Fields in this page:

Field	Description
Enable WDS	Check to enable the WDS function.
Add WDS AP	This is where you enter the MAC address of the peer AP's wireless interface that you are connecting to.

Function buttons for this setting block:

Apply Changes

Click to add this entry into the **Current WDS AP List**.

The **Current WDS AP List** lists the peer MAC addresses of the WDS link. Any AP with its MAC

address listed in this WDS AP list may have a WDS link to the device. You can select the entries at the Select column and apply to the following function buttons.

Function buttons for the **Current WDS AP List**:

Delete Selected

Delete the selected entries from the list.

Delete All

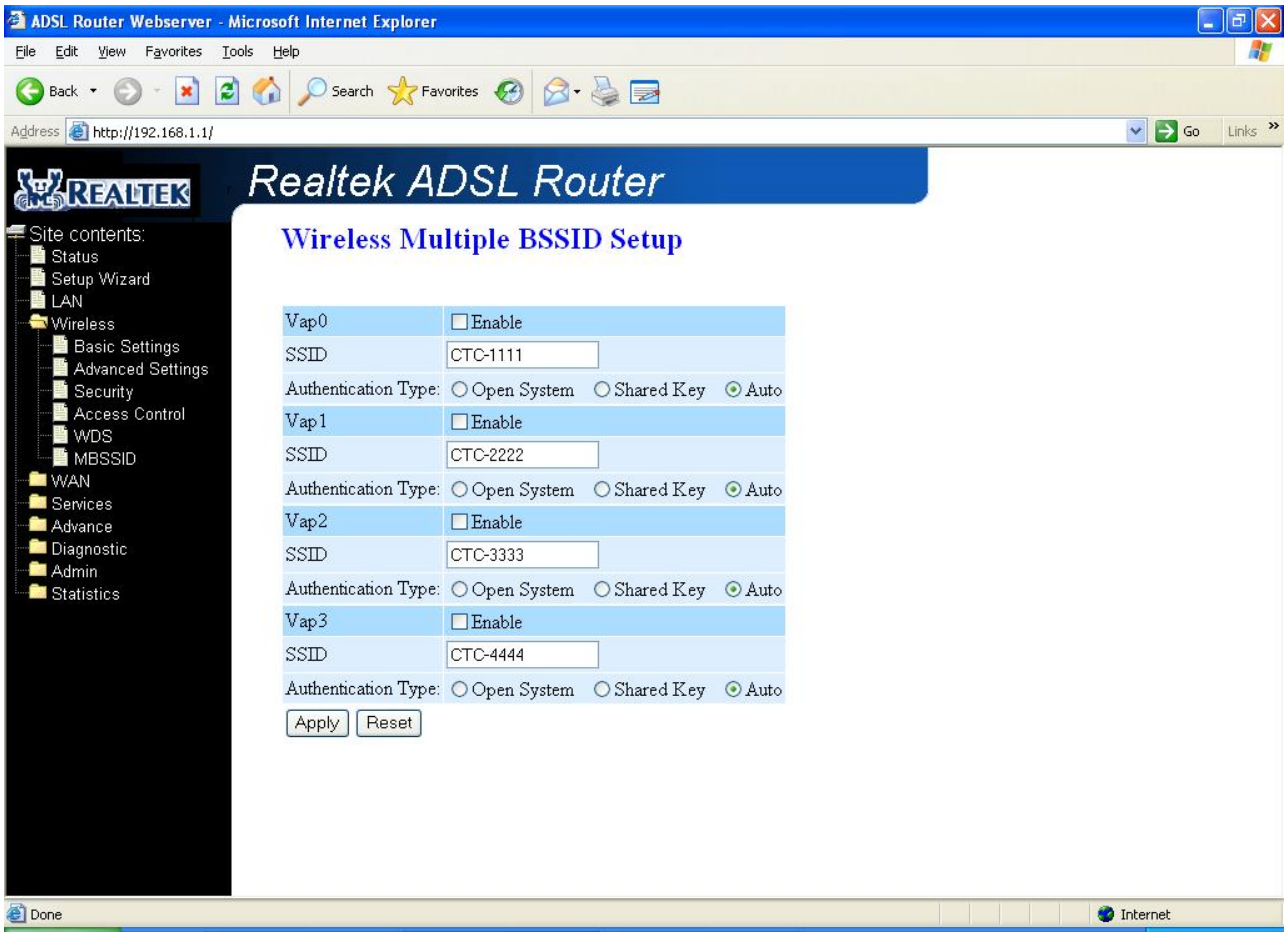
Flush the list.

3.3.6 MBSSID

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity.Multiple Broadcast service set identifier (**MBSSID**) can support 8 separate SSIDs.This logically divides the access point into several virtual access points all within a single hardware platform.is a system that interconnects BSS to build a premise wide network. You can configure your 4-Ports 11g Wireless ADSL2/2+ Router as **MBSSID** function using the **Wireless – MBSSID** page.

Here are some possible settings you could assign to each SSID:

- **Virtual Local Area Network**. If your network uses VLANs, you can assign an SSID to VLAN1, and the access point groups client devices using that SSID into VLAN1. This enables the separation of wireless applications based on security and performance requirements. For example, you could enable encryption and authentication on one SSID to protect private applications and no security on another SSID to maximize open connectivity for public usage.
- **SSID broadcasting**. In some cases, such as public Internet access applications, you can broadcast the SSID to enable user radio cards to automatically find available access points. For private applications, it's generally best to not broadcast the SSID for security reasons -- it invites intruders. Multiple SSIDs means you can mix and match the broadcasting of SSIDs.
- **Maximum number of client associations**. You can set the number of users that can associate via a particular SSID, which makes it possible to control usage of particular applications. This can help provide a somewhat limited form of bandwidth control for particular applications.



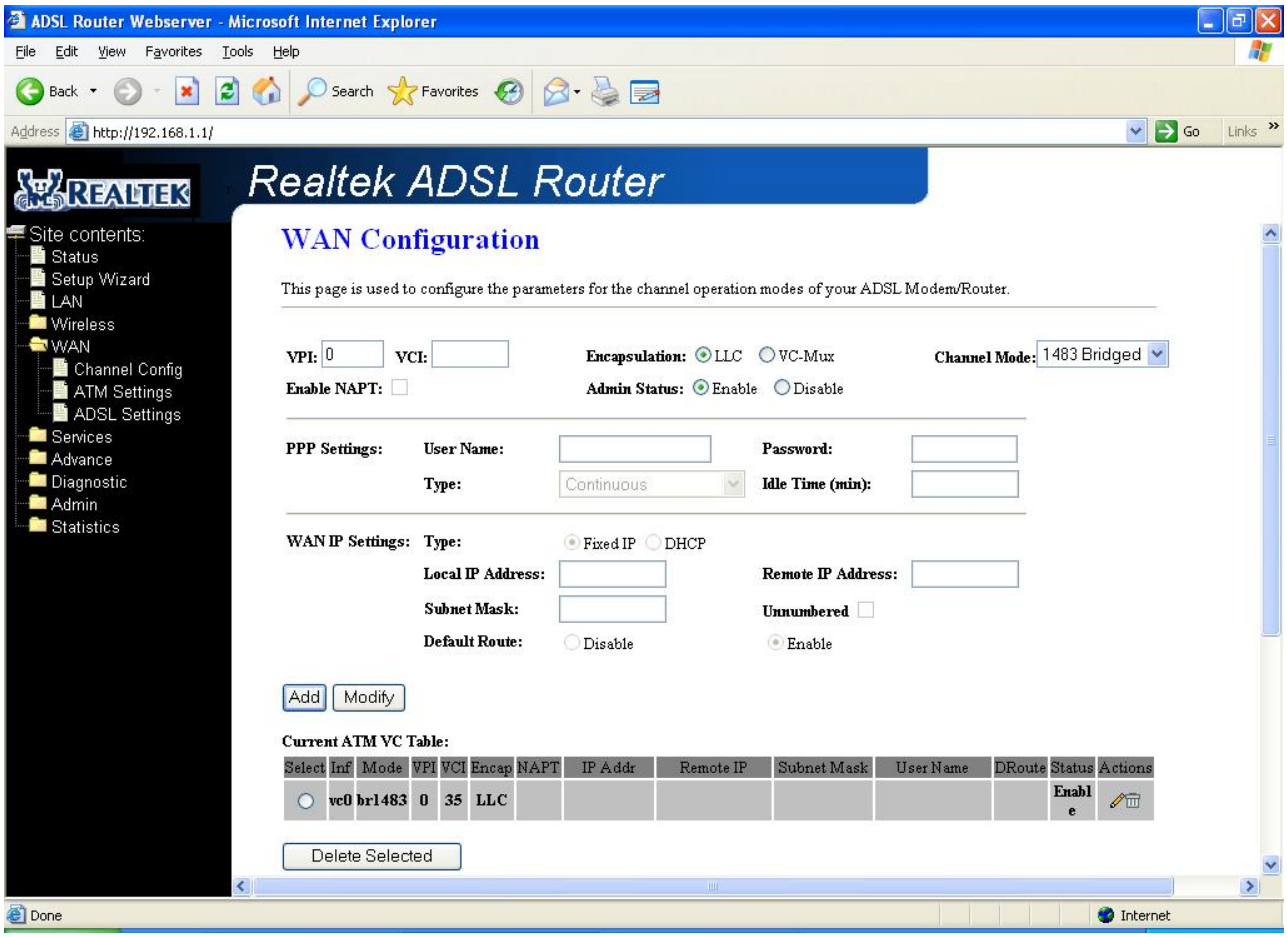
- **Enable:** Enables/disables multiple SSID.
- **SSID:** Set the SSID manually. The SSID is up to 32 characters.
- **Apply:** Click Apply to confirm your setting.
- **Reset:** Click Reset to give up all your current setting

3.4 WAN Configuration

There are three sub-menu for WAN configuration: [Channel Config], [ATM Settings], and [ADSL Settings].

3.4.1 Channel Configuration

ADSL modem/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. Please reference to the section – **Channel Mode Configuration** for details.



Function buttons in this page:

Add

Click **Add** to complete the channel setup and add this PVC channel into configuration.

Modify

Select an existing PVC channel by clicking the radio button at the **Select** column of the

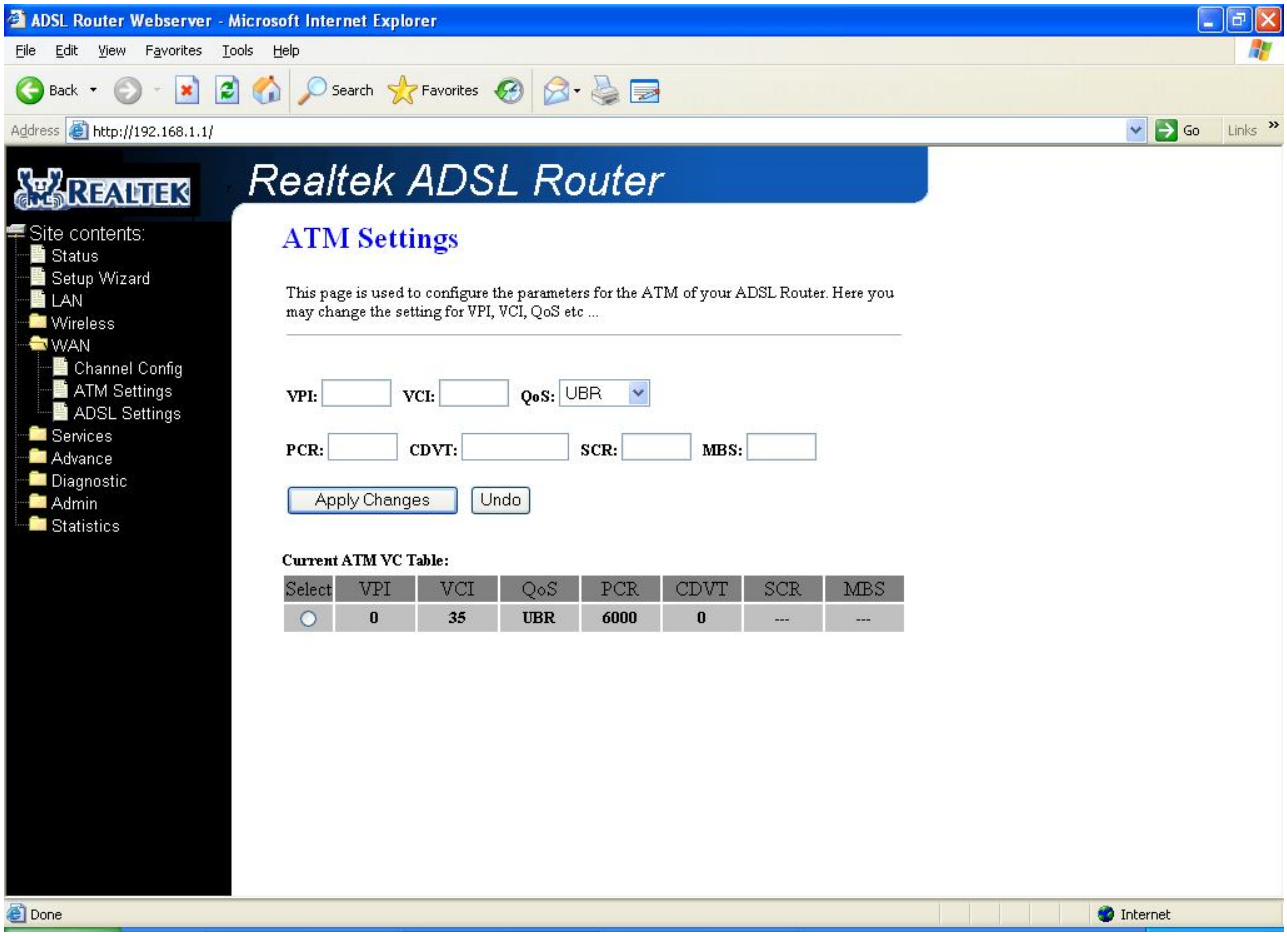
Current ATM VC Table before we can modify the PVC channel. After selecting an PVC channel, we can modify the channel configuration at this page. Click **Modify** to complete the channel modification and apply to the configuration.

Delete

Select an existing PVC channel to be deleted by clicking the radio button at the **Select** column of the **Current ATM VC Table**. Click **Delete** to delete this PVC channel from configuration.

3.4.2 ATM Setting

The page is for ATM PVC QoS parameters setting. The DSL device support 4 QoS mode —UBR/CBR/rt-VBR/nrt-VBR.



Fields in this page:

Field	Description
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.
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.

Function buttons in this page:

Apply Changes

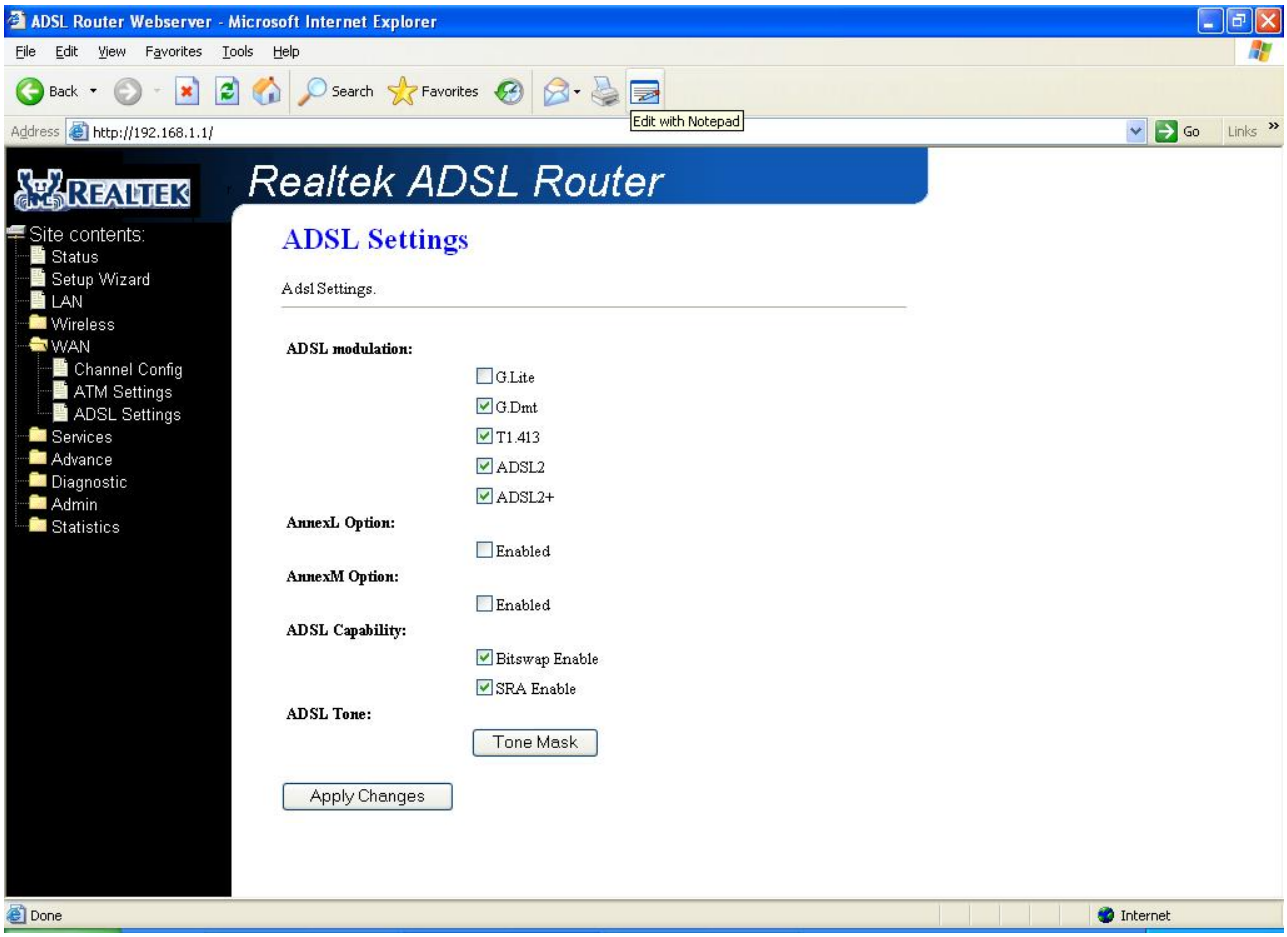
Set new PVC OoS mode for the selected PVC. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

Undo

Discard your settings.

3.4.3 ADSL Setting

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



Fields in this page:

Field	Description
ADSL modulation	Choose prefered xdsl standard protocols. 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	Enable/Disable ADSL2/ADSL2+ Annex L capability.
AnnexM Option	Enable/Disable ADSL2/ADSL2+ Annex M capability.
ADSL Capability	“Bitswap Enable” : Enable/Disable bitswap capability. “SRA Enable” : Enable/Disable SRA (seamless rate adaptation) capability.

Function buttons in this page:

Tone Mask

Choose tones to be masked. Mased tones will not carry any data.

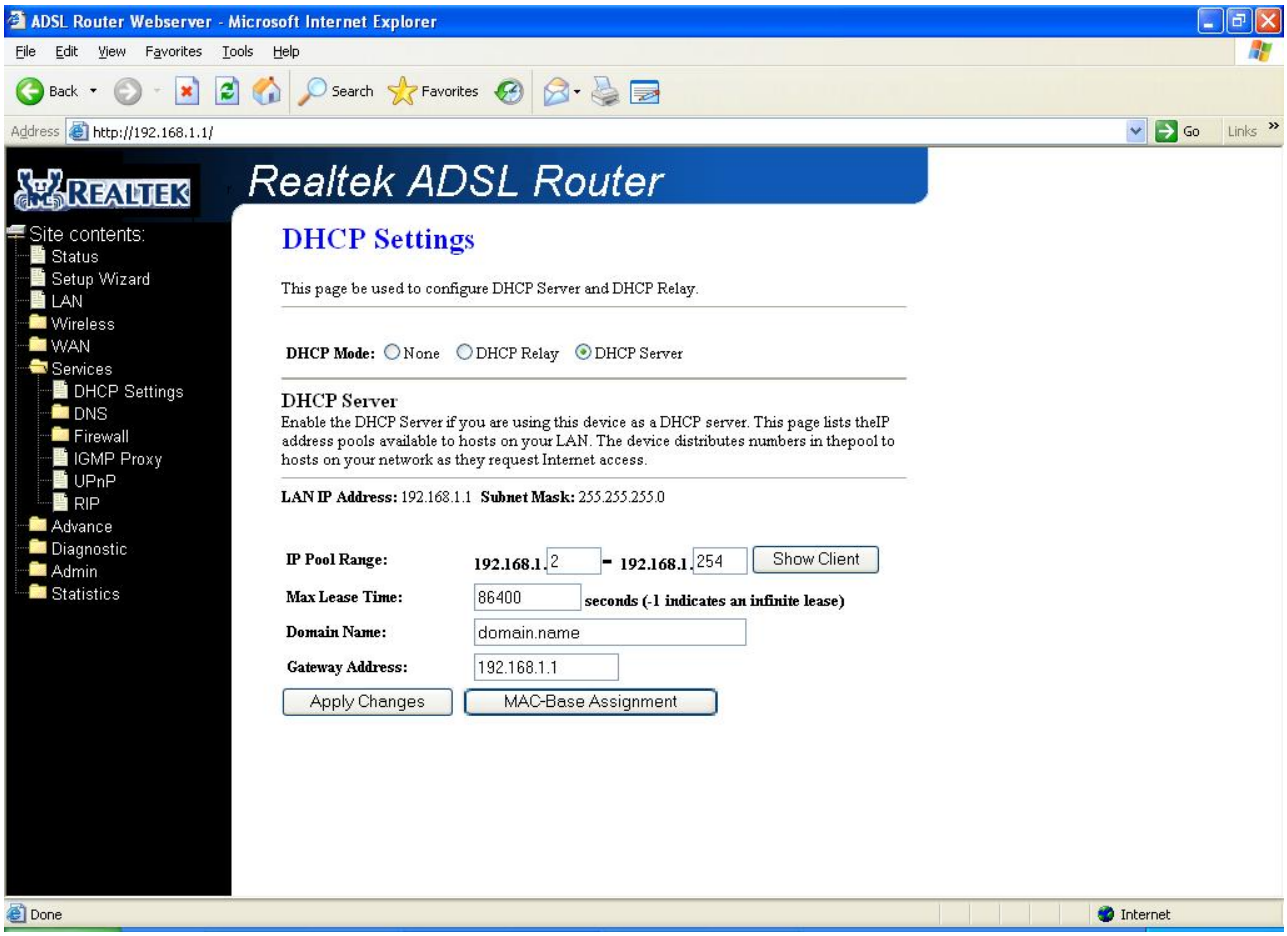
Apply Changes

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

3.5 Services Configuration

3.5.1 DHCP Mode

You can configure your network and DSL device to use the Dynamic Host Configuration Protocol (DHCP). This page provides DHCP instructions for implementing it on your network by selecting the role of DHCP protocol that this device wants to play. 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 **DHCP Server** page; while acting as DHCP Relay, you can setup the relay at the **DHCP Relay** page.



3.5.2 DHCP Server Configuration

By default, the device is configured as a DHCP server, with a predefined IP address pool of 192.168.1.2 through 192.168.1.100 (subnet mask 255.255.255.0).

Field	Description
IP Pool Range	Specify the lowest and highest addresses in the pool.
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	The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway Address.

Function buttons in this page:

Apply Changes

Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

Undo

Discard your changes.

3.5.3 DHCP Relay Configuration

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.

Fields in this page:

Field	Description
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.

Function button in this page

Apply Changes

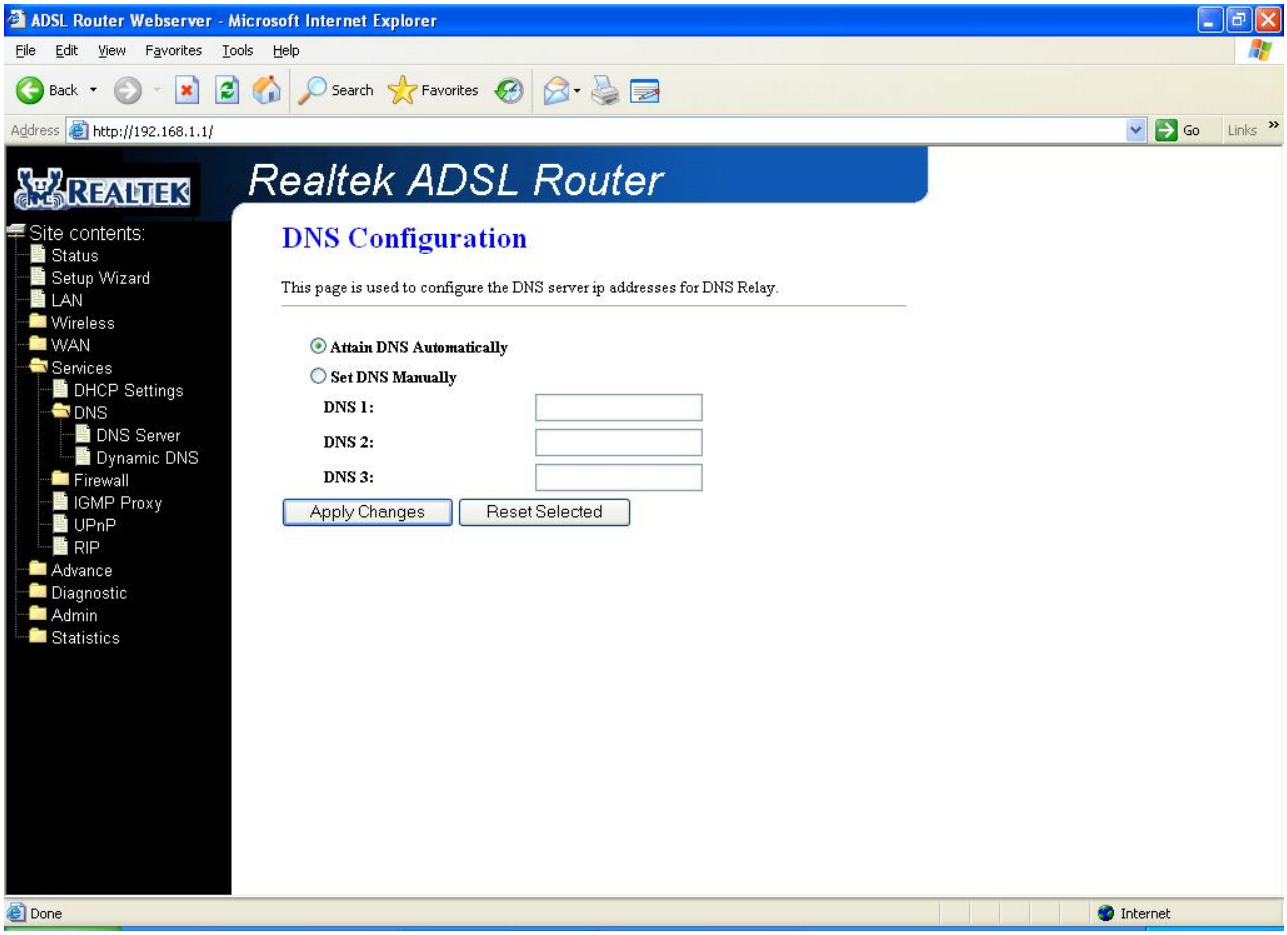
Click to save the setting to the configuration.

3.5.4 DNS Configuration

There are two submenus for the DNS Configuration: [DNS Server] and [Dynamic DNS]

3.5.4.1 DNS Server

This page is used to select the way to obtain the IP addresses of the DNS servers.



Field	Description
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.

Function buttons in this page:

Apply Changes

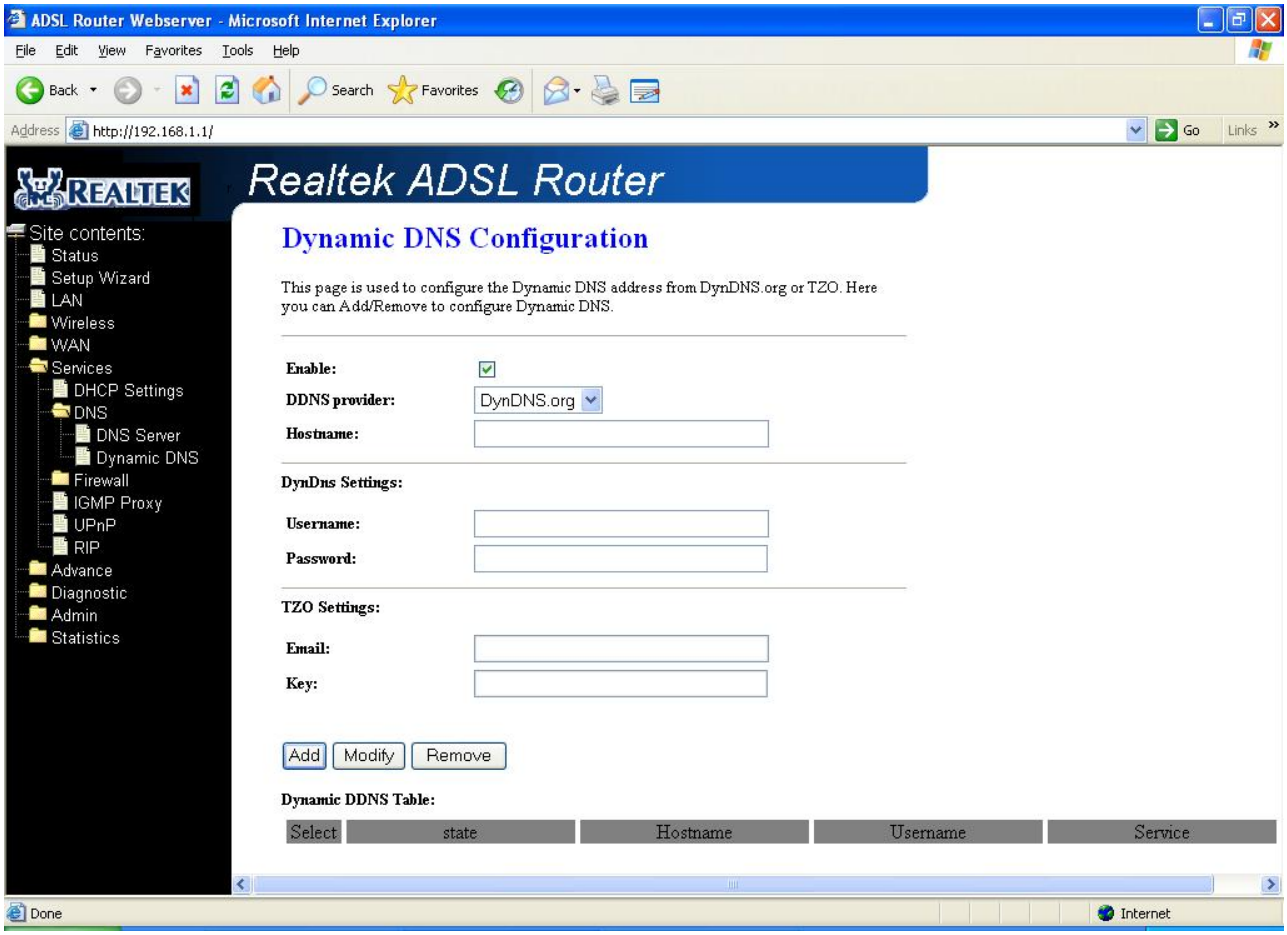
Set new DNS relay configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

Reset Selected

Discard your changes.

3.5.4.2 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 allow 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.



On the **Dynamic DNS** page, configure the following fields:

Field	Description
Enable	Check this item 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 occurs depends on the service you select.
Hostname	Domain name to be registered with the DDNS server.
Interface	This field defaults to your device's WAN interface over which your device will be accessed.
Username	User-name assigned by the DDNS service provider.
Password	Password assigned by the DDNS service provider.

Function buttons in this page:

Add

Click Add to add this registration into the configuration.

Remove

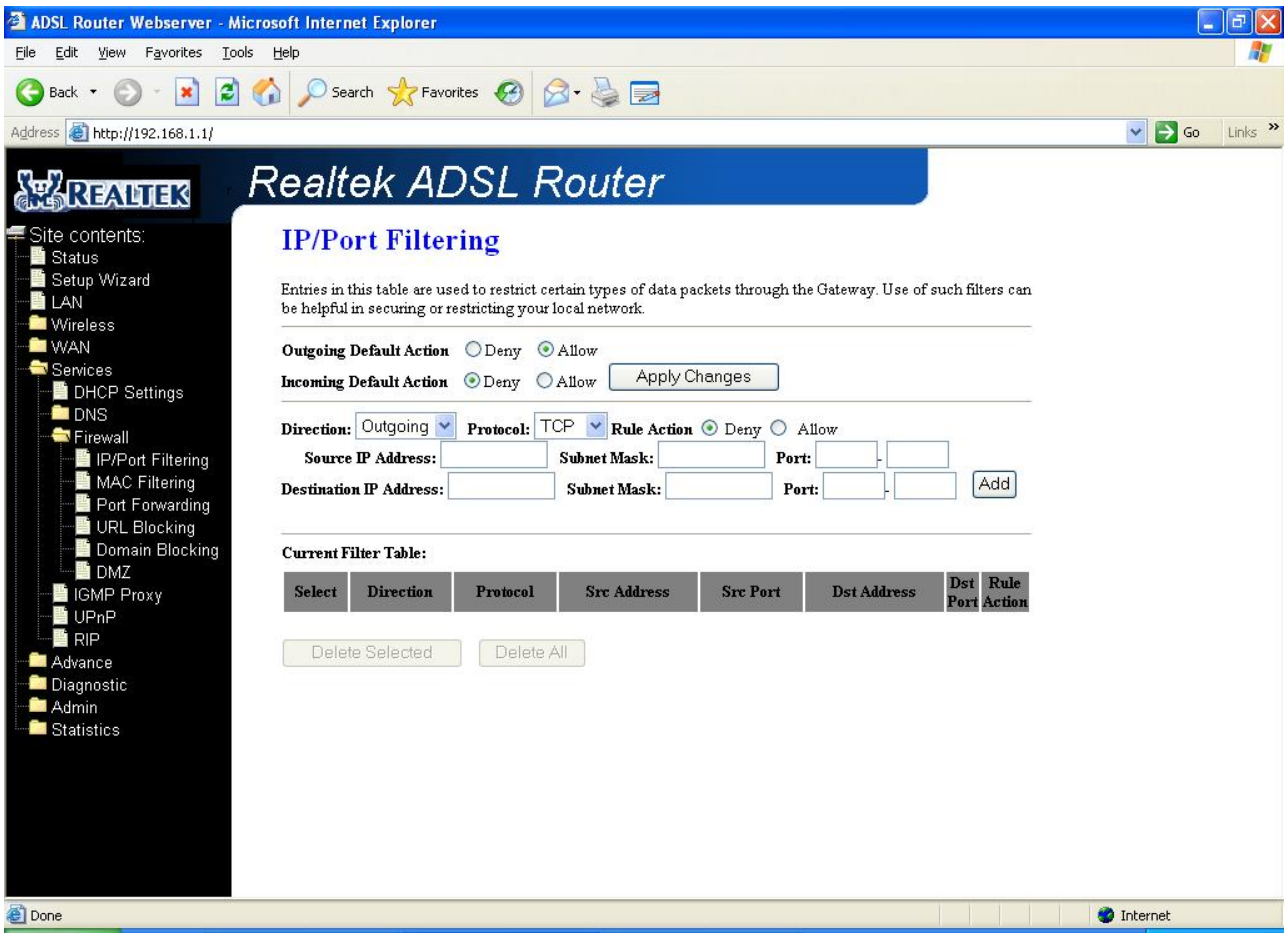
Select an existing DDNS registration by clicking the radio button at the **Select** column of the **Dynamic DNS Table**. Click **Remove** button to remove the selected registration from the configuration.

3.5.5 Firewall Configuration

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

3.5.5.1 IP/Port Filtering

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



Fields on the first setting block:

Field	Description
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.

Function button for this first setting block:

Apply Changes

Click to save the setting of default actions to the configuration.

Fields on the second setting block:

Field	Description
Rule Action	Deny or allow traffic when matching this rule.
Direction	Traffic forwarding direction.
Protocol	There are 3 options available: TCP, UDP and ICMP.
Src IP Address	The source IP address assigned to the traffic on which filtering is applied.
Src Subnet Mask	Subnet-mask of the source IP.
Src Port	Starting and ending source port numbers.
Dst IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Dst Subnet Mask	Subnet-mask of the destination IP.
Dst Port	Starting and ending destination port numbers.

Function buttons for this second setting block:

Apply Changes

Click to save the rule entry to the configuration.

Function buttons for the **Current Filter Table**:

Delete Selected

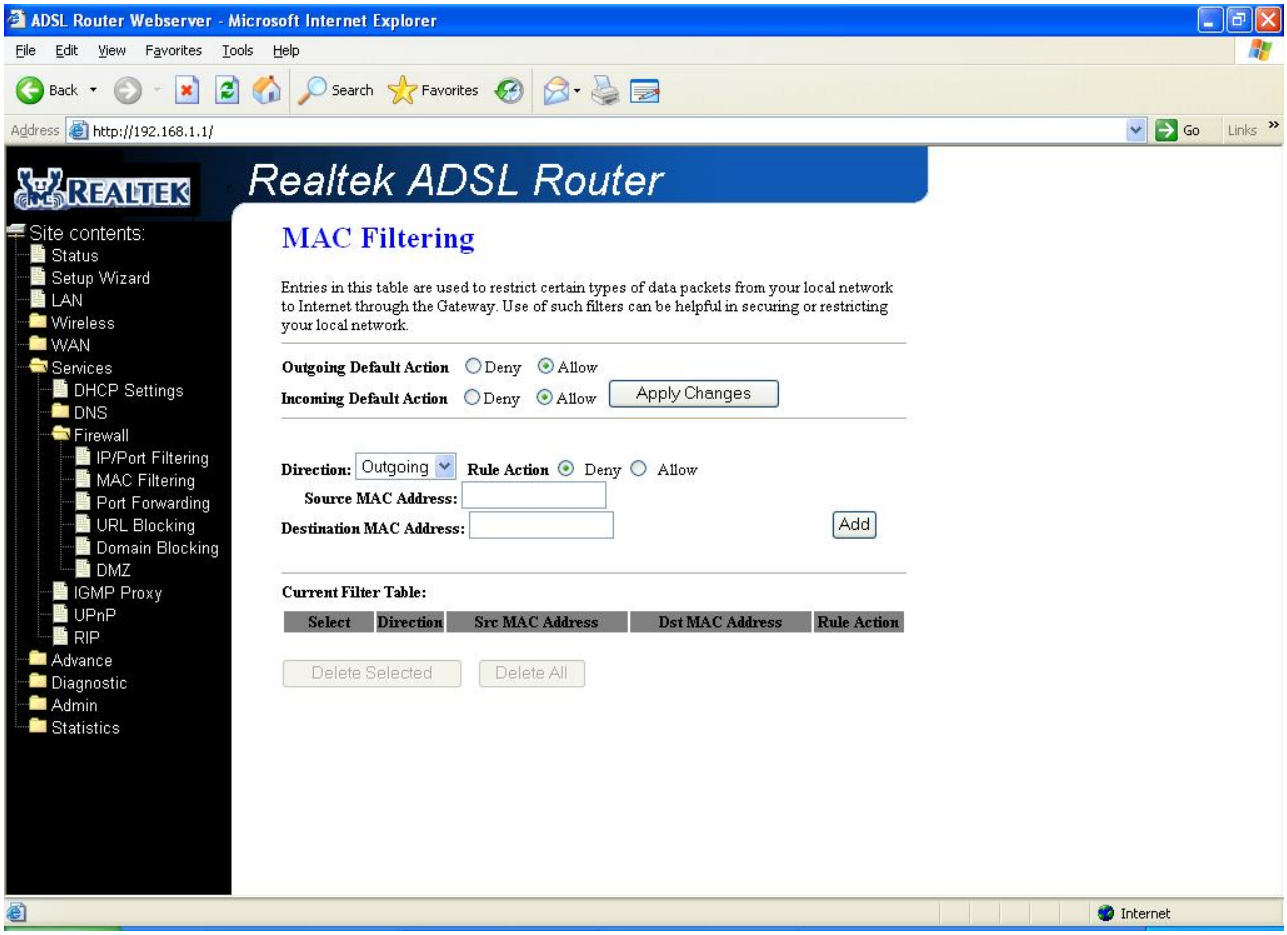
Delete selected filtering rules from the filter table. You can click the checkbox at the **Select** column to select the filtering rule.

Delete All

Delete all filtering rules from the filter table.

3.5.5.2 MAC Filtering

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



Fields on the first setting block:

Field	Description
Outgoing Default Action	Specify the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Action	Specify the default action on the WAN to LAN bridging/forwarding path.

Function button for this first setting block:

Apply Changes

Click to save the setting of default actions to the configuration.

Fields on the second setting block:

Field	Description
Rule Action	Deny or allow traffic when matching this rule.
Direction	Traffic bridging/forwarding direction.

Src MAC Address	he source MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.
Dst MAC Address	The destination MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.

Function buttons for this second setting block:

Apply Changes

Click to save the rule entry to the configuration.

Function buttons for the **Current Filter Table**:

Delete Selected

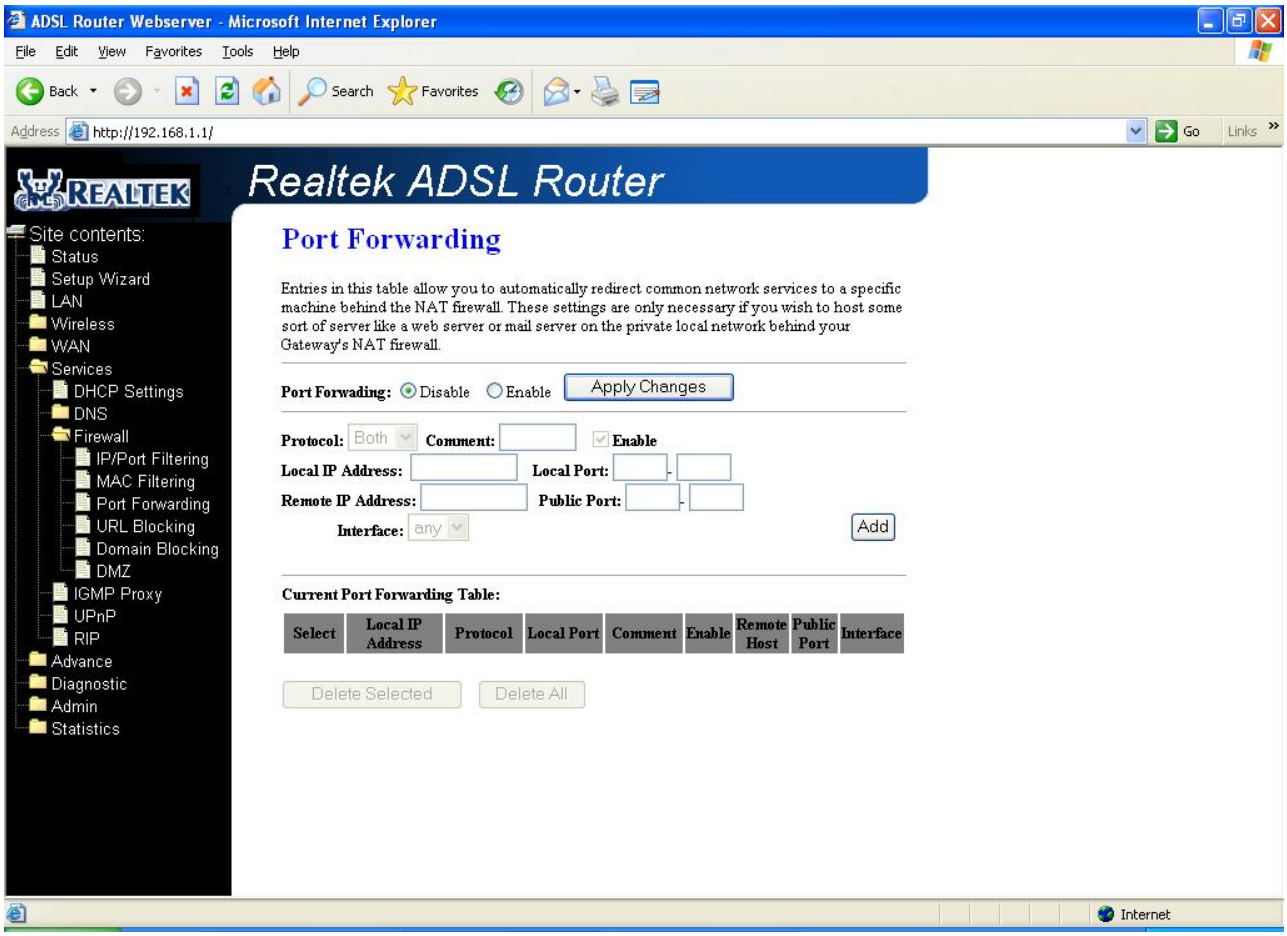
Delete selected filtering rules from the filter table. You can click the checkbox at the **Select** column to select the filtering rule.

Delete All

Delete all filtering rules from the filter table.

3.5.5.3 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.



Fields in this page:

Field	Description
Enable Port Forwarding	Check this item to enable the port-forwarding feature.
Protocol	There are 3 options available: TCP, UDP and Both.
Enable	Check this item to enable this entry.
Local IP Address	IP address of your local server that will be accessed by Internet.
Port	The destination port number that is made open for this application on the LAN-side.
Remote IP Address	The source IP address from which the incoming traffic is allowed. Leave blank for all.
External Port	The destination port number that is made open for this application on the WAN-side
Interface	Select the WAN interface on which the port-forwarding rule is to be applied.

Function buttons for the setting block:

Apply Changes

Click to save the rule entry to the configuration.

Function buttons for the **Current Port Forwarding Table**:

Delete Selected

Delete the selected port forwarding rules from the forwarding table. You can click the checkbox at the **Select** column to select the forwarding rule.

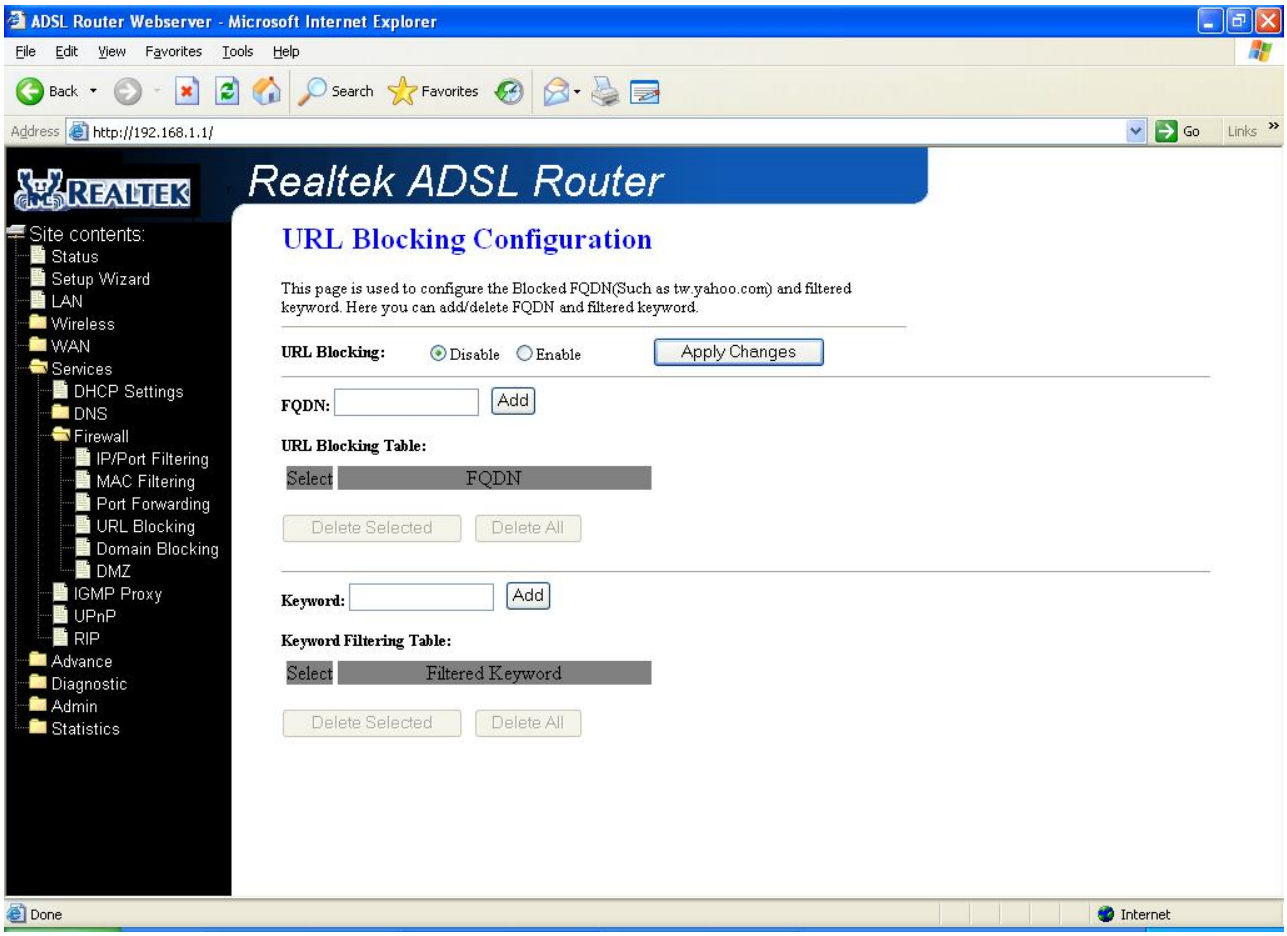
Delete All

Delete all forwarding rules from the forwarding table.

3.5.5.4 URL Blocking

A URL is a web address that is normally typed into a web browser. For instance www.yahoo.com, www.msn.com are all URLs. URL Blocking allows you to block URLs based upon keywords that you enter into a box. Blocking URLs prevents people on your network from accessing these websites. These keywords may be full URL's or they may just be words.

FQDN (Fully Qualified Domain Name) means the complete domain name for a specific computer (host) on the Internet. It provides enough information so that it can be converted into a physical IP address. The FQDN consists of host name and domain name. For example, **www.google.com** is the FQDN on the Web for the publisher of this database. The **WWW** is the host. On the Web, there are millions of hosts named WWW in order to maintain uniformity. **GOOGLE.COM** is the domain name, with **.COM** being the top level domain (TLD) name.



- **URL Blocking Capability:** Check to turn ON or OFF the URL Blocking capability.

- **Apply :** Click **Apply** to confirm your setting.

- **FQDN:** The complete domain name for a specific computer (host) on the Internet.
- **Add FQDN:** Click **Add FQDN** and add in new list.
- **Delete Selected FQDN:** Delete the selected FQDN List from the table.
- **Keyword:** enter the filtered keyword.

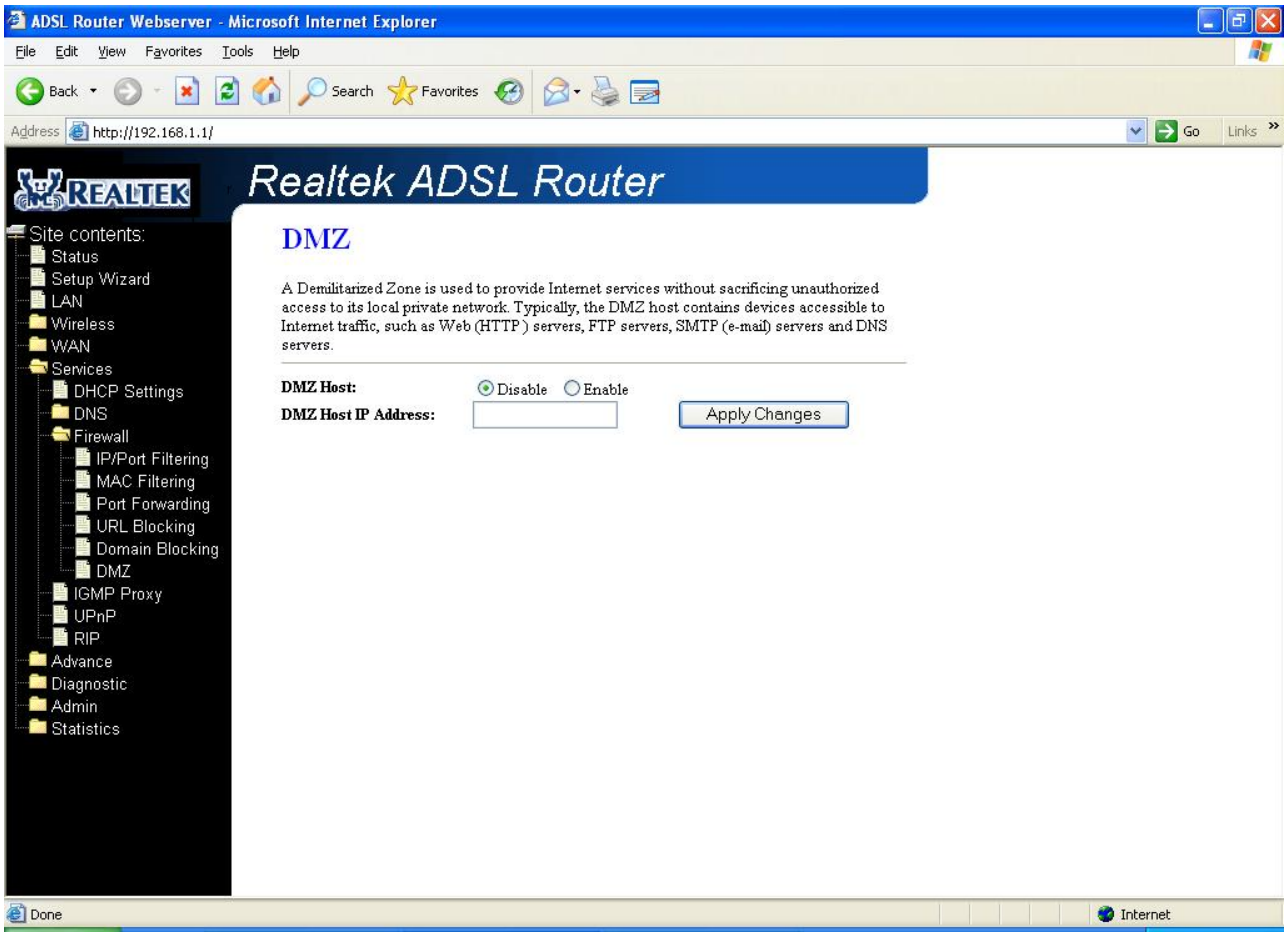
Function buttons in this page:

Apply Changes

Click to save the setting to the configuration.

3.5.5.5 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.



Fields in this page:

Field	Description
Enable DMZ	Check this item to enable the DMZ feature.
DMZ Host IP Address	IP address of the local host. This feature sets a local host to be exposed to the Internet.

Function buttons in this page:

Apply Changes

Click to save the setting to the configuration.

3.5.6 IGMP Proxy Configuration

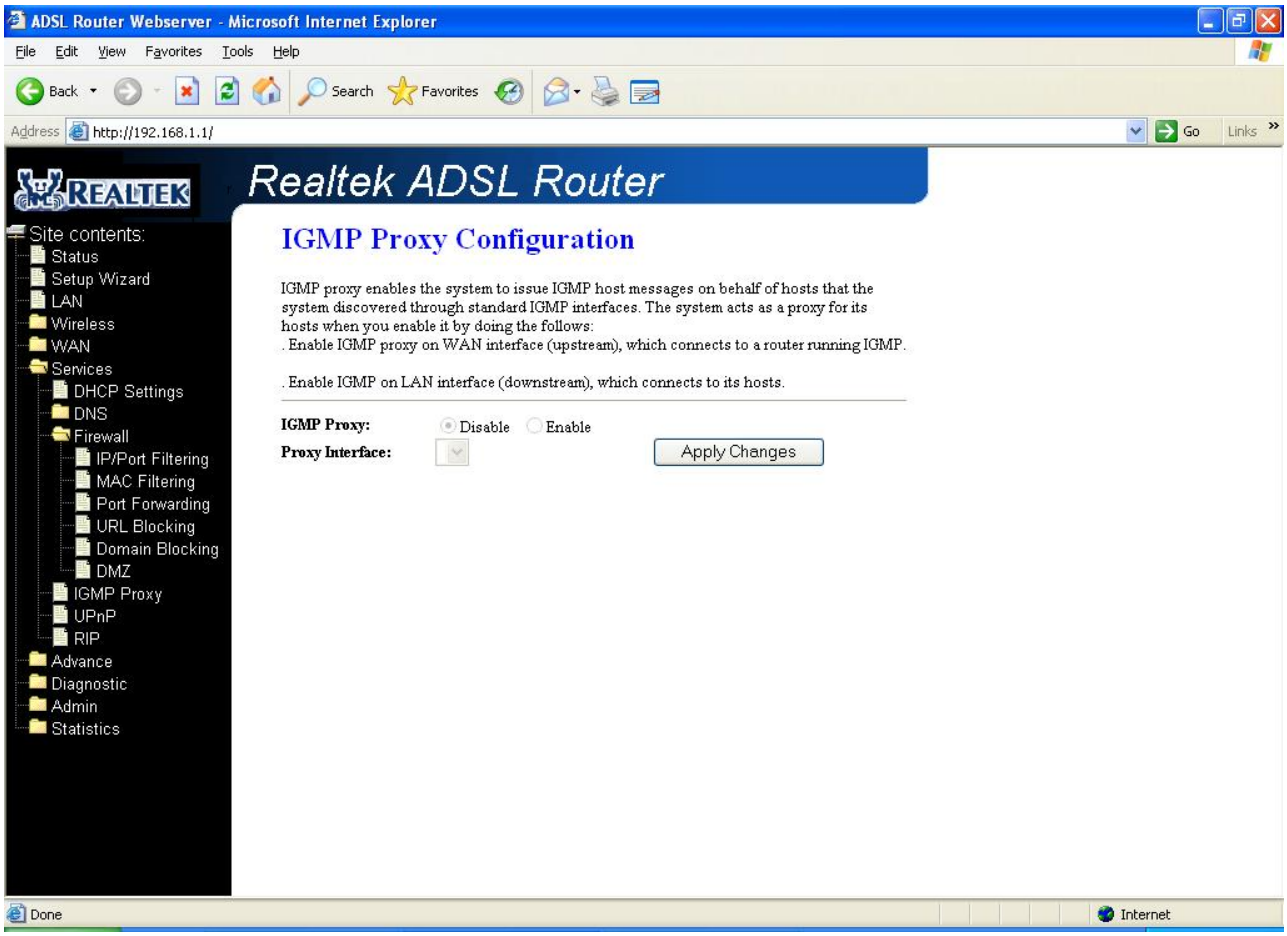
Multicasting is useful when the same data needs to be sent to more than one hosts. Using multicasting as opposed to sending the same data to the individual hosts uses less network bandwidth. The multicast feature also enables you to receive multicast video stream from multicast servers.

IP hosts use Internet Group Management Protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. This device supports IGMP proxy that handles IGMP messages. When enabled, this device acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast group on the WAN side.

When a host wishes to join a multicast group, it sends IGMP REPORT message to the device's IGMP downstream interface. The proxy sets up a multicast route for the interface and host requesting the video content. It then forwards the Join to the upstream multicast router. The multicast IP traffic will then be forwarded to the requesting host. On a leave, the proxy removes the route and then forwards the leave to the upstream multicast router.

The IGMP Proxy page allows you to enable multicast on WAN and LAN interfaces. The LAN interface is always served as downstream IGMP proxy, and you can configure one of the available WAN interfaces as the upstream IGMP proxy.

- Upstream: The interface that IGMP requests from hosts are sent to the multicast router.
- Downstream: The interface data from the multicast router are sent to hosts in the multicast group database.



Fields in this page:

Field	Description
IGMP Proxy	Enable/disable IGMP proxy feature
Proxy Interface	The upstream WAN interface is selected here.

Function buttons in this page:

Apply Changes

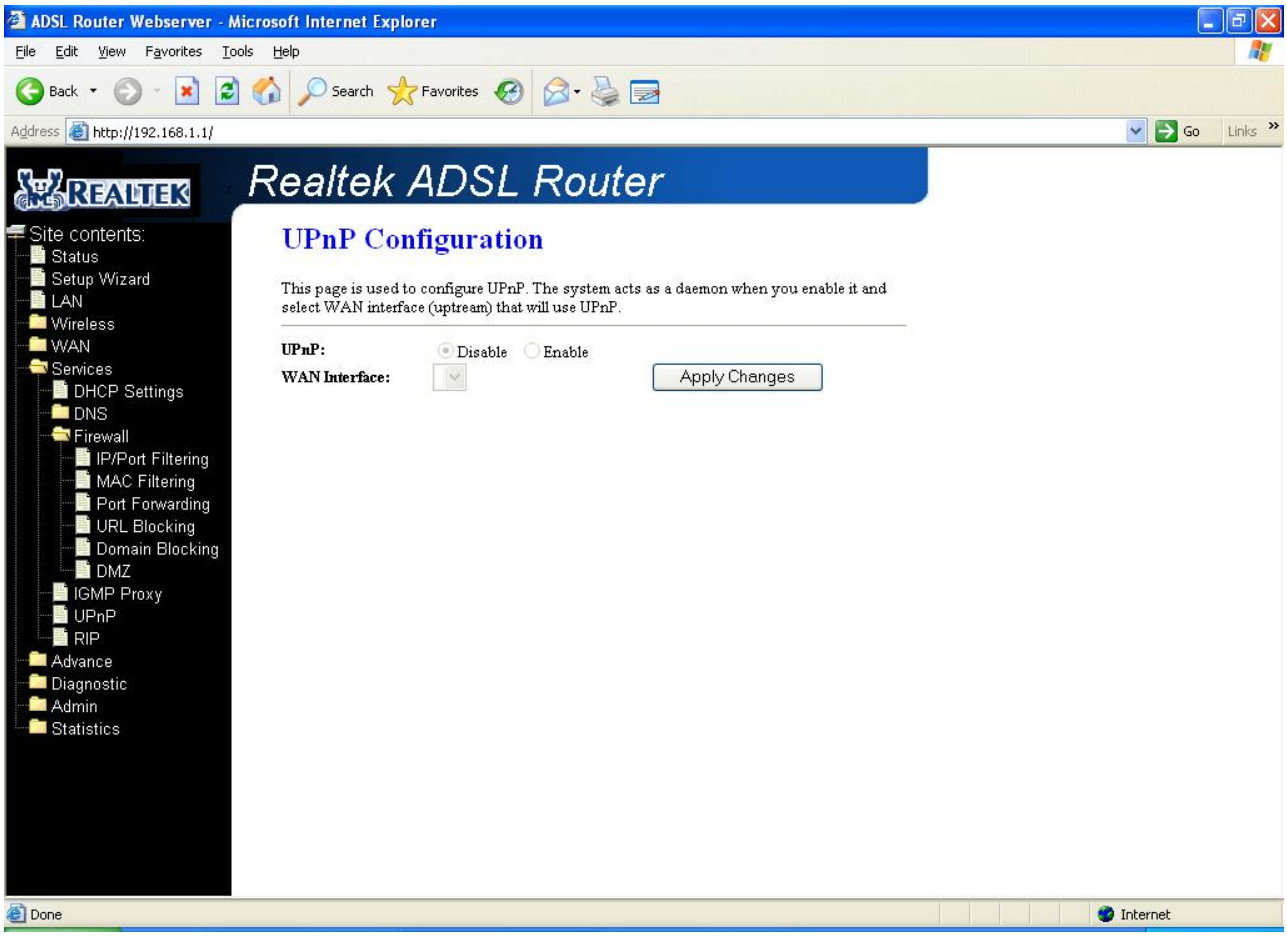
Click to save the setting to the configuration.

3.5.7 UPnP Configuration

The DSL device 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 DSL device as a control point back to the host making the request.



Fields in this page

Field	Description
UPnP	Enable/disable UPnP feature.
WAN Interface	Select WAN interface that will use UPnP from the drop-down lists.

Function buttons in this page:

Apply Changes

Click to save the setting to the system configuration.

3.5.8 RIP Configuration

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line.

Most small home or office networks do not need to use RIP; they have only one router, such as the ADSL Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the ADSL Router). The ADSL Router and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network..

Fields on the first setting block:

Field	Description
RIP	Enable/disable RIP feature.

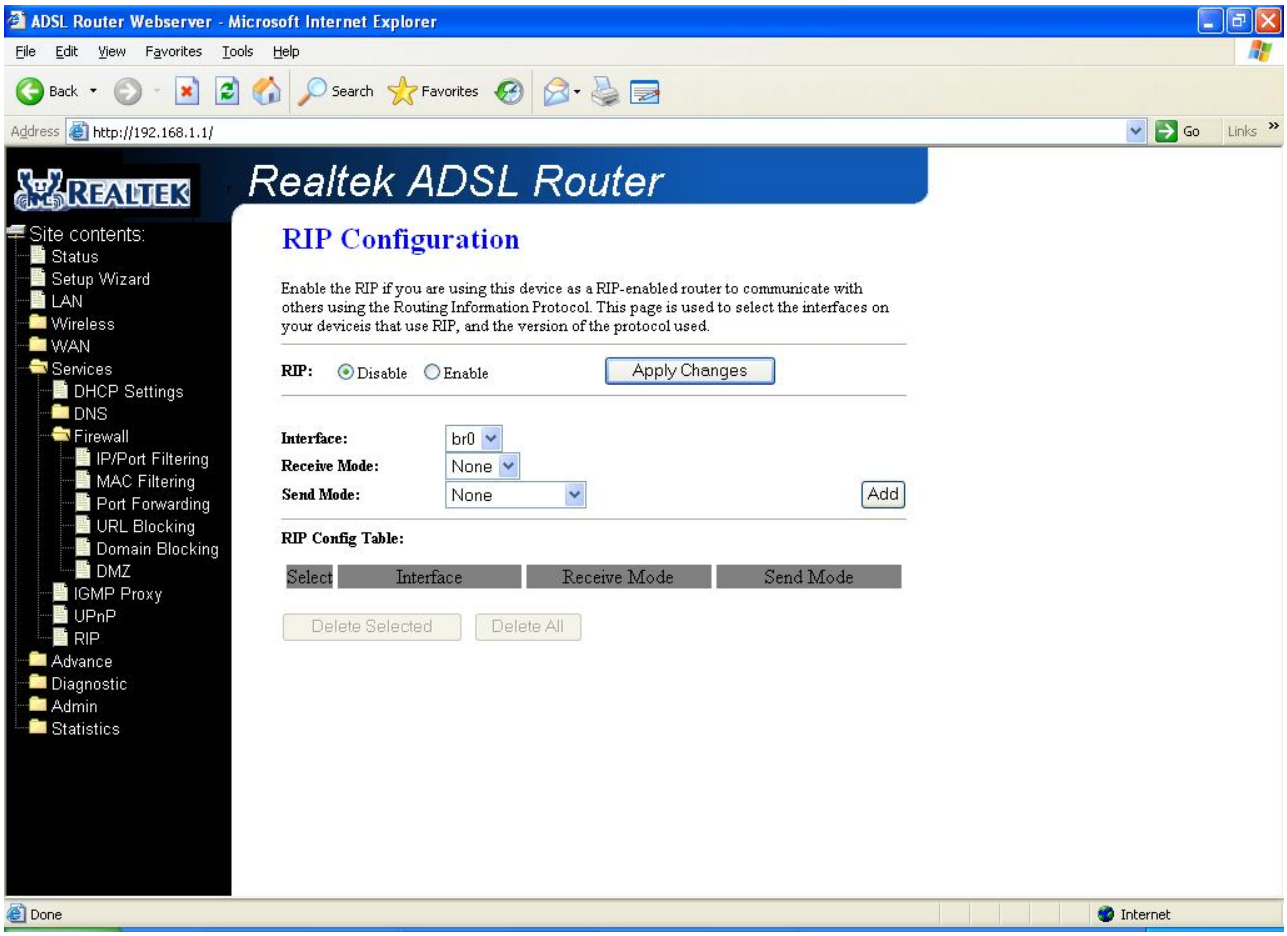
Function buttons for the second setting block in this page:

Apply Changes

Click to save the setting of this setting block to the system configuration

Fields on the second setting block:

Field	Description
Interface	The name of the interface on which you want to enable RIP.
Receive Mode	Indicate the RIP version in which information must be passed to the DSL device in order for it to be accepted into its routing table.
Send Mode	Indicate the RIP version this interface will use when it sends its route information to other devices.



Function buttons for the second setting block in this page:

Add

Add a RIP entry and the new RIP entry will be display in the table

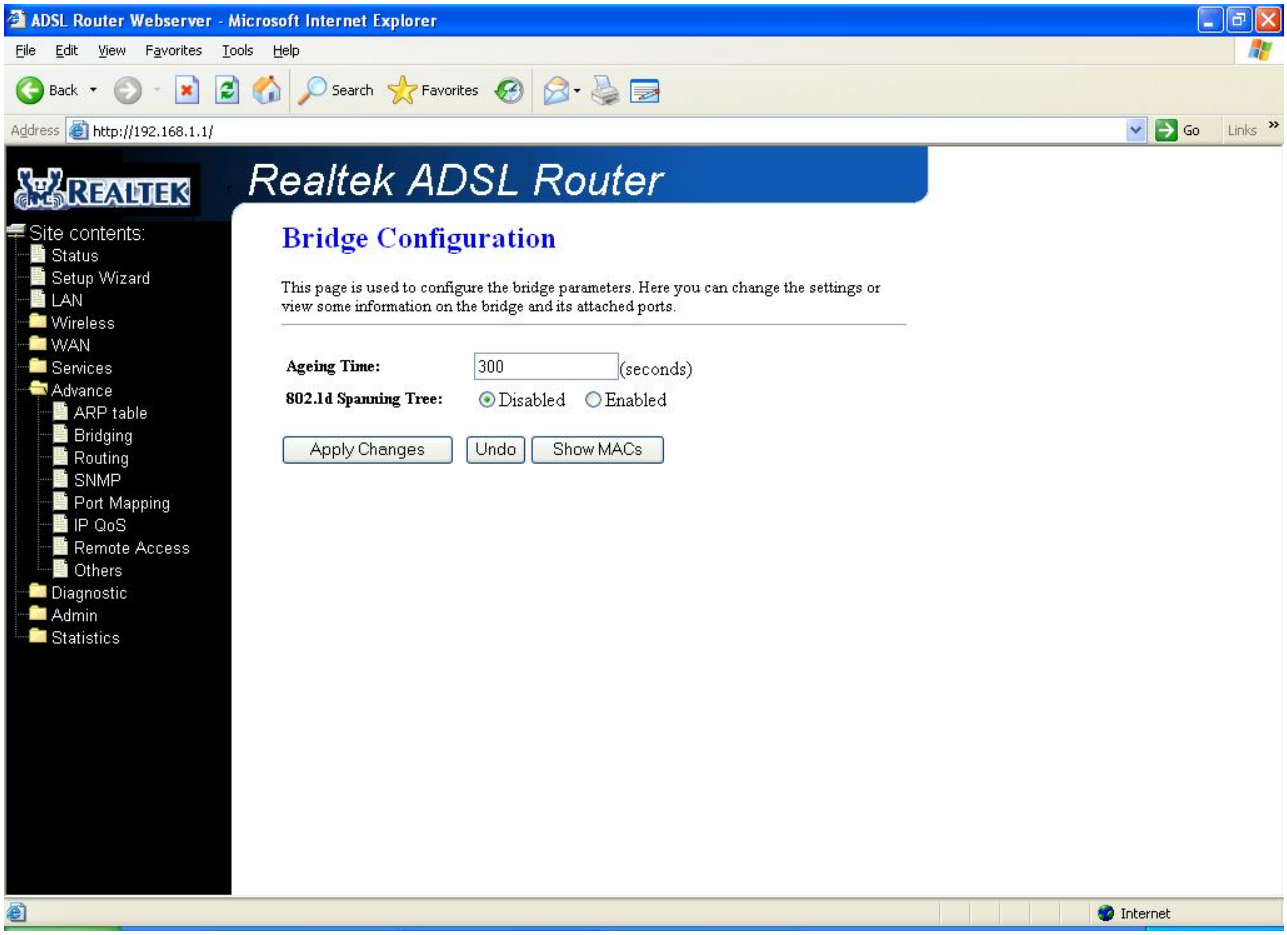
Delete Selected Entry

Delete a selected RIP entry. The RIP entry can be selected on the **Select** column of the **RIP Config Table.**

3.6 Advance Configuration

3.6.1 Bridging

You can enable/disable Spanning Tree Protocol and set MAC address aging time in this page.



Fields in this page:

Field	Description
Ageing 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).
802.1d Spanning Tree	Enable/disable the spanning tree protocol

Function buttons in this page:

Apply Changes

Save this bridge configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section “Admin” for details.

Show MACs

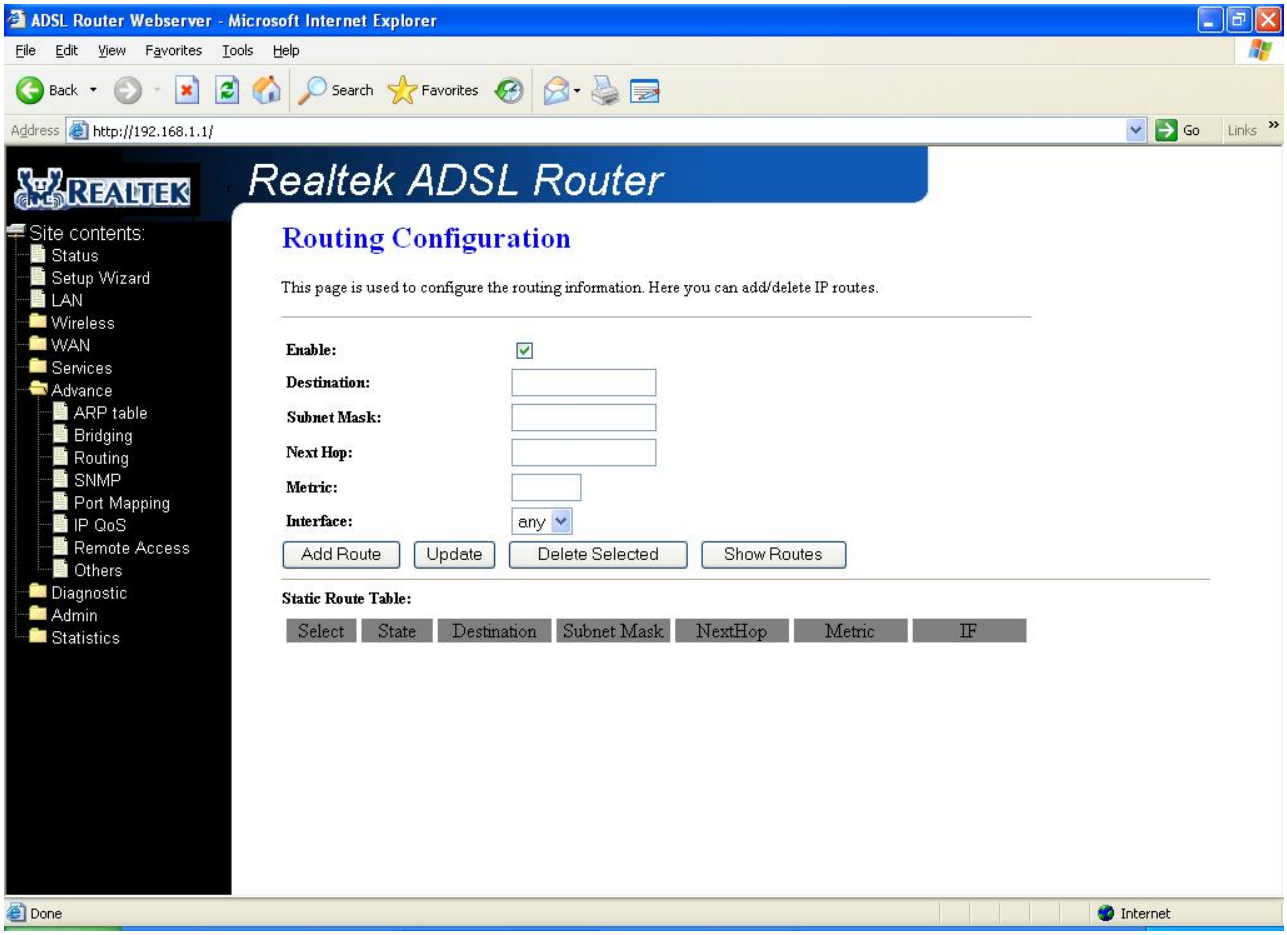
List MAC address in forwarding table.

3.6.2 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 DSL device 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 DSL device. 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 DSL device 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.



Fields in this page:

Field	Description
Enable	Check 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.

Function buttons in this page:

Add Route

Add a user-defined destination route.

Update

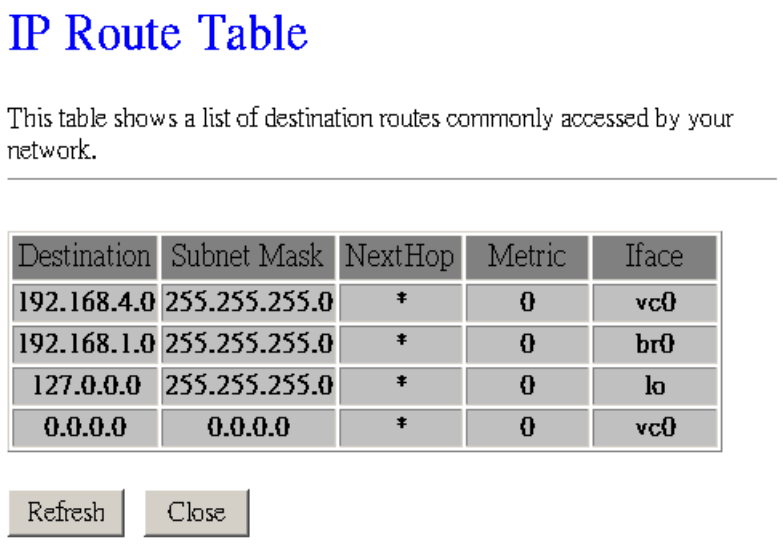
Update the selected destination route on the **Static Route Table**.

Delete Selected

Delete a selected destination route on the **Static Route Table**.

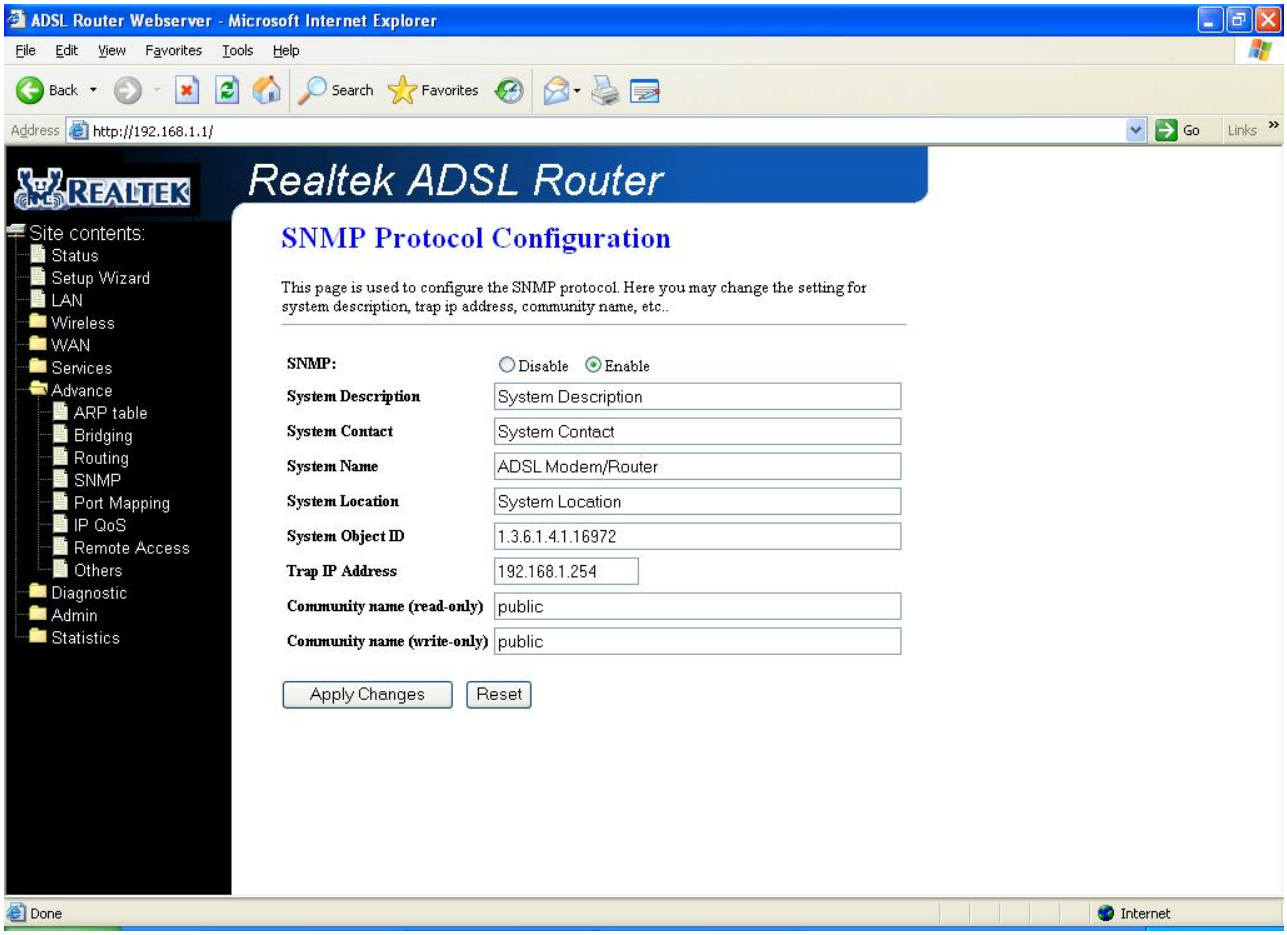
Show Routes

Click this button to view the DSL device's routing table. The IP Route Table displays, as shown in Figure.



3.6.3 SNMP Configuration

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.



Fields in this page:

Field	Description
System Description	System description of the DSL device.
System Contact	Contact person and/or contact information for the DSL device.
System Name	An administratively assigned name for the DSL device.
System Location	The physical location of the DSL device.
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.
Community name (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.

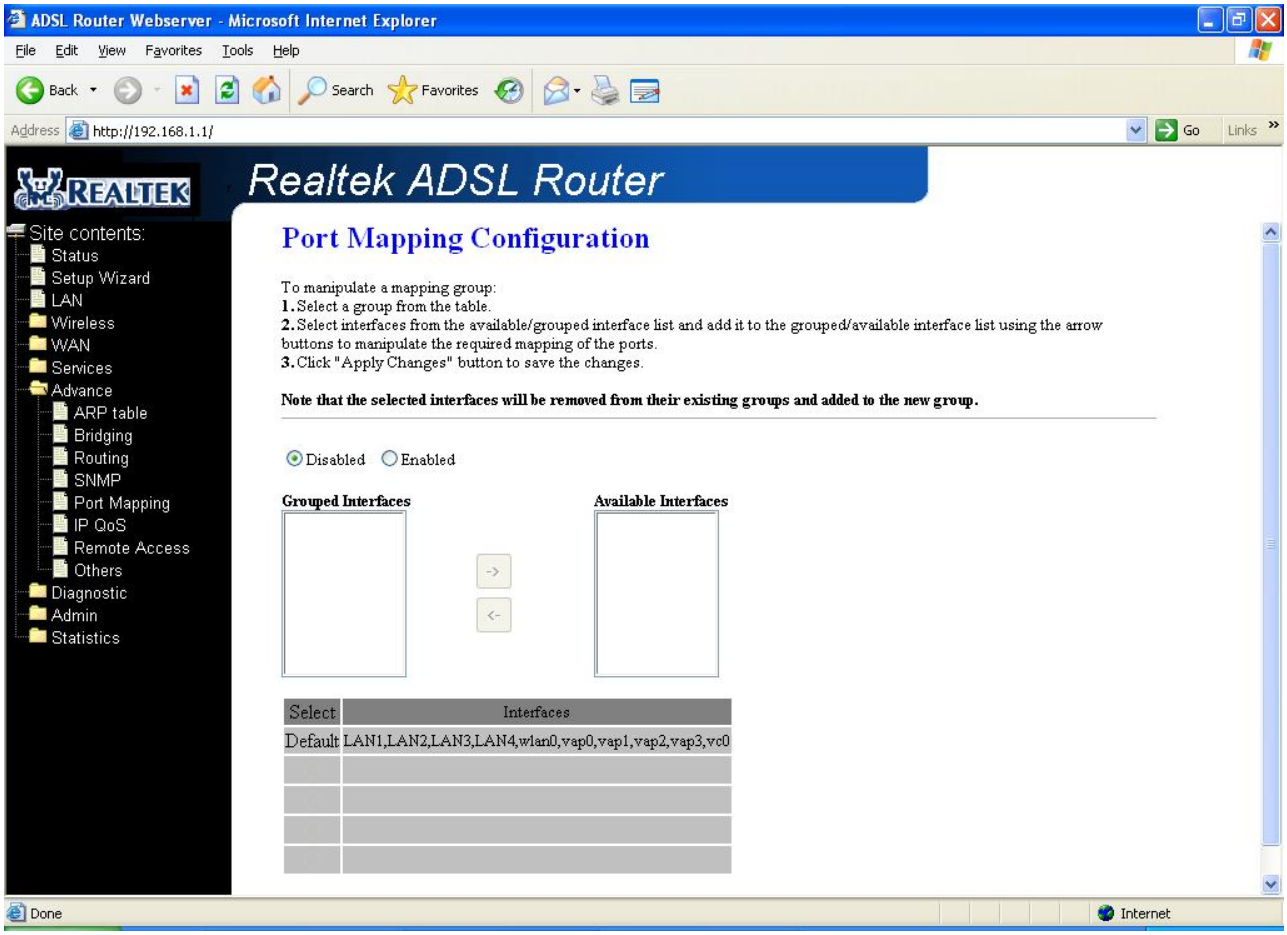
Function buttons in this page:

Apply Changes

Save SNMP configuration. New configuration will take effect after saving into flash memory and rebooting the system. See section “Admin” for details.

3.6.4 Port Mapping

The DSL device 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 DSL device 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.



Fields in this page:

Field	Description
Enabled/Disabled	Radio buttons to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.
“Interface groups	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.

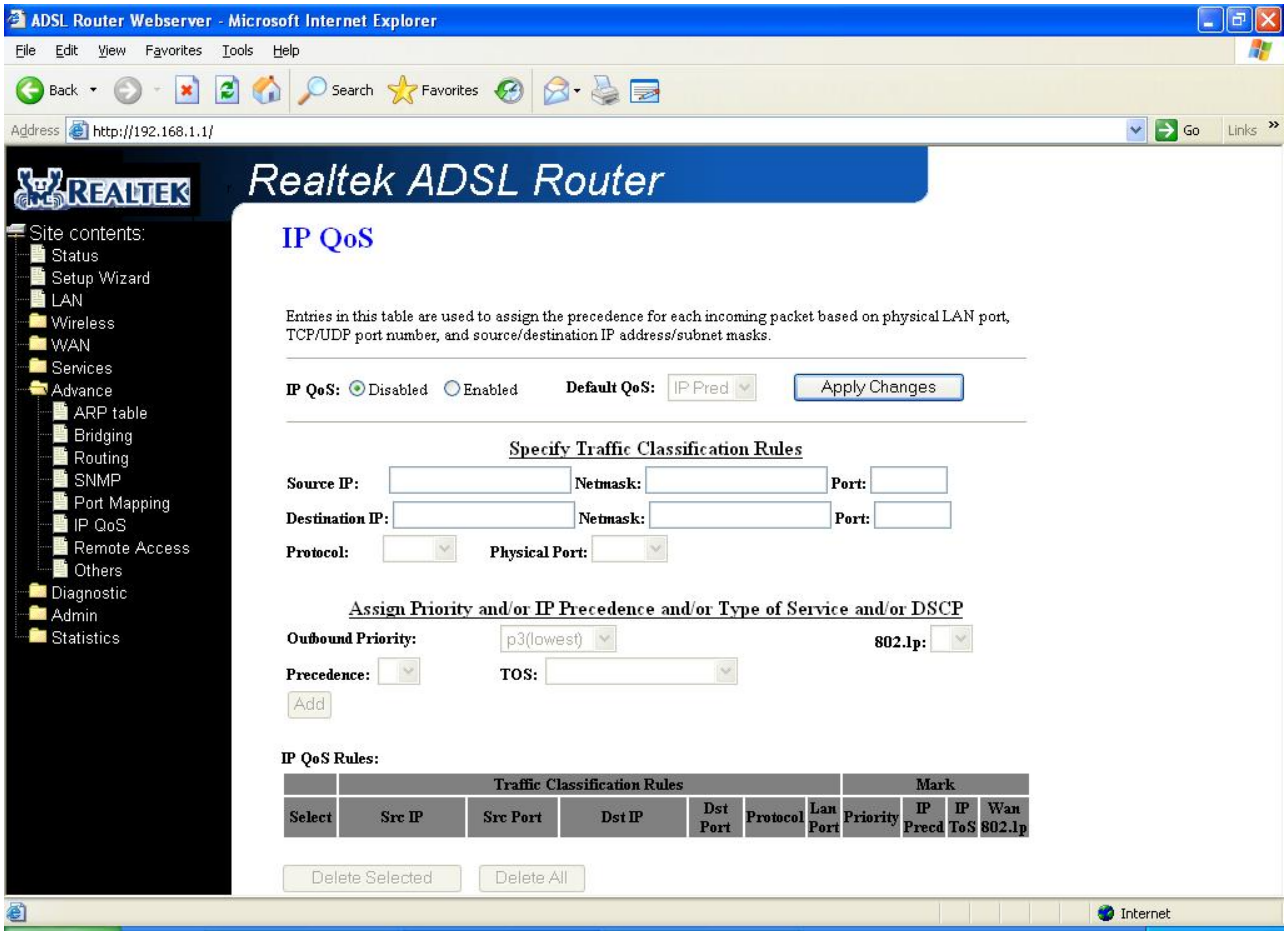
Function buttons in this page:

Apply Changes

Save configuration to system. New configuration will take effect after saving into flash memory and rebooting the system. See section “Admin” for details.

3.6.5 IP QoS

The DSL device 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. 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.



Fields on the first setting block of this page:

Field	Description
IP QoS	Enable/disable the IP QoS function.
Source IP	The IP address of the traffic source.
Source Netmask	The source IP netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Destination Netmask	The destination IP netmask. This field is required if the destination IP has been entered.

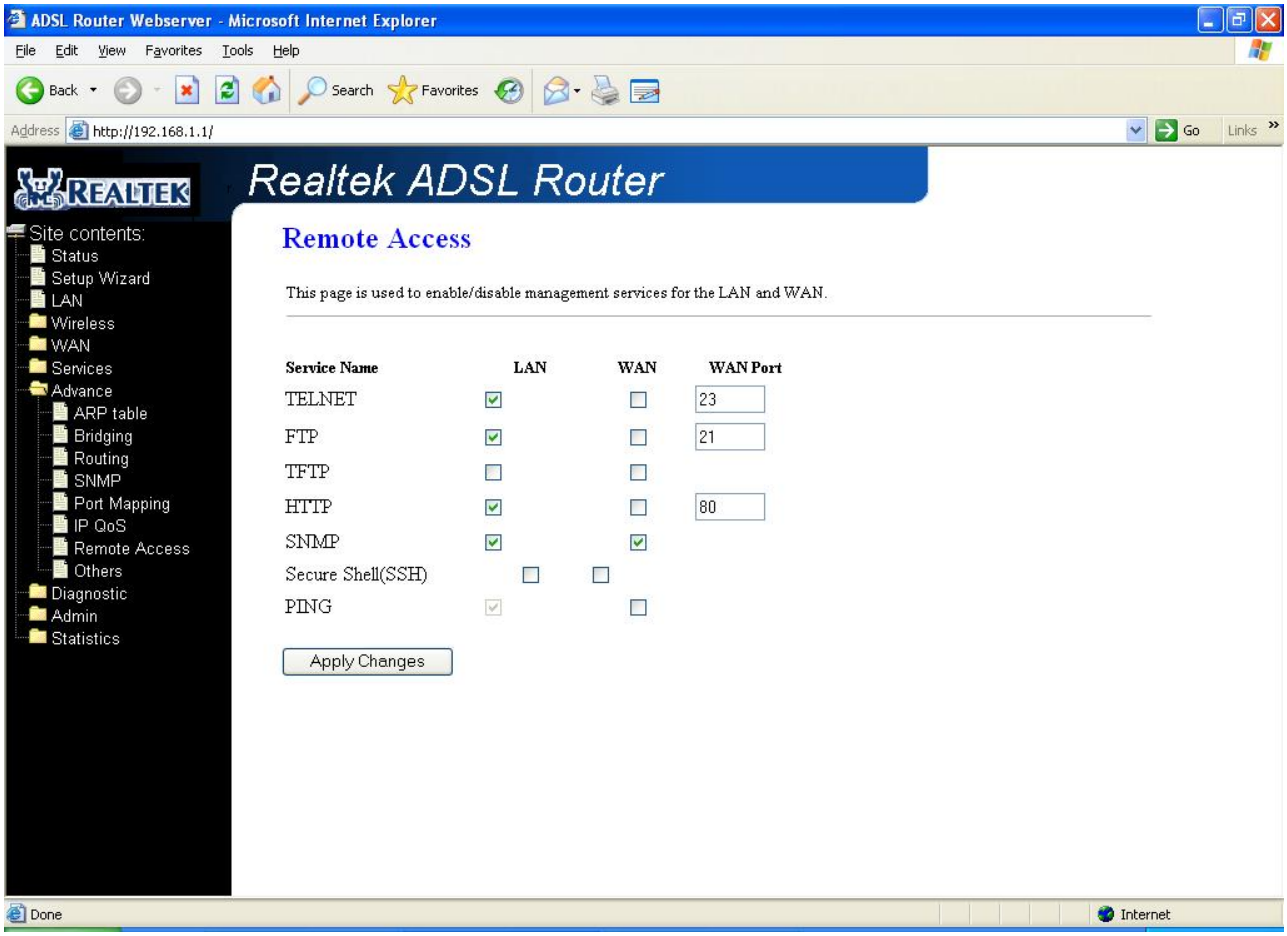
Protocol	The selections are TCP, UDP, ICMP and the blank for none. This field is required if the source port or destination port has been entered.
Source Port	The source port of the selected protocol. You cannot configure this field without entering the protocol first.
Destination Port	The destination port of the selected protocol. You cannot configure this field without entering the protocol first.
Physical Port	The incoming ports. The selections include LAN ports, wireless port, and the blank for not applicable.

Fields on the second setting block of this page:

Field	Description
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.
IP Precedence	Select this field to mark the IP precedence bits in the packet that match this classification rule.
IP Type of Service	Select this field to mark the IP TOS bits in the packet that match this classification rule.
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.

3.6.6 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.



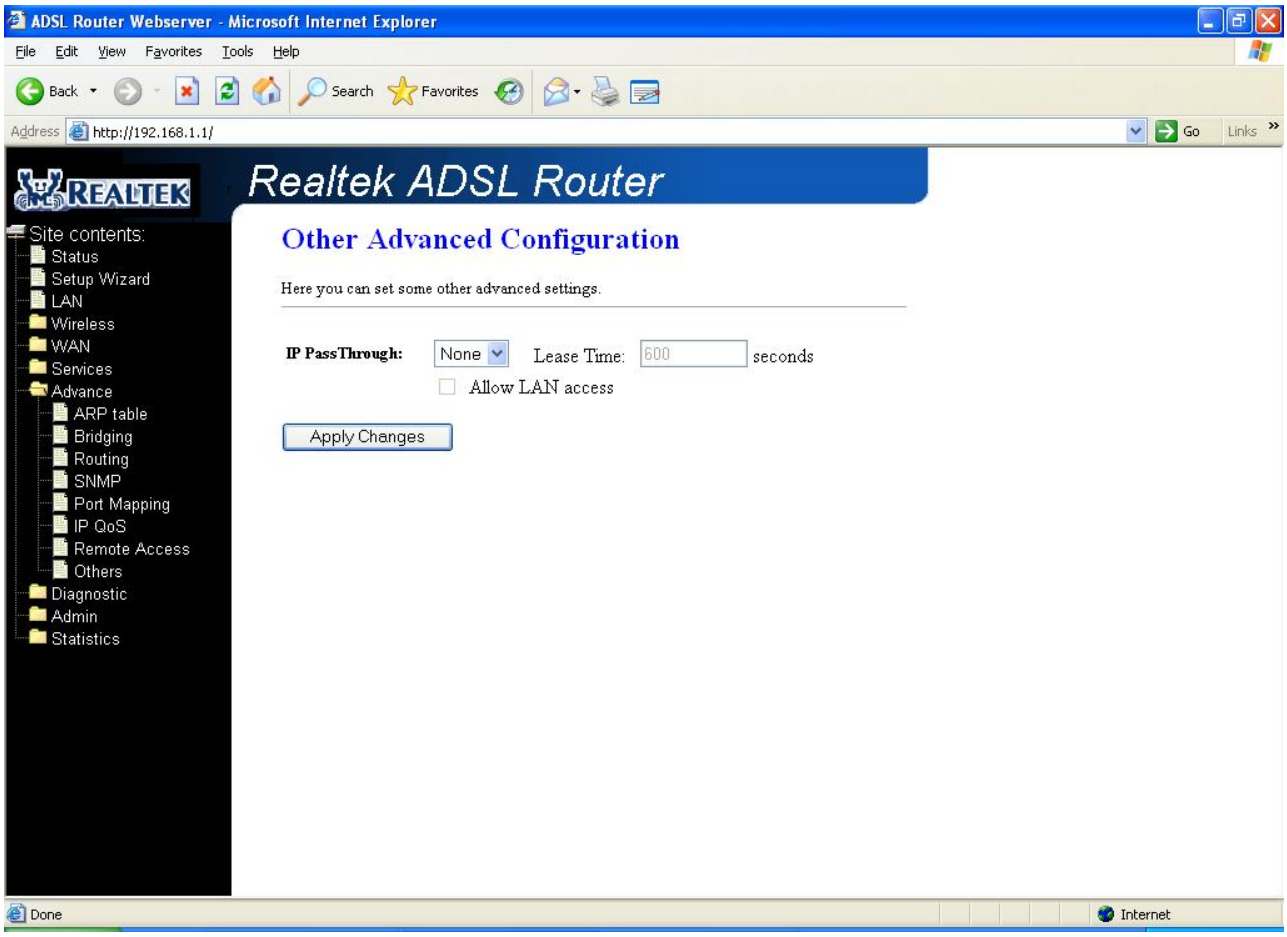
Fields in this page:

Field	Description
LAN	Check/un-check the services on the LAN column to allow/un-allow the services access from LAN side; and “WAN”:
WAN	Check/un-check the services on the WAN column to allow/un-allow 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 DSL device.

3.6.7 Other Advanced Configuration

IP Pass Through: Although the Router mode is capable of terminating the PPP in the modem and hence does not require PPPoE client software on the host PC, there are some disadvantages to Router mode when only single-user support is required. For instance, Router mode uses NAT which requires ALG support. **IP Pass Through** also terminates the PPP in the modem and does not require a PPPoE client on the PC. However, **IP Pass Through** does not use NAT and is not limited by ALGs. **IP Pass Through** will work with Ethernet interface to the PC.

When **IP Pass Through** is enabled, only one PC is able to access the Internet, and the DHCP server will duplicate the WAN IP address from the ISP to the local client PC. Only the PC with the WAN IP address can access the Internet.



- **IP Pass Through:** Select the WAN connection profile from the drop down manual on which the rule will take effect.
- **Lease time:** The Lease time is the amount of time a network user will be allowed to connect with DHCP server.
- **Allow LAN access:** Click to enable **LAN Access**.
- **Submit:** Click **Submit** to complete the setting.

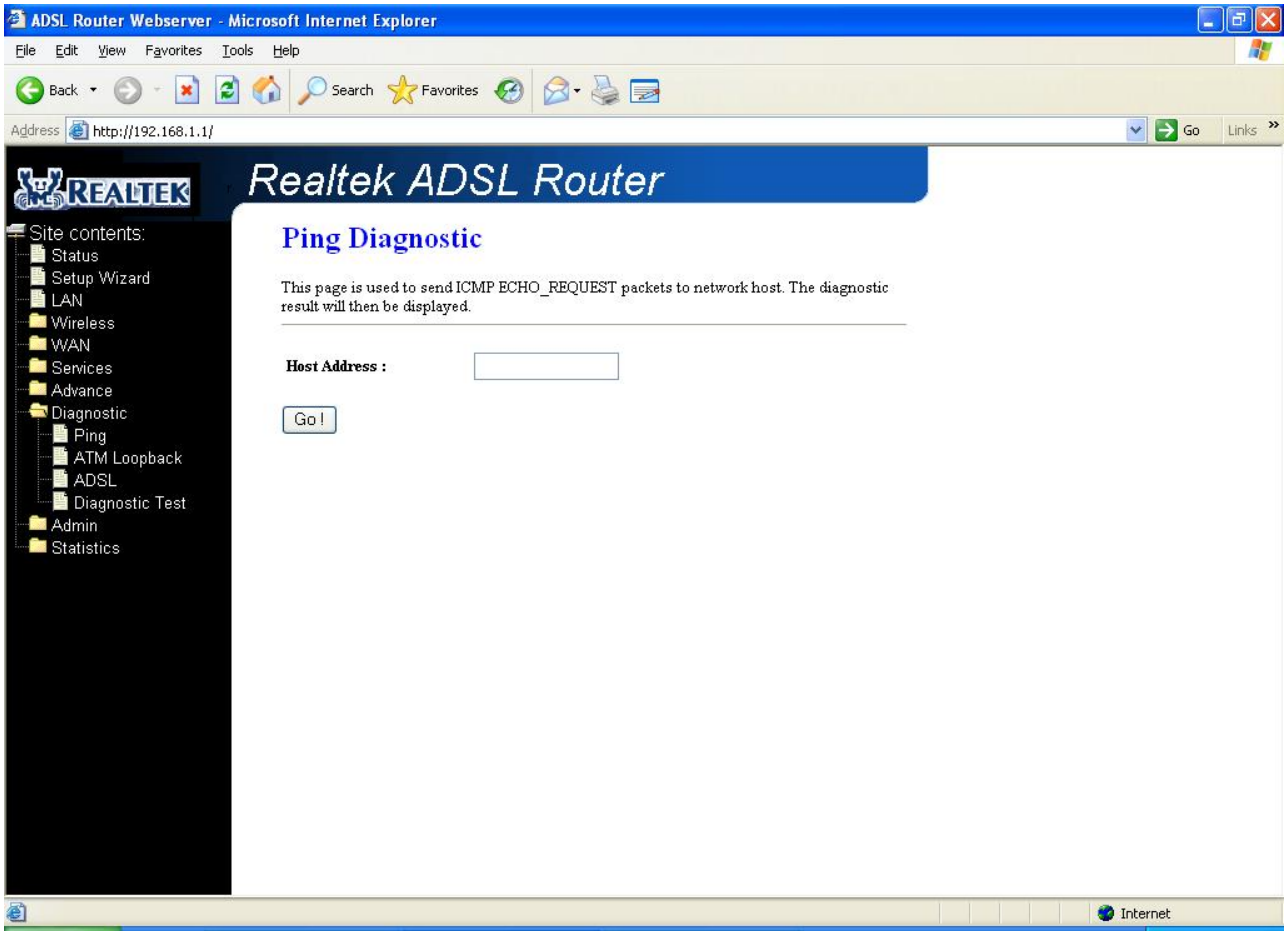
To complete and save the setting, click **SAVE** after clicking the **Submit** button.

3.7 Diagnostic

The **Diagnostics** page allows you to run a series of diagnostic tests of your system software and hardware connections.

3.7.1 Ping

Once you have your DSL device configured, it is a good idea to make sure you can ping the network. Figure below shows the default Ping Test screen, which can be accessed by clicking on the Ping Test link from the Tools screen. If you have your PC connected to the 4-Ports 11g Wireless ADSL2/2+ Router via the default DHCP configuration, you should be able to Ping the network address 192.168.1.1. If the pings for both the WAN side and the LAN side are complete, and your have the proper protocol configures, you should be able to surf the Internet.Click **Go!** To start the ping command, the ping result will then be shown in this page.

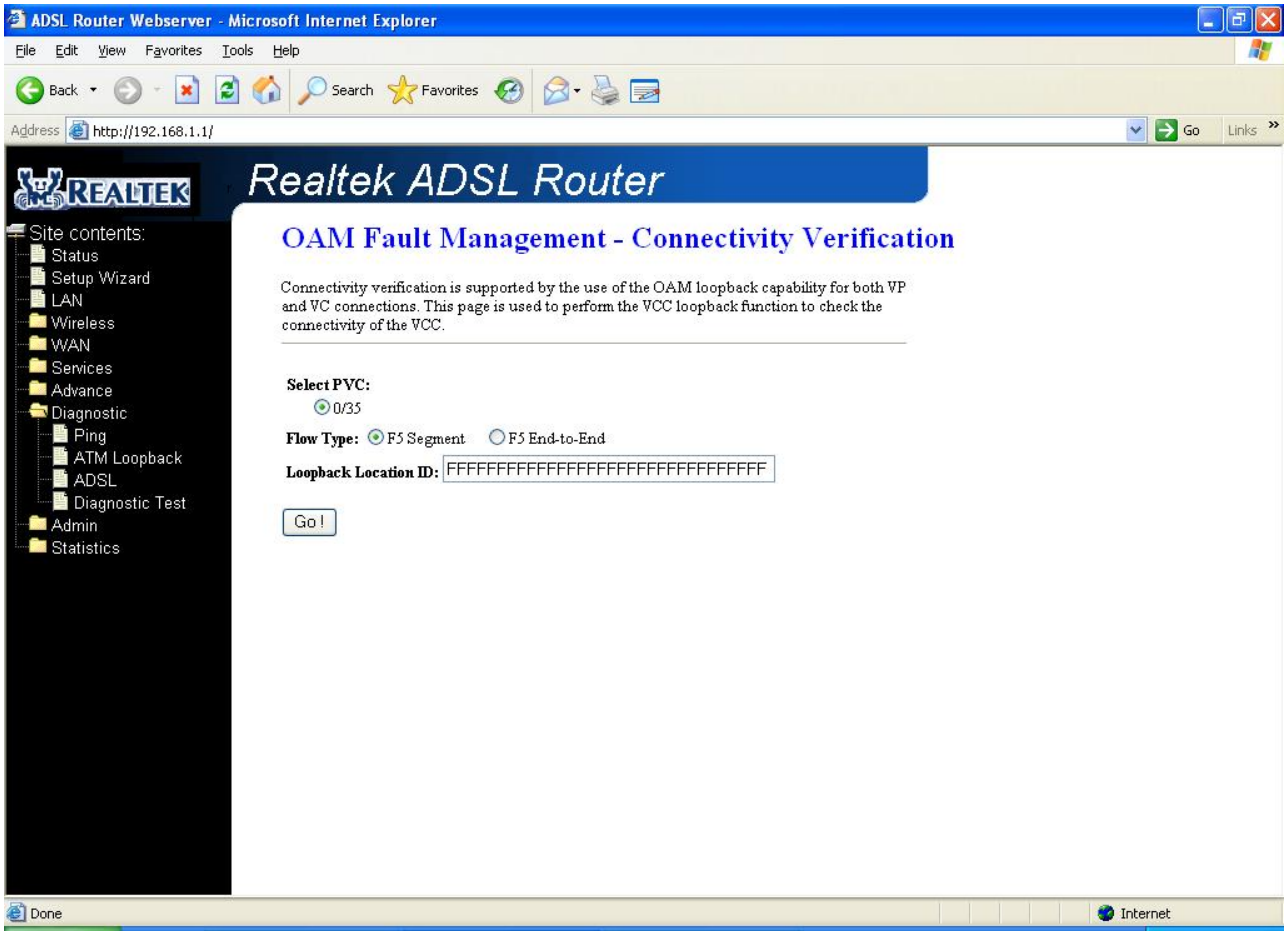


Fields in this page:

Field	Description
Host Address	The IP address you want to ping.

3.7.2 ATM Loopback

The **ATM Loopback** is used to check weather your Modem is properly connected to the WAN network. This test may take a few seconds to complete. Before running this test, make sure you have at least one WAN connection configured and have valid ADSL link; if the ADSL link is not connected, the test will fail. Figure below illustrates the ATM Test screen with one pvc pre-configured.

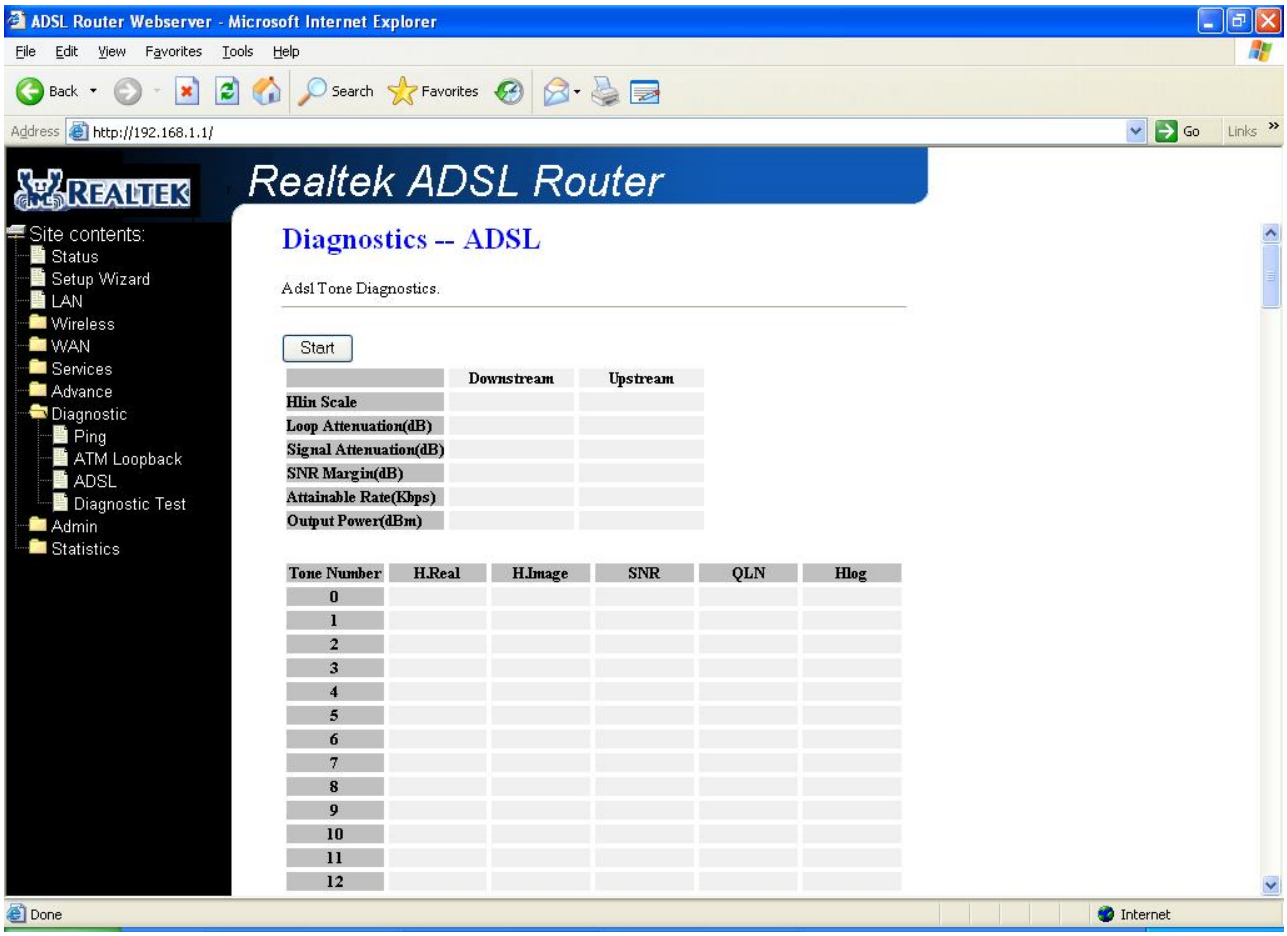


Fields in this page:

Field	Description
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.

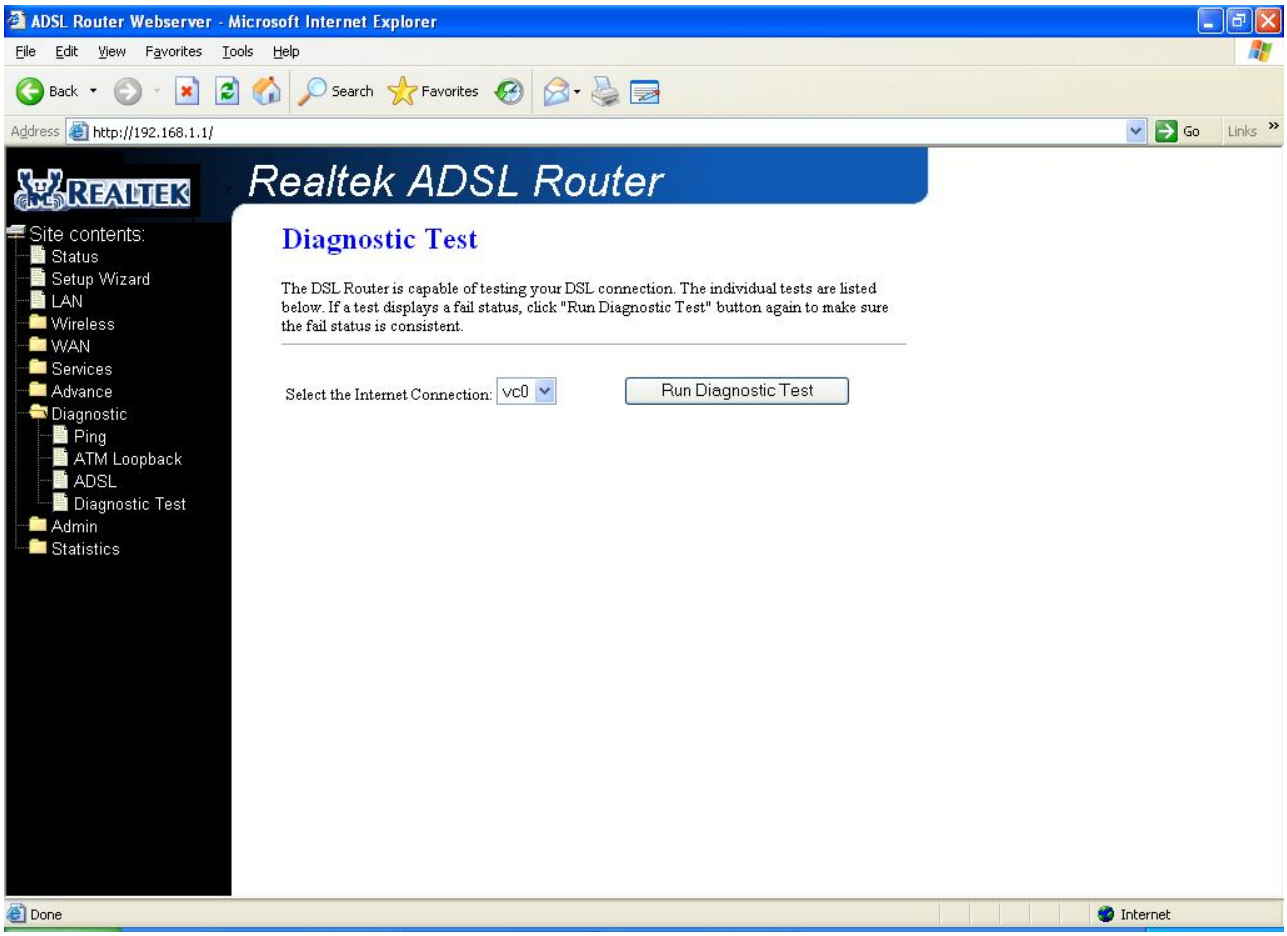
3.7.3 ADSL

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



3.7.4 Diagnostic Test

The page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides. Select an internet connection and click **Run Diagnostic Test** button to do the diagnostic test . The diagnostics utility will run a series of tests to check whether the device's connections are up and working. This will take only a few seconds. The program will report whether the test status is **Pass** or **Fail.**



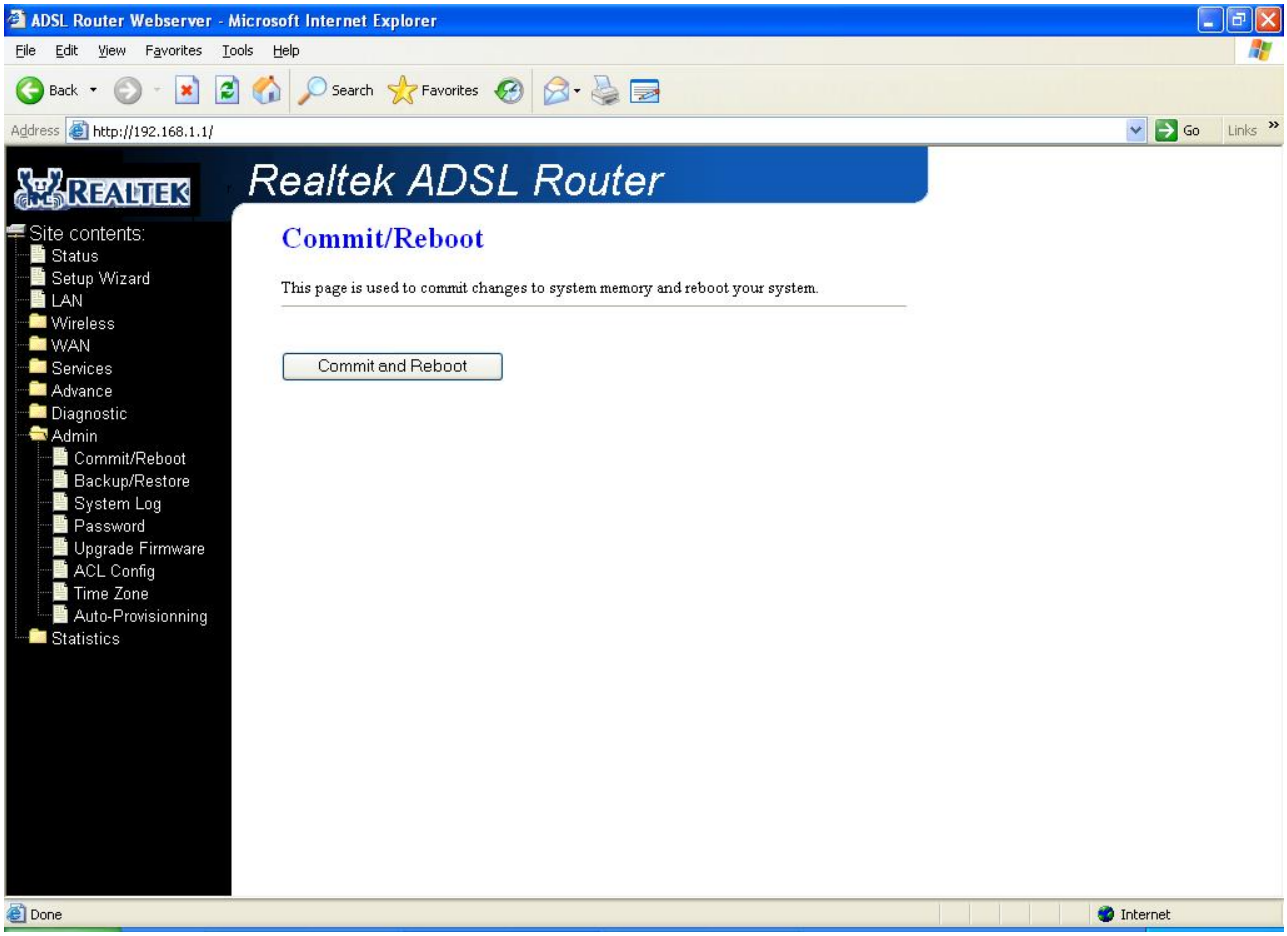
Fields in this page:

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

3.8 Admin

3.8.1 Commit/Reboot

Whenever you use the Web configuration to change system settings, the changes are initially placed in temporary storage. These changes will be lost if the device is reset or turn off. To save your change for future use, you can use the commit function.



Function buttons in this page:

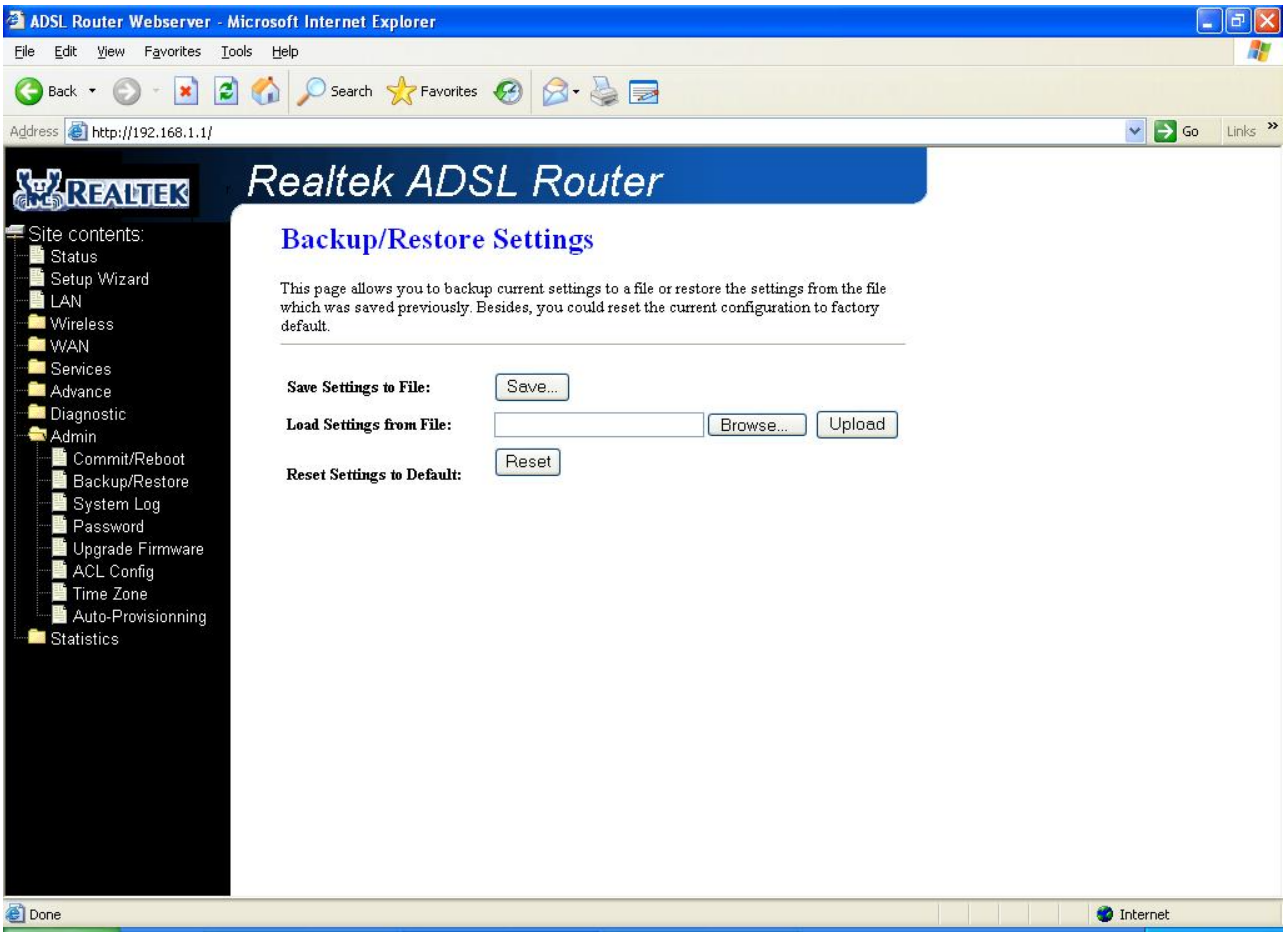
Commit and Reboot

Whenever you use the web console to change system settings, the changes are initially placed in temporary storage. To save your changes for future use, you can use the Commit/Reboot function. This function saves your changes from RAM to flash memory and reboot the system.

IMPORTANT! Do not turn off your modem or press the Reset button while this procedure is in progress.

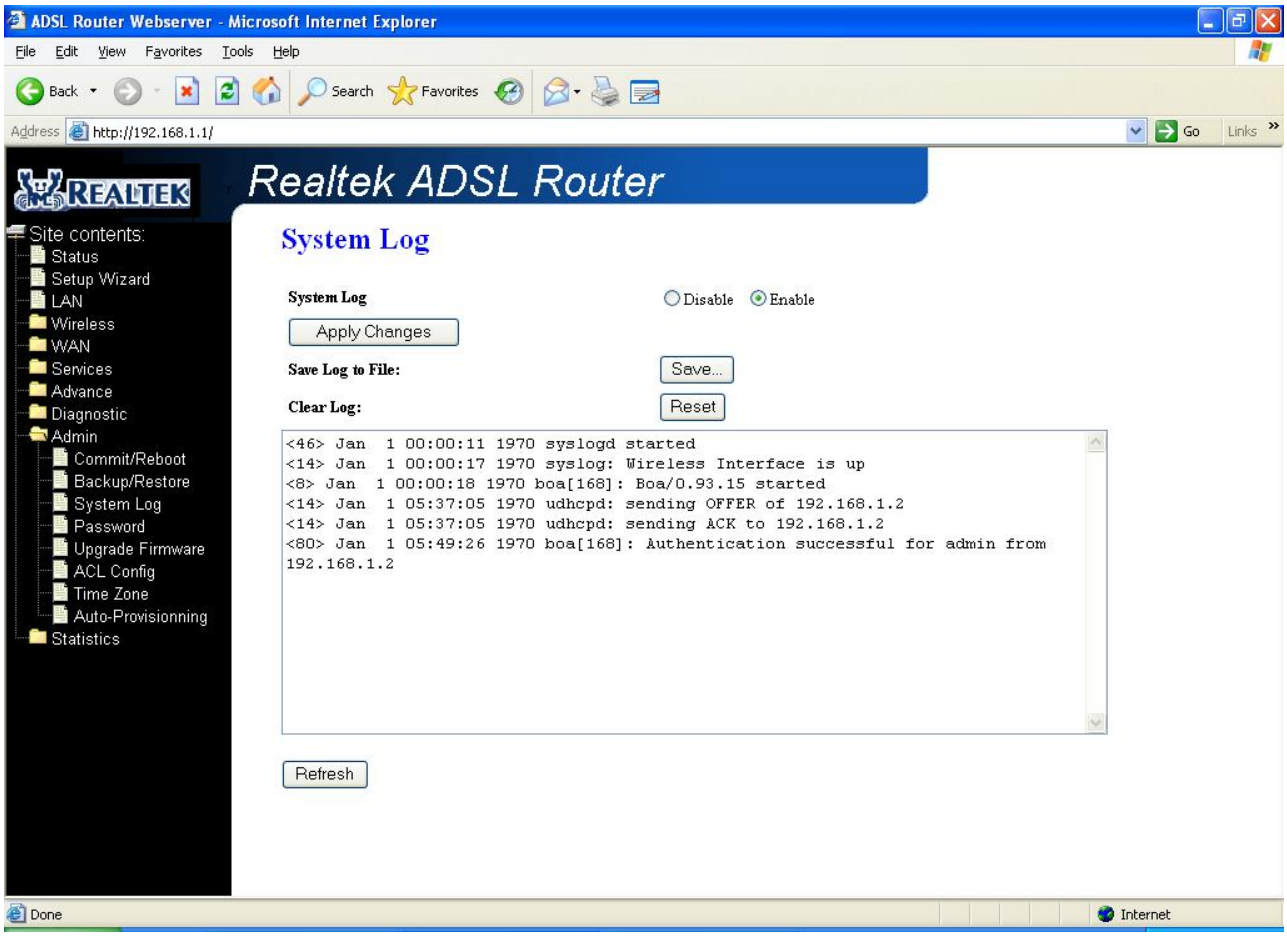
3.8.2 Backup/Restore

This page allows you to backup and restore your configuration into and from file in your host.



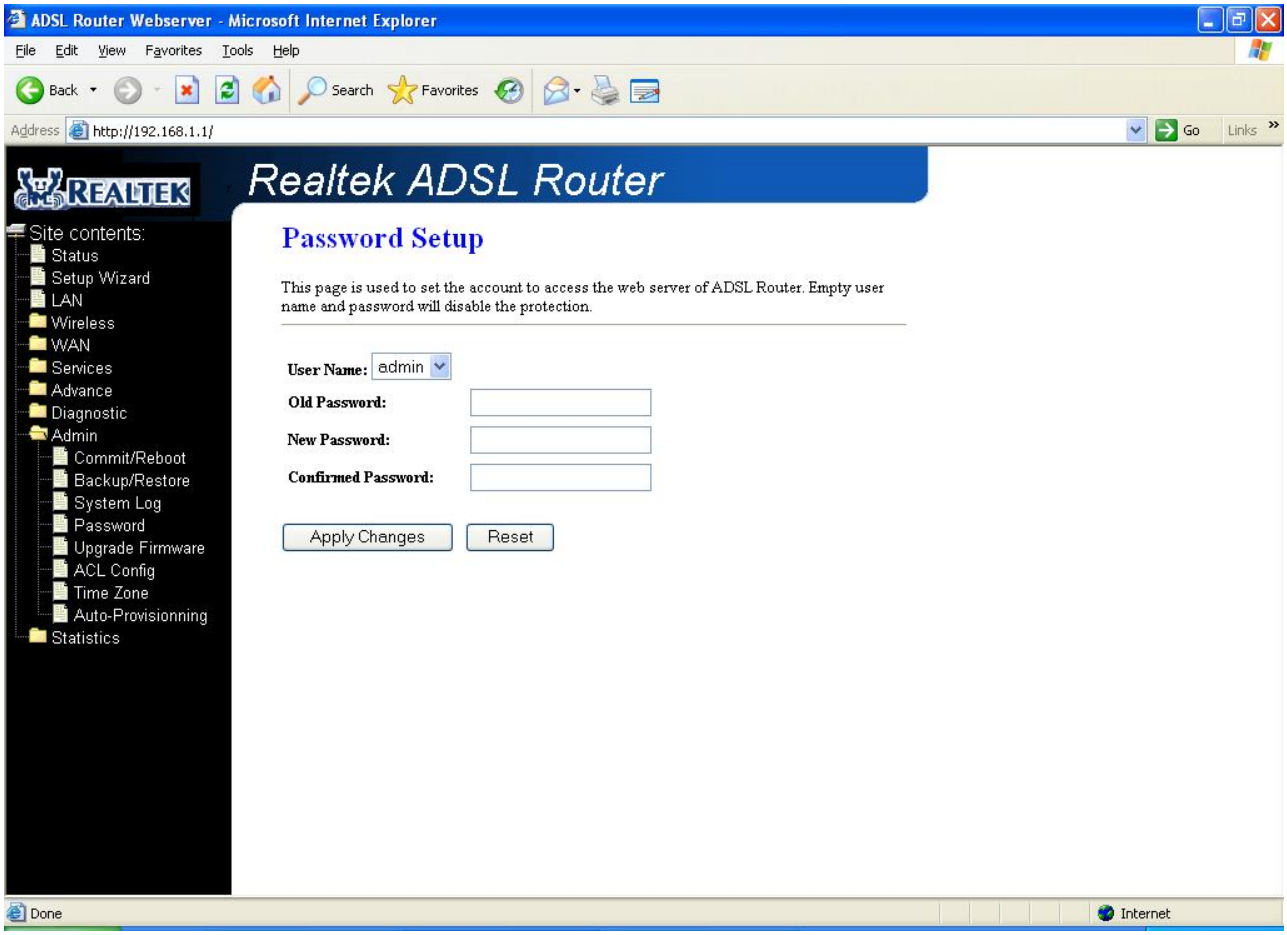
3.8.3 System Log

This page shows the system log.



3.8.4 Password

The first time you log into the system, 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.



Fields in this page:

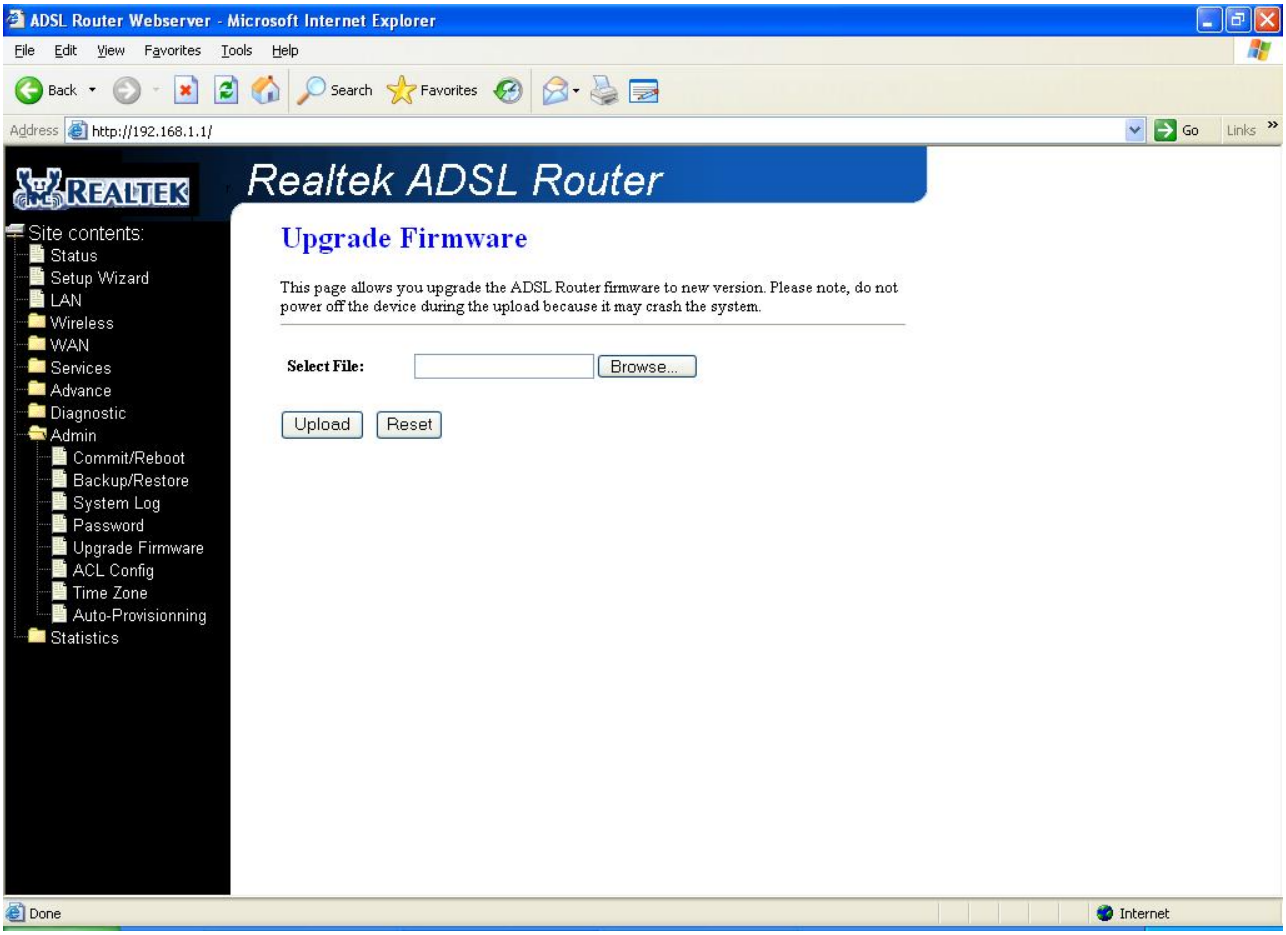
Field	Description
User Name	Selection of user levels are: admin and user.
Old Password	Enter the old password for this selected login.
New Password	Enter the new password here.
Confirmed Password	Enter the new password here again to confirm.

3.8.5 Upgrade Firmware

To upgrade the firmware for the DSL device:

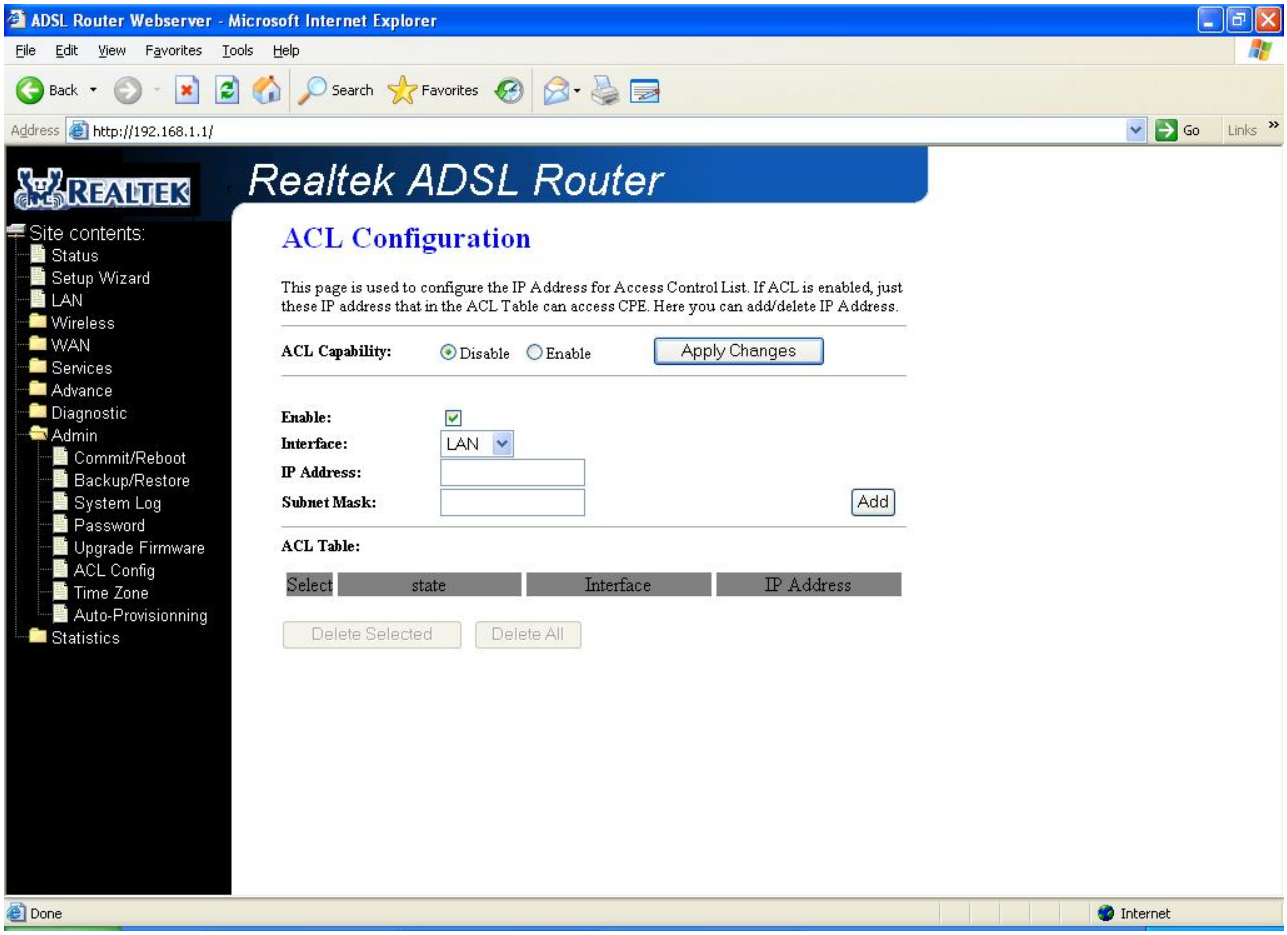
- Click the **Browse** button to select the firmware file.
- Confirm your selection.
- Click the **Upload** button to start upgrading.

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



3.8.6 ACL

The Access Control List (ACL) is a list of permissions attached to the DSL device. 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.

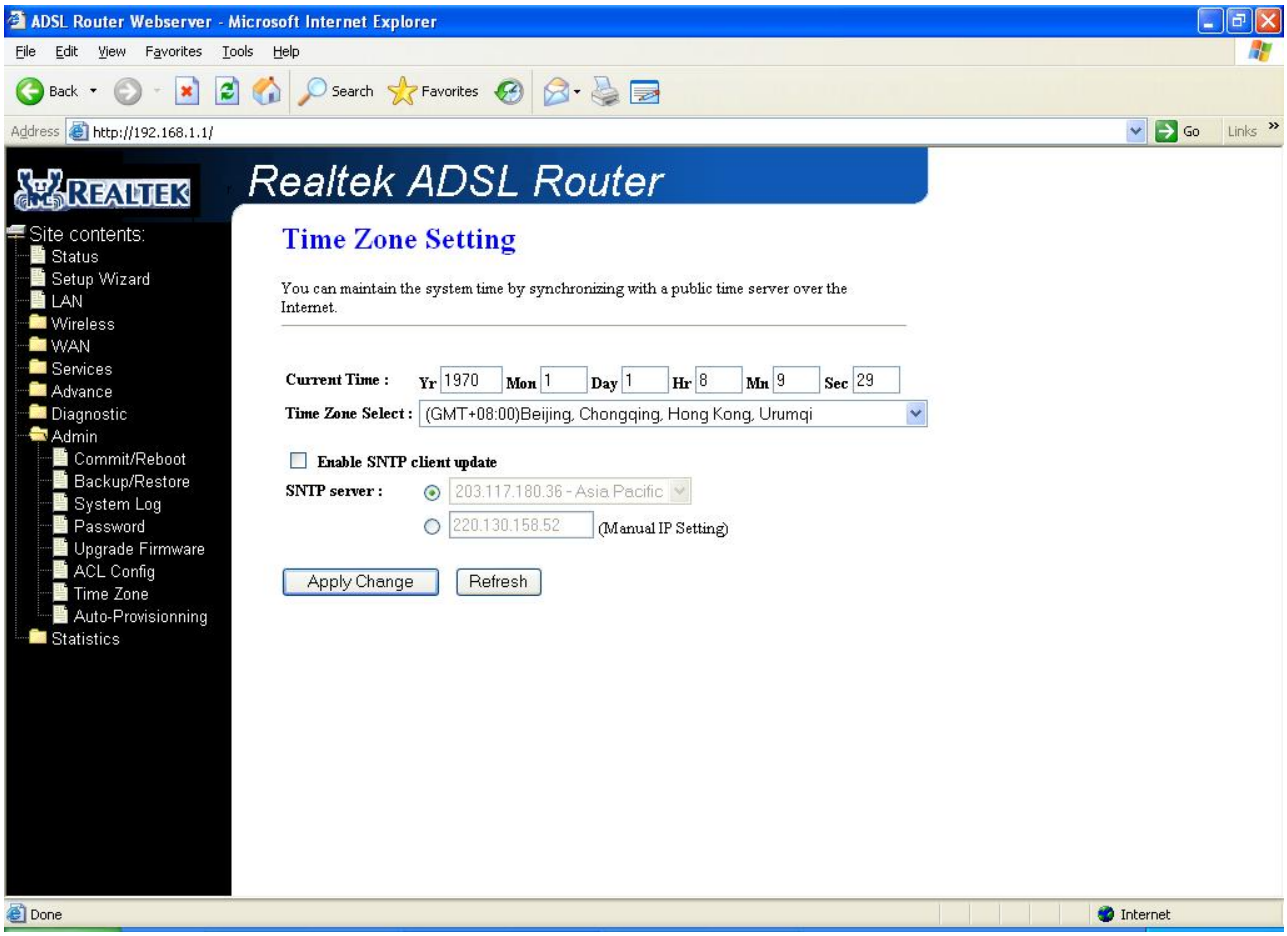


Fields in this page:

Field	Description
ACL Capability	Enable/disable the ACL function
Enable	Check to enable this ACL entry
Interface	Select the interface domain: LAN or WAN
IP Address	Enter the IP address that allow access to this device.

3.8.7 Time Zone

Simple Network Timing Protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. The DSL device 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 DSL device



Fields in this page:

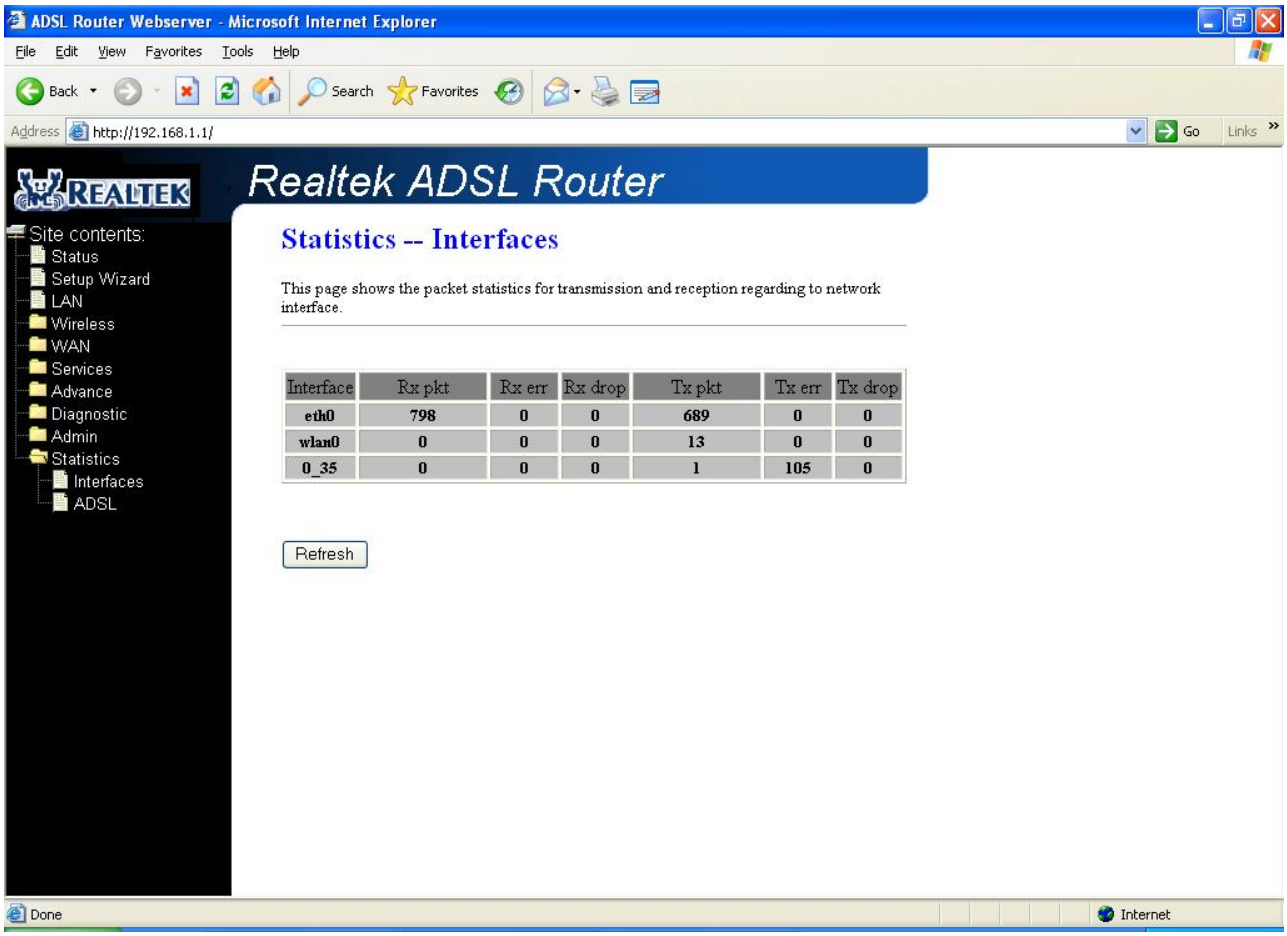
Field	Description
Current Time	The current time of the specified time zone. You can set the current time by yourself or configured by SNTP.
Time Zone Select	The time zone in which the DSL device resides.
Enable SNTP client update	Enable the SNTP client to update the system clock.
SNTP server	The IP address or the host name of the SNTP server. You can select from the list or set it manually.

3.9 Statistics

The DSL device shows the different layer of network statistics information.

3.9.1 Interfaces

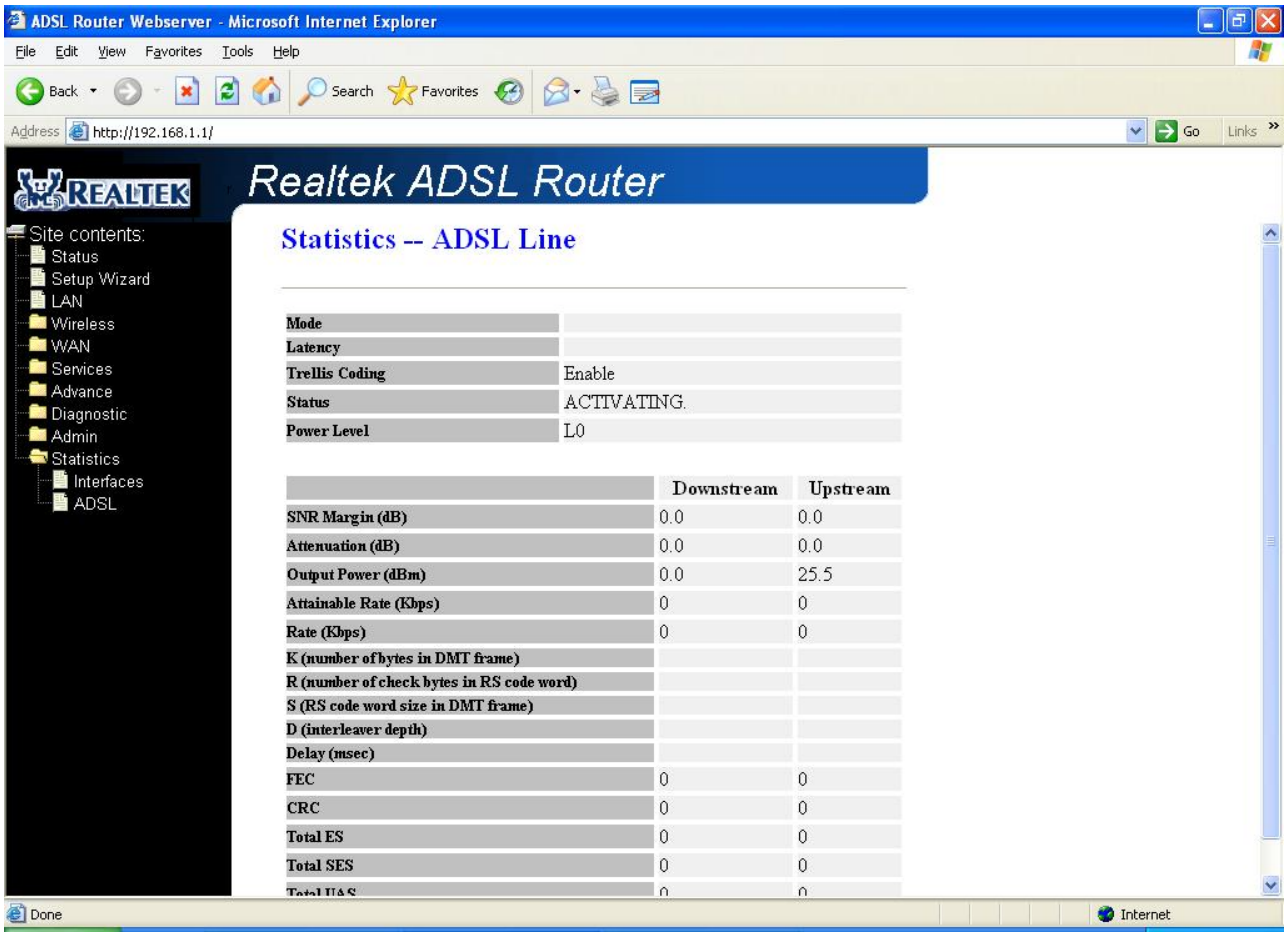
You can view statistics on the processing of IP packets on the networking interfaces. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.



To display updated statistics showing any new data since you opened this page, click **Refresh**.

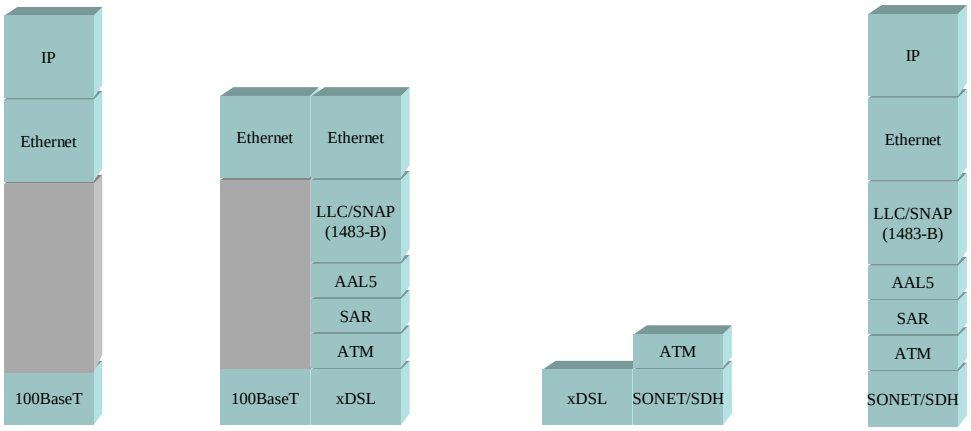
3.9.2 ADSL

This page shows the ADSL line statistic information.



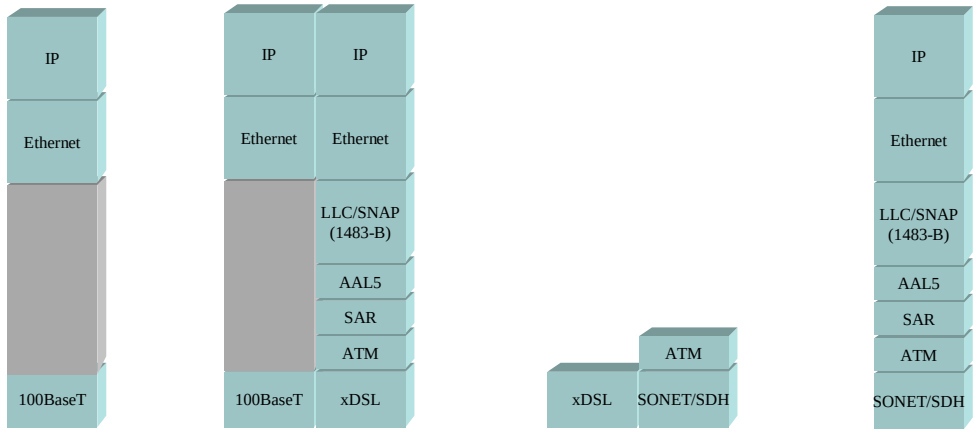
Appendix A: Protocol Stacks

1483 Bridged Model



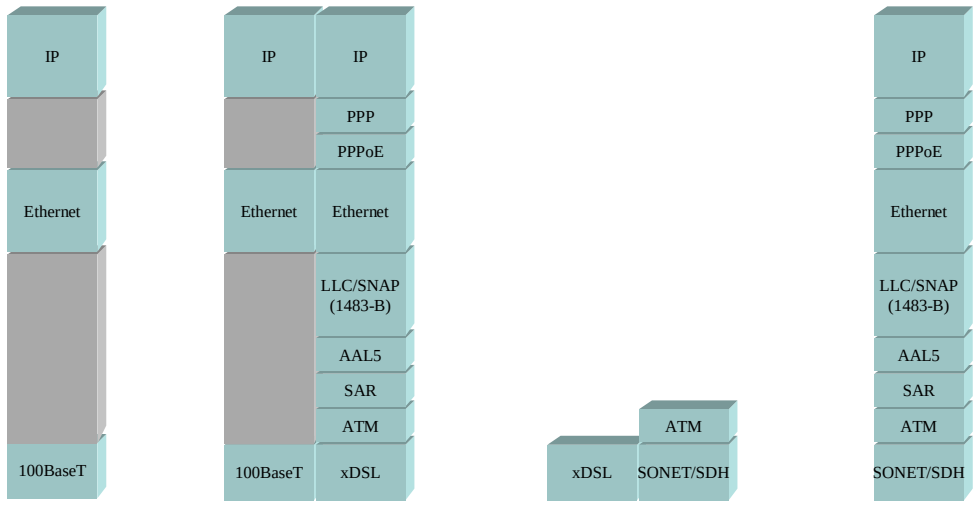
1483 Bridged Channel Mode Scenario

1483 MER Model



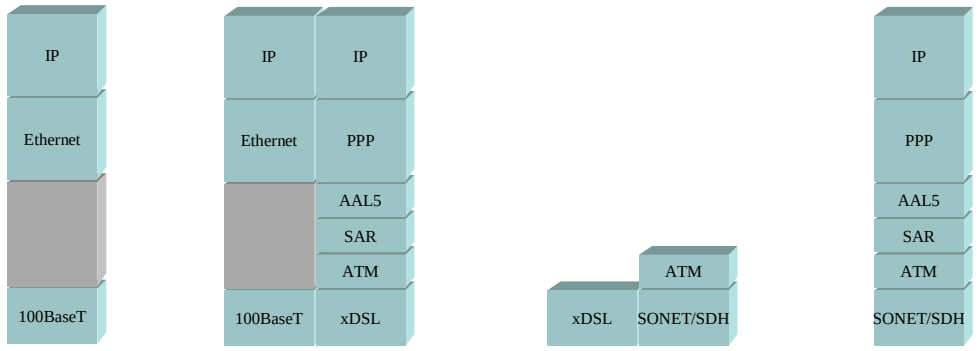
1483 MER Channel Mode Scenario

PPPoE Model



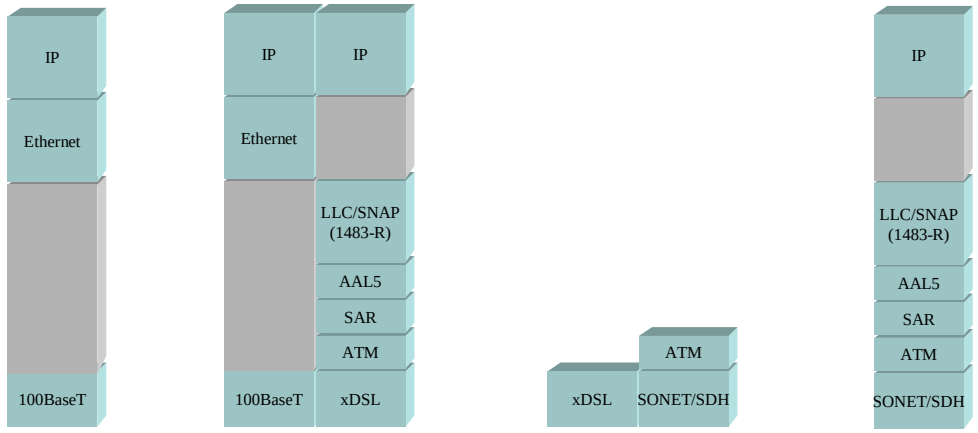
PPPoE Channel Mode Scenario

PPPoA Model



PPPoA Channel Mode Scenario

1483 Routed Model



1483 Routed Channel Mode Scenerio

Appendix B: Frequently Asked Questions

The Frequently Asked Questions addresses common questions regarding 4-Ports 11g Wireless ADSL2/2+ Router settings.

Some of these questions are also found throughout the guide, in the sections to which they reference.

1. **How do I determine if a link between the Ethernet card (NIC) and the 4-Ports 11g Wireless ADSL2/2+ Router has been established?**

Ans. A ping test would determine if a connection is established between your 4-Ports 11g Wireless ADSL2/2+ Router and computer. Using, the ping command, ping the IP address of the 4-Ports 11g Wireless ADSL2/2+ Router, in this case, 192.168.1.1 (default). For more information on Ping Testing, refer to Appendix C: Troubleshooting Guide. Alternatively, if the Ethernet LINK LED is solidly on, then the Ethernet link is established.

2. **How do I determine if a link between the 4-Ports 11g Wireless ADSL2/2+ Router and the Internet has been established?**

Ans. Similar to the previous question, a ping test would determine whether or not a connection is established. However, this time use a URL instead of and IP Address, such as www.google.com. Alternatively, if the ADSL LED is solidly on, then the ADSL link is established.

3. **How can I find/verify my 4-Ports 11g Wireless ADSL2/2+ Router and/or computer Ethernet MAC Address?**

Ans. Refer to **Status – Info** section for details.

4. **I can't get the Internet game, server, or application to work properly.**

Ans. If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one computer to the Internet using DeMilitarized Zone (DMZ) setting. Refer to **Advance – Port Forwarding** section for the setting detail.

5. **I need to upgrade the firmware.**

Ans. In order to upgrade the firmware with the latest features, check with your local dealer or ISP for technical support.

6. I forgot my password.

Ans. Reset the 4-Ports 11g Wireless ADSL2/2+ Router to factory default by pressing the Reset button for 5~15 seconds and then releasing it.

If you are still getting prompted for a password when saving settings, then perform the following steps:

1. Access the 4-Ports 11g Wireless ADSL2/2+ Router's web-based utility by going to http://192.168.1.1 or the IP address of the 4-Ports 11g Wireless ADSL2/2+ Router. Enter the default username and password **Admin**, and click the **Tools – User Management** tab.
2. Enter a different password in the 4-Ports 11g Wireless ADSL2/2+ Router Password field, and enter the same password in the second field to confirm the password.
3. Click the **Apply** button then click **Save All** to activate your setting.

7. What is MAC Address?

Ans. Short for **M**edia **A**ccess **C**ontrol Address. It is a hardware address that uniquely identifies each node of a Ethernet networking device. This address is usually permanent.

8. What is NAT (Network Address Translation) and what is it used for?

Ans. NAT translates multiple IP Address on the private LAN to one public IP Address (in WAN) that is sent out to the Internet. NAT adds a level security since the IP address of a PC connected to the private LAN is never transmitted on the Internet.

9. What can I do when I am not able to get the web configuration screen for this 4-Ports ADSL2/2+ Router?

Ans. Remove the proxy settings on your Internet Browsers or remove the dial-up settings on your browser.

10. What is DMZ (DeMilitarized zone)?

Ans. DMZ allows one IP Address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ features.

18. What is the maximum IP addresses supported by this 4-Ports 11g Wireless ADSL2/2+ Router?

Ans. The 4-Ports 11g Wireless ADSL2/2+ Router can support up to 253 IP addresses.

Appendix C: Troubleshooting Guide

The Troubleshooting Guide provides answers to common problems regarding the 4-Ports 11g Wireless ADSL2/2+ Router settings, connections, and computer settings.

1. The 4-Ports 11g Wireless ADSL2/2+ Router does not work (None of the LEDs light up)

Ans. Check the following:

1. Make sure that the 4-Ports ADSL2/2+ Router is plugged into a power socket.
2. Make sure that you are using the correct power supply for your 4-Ports ADSL2/2+ Router device.
3. Make sure the power switch on the 4-Ports 11g Wireless ADSL2/2+ Router is turned on.

2. I changed the LAN IP Address in the LAN configuration page and my PC is no longer able to detect the 4-Ports 11g Wireless ADSL2/2+ Router.

Ans. After changing the LAN IP Address of the 4-Ports 11g Wireless ADSL2/2+ Router, proceed to the following step before a PC is able to recognize the 4-Ports 11g Wireless ADSL2/2+ Router:

1. Click **"Start"** → **"Run"**.
2. In the open field, enter **"cmd"** then click **"OK"**.
3. In the command prompt, type **"ipconfig/release"** then press **"Enter"**.
4. Type **"ipconfig / renew"** then press **"Enter"**.

3. LAN (Link/Act) LED does not light up.

Ans. Check the following:

1. Make sure that the LAN cables are securely connected to the 10/100Base-T port.
2. Make sure that you are using the correct cable type for your Ethernet equipment.
3. Make sure the computer's Ethernet port is configured for auto-negotiation.

4. Failed to configure the 4-Ports 11g Wireless ADSL2/2+ Router through web browser (By a client PC in LAN)

Ans. Check the following:

1. Check the hardware connection of the 4-Ports 11g Wireless ADSL2/2+ Router's LAN port. The LED will lit when a proper connection is made.
2. Check your Windows TCP/IP setting (Refer to Chapter 3 for setting details).
3. Open the Windows System Command Prompt:

   - For Windows 9x/ME: Manually enter **winipcfg**, then press **Enter**.
   - For Windows 2000/XP/Vista: Manually enter **ipconfig/all**, then press **Enter**.

4. You should have the following information listed on your Window System:

   - **IP Address: 192.168.1.x**
   - **Submask: 255.255.255.0**
   - **Default Gateway IP: 192.168.1.1**

5. I forgot or lost my Administrator Password.

Ans. Reset the 4-Ports 11g Wireless ADSL2/2+ Router to factory default by pressing the **"Reset"** button for 5~15 seconds.

If you are still getting prompted for a password when saving settings:

1. Access the Router's web interface by going to **http://192.1681.1.**
2. Enter the default **"username"** and **"password"** then click **"Enter"** to log in.
3. Click on **"Tools"** then click "**User Management"**.
4. Enter a new **"Password"** and new **"Username"** in the **"Username"** and "**Password"** field, and enter the same password in the second field to confirm the password.
5. Click **"Apply"** after setup then click **Save All** to activate your setting.

6. I need to upgrade the Firmware.

Ans. In order to upgrade the Firmware with the latest features, check your local dealer or ISP for technical support. Before proceed the upgrading process, check the following details:

1. Download the latest Firmware and save at your pointed location.
2. Read the firmware release note carefully before proceed the upgrading process.
3. Refer to **Tools - Update Gateway** section for the upgrading process.

7. Testing LAN path to your 4-Ports 11g Wireless ADSL2/2+ Router.

Ans. To verify whether the LAN path from your PC to your 4-Ports 11g Wireless ADSL2/2+ Router is properly connected, you can **"Ping"** the 4-Ports 11g Wireless ADSL2/2+ Router with the following procedures:

1. From the Windows toolbar, click **"Start"** and select **"Run".**
2. In the open field, type **"Ping 192.168.1.1"** and click **"OK"**
3. If the path is working, you should see the message in the following format:
   Reply from 192.168.1.1 bytes = 32 time < 10ms TTL = 60
4. If the path is not working, you should see the following message:
   Request timed out

If the path is not functioning correctly:

1. Make sure the LAN port LED indicator is on.
2. Check whether you are using the correct LAN cable.
3. Check your Ethernet Adaptor installation and configurations.
4. Verify that the IP address for your 4-Ports 11g Wireless ADSL2/2+ Router and your workstation are correct and that the addresses are on the same subnet.

Appendix D: Glossary

The Glossary provides an explanation of terms and acronyms discussed in this user guide.

10BASE-T: IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx: IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.1x: 802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management. The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys.

ATM: Asynchronous Transfer Mode: A method of transfer in which data is organized into 53-byte cell units. ATM cells are processed asynchronously in relation to other cells.

BC: Broadcast: Communication in which a sender transmits to everyone in the network.

BER: Bit Error Rate: Percentage of Bits that contain errors relative to the total number of bits transmitted.

Bridge: A device that connects two networks and decides which network the data should go to.

Bridge Mode: Bridge Mode is used when there is one PC connected to the LAN-side Ethernet or USB port. IEEE 802.1D method of transport bridging is used to bridge between the WAN (ADSL) side and the LAN (Ethernet or USB) side, i.e., to store and forward.

CBR: Constant Bit Rate: A constant transfer rate that is ideal for streaming (executing while still downloading) data, such as audio or video files.

Cell: A unit of transmission in ATM, consisting of a fixed-size frame containing a 5-octet header and a 48-octet payload.

CHAP: Challenge Handshake Authentication Protocol: Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

CLP: Cell Loss Priority: ATM cells have two levels of priority, CLP0 and CLP1. CLP0 is of higher priority, and in times of high traffic congestion, CLP1 error cells may be discarded to preserve the Cell Loss Ratio of the CLP0 cells.

CO: Central Office: In a local loop, a Central Office is where home and office phone lines come together and go through switching equipment to connect them to other Central Offices. The distance from the Central Office determines whether or not an ADSL signal can be supported in a given line.

CPE: Customer Premises Equipment. This specifies equipment on the customer, or LAN, side.

CRC: Cyclic Redundancy Checking: A method for checking errors in a data transmission between two computers. CRC applies a polynomial function (16 or 32-bit) to a block of data. The result of that polynomial is appended to the data transmission. Upon receipt, the destination computer applies the same polynomial to the block of data. If the host and destination computer share the same result, the transmission was successful. Otherwise, the sender is notified to re-send the data block.

DHCP: Dynamic Host Configuration Protocol: A communications protocol that allows network administrators to manage and assign IP addresses to computers within the network. DHCP provides a unique address to a computer in the network which enables it to connect to the Internet through Internet Protocol (IP). DHCP can lease and IP address or provide a permanent static address to those computers who need it (servers, etc.).

DMZ: Demilitarized Zone: A computer Host or network that acts as a neutral zone between a private network and a public network. A DMZ prevents users outside of the private network from getting direct access to a server or any computer within the private network. The outside user sends requests to the DMZ, and the DMZ initiates sessions in the public network based on these requests. A DMZ cannot initiate a session in the private network, it can only forward packets to the private network as they are requested.

DNS: Domain Name System: A method to locate and translate Domain Names into Internet Protocol (IP) addresses, where a Domain Name is a simple and meaningful name for an Internet address.

DSL: Digital Subscriber Line: A technology that provides broadband connections over standard phone lines.

DSLAM: Digital Subscriber Line Access Multiplexer: Using multiplexing techniques, a DSLAM receives signals from customer DSL lines and places the signals on a high-speed backbone line. DSLAMs are typically located at a telephone company's CO (Central Office).

Encapsulation: The inclusion of one data structure within another. For example, packets can be encapsulated in an ATM frame during transfer.

FEC: Forward Error Correction: An error correction technique in which a data packet is processed through an algorithm that adds extra error correcting bits to the packet. If the transmitted message is received in error, these bits are used to correct the errored bits without retransmission.

Firewall: A firewall is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

Fragmentation: Breaking a packet up into smaller packets that is caused either by the transmission medium being unable to support the original size of the packet or the receiving computer not being able to receive a packet of that size. Fragmentation occurs when the sender's MTU is larger than the receiver's MRU.

FTP: File Transfer Protocol. A standardized internet protocol which is the simplest way to transfer files from one computer to another over the internet. FTP uses the Internet's TCP/IP protocols to function.

Full Duplex: Data transmission can be transmitted and received on the same signal medium and at the same time. Full Duplex lines are bidirectional.

G.dmt: Formally G.992.1, G.dmt is a form of ADSL that uses Discrete MultiTone (DMT) technology. G.dmt incorporates a splitter in its design.

G.lite: Formally G.992.2, G.lite is a standard way to install ADSL service. G.lite enables connections speeds up to 1.5 Mbps downstream and 128 kbps upstream. G.lite does not need a splitter at the user end because splitting is preformed at the remote end (telephone company).

Gateway: A point on the network which is an entrance to another network. For example, a router is a gateway that connects a LAN to a WAN.

Half Duplex: Data transmission can be transmitted and received on the same signal medium, but not simultaneously. Half Duplex lines are bi-directional.

HEC: Headed Error Control: ATM error checking by using a CRC algorithm on the fifth octet in the ATM cell header to generate a check character. Using HEC, either a single bit error in the header can be corrected or multiple bit errors in the header can be detected.

HNP: Home Network Processor

Host: In context of Internet Protocol, a host computer is one that has full two way access to other computers on the Internet.

IP: Internet Protocol: The method by which information is sent from one computer to another through the Internet. Each of these host computers have a unique IP address which distinguishes it from all the other computers on the internet. Each packet of data sent includes the sender's IP address and the receiver's IP address.

LAN: Local Area Network: A group of computers, typically covering a small geographic area, that share devices such as printers, hard disk drives, scanners, and optical drives. Computers in a LAN typically share an internet connection through some sort of router that connects the computers to a WAN.

LLC: Logical Link Control: Provides an interface point to the MAC sublayer. LLC Encapsulation is needed when several protocols are carried over the same Virtual Circuit.

MAC Address: Media Access Control Address: A unique hardware number on a computer or device that identifies it and relates it to the IP address of that device.

MC: Multicast: Communication involving a single sender and multiple specific receivers in a network.

MRU: Maximum Receive Unit: MRU: Maximum Receive Unit (MRU) is the largest size packet that can be received by the modem. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

MSS: Maximum Segment Size: The largest size of data that TCP will send in a single, unfragmented IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their Maximum Segment Size during the TCP connection handshake.

MTU: Maximum Transmission Unit: The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU).

NAPT: Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the

individual device IP addresses translated by the NAPT.

NAT: Network Address Translation: The translation of an IP address of one network to a different IP address known by another network. This gives an outside (WAN) network the ability to distinguish a device on the inside (LAN) network, as the inside network has a private set of IP address assigned by the DHCP server not known to the outside network.

PAP: Password Authentication Protocol: An authentication protocol in which authorization is done through a user name and password.

PDU: Protocol Data Unit: A frame of data transmitted through the data link layer 2.

Ping: Packet Internet Groper: A utility used to determine whether a particular device is online or connected to a network by sending test packets and waiting for a response.

PPP: Point-to-Point Protocol: A method of transporting and encapsulating IP packets between the user PC and the ISP. PPP is full duplex protocol that is transmitted through a serial interface.

Proxy: A device that closes a straight connection from an outside network (WAN) to an inside network (LAN). All transmissions must go through the proxy to get into or out of the LAN. This makes the internal addresses of the devices in the LAN private.

PVC: Permanent Virtual Circuit: A software defined logical connection in a network; A Virtual Circuit that is permanently available to the user.

RIP: Routing Information Protocol: A management protocol that ensures that all hosts in a particular network share the same information about routing paths. In a RIP, a host computer will send its entire routing table to another host computer every X seconds, where X is the supply interval. The receiving host computer will in turn repeat the same process by sending the same information to another host computer. The process is repeated until all host computers in a given network share the same routing knowledge.

RIPv1: RIP Version 1: One of the first dynamic routing protocols introduced used in the internet, RIPv1 was developed to distribute network reach ability information for what is now considered simple topologies.

RIPv2: RIP Version 2: Shares the same basic concepts and algorithms as RIPv1 with added features such as subnet masks, authentication, external route tags, next hop addresses, and multicasting in addition to

broadcasting.

Router Mode: Router Mode is used when there is more than one PC connected to the LAN-side Ethernet and/or USB port. This enables the ADSL WAN access to be shared with multiple nodes on the LAN. Network Address Translation (NAT) is supported so that one WAN-side IP address can be shared among multiple LAN-side devices. DHCP is used to serve each LAN-side device and IP address.

SNAP: SubNetwork Attachment Point.

SNMP: Simple Network Management Protocol: Used to govern network management and monitor devices on the network. SNMP is formally described in RFC 1157.

SNR: Signal-to-Noise Ratio: Measured in decibels, SNR is a calculated ratio of signal strength to background noise. The higher this ratio, the better the signal quality.

Subnet Mask: Short for SubNetwork Mask, subnet mask is a technique used by the IP protocol to filter messages into a particular network segment, called a subnet. The subnet mask consists of a binary pattern that is stored in the client computer, server, or router. This pattern is compared with the incoming IP address to determine whether to accept or reject the packet.

TCP: Transfer Control Protocol: Works together with Internet Protocol for sending data between computers over the Internet. TCP keeps track of the packets, making sure that they are routed efficiently.

TFTP: Trivial File Transfer Protocol: A simple version of FTP protocol that has no password authentication or directory structure capability.

Trellis Code: An advanced method of FEC (Forward Error Correction). When enabled, it makes for better error checking at the cost of slower packet transmission. Setting Trellis Code to Disabled will cause increased packet transmission with decreased error correction.

TTL: Time To Live: A value in an IP packet that indicates whether or not the packet has been propagating through the network too long and should be discarded.

UBR: Unspecified Bit Rate: A transfer mode that is usually used in file transfers, email, etc. UBR can vary depending on the data type.

UDP: User Datagram Protocol: A protocol that is used instead of TCP when reliable delivery is not required.

Unlike TCP, UDP does not require an acknowledgement (handshake) from the receiving end. UDP sends packets in one-way transmissions.

VBR-nrt: Variable Bit Rate – non real time: With VBR-nrt, cell transfer is variable upon certain criteria.

VC: Virtual Circuit: A virtual circuit is a circuit in a network that appears to be a physically discrete path, but is actually a managed collection of circuit resources that allocates specific circuits as needed to satisfy traffic requirements.

VCI: Virtual Channel Identifier: A virtual channel identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel.

VC-Mux: Virtual Circuit based Multiplexing: In VC Based Multiplexing, the interconnect protocol of the carried network is identified implicitly by the VC (Virtual Circuit) connecting the two ATM stations (each protocol must be carried over a separate VC).

VPI: Virtual Path Identifier: Virtual path for cell routing indicated by an eight bit field in the ATM cell header.

WAN: Wide Area Network: A WAN covers a large geographical area. A WAN is consisted of LANs and the Internet is consisted of WANs.