

**IEEE 802.11n
Wireless LAN 4-port
ADSL2+ Router**

User's Manual

January 2011

FCC Warning

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

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

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of about eight inches (20cm) between the radiator and your body.

This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter. IEEE802.11b or 802.11g operation of this product in the USA is firmware-limited to channels 1 through 11.

Notice

Changes or modifications to the equipment, which are not approved by the party responsible for compliance could affect the user's authority to operate the equipment. Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information.

Copyright

2011 All Rights Reserved.

No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:

All trade names and trademarks are the properties of their respective companies.

Revision History

Revision	History
V1	1 st Release

Table of Contents

1. Introduction	5
1.1 Features	5
1.2 Package Contents	8
1.3 System Requirements.....	8
1.4 LEDs Indication & Connectors of Wireless Router	8
1.5 Connect Related Device	9
2. PC Configuration	10
2.1 TCP/IP Networking Setup	10
3. Configure Wireless Router via Web Based Utility	21
3.1 Login	21
3.2 Status	23
3.3 LAN	23
3.4 Wireless	24
3.4.1 Basic Settings	24
3.4.2 Advanced Settings.....	26
3.4.3 Security.....	27
3.4.4 Access Control.....	28
3.4.5 WPS	28
3.4.6 MBSSID	29
3.5 WAN.....	30
3.5.1 Channel Configuration.....	30
3.5.2 ATM Settings	31
3.5.3 ADSL Settings	33
3.6 Service.....	34
3.6.1 DHCP.....	34
3.6.2 DNS.....	36
3.6.3 Firewall.....	37
3.6.3.1 IP/Port Filtering	37
3.6.3.2 MAC Filtering.....	39
3.6.3.3 Port Forwarding.....	39
3.6.3.4 URL Blocking.....	40
3.6.3.5 Domain Blocking.....	41
3.6.3.6 DMZ	42
3.6.4 IGMP Proxy	43
3.6.5 UPnP	44

3.6.6 RIP	45
3.7 Advance	46
3.7.1 ARP Table	46
3.7.2 Bridging	47
3.7.3 Routing	48
3.7.4 SNMP	49
3.7.5 Port Mapping	50
3.7.6 IP QoS	51
3.7.7 Remote Access	53
3.7.8 Others	54
3.8 Diagnostic.....	55
3.8.1 Ping.....	55
3.8.2 ATM Loopback.....	56
3.8.3 ADSL	57
3.8.4 Diagnostic Test	58
3.9 Admin	58
3.9.1 Commit/Reboot	58
3.9.2 Backup/Restore.....	59
3.9.3 Password.....	60
3.9.4 Upgrade Firmware	61
3.9.5 ACL Configuration.....	62
3.9.6 Time Zone	63
3.9.7 TR-069 Configuration.....	64
3.10 Statistics	66
3.10.1 Interface.....	66
3.10.2 ADSL	67

1. Introduction

This full rate ADSL2+ router is an all-in-one Wireless ADSL2+ router for Home and SOHO applications. This gateway are with full-featured ADSL router that provides high-speed Internet access, 4-port Ethernet switch direct connections to individual PCs or local area network with 10/100 Base-T Ethernet and a 300Mbps IEEE802.11n wireless connectivity. WA41R uses advanced ADSL chipset solution with complete set of industry standard features for high-speed Internet access. Also built-in 300 Mbps IEEE802.11n wireless services can provide you easy and convenient way to connect the PCs and Internet. User can enjoy higher quality multimedia and real-time applications such as online gaming, Video-on-Demand, VoIP and other bandwidth consuming services. Also the feature-rich routing functions are seamlessly integrated to ADSL service for existing corporate or home users. This product is made in ISO9001 approved factory and complies with FCC part15 regulations and CE approval.

1.1 Features

◆ High Speed Internet Access

This ADSL router complies with ADSL / ADSL2 / ADSL2+ standards. It can support downstream rates of up to 24Mbps and upstream rates of up to 1Mbps. This ADSL router is compliant with the following standards.

- ANSI T1.413 issue 2
- ITU-T G.992.1 (G.dmt)
- ITU-T G.992.2 (G.lite)
- G.994.1 (G.hs, Multimode)
- ITU-T G.992.3 (ADSL2 G.dmt.bis)
- ITU-T G.992.4 (ADSL2 G.lite.bis)
- ITU-T G.992.5 (ADSL2+; Annex A, B, L & M)
- Reach Extended ADSL (RE ADSL)

◆ Multi-connection protocol support

- Support up to 8 PVCs
- ATM forum uni 3.1/4.0 PVC
- Multi Protocol over AAL5 (RFC1483 / 2684)
- VC and LLC Multiplexing
- PPP over Ethernet (RFC 2516)
- PPP over ATM (RFC 2364)
- Traffic shaping (ATM QoS) UBR, CBR, VBR, VBR-rt, VBR-nrt
- OAM F4 and F5 segment end-to-end loop-back, AIS, and RDI OAM cells
- VPI is 0-255 and VIC is 32-65535

- ◆ **Bridging / Routing support**
 - Ethernet to ADSL self-learning Transparent Bridging (IEEE 802.1d)
 - IP routing-RIPv2 (backward compatible with RIPv1)
 - Static IP routing
 - Routing (TCP/IP/UDP/ARP/ICMP)
 - IP Multicast IGMP v1/v2

- ◆ **IP Management**
 - NAT (Network Address Translation)
 - NAT (Network Address and Port Translation)
 - DHCP Server / Relay / Client (WAN port)
 - VPN (IPSec, PPTP, L2TP) Pass-Through
 - DNS Proxy
 - Dynamic DNS
 - UPnP support
 - Virtual Server (Port forwarding & DMZ host)

- ◆ **WLAN Network**
 - Compatible with IEEE 802.11n/b/g
 - 64/128 bits WEP Encryption
 - WPA-PSK, TKIP / WPA2-AES, PSK
 - Supports Quality of Service (QoS), 802.11e, WMM
 - MAC Address Filtering

- ◆ **Security**
 - PPP over PAP (Password Authentication Protocol; RFC1334)
 - PPP over CHAP (Challenge Authentication Protocol; RFC1994)
 - DOS Protection
 - Stateful Packet Inspection (SPI)
 - Built-in NAT Firewall
 - IP-based Packet filtering
 - Password Protected System Management

- ◆ **Web-Based Management**
 - Web-Based GUI configuration / Management
 - CLI (Command Line Interface) via serial interface or Telnet over Ethernet
 - Telnet Remote Management

- Firmware upgrade via FTP / TFTP
- SNMP Support
- HTTPS Support
- Built-in Diagnostic Tool
- TR-069 support

◆ **Network Address Translation (NAT)**

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

◆ **Universal Plug and Play (UPnP)**

Universal Plug and Play is a standard that uses Internet and Web protocols to enable devices such as PCs, peripherals, intelligent appliances, and wireless devices to be plugged into a network and automatically know about each other. This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs.

◆ **Dynamic DNS Support**

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS client.

◆ **DHCP Support**

DHCP (Dynamic Host Configuration Protocol) allows individual clients to obtain TCP/IP configuration at start-up from a centralized DHCP server. The ADSL router has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. It can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

◆ **SNMP (Simple Network Management Protocol) Support**

It's an easy way to remote control the router via SNMP.

◆ **Multiple PVC (Permanent Virtual Circuits) Support**

- Supports OAM F4/F5 loop-back, AIS and RDI OAM cells.
- ATM Forum UNI 3.1/4.0 PVC
- Support up to 8PVCs.

1.2 Package Contents

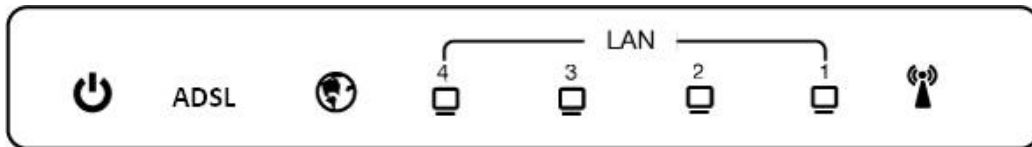
- One ADSL Router
- One CD-ROM (user's manual)
- One Ethernet Cable (RJ-45)
- One phone cable (RJ-11)
- One power adapter




1.3 System Requirements

- Computers with an installed Ethernet adapter.
- Valid Internet Access account and Ethernet based DSL or Cable modem.
- 10/100Base-T Ethernet cable with RJ-45 connector.
- TCP/IP protocol must be installed on all PCs.
- System with MS Internet Explorer ver. 5.0 or later, or Netscape Navigator ver. 4.7 or later.

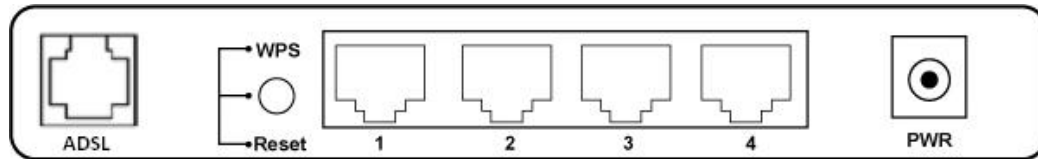
1.4 LEDs Indication & Connectors of Wireless Router

Front Panel LEDs Indication



LED	Light Status	Description
	On	Wireless Router is powered on.
	Off	Wireless Router is powered off.
ADSL	On	WAN port is successfully connected
	Blinking	Data is being sent or received.
INTERNET 	Blinking	Router is transferring data between Internet and router
LAN (1, 2, 3, 4)	On	LAN port is successfully connected.
	Blinking	Data is being sent or received.
WLAN 	Slow Blinking	WLAN is successfully connected.
	Blinking	Data is being sent or received.

Back Panel Connectors



Button/Port	Description
Reset	Reset configurations to default. You would use the reset button only when a program error has caused your Wireless AP router to hang. Press the button and hold after 6 seconds.
WPS	Click WPS button 1 to 3 seconds while you are connecting a PC or wireless adapter with WPS function (you must enable WPS' PBC function).
LAN (1x, 2x, 3x, 4x)	Ethernet RJ-45 connector, connect to PC with a RJ-45 Ethernet cable.
ADSL	Ethernet RJ-11 connector, connect to ADSL access device, such as the Cable modem or ADSL modem.
PWR	Power connector, connect to the power adapter packaged with the AP router.

1.5 Connect Related Device

1) Connect Router to **LINE**

Plug the provided **RJ-11 phone cable** into **ADSL port** on the back panel of the router and insert the other end into splitter or wall phone jack.

2) Connect Router to **LAN**

Plug **RJ-45 Ethernet Cable** into **LAN port** on the back panel of the router and insert the other end of the Ethernet cable on your PC's Ethernet port or switch / hub.

3) Connect Router to Power Adapter

Plug **Power Adapter** to **PWR port** on the back panel of the router and the other end to a power outlet.

Warning: Only use the power adapter is provided from this package, use other power adapter may cause hardware damage

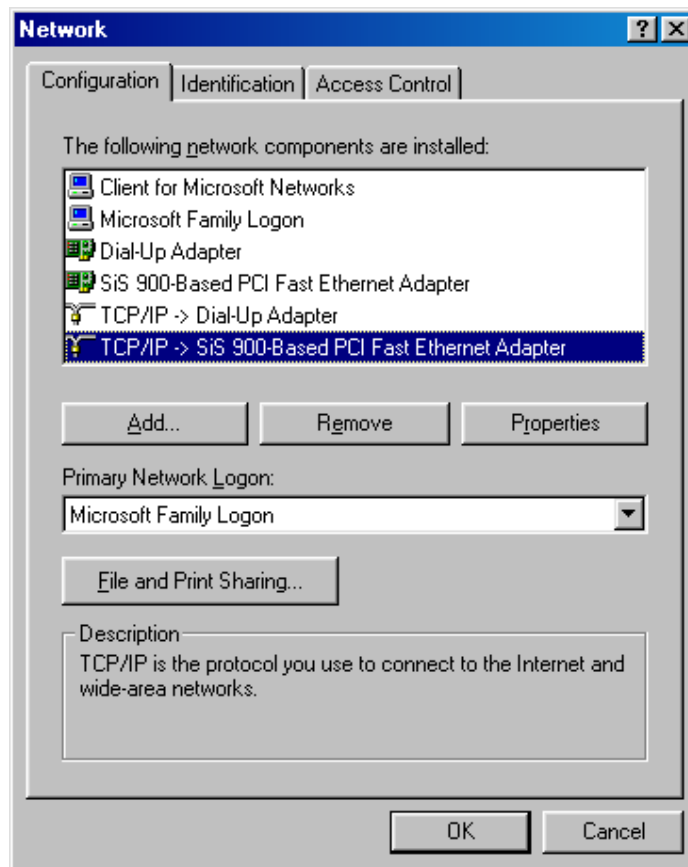
2. PC Configuration

You can connect Wireless LAN ADSL2+ router with PC through either Ethernet cable. You can change the settings via WEB browser.

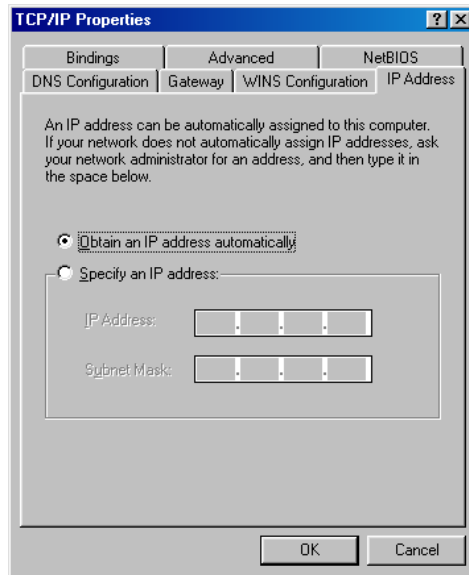
2.1 TCP/IP Networking Setup

Checking TCP/IP Settings for Windows 9x/Me

a) Select “Start → Control Panel → Network”, the window below will appear,

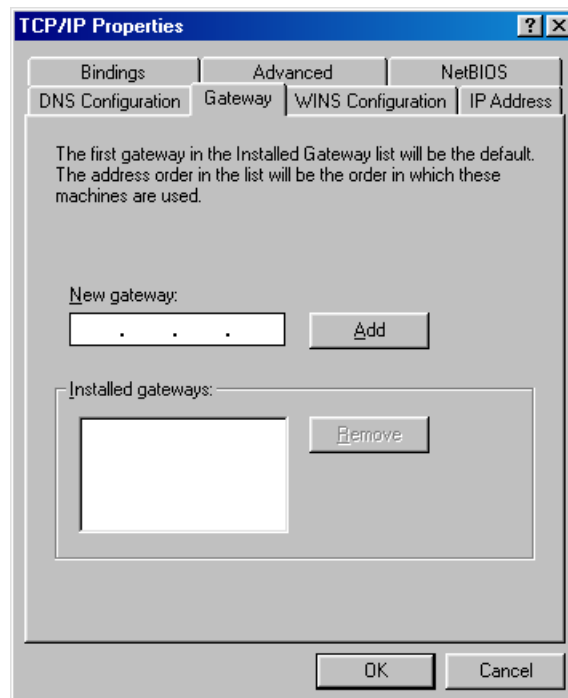


b) Click “Properties”, the window below will appear and then click “IP Address” tab,

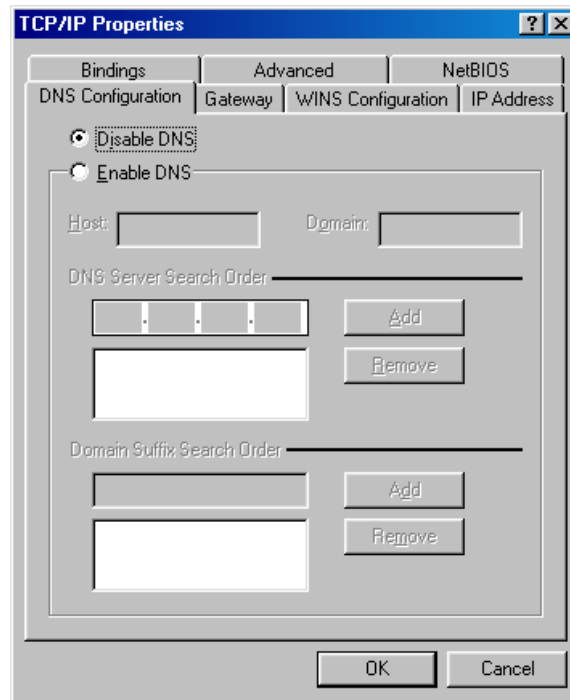


- If you decide to use DHCP, select **“Obtain an IP address automatically”**, then click **“OK”** to confirm your settings. Once you restart your system, Wireless Router will obtain an IP address for this system.
- If you decide to use fixed IP address for your system, select **“Specify an IP address”**, and make sure that **IP Address** and **Subnet Mask** are correct.

c) Select **“Gateway”** tab and enter correct gateway address in **“New gateway”** field, then click **“Add”**,

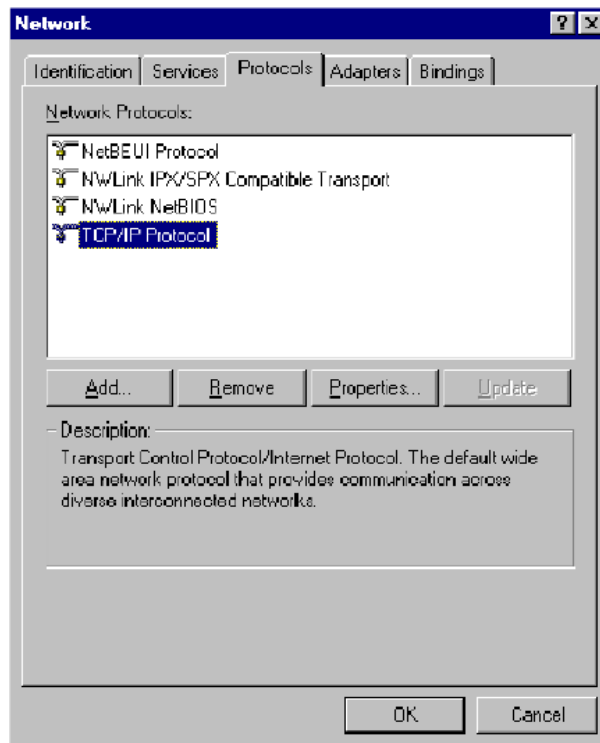


d) Select “DNS Configuration” tab and make sure select “Enable DNS”, enter the DNS address provides from your ISP in the “DNS Server Search Order” field, then click “Add”,

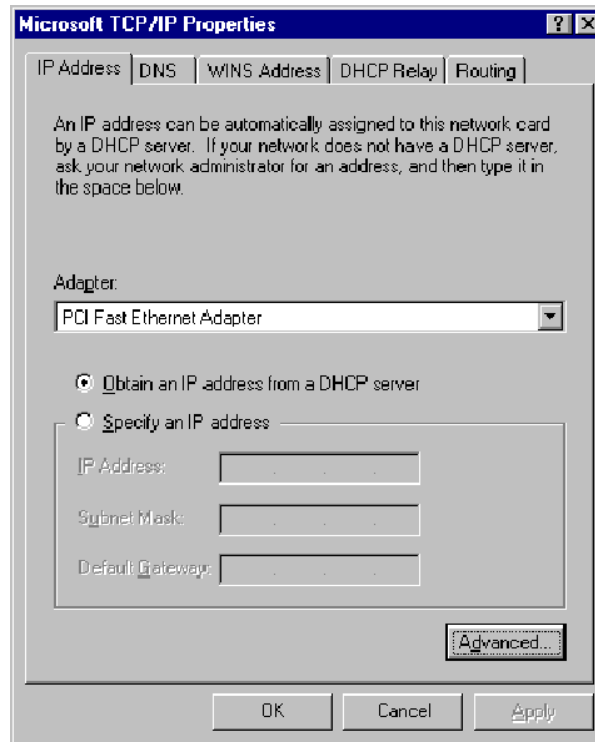


Checking TCI/IP Setting for Windows NT4.0

a) Select “Control Panel → Network”, window below will appear, click “Protocols” tab then select “TCP/IP protocol”,

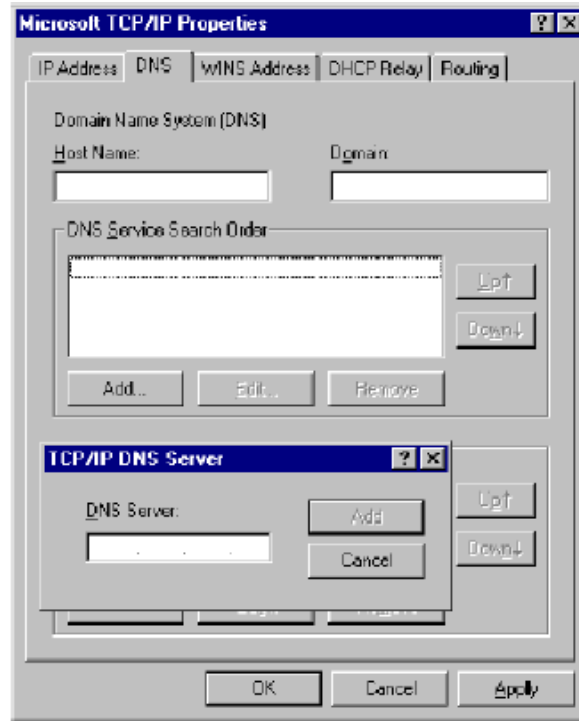


b) Click “Properties”, window below will appear.



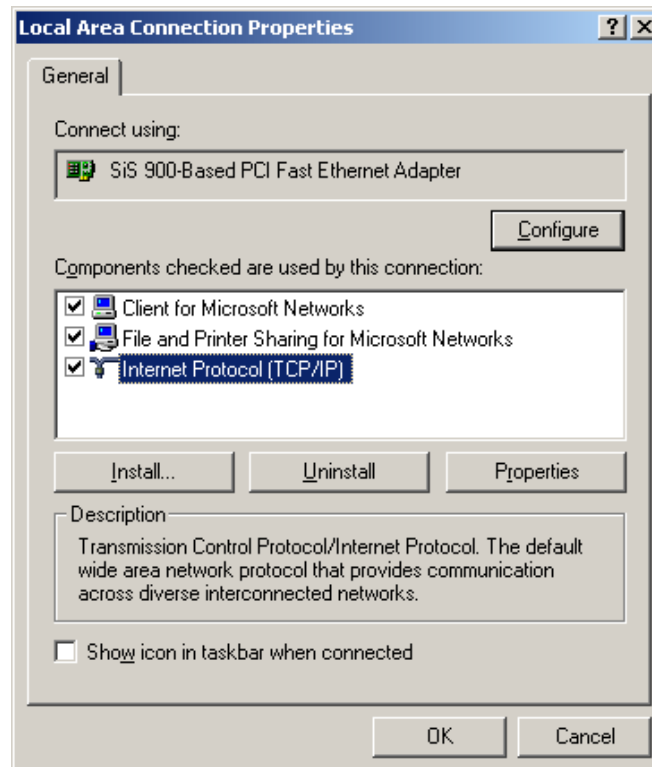
- Select the network card on your system from “Adapter” field.
- If you decide to use IP address from Wireless Router, select “Obtain an IP address from a DHCP server”.
- If you decide to use the IP address you are desired, select “Specify an IP address”. Make sure enter correct addresses in “IP Address” and “Subnet Mask” fields.
- You must set Wireless Router’s IP address as “Default Gateway”.

c) To enter DNS address is provided from your ISP. Select “DNS” tab, click “Add” under “DNS Service Search Order” list, then enter DNS Server IP address in “TCP/IP DNS Server” window and click “Add”.

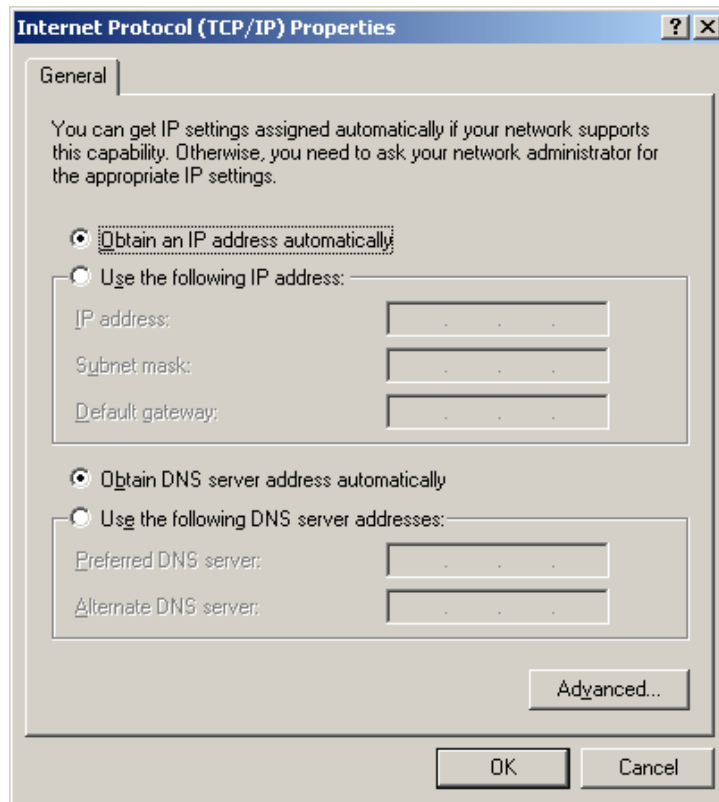


Checking TCP/IP Settings for Windows 2000

a) Select "Start → Control Panel → Network and Dial-up Connection" and right click "Local Area Connection" then click "Properties",



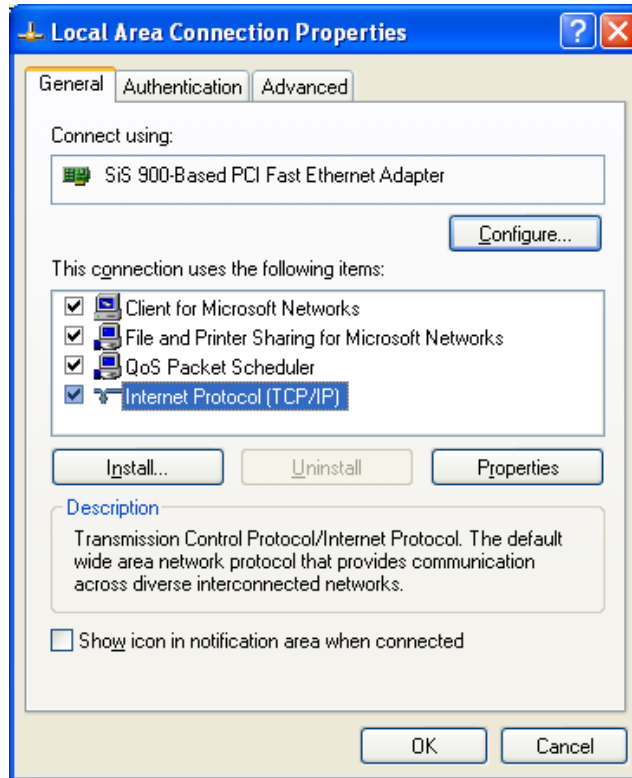
b) Select the “Internet Protocol (TCP/IP)” for the network card on your system, then click “Properties”, window below will appear.



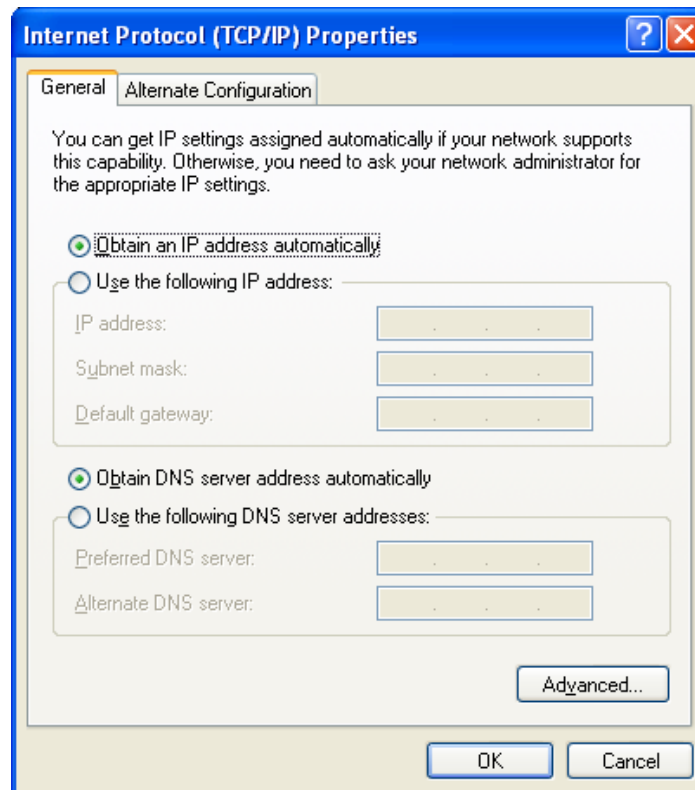
- If you decide to use IP address from Wireless Router, select “Obtain an IP address automatically”.
- If you decide to use the IP address you are desired, select “Use the following IP address”. Make sure enter correct addresses in “IP Address” and “Subnet Mask” fields.
- You must set Wireless Router’s IP address as “Default Gateway”.
- If the DNS Server fields are empty, select “Use the following DNS server addresses” and enter the DNS address is provided by your ISP, then click “OK”.

Checking TCP/IP Settings for Windows XP

a) Click “Start”, select “Control Panel → Network Connection” and right click “Local Area Connection” then select “Properties”, window below will appear.



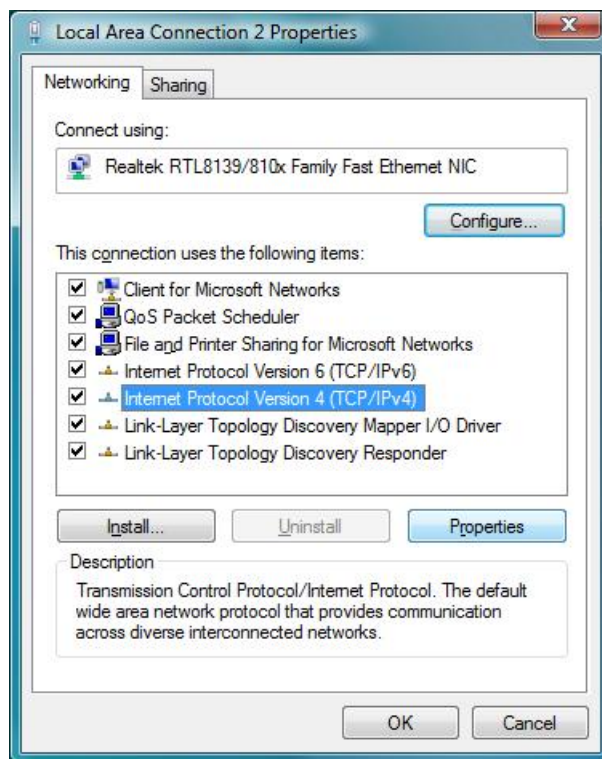
b) Select "Internet Protocol (TCP/IP)" then click "Properties", window below will appear.



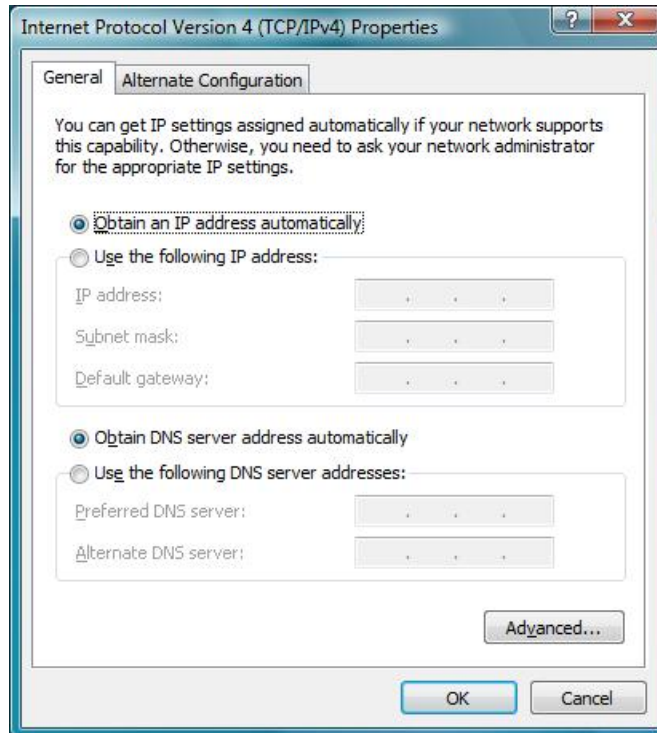
- If you decide to use IP address from Wireless Router, select “Obtain an IP address automatically”.
- If you decide to use the IP address you are desired, select “Use the following IP address”. Make sure enter correct addresses in “IP Address” and “Subnet Mask” fields.
- You must set Wireless Router’s IP address as “Default Gateway”.
- If the DNS Server fields are empty, select “Use the following DNS server addresses” and enter the DNS address is provided by your ISP, then click “OK”.

Checking TCP/IP Settings for Windows Vista

a) Click “Start” → “Control Panel” → “Manage Network Connections” and right click “Local Area Connection” then select “Properties”, window below will appear.



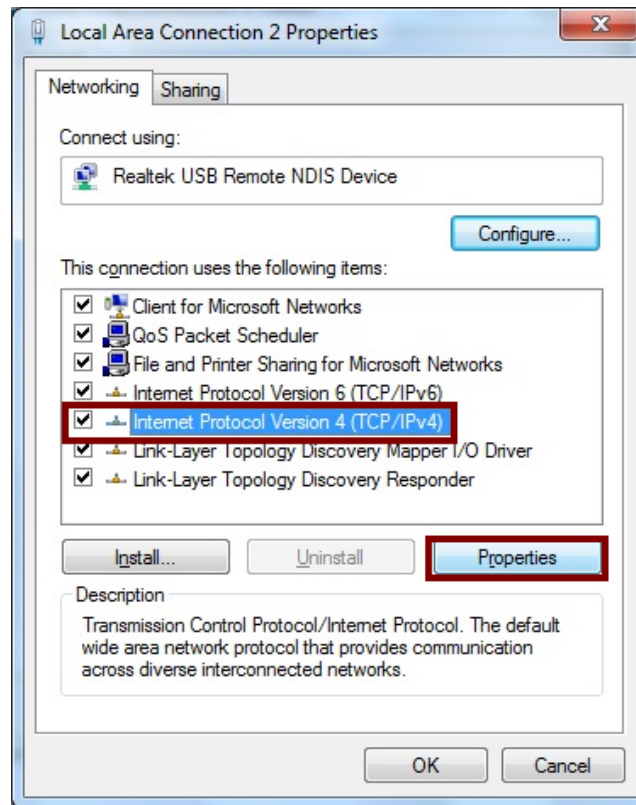
b) Select “Internet Protocol (TCP/IP)” then click “Properties”, window below will appear.



- If you decide to use IP address from Wireless Router, select “Obtain an IP address automatically”.
- If you decide to use the IP address you are desired, select “Use the following IP address”. Make sure enter correct addresses in “IP Address” and “Subnet Mask” fields.
- You must set Wireless Router’s IP address as “Default Gateway”.
- If the DNS Server fields are empty, select “Use the following DNS server addresses” and enter the DNS address is provided by your ISP, then click “OK”.

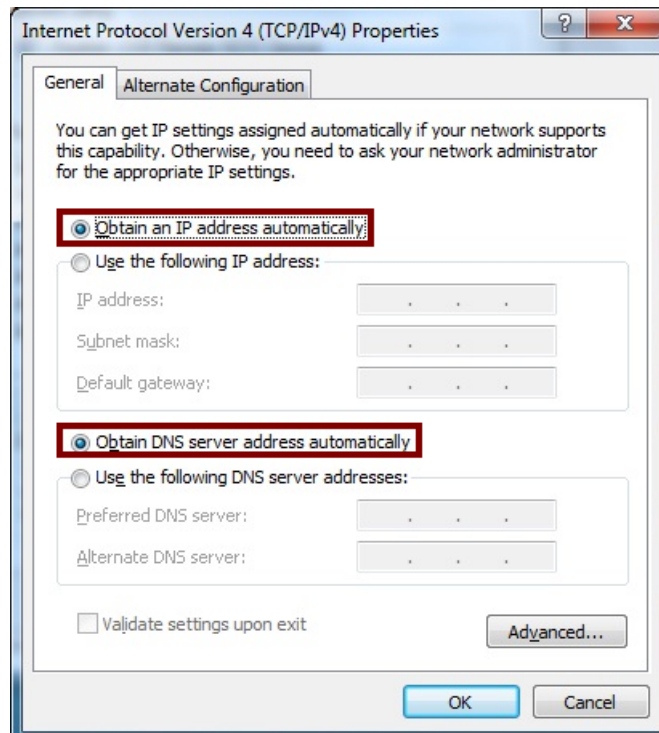
Checking TCP/IP Settings for Windows 7

a) Click “Start” → “Control Panel” → Double-click Network and Sharing Center icon → Select “Local Area Connection #”. (Local network your ADSL hooked up with) → Select “Properties” → Select “Internet Protocol Version 4 (TCP/IPv4)” then click “Properties”



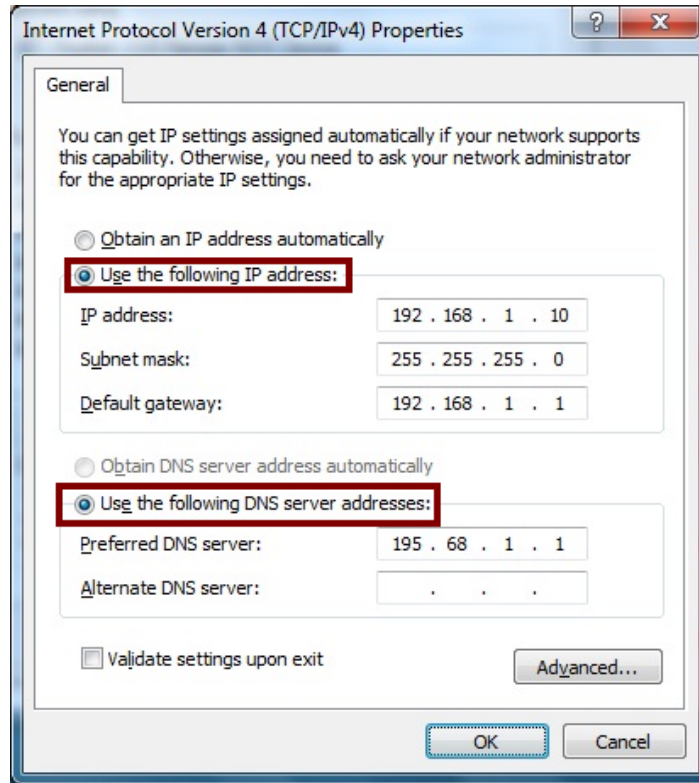
Configure IP address Automatically:

b) Select "Obtain an IP address automatically" and "Obtain DNS server address automatically" Click "OK" to finish the configuration.



Configure IP Address Manually:

- c) Select “Use the following IP address” and “Use the following DNS server addresses”.



IP address: Fill in IP address 192.168.1.x (x is a number between 2 to 254).

Subnet mask: Default value is 255.255.255.0.

Default gateway: Default value is 192.168.1.1.

Preferred DNS server: Fill in preferred DNS server IP address.

Alternate DNS server: Fill in alternate DNS server IP address.

- If you decide to use IP address from Wireless Router, select “Obtain an IP address automatically”.
- If you decide to use the IP address you are desired, select “Use the following IP address”. Make sure enter correct addresses in “IP Address” and “Subnet Mask” fields.
- You must set Wireless Router’s IP address as “Default Gateway”.
- If the DNS Server fields are empty, select “Use the following DNS server addresses” and enter the DNS address is provided by your ISP, then click “OK”.

You can use ping command under DOS prompt to check if you have setup TCP/IP protocol correctly and if your computer has successfully connected to this router.

- 1) Type ping 192.168.1.1 under DOS prompt and the following messages will appear:

```
cmd: Command Prompt
Microsoft Windows [Version 6.1.7100]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\GIGA>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\GIGA>_
```

If the communication link between your computer and router is not setup correctly, after you type ping 192.168.1.1 under DOS prompt following messages will appear:

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

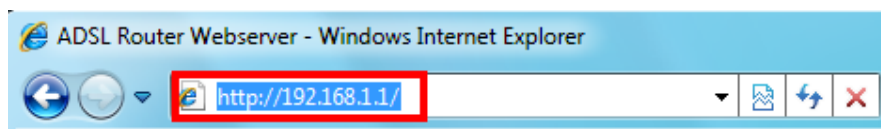
This failure might be caused by cable issue or something wrong in configuration procedure.

3. Configure Wireless Router via Web Based Utility

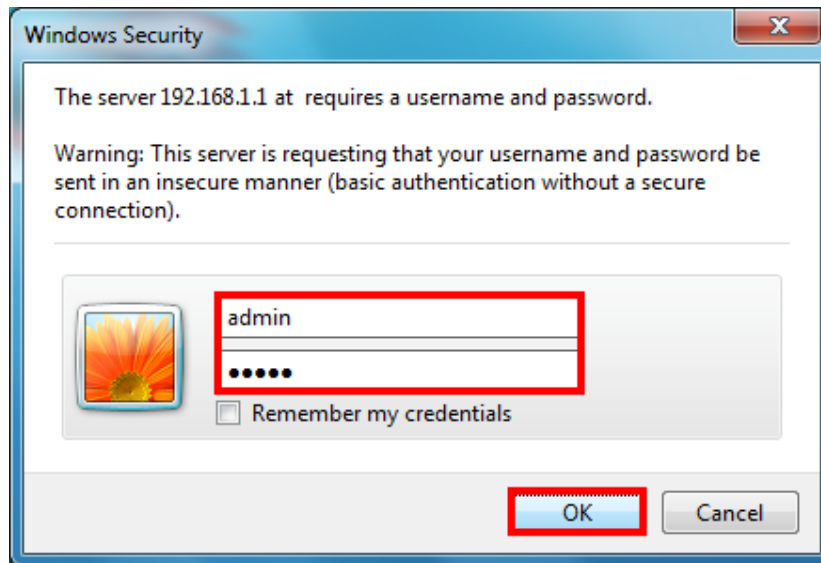
Wireless LAN ADSL2+ Router supports a Web-based (HTML) GUI to allow users to configure Router setting via Web browser.

3.1 Login

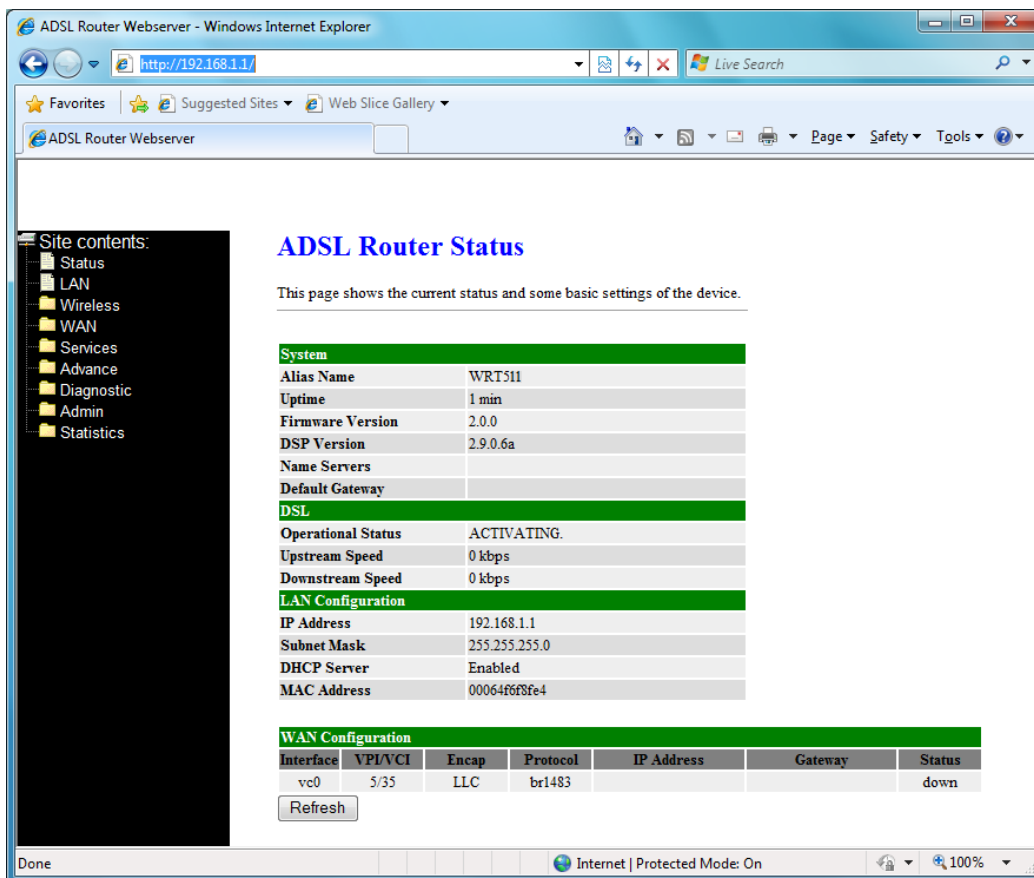
- 1) Launch the Web browser.
- 2) Enter the default IP address <http://192.168.1.1>



- 3) Entry of the username and password will be displayed. Enter the default **login User Name** and **Password** as **admin** and **admin**.

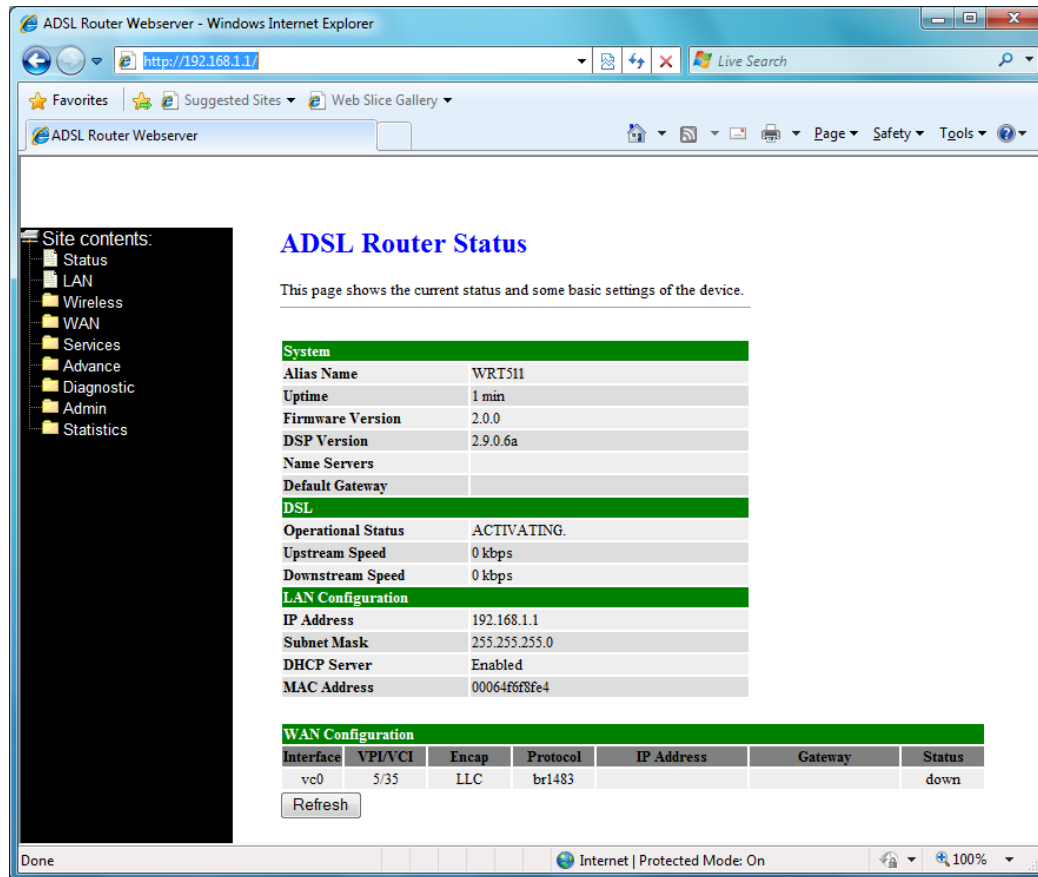


The main webpage will be displayed as below:



3.2 Status

This page displays the ADSL router's current status and settings. Click "Refresh" button to update the status.



The screenshot shows a Windows Internet Explorer browser window displaying the ADSL Router Webserver interface. The address bar shows the URL <http://192.168.1.1/>. The page title is "ADSL Router Status". A left-hand navigation menu lists various sections: Status, LAN, Wireless, WAN, Services, Advance, Diagnostic, Admin, and Statistics. The main content area is titled "ADSL Router Status" and includes a sub-header: "This page shows the current status and some basic settings of the device." Below this, there are three main sections: "System", "DSL", and "LAN Configuration".

System

Alias Name	WRT511
Uptime	1 min
Firmware Version	2.0.0
DSP Version	2.9.0.6a
Name Servers	
Default Gateway	

DSL

Operational Status	ACTIVATING.
Upstream Speed	0 kbps
Downstream Speed	0 kbps

LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00064f6f8fe4

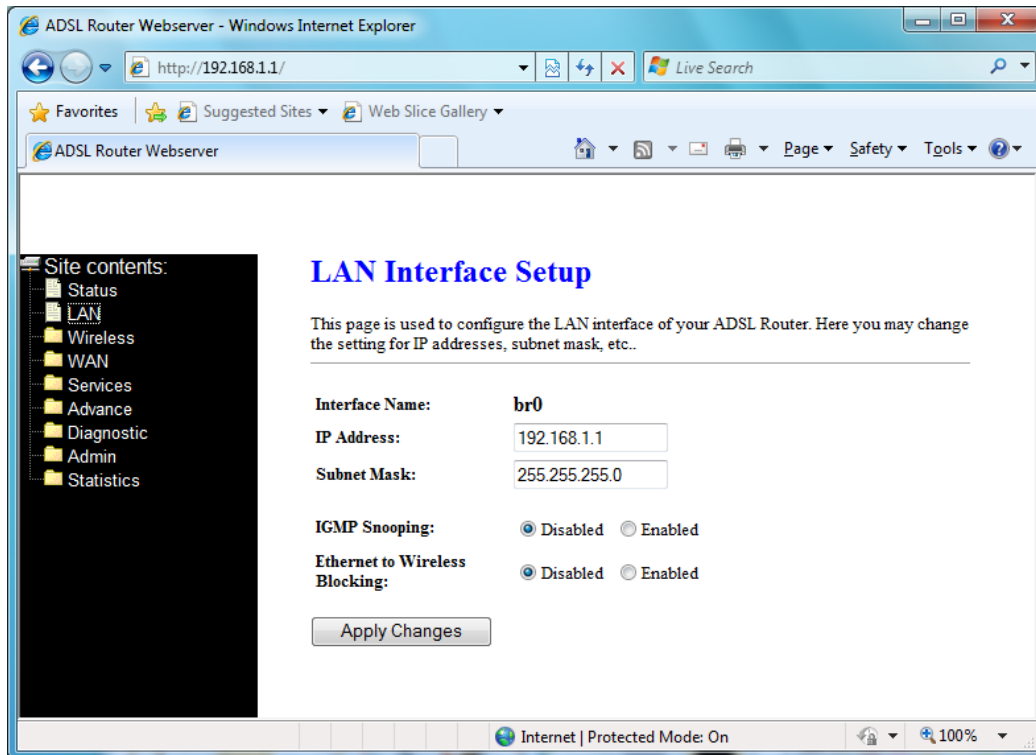
WAN Configuration

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

Below the WAN Configuration table is a "Refresh" button. The browser's status bar at the bottom indicates "Internet | Protected Mode: On" and a zoom level of 100%.

3.3 LAN

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



IP Address -- The IP Address which your LAN hosts use to identify the device's LAN port.

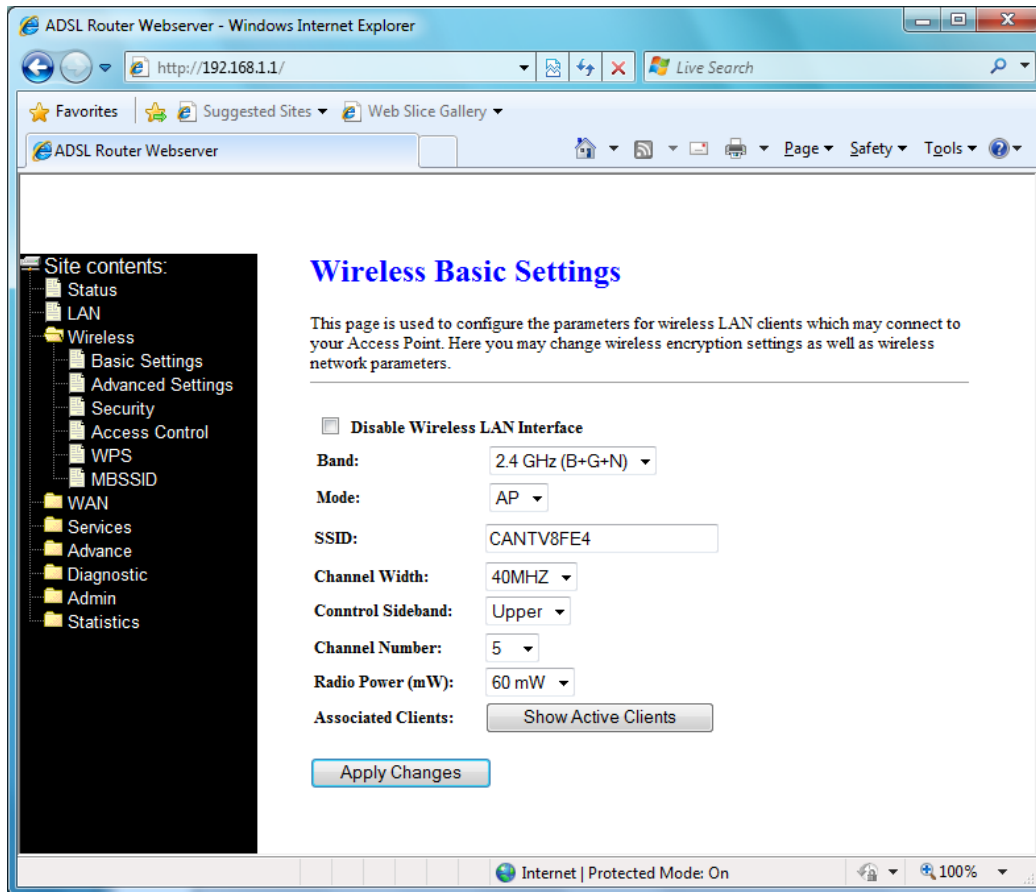
Subnet Mask -- LAN Subnet mask.

Apply Change -- Click to save the setting to the configuration. New parameters will take effect after save into flash memory and reboot the system.

3.4 Wireless

3.4.1 Basic Settings

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



Band: This is the range of frequencies the gateway will use to communicate with your wireless devices. As you're looking for products in stores or on the Internet, you might notice that you can choose equipment that supports six different wireless networking technologies: 2.4 GHz(B), 2.4 GHz(G), 2.4 GHz(B+G), 2.4 GHz(N), 2.4 GHz(G+N), and 2.4 GHz(B+G+N).

Mode: Default set to AP mode.

SSID: Specify the network name. Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the make up your own name and use it on each computer. The name can be up to 20 characters long and contain letters and numbers.

Channel Width: There have 2 options – 20MHZ and 40 MHZ

Control Sideband: Specify if the extension channel should be in the Upper or Lower sideband.

Channel Number: Sets the channel on which the gateway operates.

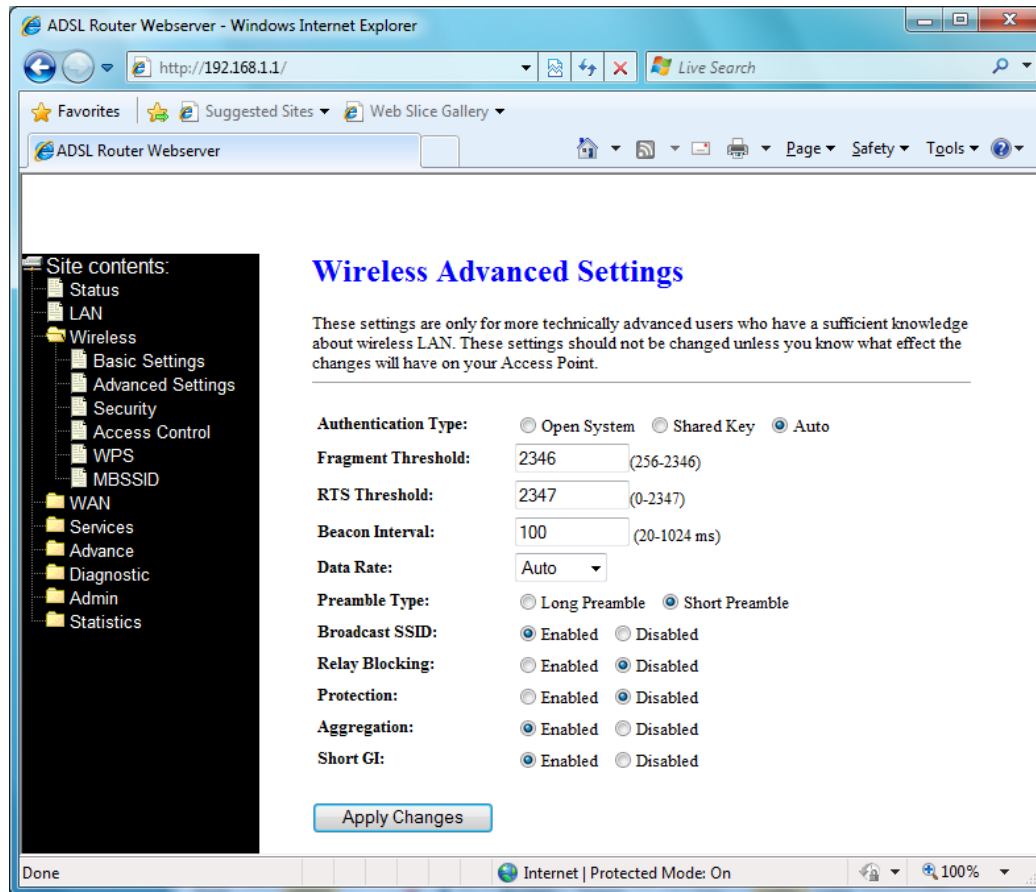
Radio Power (mW): A milliwatt (mW) is also a unit of power. To put it simply, a milliwatt is 1/1,000 of a watt. The reason you need to be concerned with milliwatts is because most of the 802.11 equipment that you will be using transmits at power levels between 1 and 100

mW

Associated Clients: This table shows MAC address, transmission, reception packet counters and encrypted status for each associated wireless clients.

3.4.2 Advanced Settings

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



Authentication Type: There has 3 types – Open System, Shared Key, and Auto

Fragment Threshold: Fragmentation Threshold sets the frame size of incoming messages (ranging from 256 to 2346 bytes) used as fragmentation boundary. If the frame size is too big, the heavy interference affects transmission reliability. If the frame size is too small, it decreases transmission efficiency. Default setting is 2346.

RTS Threshold: Lower the signal RTS (Request To Send) to promote the transmission efficiency in condition of noisy environment or too many clients. Default setting is 2347.

Beacon Interval: Beacon Interval means the period of time between one beacon and the next one. The default value is 100 (the unit is millisecond, or 1/1000 second). Lower the Beacon Interval to improve transmission performance in unstable environment or for

roaming clients, but it will be power consuming.

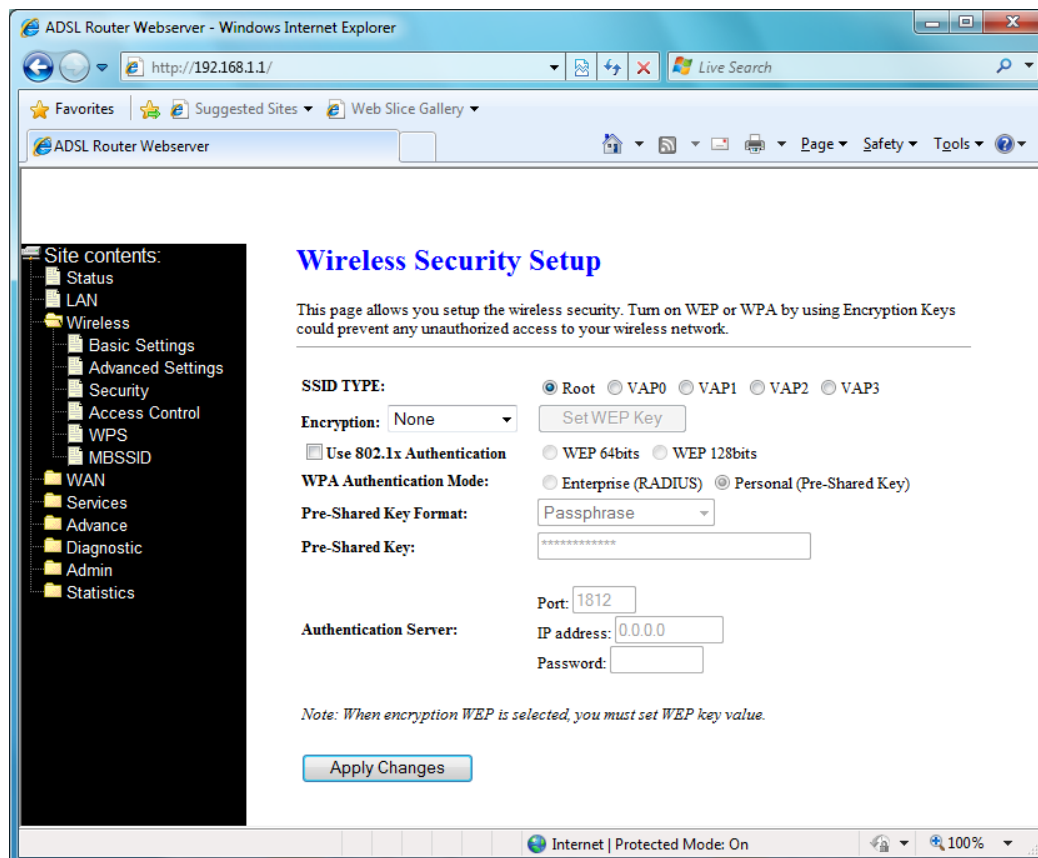
Data Rate: Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, it's not necessary to change this value unless you know what will happen after change the value. [Auto] is recommended to maximize performance.

Preamble type: Preamble is the first sub field of PPDU, which is the appropriate frame format for transmission to PHY (Physical layer). There are two options, Short Preamble and Long Preamble.

Short GI: Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections

3.4.3 Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.



Encryption: There have 4 encryption options – WEP, WAP (TKIP), WPA2(AES), and WPA2 Mixed.

WPA authentication mode: WPA operates in either WPA-PSK mode (Pre-Shared Key or

WPA-Personal) or WPA-802.1x mode (RADIUS or WPA-Enterprise). In the Personal mode, a pre-shared key or passphrase is used for authentication. In the Enterprise mode, which is more difficult to configure, the 802.1 x RADIUS servers and an Extensible Authentication Protocol (EAP) are used for authentication.

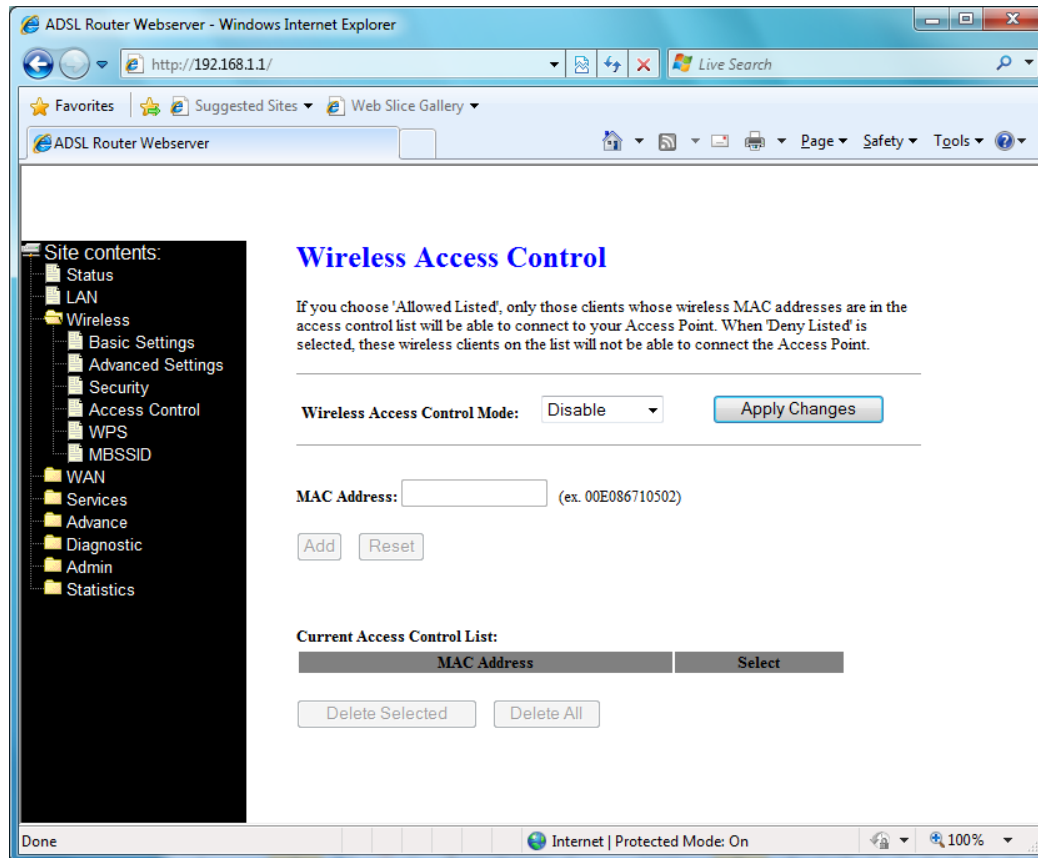
Pre-Shared Key Format: select Passphrase mode or Hex mode for the Pre-Shared Key.

Pre-Shared Key: Enter the Pre-Shared via using the Passphrase mode or Hex mode.

Authentication RADIUS server: fill the port, IP address and the password of the RADIUS server.

3.4.4 Access Control

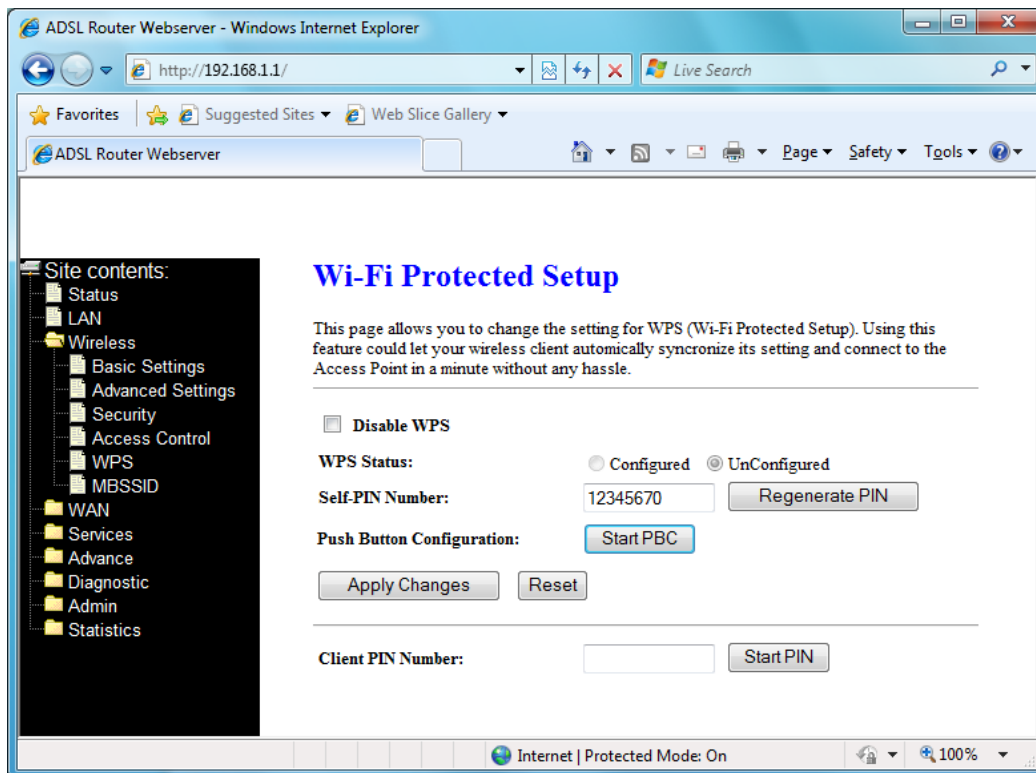
If you know choose **“Allowed Listed”** from Wireless Access Control mode, only those clients whose wireless MAC address are in the access control list will be able to connect to your Access Point. When **“Deny Listed”** is selected, these wireless clients on the list will not be able to connect the AP.



3.4.5 WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the

Access Point in a minute without any hassle.



In PIN method (PIN-Personal Identification Number), When your 11n router acts as a Registrar, you must enter **“Self-PIN Number”** on WPS configuration section, this Enrollee PIN code should be provided by the Enrollee. If your 11n router acts as an Enrollee, in WPS configuration section, the **“Regenerate PIN”** will automatically generate for you. The purpose of PIN code is to provide the security key to Registrar (AP/Server). Therefore, WPS (Wi-Fi Protected Setup) can be established completely.

In PBC Method (PBC-Push Button Communication), while the AP router acts as Registrar or Enrollee, and click **“Start PBC”** button, the WPS (Wi-Fi Protected Setup) will establish the connection automatically.

3.4.6 MBSSID

This page allows you to setup wireless multiple BSSID configuration. The Base Service Set Identifier (BSSID) is typically the MAC address of the radio. This Wireless LAN ADSL2+ Router also supports multiple BSSIDs (MBSSID) on a single AP.

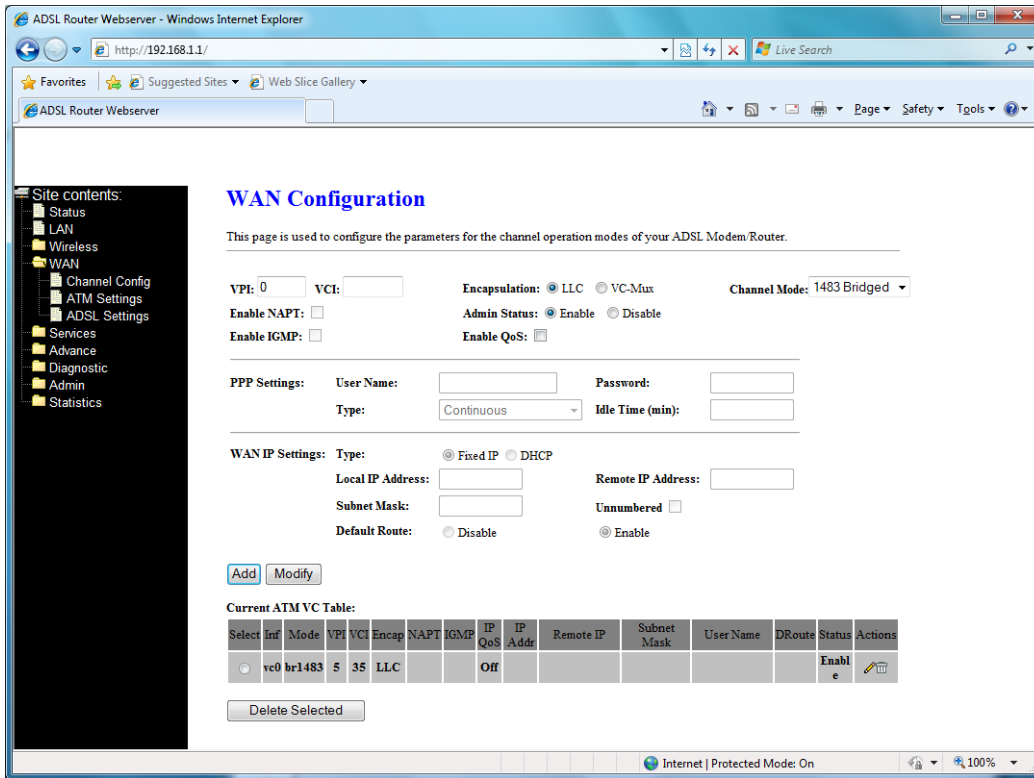


3.5 WAN

There are three sub-menus for WAN configuration: **Channel Config**, **ATM Settings**, and **ADSL Settings**.

3.5.1 Channel Configuration

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



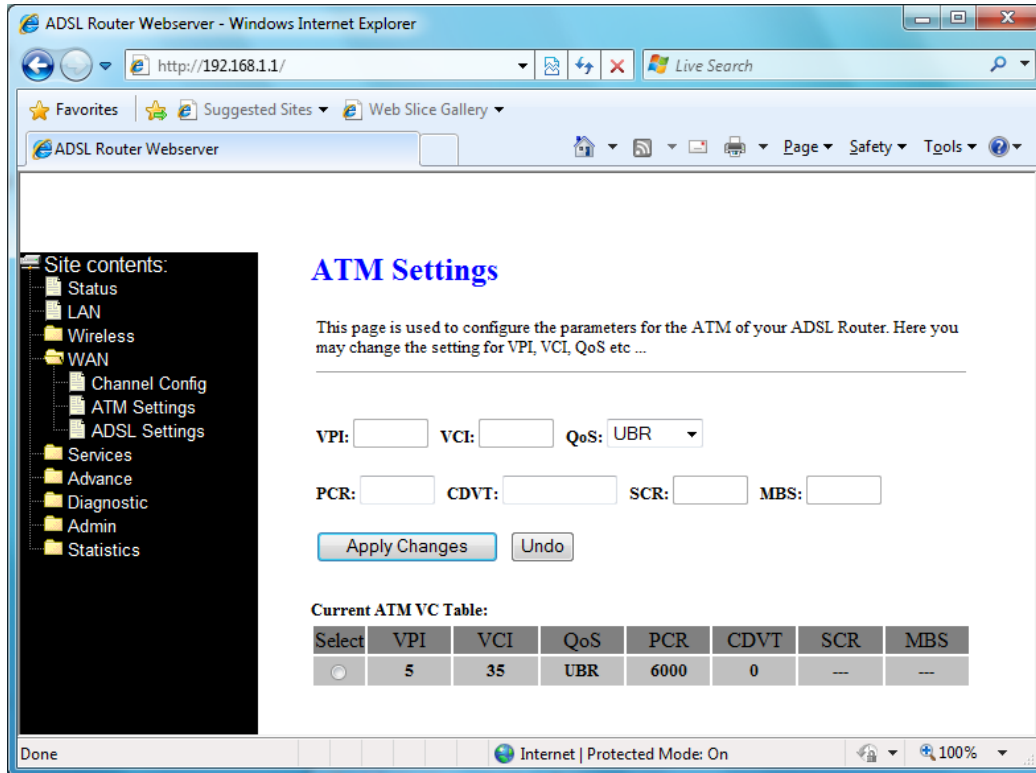
Add -- Click **Add** to complete the channel setup and add this PVC channel into configuration.

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 a 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.

3.5.2 ATM Settings

This page is for ATM PVC QoS parameters setting. The DSL device supports 4 QoS modes – **CBR**, **rt-VBR**, **nrt-VBR**, and **UBR**.



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.

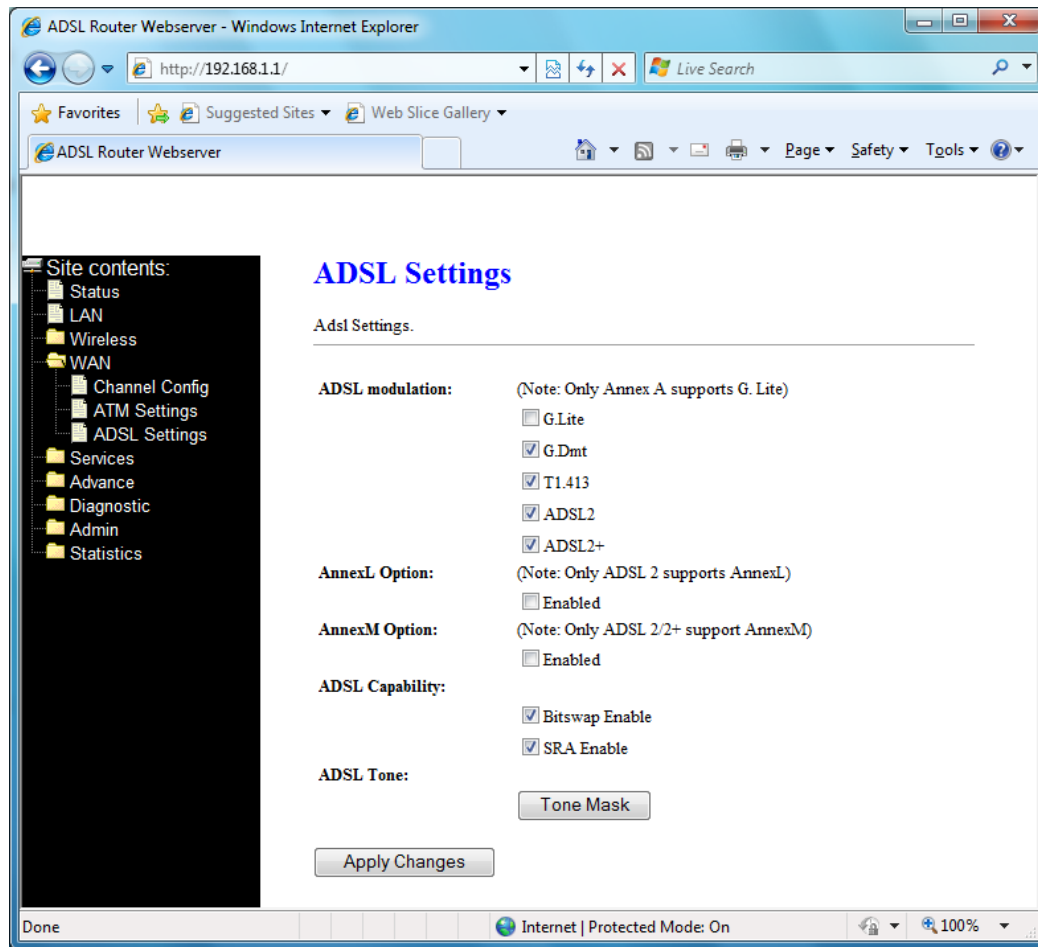
MBS -- Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.

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.

3.5.3 ADSL Settings

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



ADSL modulation -- Choose preferred 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.

Tone Mask -- Choose tones to be masked. Masked tones will not carry any data.

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

3.6 Service

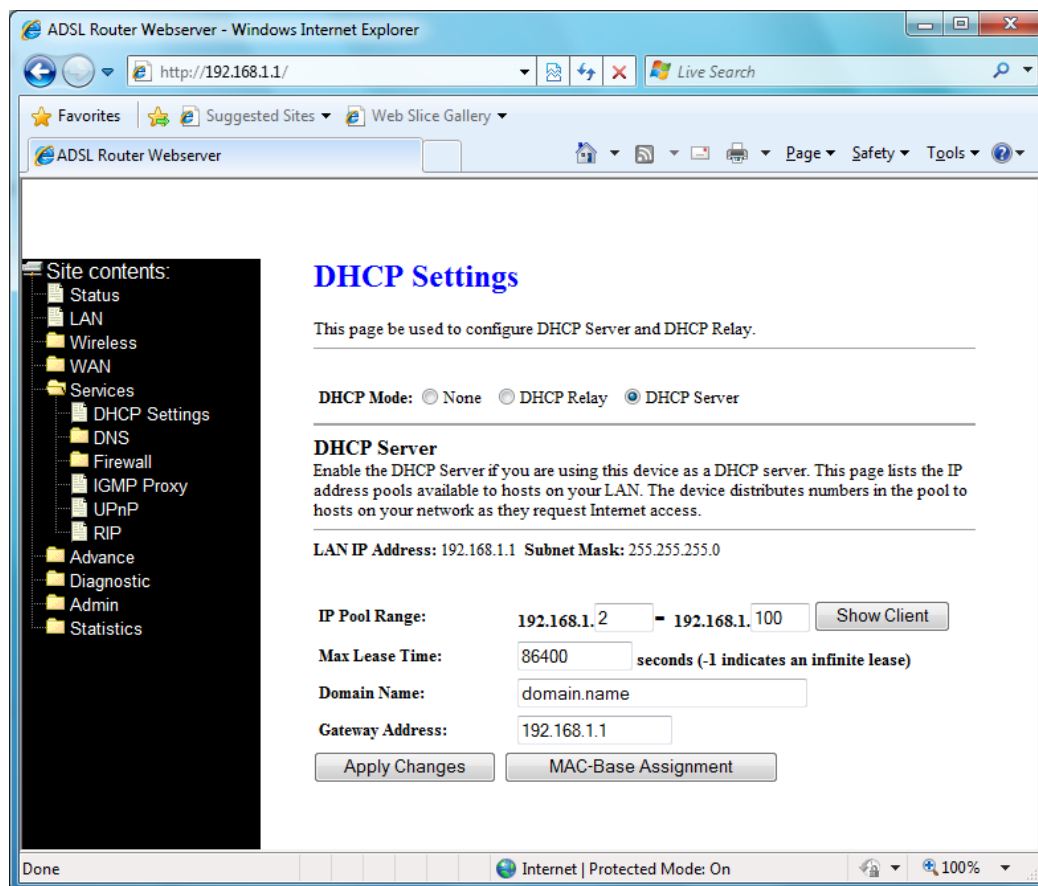
There are three sub-menus for Service configuration: **DHCP Settings**, **DNS**, **Firewall**, **UPnP**, and **RIP**.

3.6.1 DHCP

This page is used to configure **[DHCP Relay]** and **[DHCP Server]**.

[DHCP Server]

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).



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.

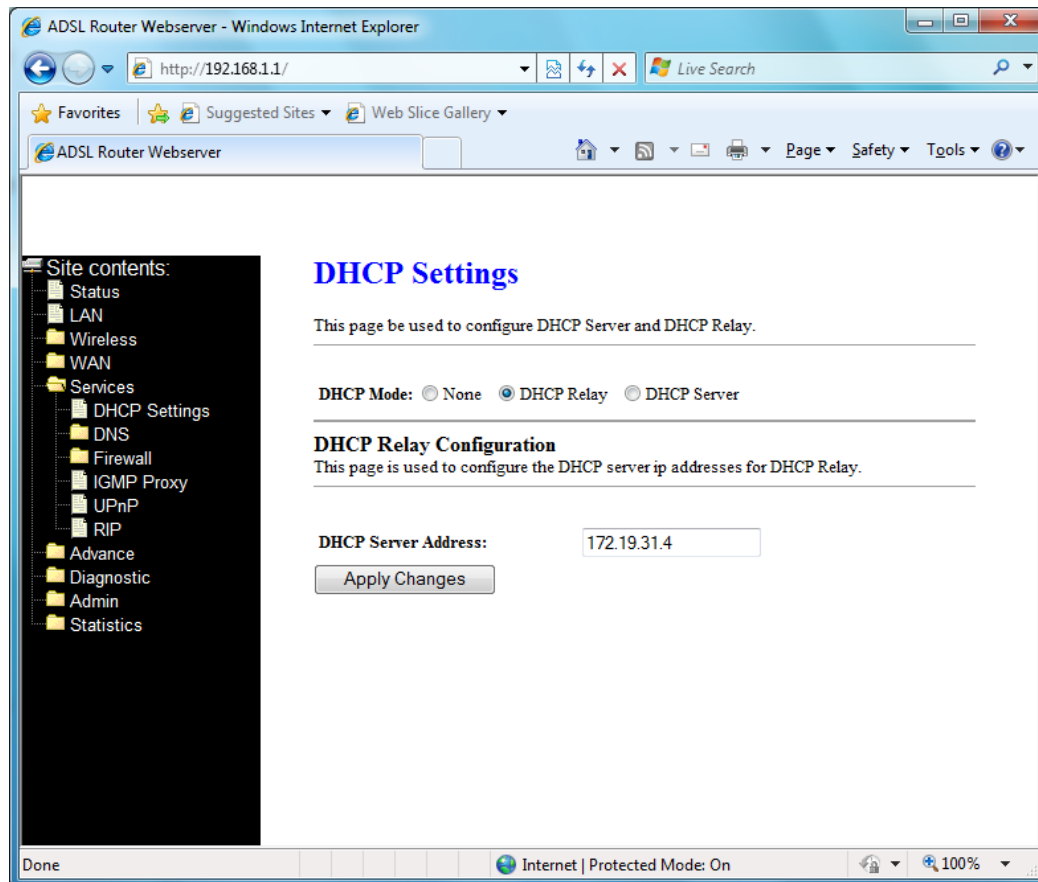
Domain Name -- A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.

Apply Changes -- Set new DHCP server configuration. New parameters will take effect after save into flash memory and reboot the system.

Undo -- Discard your changes.

[DHCP Relay]

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



DHCP Mode -- 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.

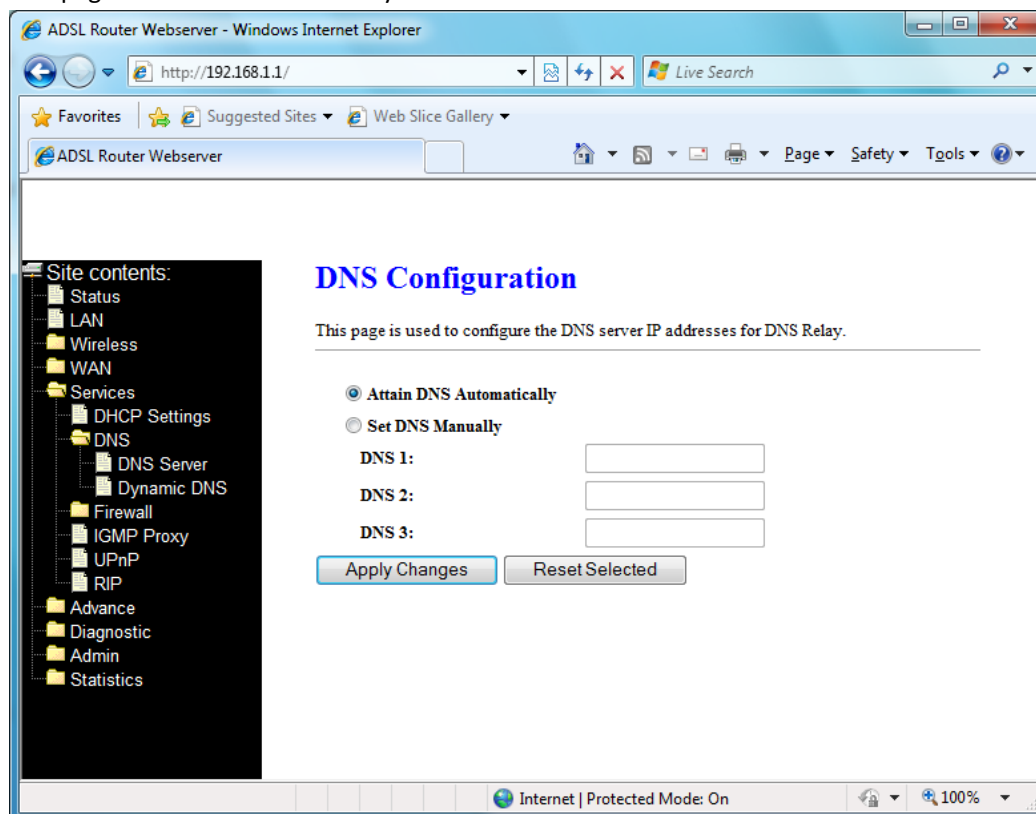
Apply Changes -- Click to save the setting to the configuration.

3.6.2 DNS

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

[DNS Server]

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



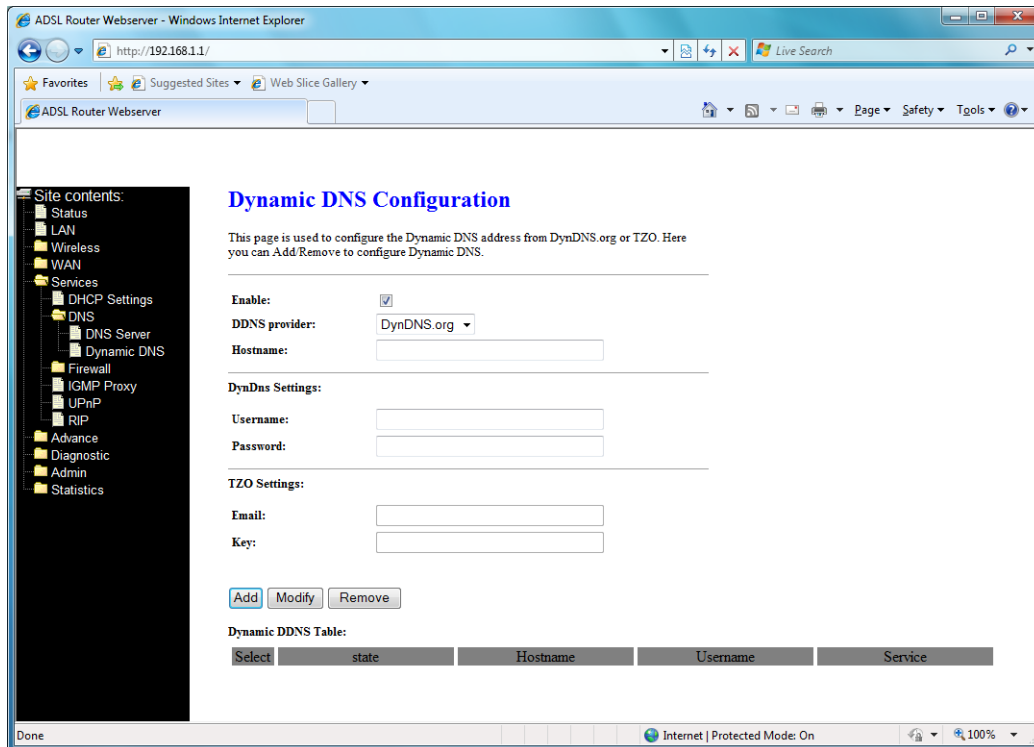
Attain DNS Automatically -- Select this item if you want to use the DNS servers obtained by the WAN interface via the auto-configuration mechanism.

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

Apply Changes -- Set new DNS relay configuration. New parameters will take effect after save into flash memory and reboot the system.

[Dynamic DNS]

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



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

Hostname -- Domain name to be registered with the DDNS server

User Name -- User-name assigned by the DDNS service provider.

Password -- Password assigned by the DDNS service provider.

Email -- Enter Email for TZO settings.

Key -- Enter key for TZO settings.

Add -- Click Add to add this registration into the configuration.

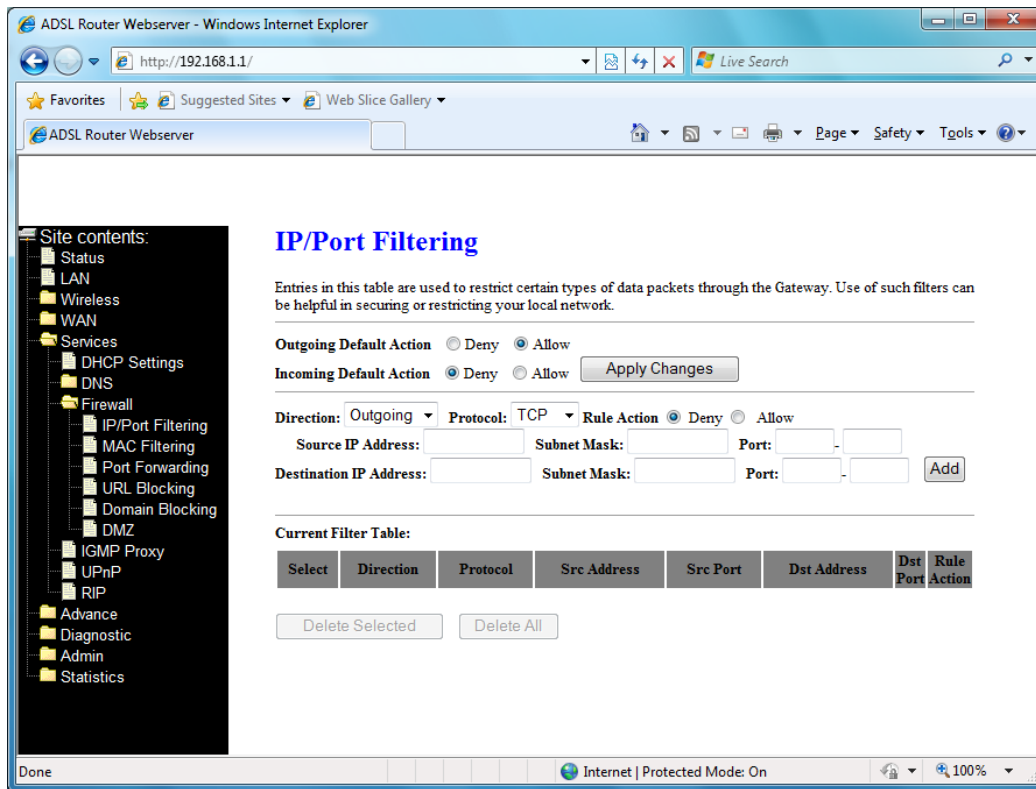
Remove -- Select an existing DDNS registration by clicking the radio button at the Select column of the Dynamic DNS Table. Click Remove button to remove the selected registration from the configuration.

3.6.3 Firewall

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

3.6.3.1 IP/Port Filtering

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



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.

Apply Changes -- Click to save the setting of default actions to the configuration.

Direction -- Traffic forwarding direction.

Protocol -- There are 3 options available: TCP, UDP and ICMP.

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

Source IP Address -- The source IP address assigned to the traffic on which filtering is applied.

Source Subnet Mask -- Subnet-mask of the source IP.

Source Port -- Starting and ending source port numbers.

Destination IP Address -- The destination IP address assigned to the traffic on which filtering is applied.

Destination Subnet Mask -- Subnet-mask of the destination IP.

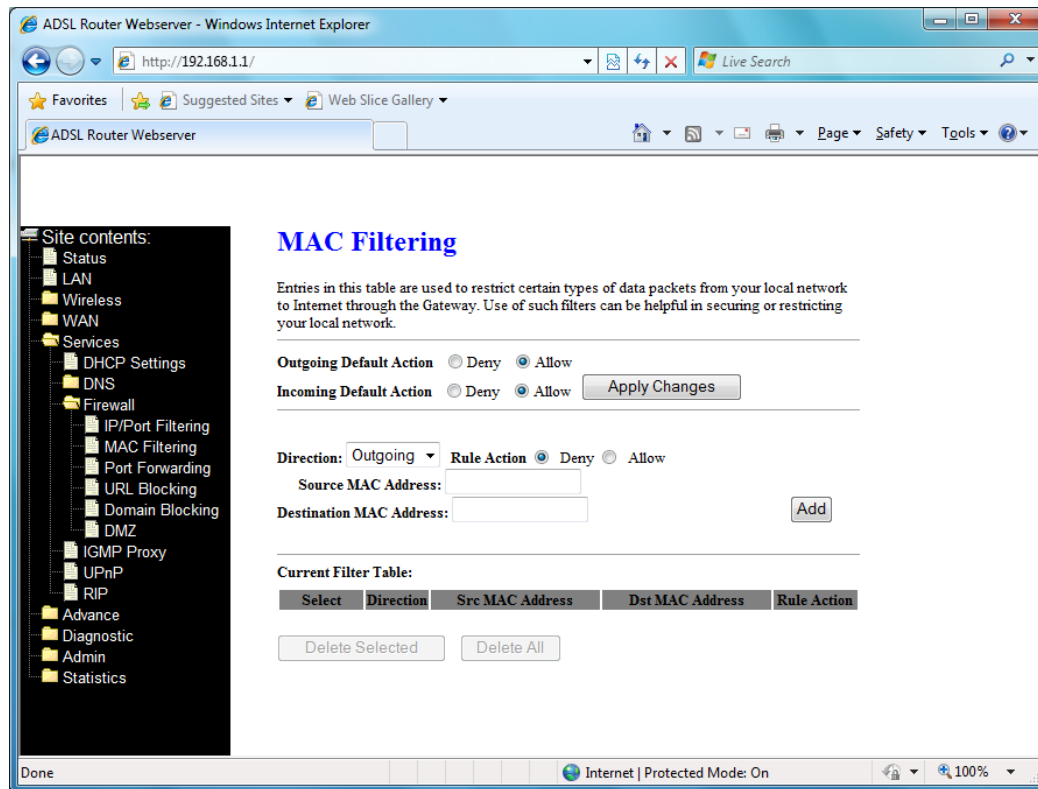
Destination Port -- Starting and ending destination port numbers.

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.

3.6.3.2 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.



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.

Apply Changes -- Click to save the setting of default actions to the configuration.

Direction -- Traffic bridging/forwarding direction.

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

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

Destination 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.

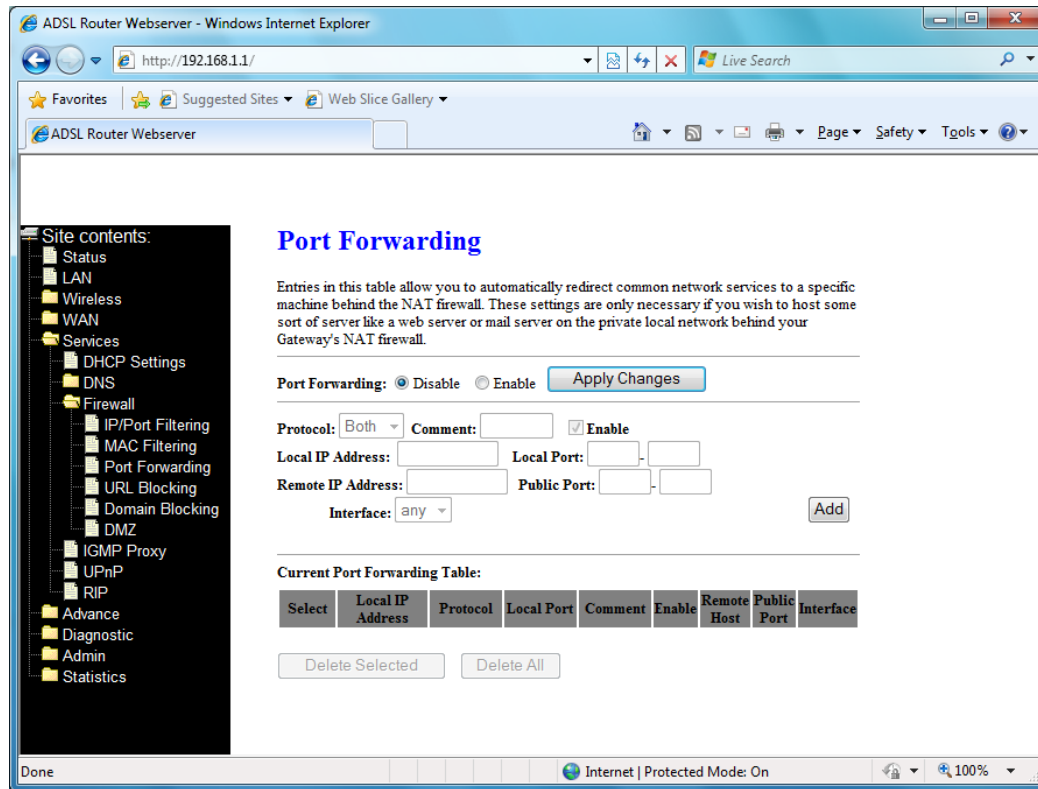
Delete Selected -- Delete selected filtering rules from the filter table. You can click the checkbox at the Select column to select the filtering rule.

Delete All -- Delete all filtering rules from the filter table.

3.6.3.3 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.



Port Forwarding -- Check this item to enable or disable the port-forwarding feature.

Protocol -- There are 3 options available: TCP, UDP and Both.

Local IP Address -- IP address of your local server that will be accessed by Internet.

Local 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.

Public 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.

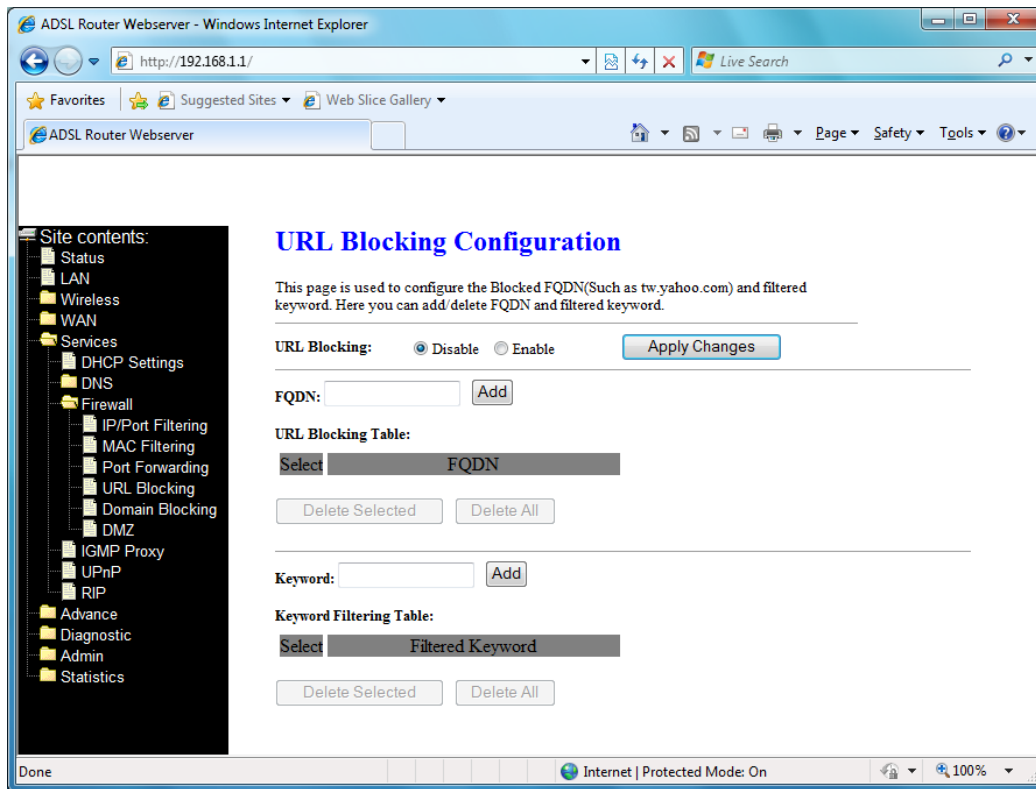
Apply Changes -- Click to save the rule entry to the configuration.

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.

3.6.3.4 URL Blocking

This page is used to configure the Blocked FQDN (such as tw.yahoo.com) and filtered keyword. Here you can add/delete FQDN and filtered keyword.



URL Blocking -- Check this item to enable or disable the URL Blocking feature.

Apply Changes -- Click to save the rule entry to the configuration.

FQDN -- Enter URL link which you want to filter in this section; and then click Add to save the change.

Delete Selected -- Delete the selected URL Blocking rules from the table. You can click the checkbox at the Select column to select the blocking rule.

Delete All -- Delete all URL blocking rules from the table.

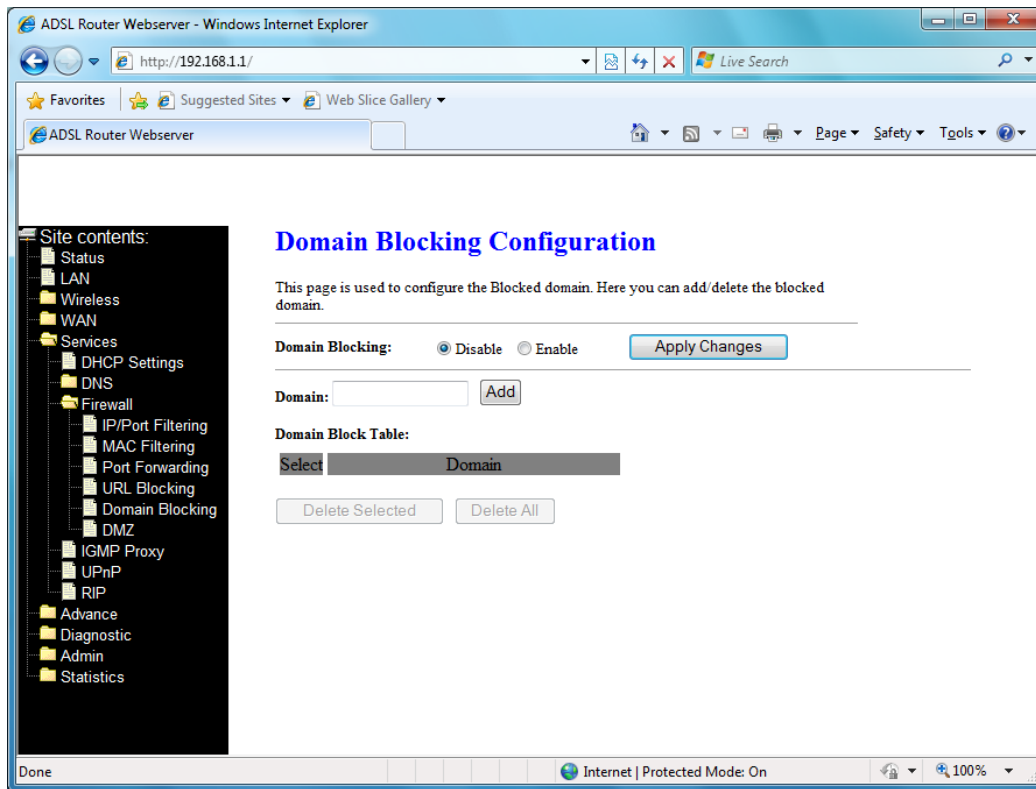
Keyword -- Enter the keyword which you want to filter in this section; and then click Add to save the change.

Delete Selected -- Delete the selected Keyword Filtering rules from the table. You can click the checkbox at the Select column to select the filtering rule.

Delete All -- Delete all Keyword Filtering rules from the table.

3.6.3.5 Domain Blocking

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



Domain Blocking -- Check this item to enable or disable the Domain Blocking feature.

Apply Changes -- Click to save the rule entry to the configuration.

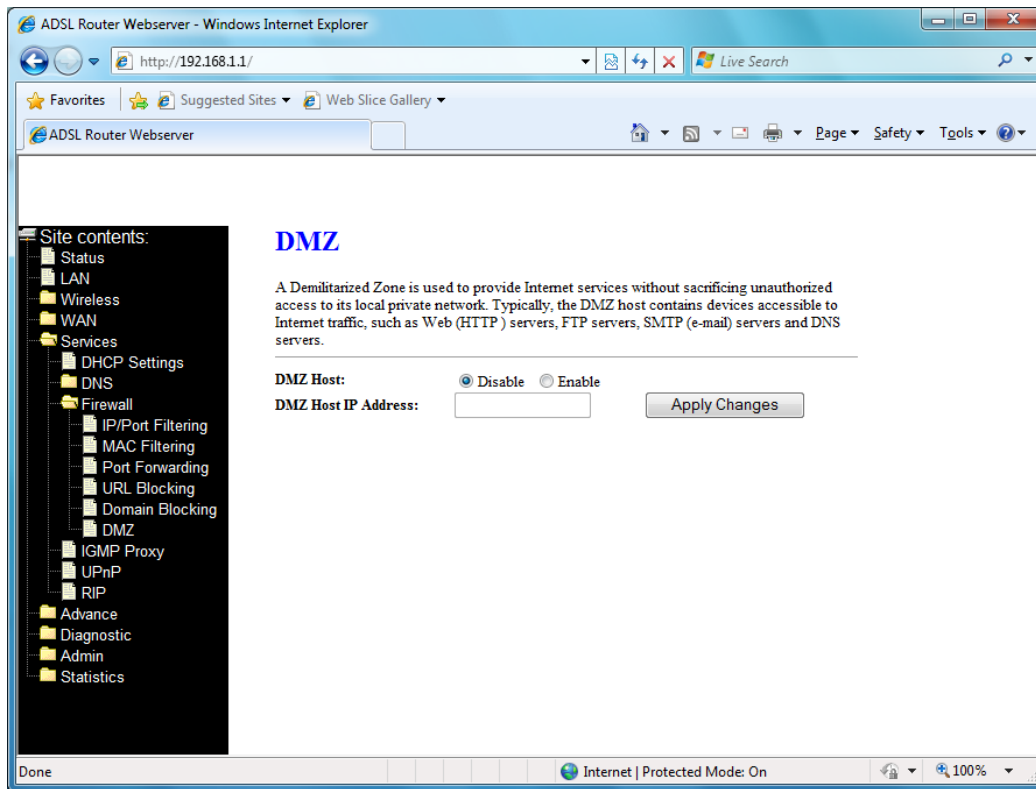
Domain -- A user-friendly name that refers to the group of hosts (subnet) that will be blocked.

Delete Selected -- Delete the selected Domain Blocking rules from the table. You can click the checkbox at the Select column to select the filtering rule.

Delete All -- Delete all Domain Blocking rules from the table.

3.6.3.6 DMZ

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



DMZ Host -- 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.

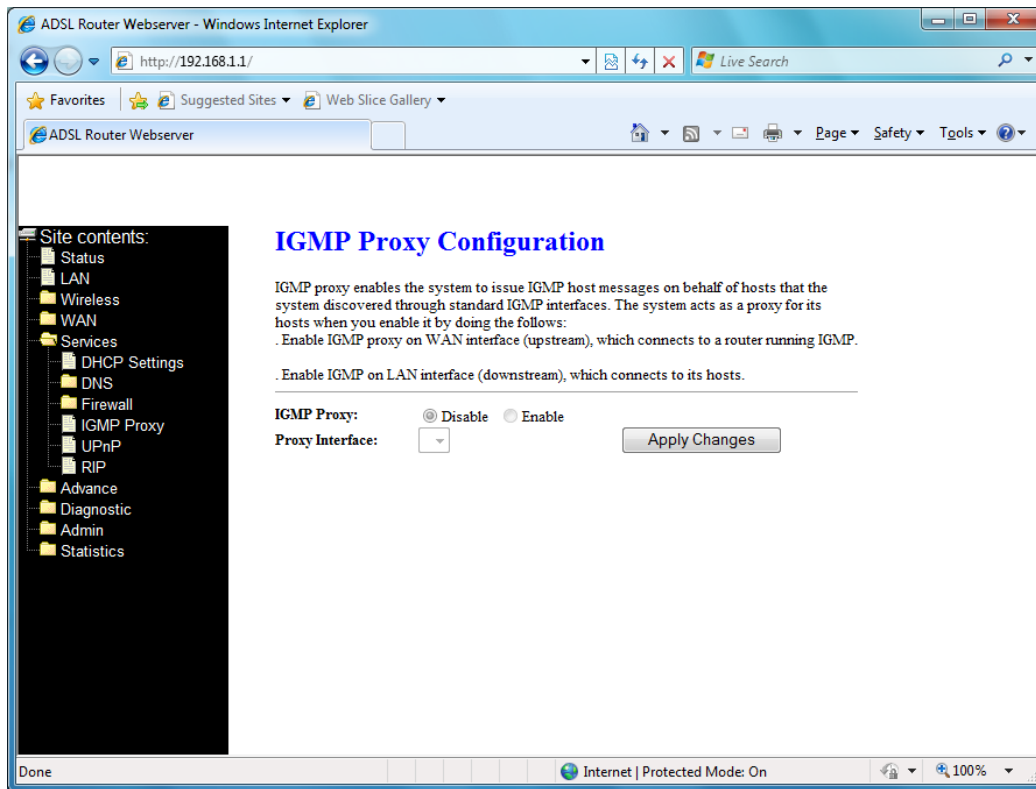
Apply Changes -- Click to save the setting to the configuration.

3.6.4 IGMP Proxy

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:

-- Enable IGMP on WAN interface (upstream), which connects to a router running IGMP.

-- Enable IGMP on LAN interface (downstream), which connects to its hosts.

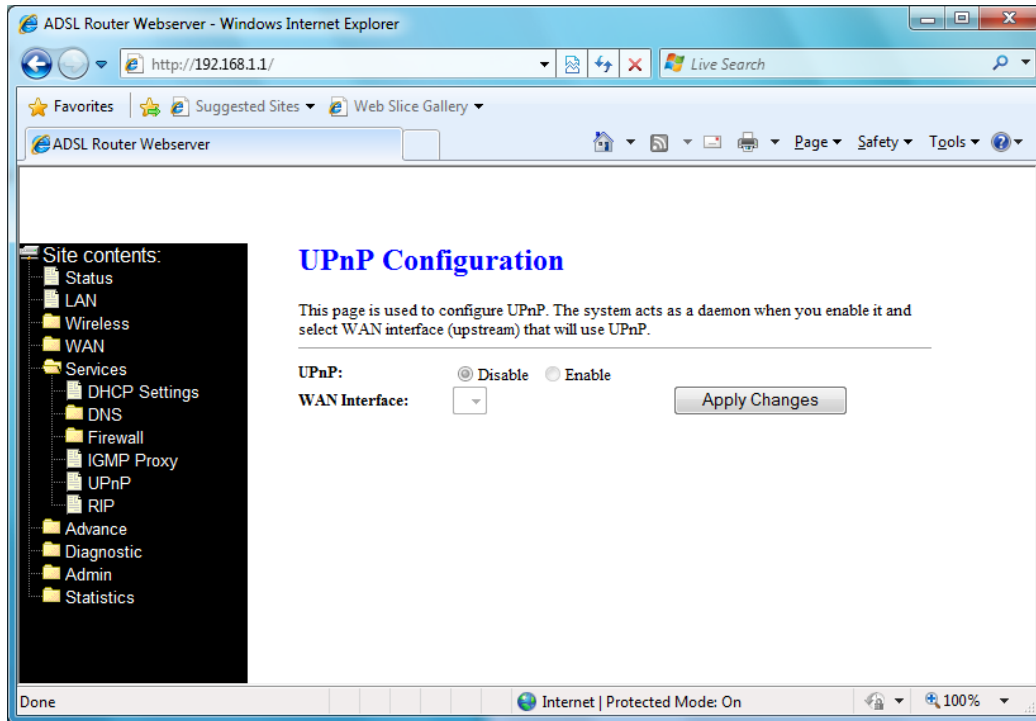


3.6.5 UPnP

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.



UPnP -- Enable/disable UPnP feature.

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

Apply Changes -- Click to save the setting to the system configuration.

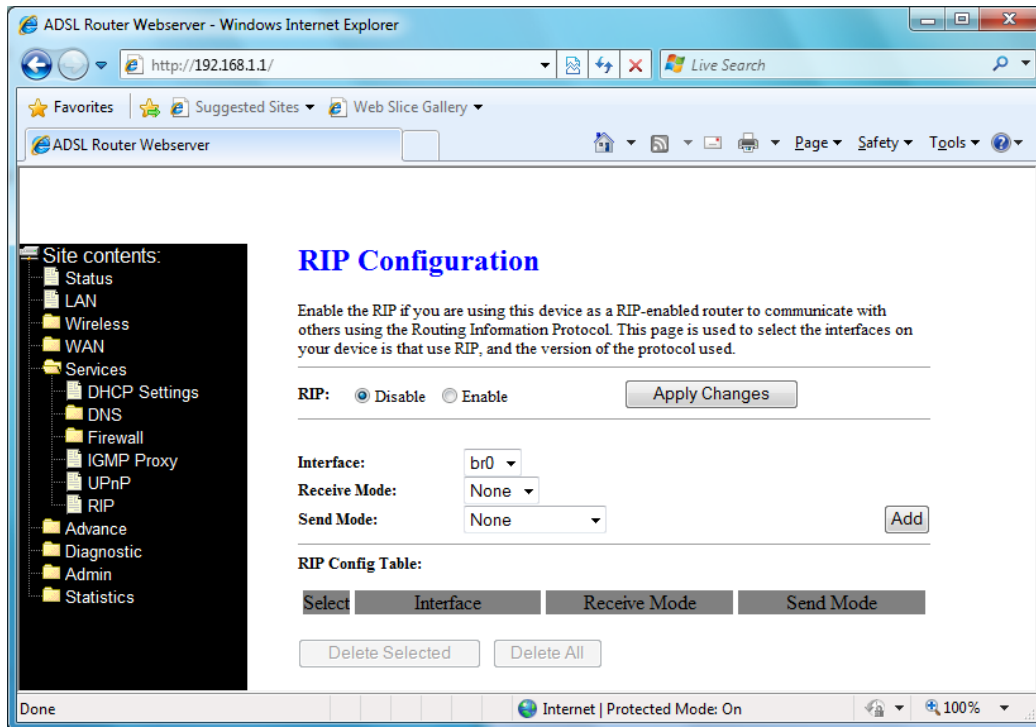
3.6.6 RIP

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.



RIP -- Enable/disable RIP feature.

Apply Changes -- Click to save the setting of this setting block to the system configuration

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.

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

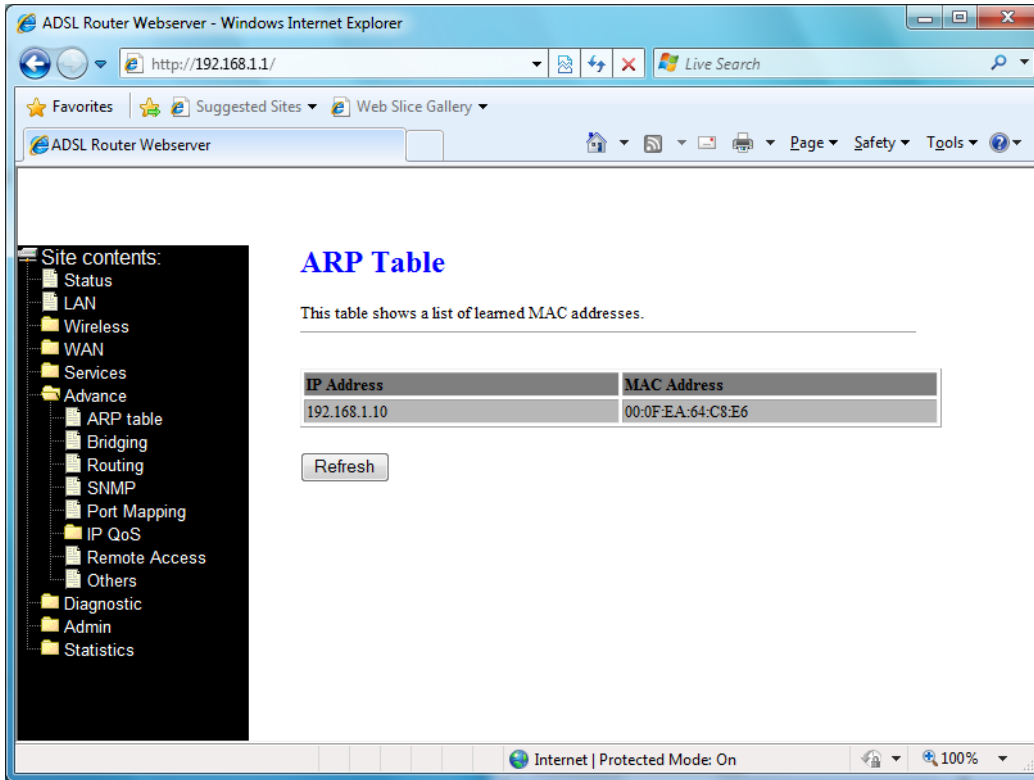
Delete Selected -- Delete a selected RIP entry. The RIP entry can be selected on the Select column of the RIP Config Table.

Delete All -- Delete all RIP rules from the table.

3.7 Advance

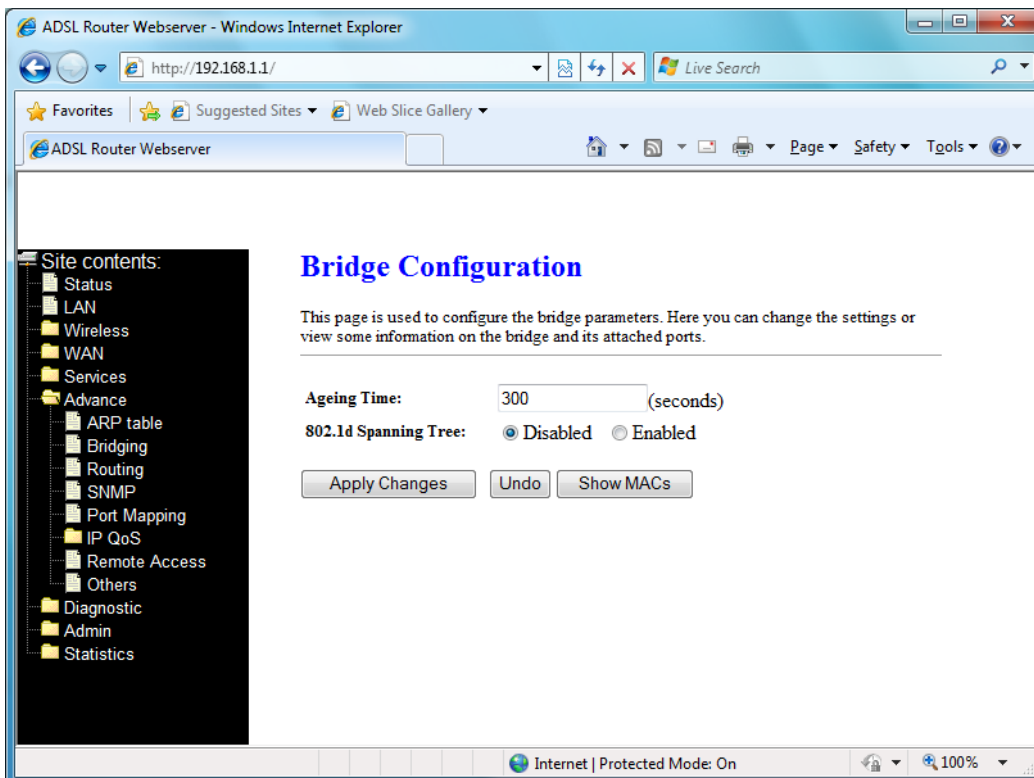
3.7.1 ARP Table

This table shows a list of learned MAC address.



3.7.2 Bridging

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

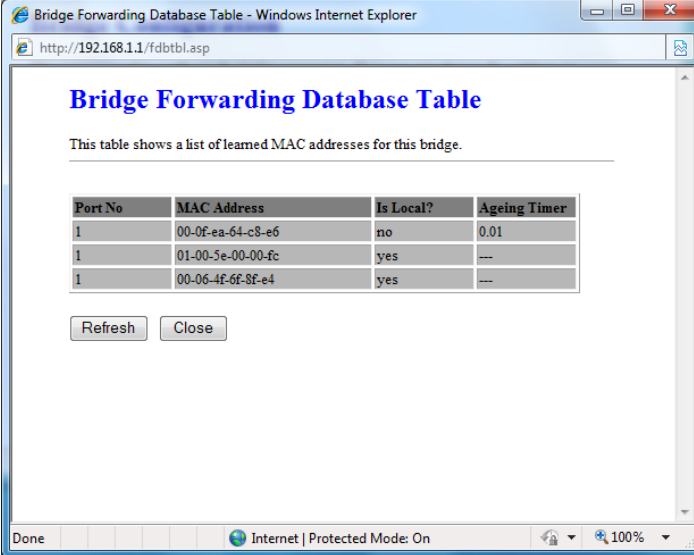


Ageing Time -- Set the Ethernet address ageing time, in seconds. After [Ageing Time] seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from Forwarding DataBase(fdb).

802.1d Spanning Tree -- Enable/disable the spanning tree protocol

Apply Changes -- Save this bridge configuration. New configuration will take effect after saving into flash memory and rebooting the system.

Show MACs -- List MAC address in forwarding table.



Bridge Forwarding Database Table - Windows Internet Explorer
http://192.168.1.1/fdbtbl.asp

Bridge Forwarding Database Table

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

Port No	MAC Address	Is Local?	Ageing Timer
1	00-0f-ea-64-c8-e6	no	0.01
1	01-00-5e-00-00-fc	yes	---
1	00-06-4f-6f-8f-e4	yes	---

Refresh Close

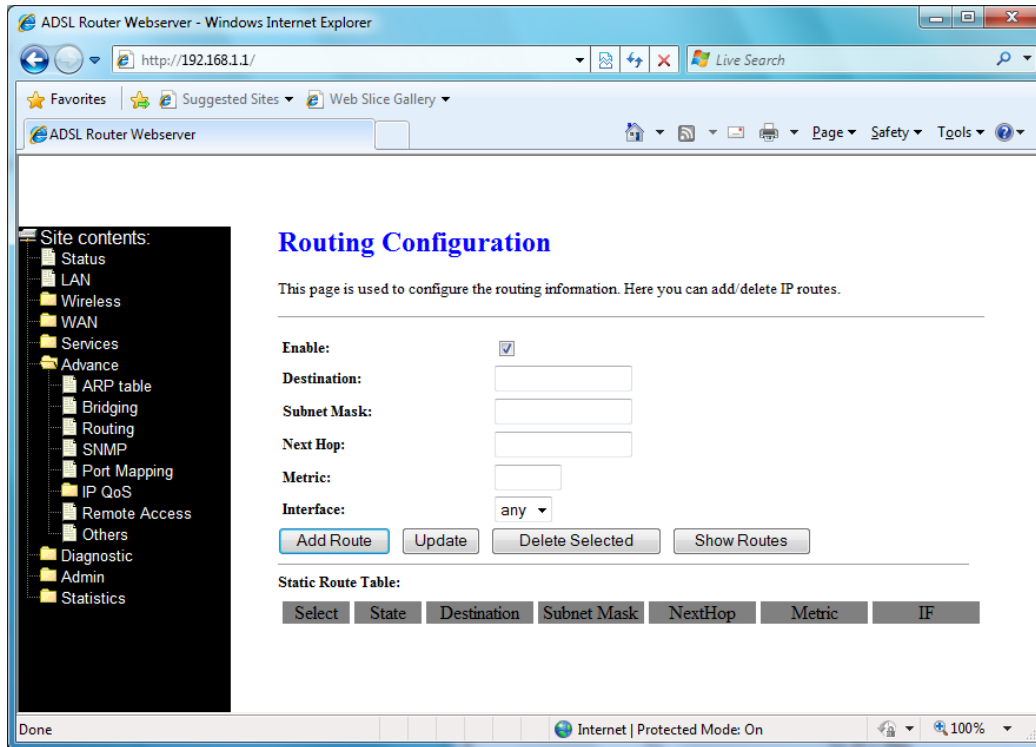
Done Internet | Protected Mode: On 100%

3.7.3 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.



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 for 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 for a static routing subnet is to be applied.

Add Route -- Add a user-defined destination route.

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

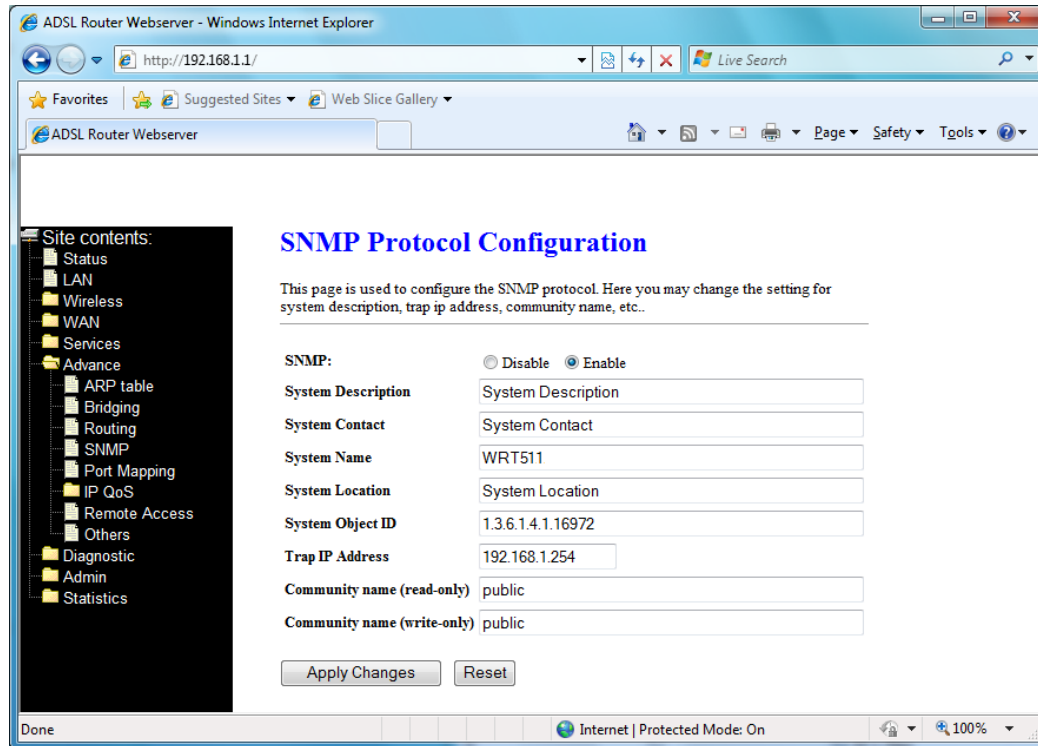
Delete Selected -- Delete a selected destination route on the Static Route Table.

Show Routes -- Click this button to view the DSL device's routing table.

3.7.4 SNMP

Simple Network Management Protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and

servers. The DSL device can be managed locally or remotely by SNMP protocol.



SNMP -- Enable/disable RIP feature.

System Description -- System descriptions 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 locations of the DSL device.

System Object ID -- Vendor object identifier. The vendor's authoritative identifications of the network management sub-system 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.

Apply Changes -- Save SNMP configuration. New configuration will take effect after saving into flash memory and rebooting the system.

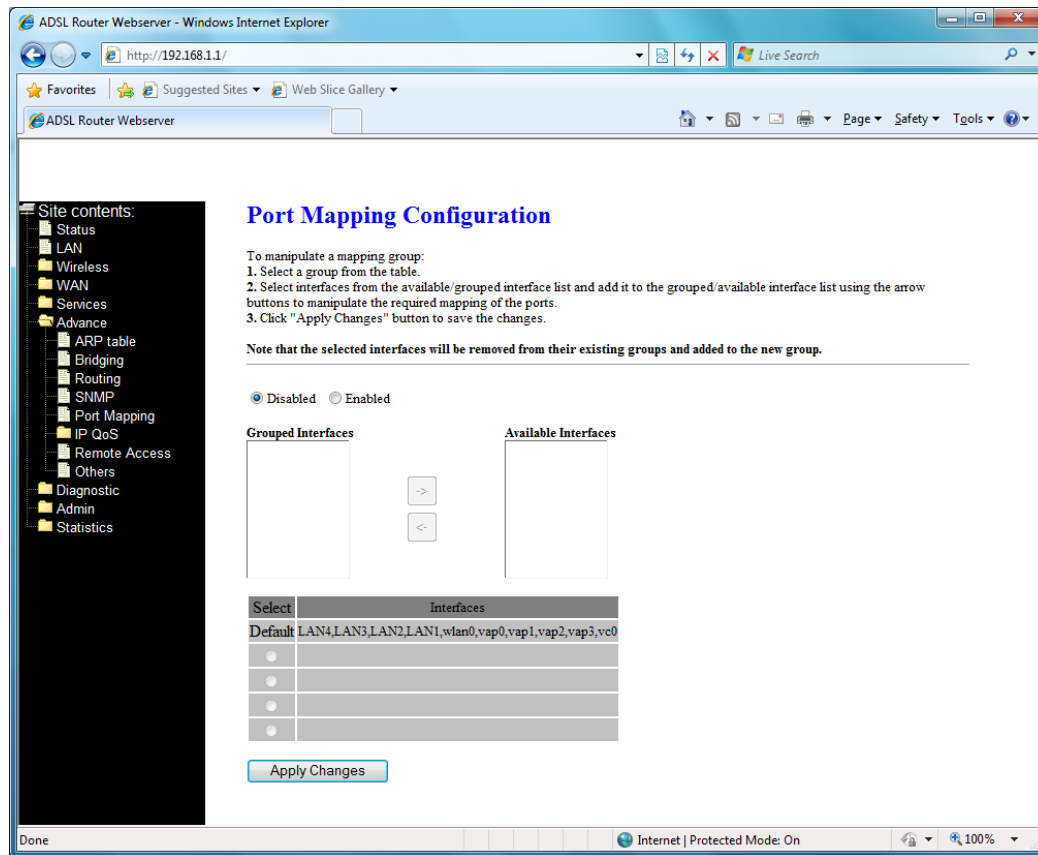
3.7.5 Port Mapping

To manipulate a mapping group:

- (1) Select a group from the table
- (2) Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required

mapping of the ports.

(3) Click “Apply Changes” button to save the changes.



3.7.6 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. A QoS rule contains two configuration blocks: **Traffic Classification** and **Action**. The **Traffic Classification** enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The **Action** enables you to assign the strictly priority level for and mark some fields in the packet that matches the Traffic Classification rule. You can configure any or all field as needed in these two QoS blocks for a QoS rule.

[Classification]

ADSL Router Webserver - Windows Internet Explorer
http://192.168.1.1/

Site contents:
Status
LAN
Wireless
WAN
Services
Advance
ARP table
Bridging
Routing
SNMP
Port Mapping
IP QoS
Classification
QoS Queue
Remote Access
Others
Diagnostic
Admin
Statistics

Classification

Configuration of classification table for IPQoS.

IP QoS: Disabled Enabled Default QoS: IP Pred

Specify Traffic Classification Rules

Source IP: Netmask: Port:
Destination IP: Netmask: Port:
Protocol: Physical Port:

Classification Results

ClassQueue: (Click to Select) 802.1p_Mark:
IP.Pred_Mark: TOS_Mark:

IP QoS Rules:

		Classification Rules				Classification Results						
Select	Status	Src IP	Src Port	Dst IP	Dst Port	Protocol	Lan Port	Interface	Priority	IP Precedence	IP ToS	802.1p

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.

Source Port -- The source port of the selected protocol. You cannot configure this field without entering the protocol first.

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.

Destination Port -- The destination port of the selected protocol. You cannot configure this field without entering the protocol first.

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

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

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

Precedence -- Select this field to mark the IP precedence bits in the packet that match this

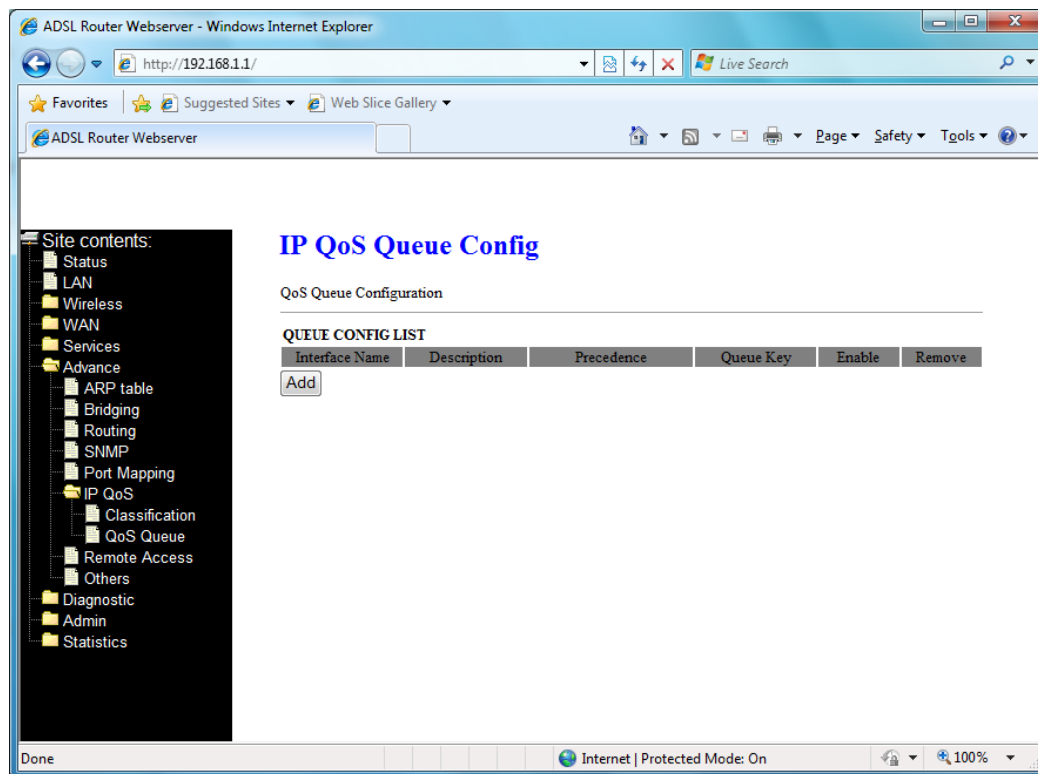
classification rule.

TOS (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.

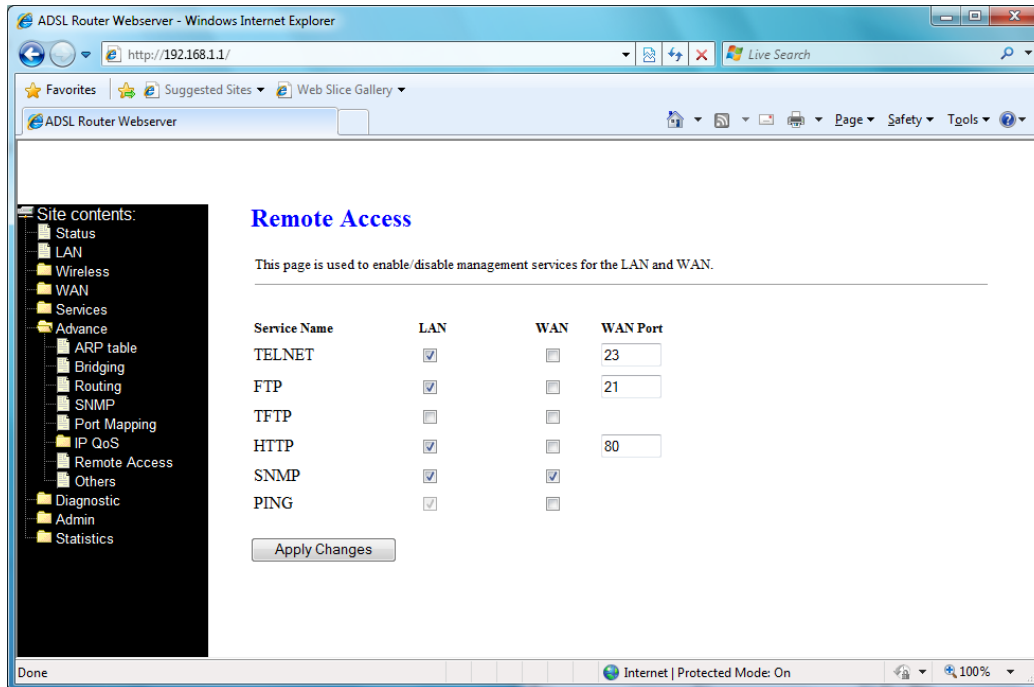
[QoS Quese]

This page displays the list of QoS Queue Configuration.



3.7.7 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.



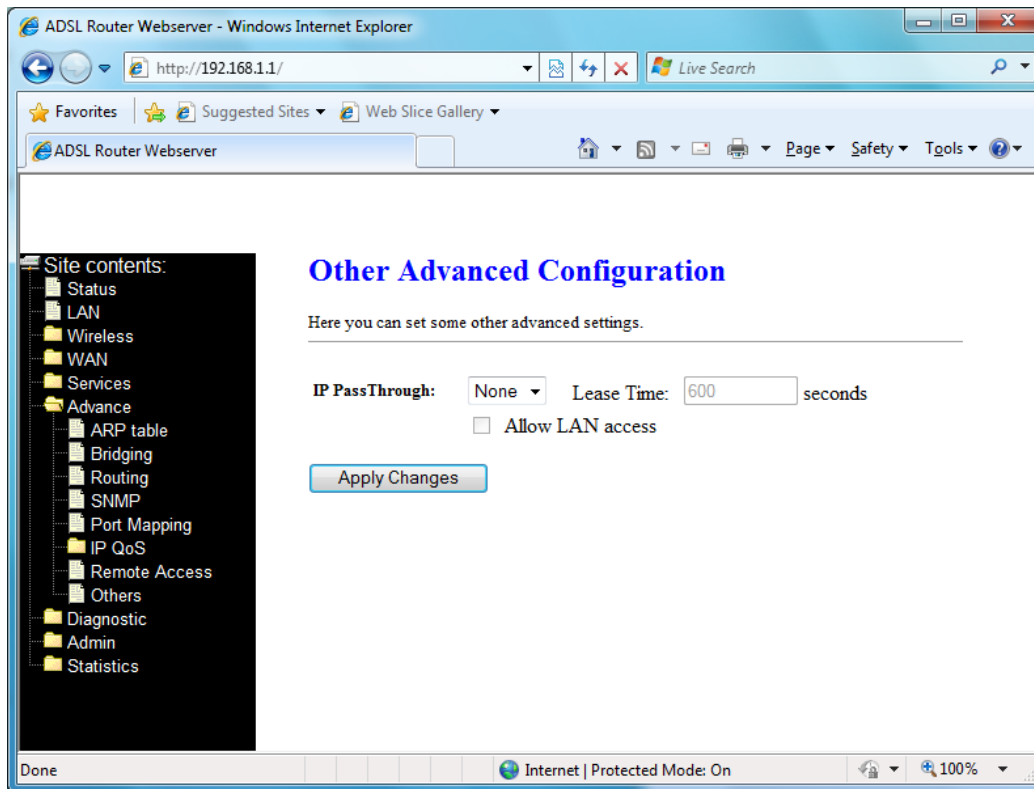
LAN -- Check/un-check the services on the LAN column to allow/un-allow the services access from LAN side; and “WAN”.

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.

3.7.8 Others

Here you can set some other advanced settings



IP Pass through -- The available interfaces are listed. You have to select one for advanced configuration.

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 IP address.

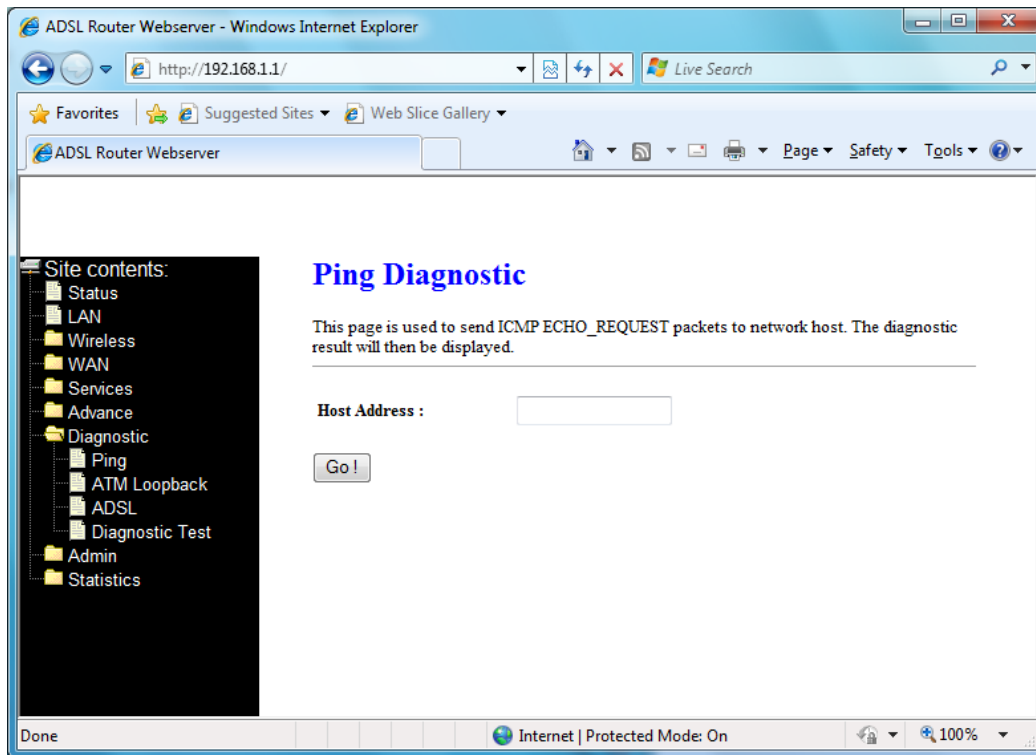
Allow LAN access – Check this option to enable the LAN access

3.8 Diagnostic

The DSL device supports some useful diagnostic tools.

3.8.1 Ping

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



Host Address -- The IP address you want to ping.

3.8.2 ATM Loopback

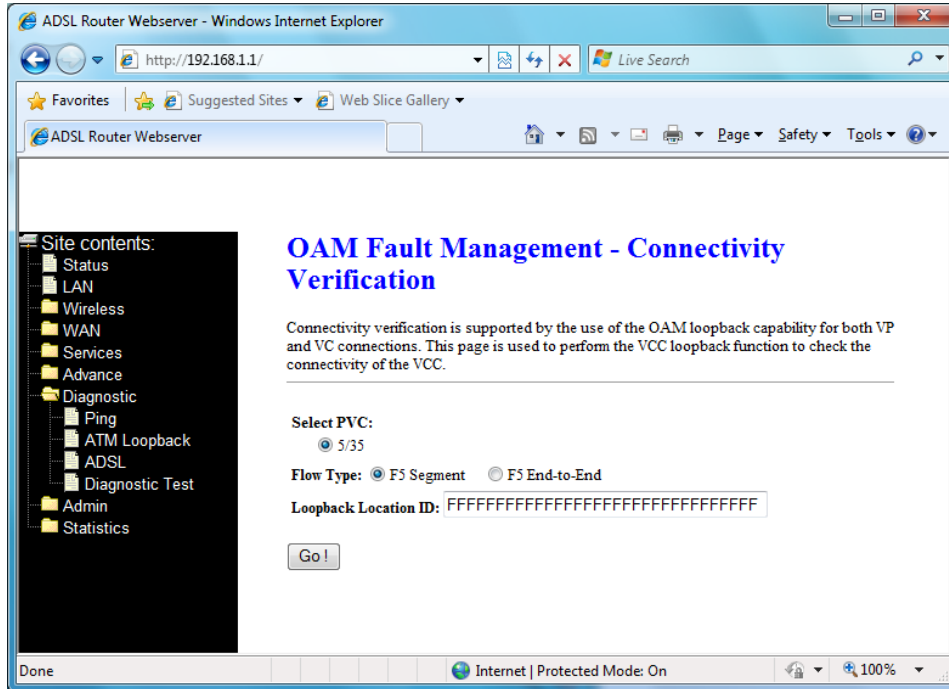
In order to isolate the ATM interface problems, you can use ATM OAM loopback cells to verify connectivity between VP/VC endpoints, as well as segment endpoints within the VP/VC. ATM uses F4 and F5 cell flows as follows:

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

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

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

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



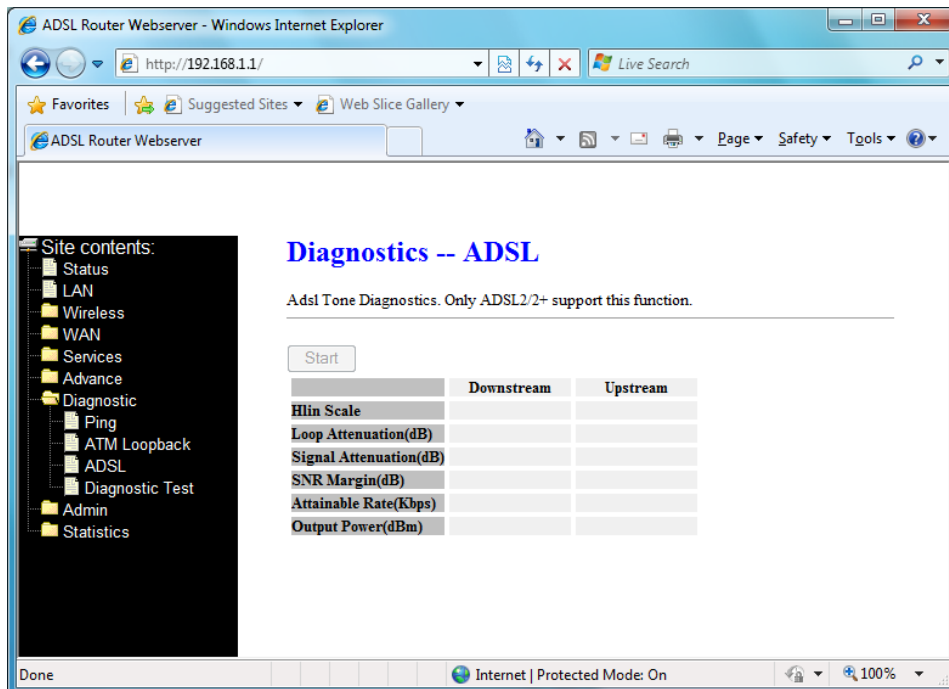
Select PVC -- Select the PVC channel you want to do the loop-back diagnostic.

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

Loopback Location ID -- The loopback location ID is the field for the loop-back cell. The default value is all Fs to indicate the endpoint of the segment or connection.

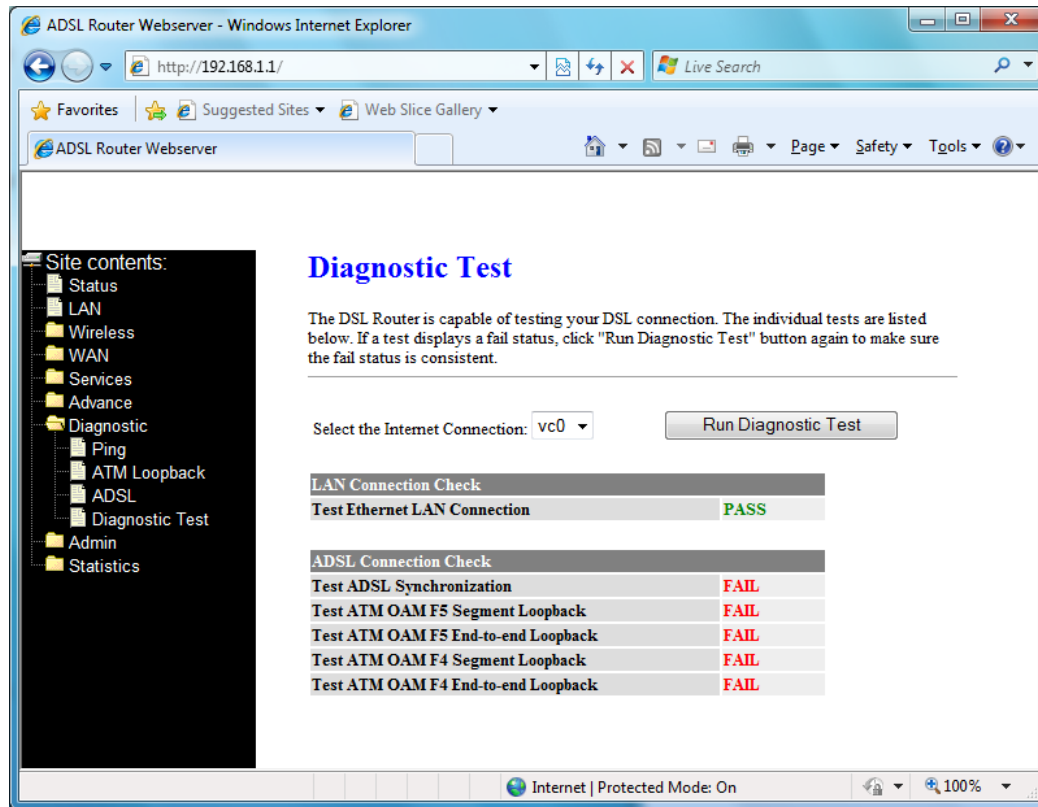
3.8.3 ADSL

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



3.8.4 Diagnostic Test

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

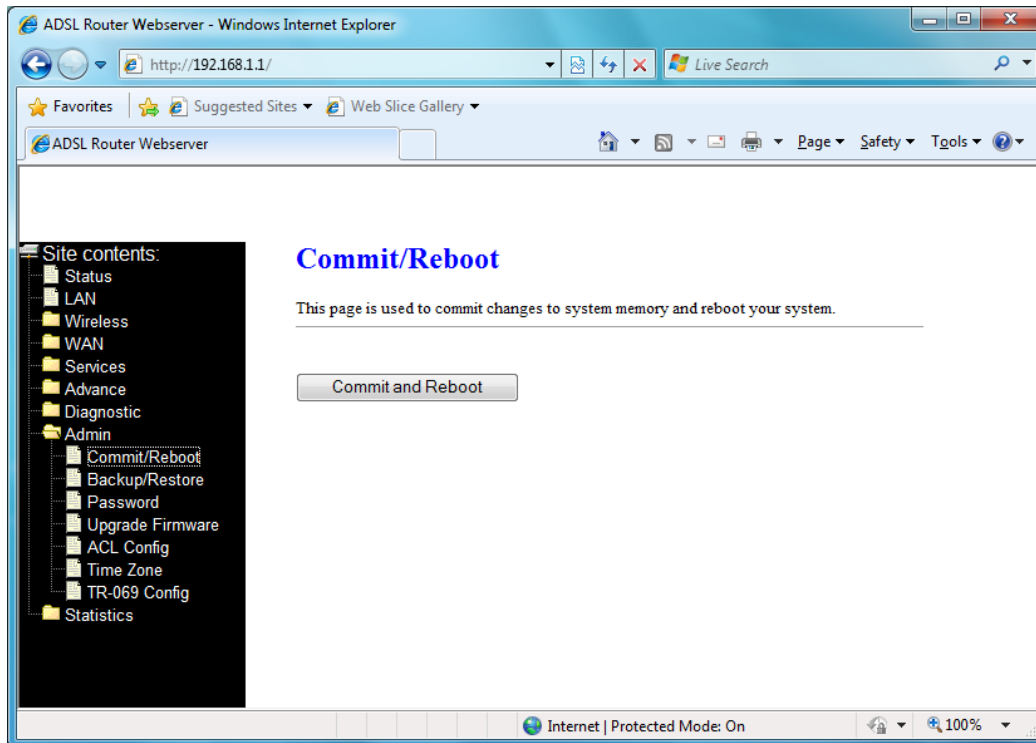


Select the Internet Connection -- The available WAN side interfaces are listed. You have to select one for the WAN side diagnostic.

3.9 Admin

3.9.1 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

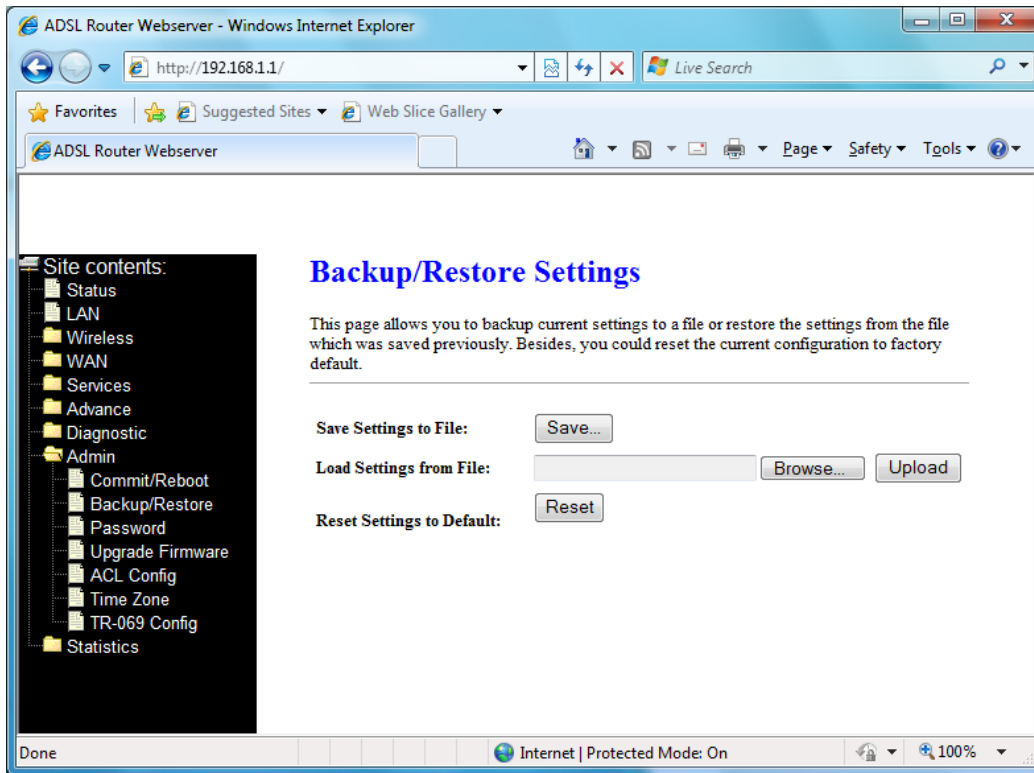


Commit and Reboot -- Whenever you use the web console to change system settings, the changes are initially placed in temporary storage. To save your changes for future use, you can use the Commit/Reboot function. This function saves your changes from RAM to flash memory and reboot the system.

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

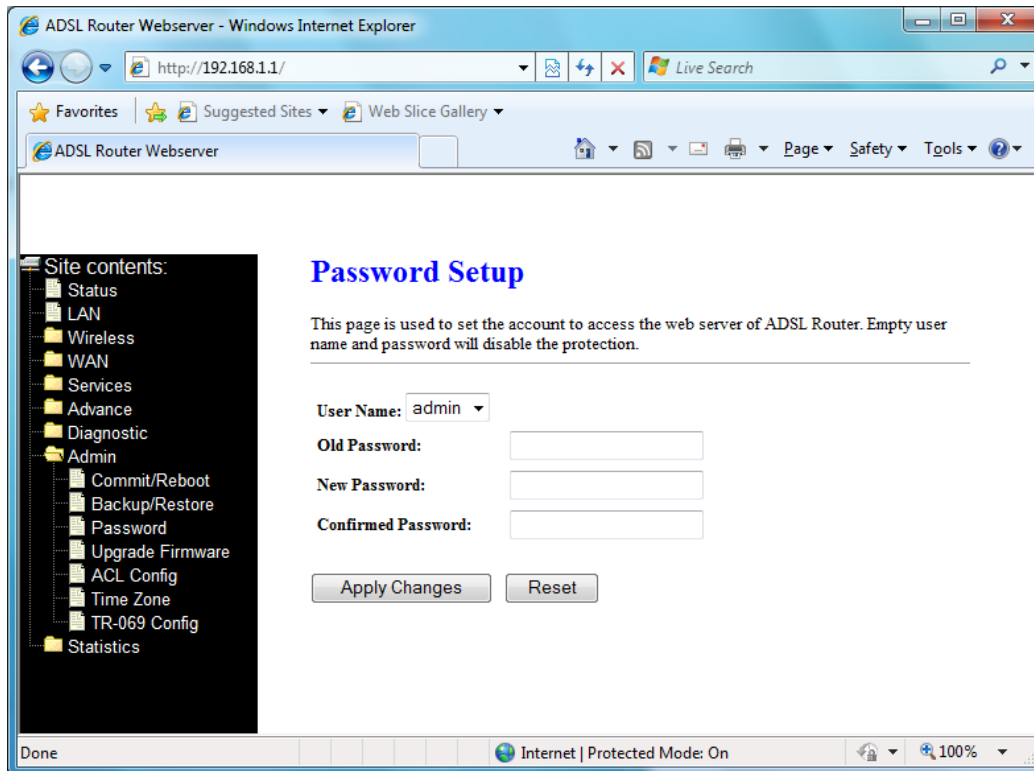
3.9.2 Backup/Restore

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



3.9.3 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.



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.

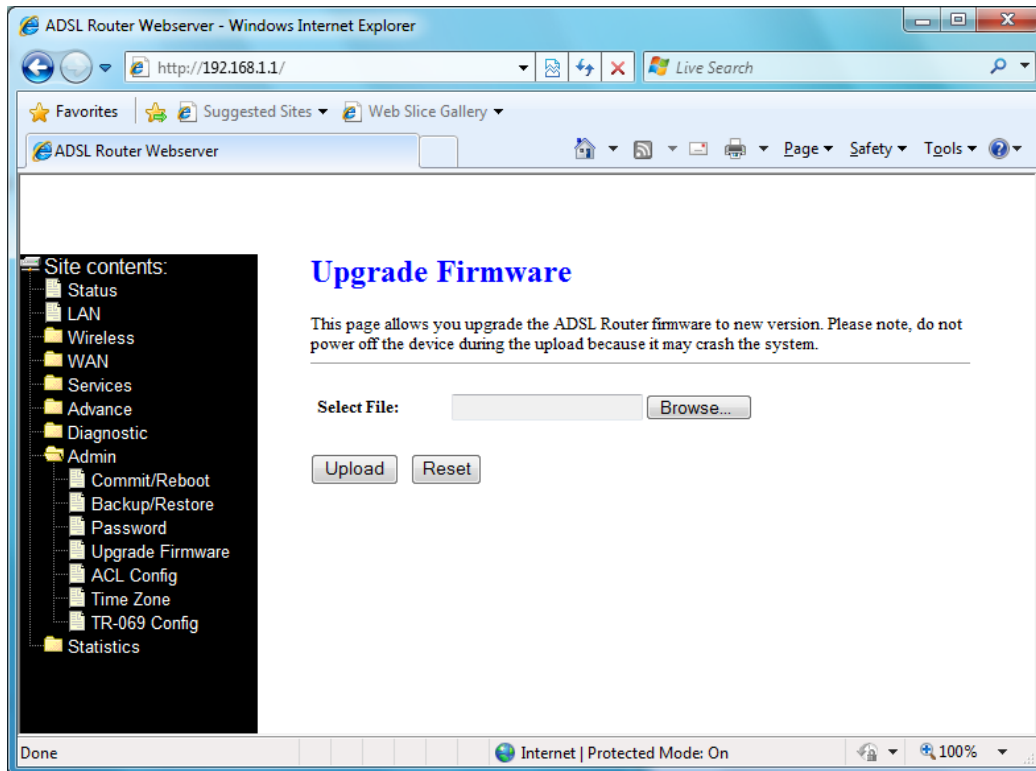
Confirmed Password -- Enter the new password here again to confirm.

3.9.4 Upgrade Firmware

To upgrade the firmware for the DSL device:

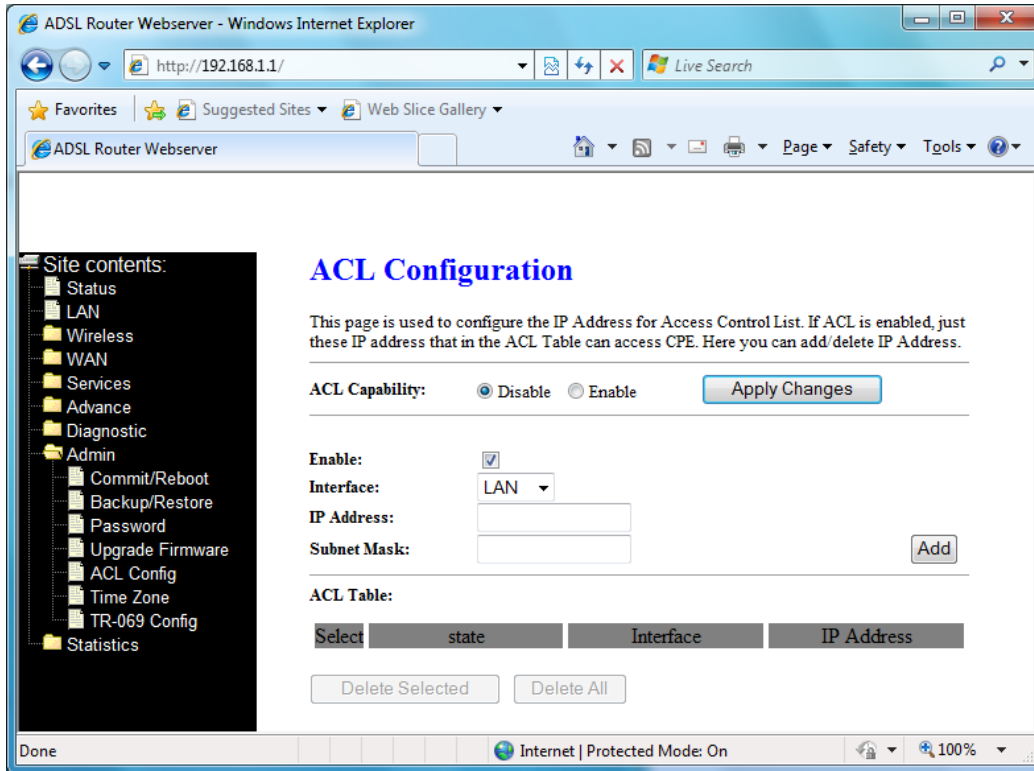
- Click the Browse button to select the firmware file.
- Confirm your selection.
- Click the Upload button to start upgrading.

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



3.9.5 ACL Configuration

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.



ACL Capability -- Enable/disable the ACL function

Enable -- Check to enable this ACL entry

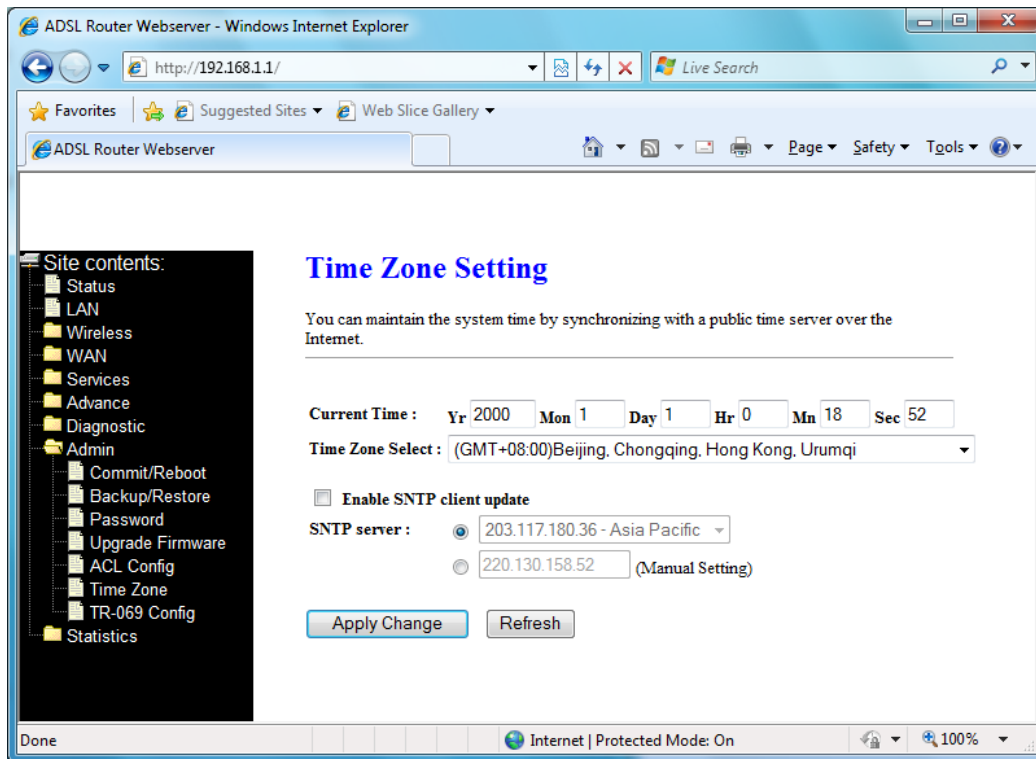
Interface -- Select the interface domain: LAN or WAN

IP Address -- Enter the IP address that allows access to this device.

Subnet Mask -- Enter the Subnet Mask that allows access to this device.

3.9.6 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.



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

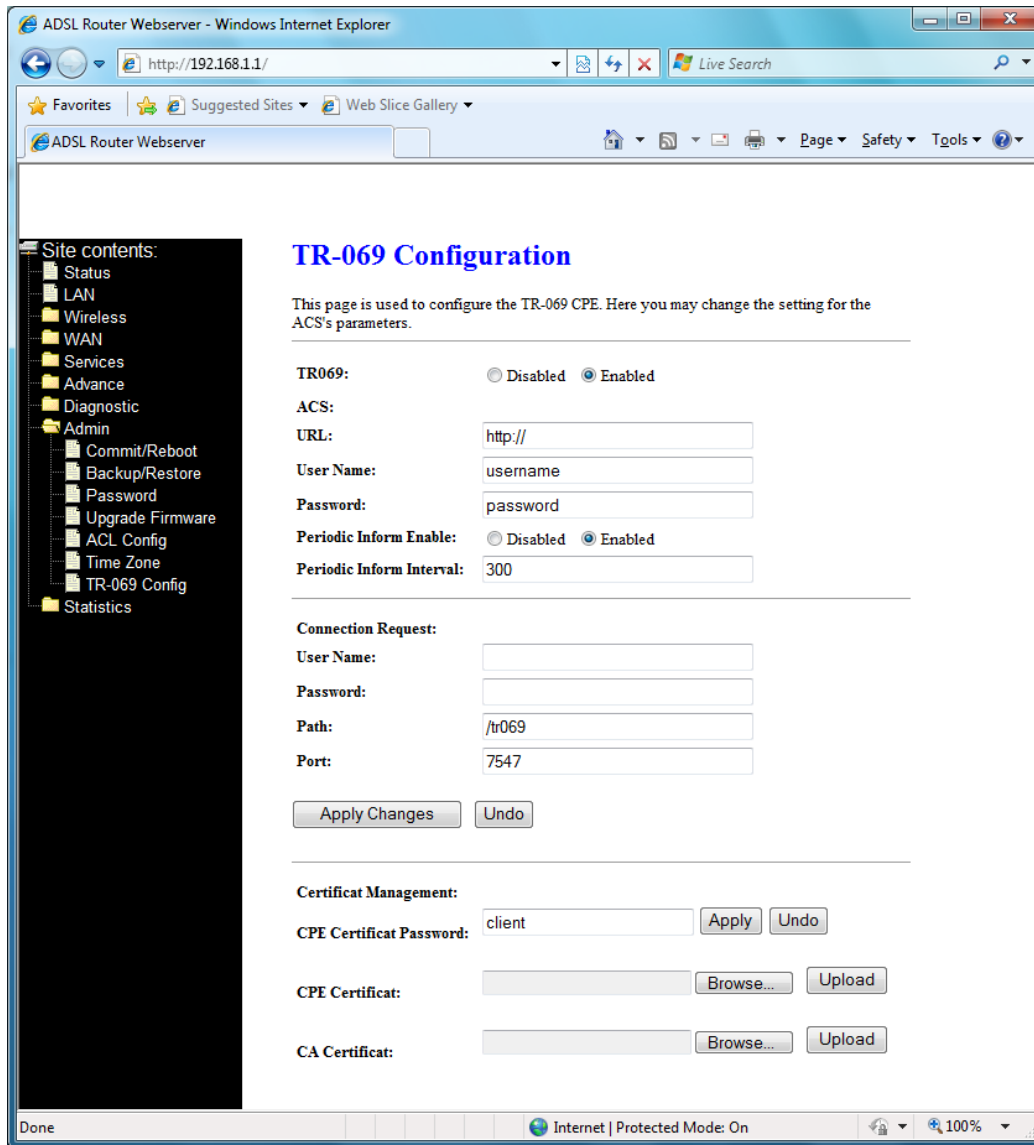
Time Zone -- Select time zone in which the DSL device resides.

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.

3.9.7 TR-069 Configuration

TR-069 is CPE Management Protocol from WAN side [**CPE WAN Management Protocol (CWMP)**], intended for communication between a CPE and Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.



[ACS]

URL -- URL of the auto configuration server (ACS) provided by the ISP

User Name -- Entry the User name for ACS which is provided by ISP.

Password -- Entry the password for ACS which is provided by ISP.

Periodic Inform Enable -- Enable/disables the RG to connect to the ACS periodically. If you enable this feature, you should enter a value in the Periodic Inform Interval field.

Periodic Inform Interval -- This field is enabled only when the Periodic Inform Enabled field is checked. It defines the amount of time (in seconds) between a successful connection with an ACS server and a new attempt to connect to an ACS server. A recommended value is 86400 seconds (1 day).

[Connection Request]

User Name -- Key in the User name for ADSL router.

Password -- Key in the password for ADSL router.

Path -- The path for connection request. Default is **"/tr069"**.

Port -- The port for connection request. Default is **"7547"**.

[Certificate Management]

CPE Certificate Password -- The password is for CPE certificate.

CPE Certificate -- Browse CPE certificate which is provided by ISP server. The CPE may use online certificate enrollment with the CA associated with the ACS. The CPE must be provided with the information needed to contact this CA.

CA Certificate -- Browse CA certificate which is provided by ISP server.

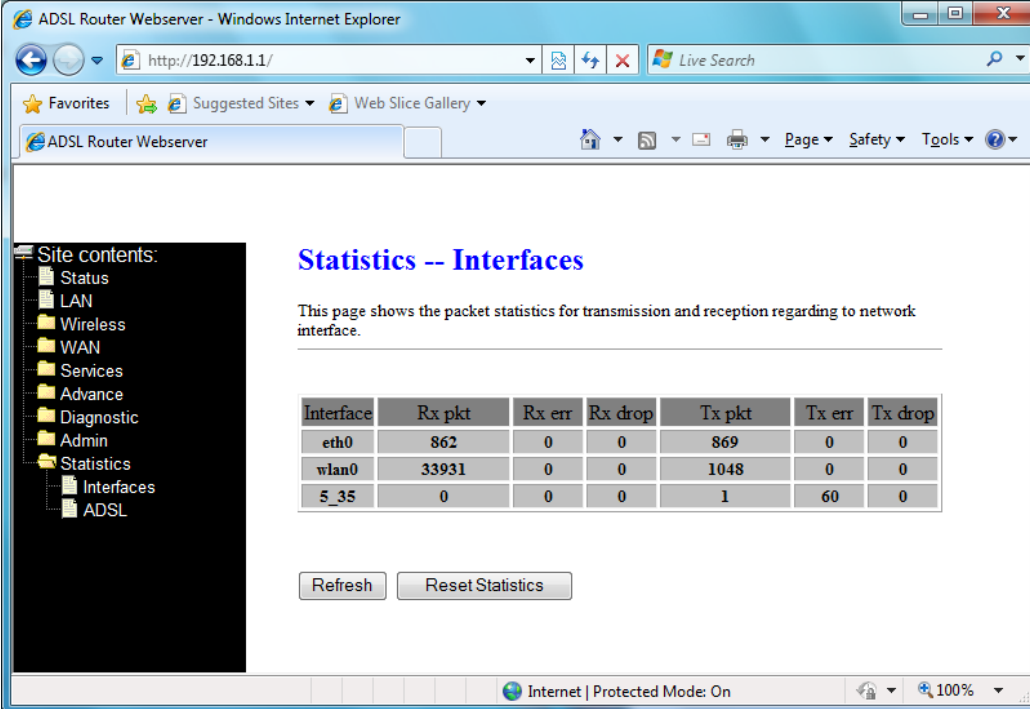
3.10 Statistics

The DSL device shows the different layer of network statistics information

3.10.1 Interface

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**.



The screenshot shows a web browser window titled "ADSL Router Webserver - Windows Internet Explorer" with the address bar set to "http://192.168.1.1/". The page content includes a left-hand navigation menu with "Statistics" expanded to show "Interfaces". The main content area is titled "Statistics -- Interfaces" and contains a table of network statistics. Below the table are "Refresh" and "Reset Statistics" buttons.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0	862	0	0	869	0	0
wlan0	33931	0	0	1048	0	0
5_35	0	0	0	1	60	0

3.10.2 ADSL

This page shows the ADSL line statistic information.

The screenshot shows a web browser window titled "ADSL Router Webserver - Windows Internet Explorer" with the address bar displaying "http://192.168.1.1/". The page content is titled "Statistics -- ADSL Line". On the left, a "Site contents:" sidebar lists various menu items, with "ADSL" selected. The main content area displays a table of ADSL line statistics.

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

Additional statistics shown in a separate table:

Mode	
Latency	
Trellis Coding	Enable
Status	ACTIVATING.
Power Level	L0
Uptime	