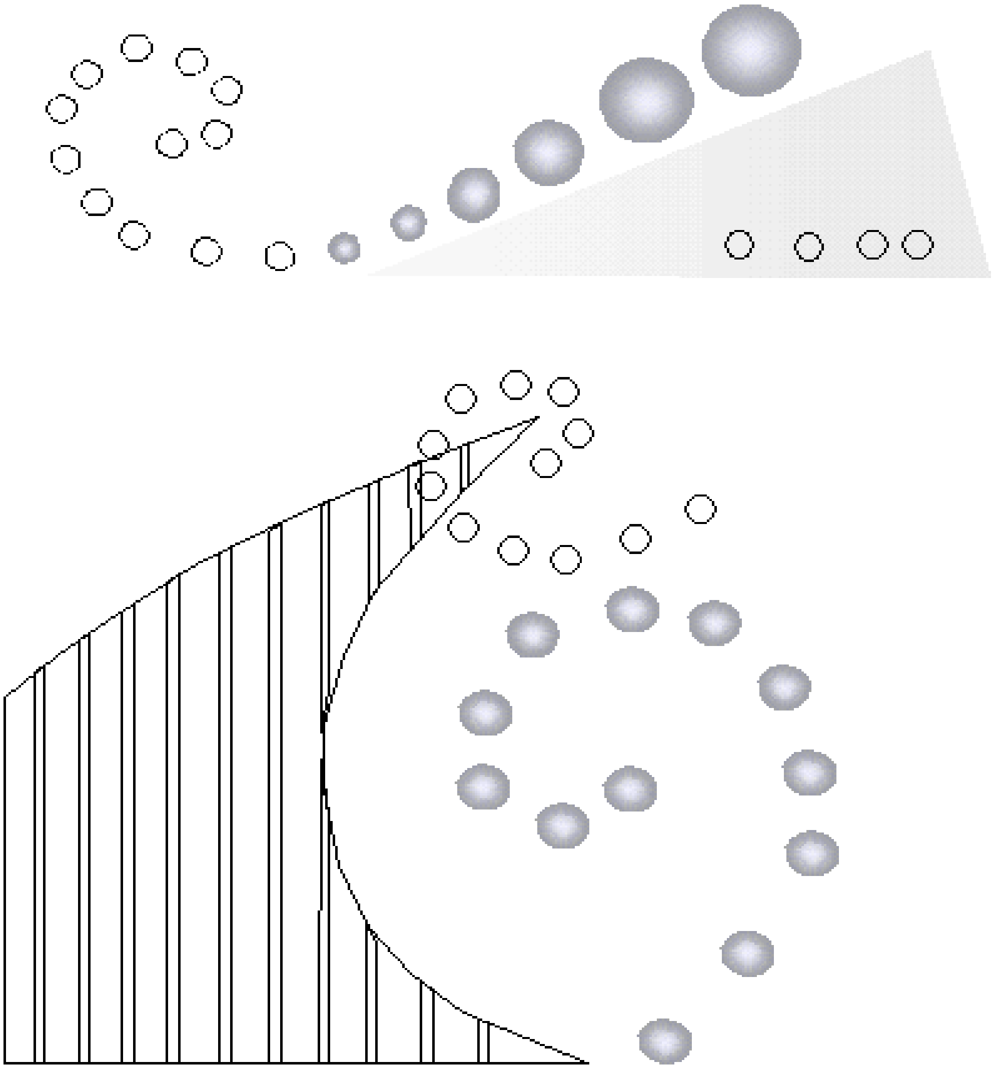
AW4062 4-port ADSL2+ Router
User's Manual



M/C: CPE-AW4062-UM

FCC Statement

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. This equipment as been tested and found to comply with the limits for a Class B computing device pursuant to Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against radio interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at is own expense, will be required to take whatever measures are necessary to correct the interface.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN55022 class B for ITE and EN 50082-1. This meets the essential protection requirements of the European Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Environment

The phone you have purchased, as well as any used batteries must not be disposed of with household waste. You should return these to your distributor if they are able to replace or dispose of them in an approved recycling centre.

Trademarks

Windows 98/2000/XT/NT™ and Internet Explorer™ are registered trademarks of Microsoft Corporation. All other company, brand and product names, like Netscape Navigator™ are trademarks or registered trademarks of their respective owners.

WARNING!

1. Read all installation instructions carefully before connecting the device to its power source.
2. To reduce the risk of electric shock, do not remove the cover from this device or attempt to dismantle it. Opening or removing covers may expose you to dangerous voltage levels. Equally, incorrect reassembly could cause electric shock on re-use of the appliance.
3. Do not expose this device to Fire, direct sunlight or excessive heat.
4. Do not expose the device to rain or moisture and do not allow it to come into contact with water.
5. Do not install the device in an environment likely to present a THREAT OF IMPACT.
6. You may clean this device using a fine damp cloth. Never use solvents (such as trichloroethylene or acetone), which may damage the phone's plastic surface. Never spray this device with any cleaning product whatsoever.
7. Take care not to scratch the surface of plastic housings.
8. The device is designed to work in temperatures from 5^{o}C to 40^{o}C.
9. The this device must be installed at least 1 meter from radio frequency equipment, such as TVs, radios, hi-fi or video equipment (which radiate electromagnetic fields).
10. Do not connect the LAN/PC port to any network other than an Ethernet network.
11. Do not attempt to upgrade your this device in an unstable power environment. This could cause unexpected issues.
12. Do not work on the system or connect or disconnect cables during lightning storms.
13. Children don't recognize the risks of electrical appliances. Therefore use or keep this device only under supervision of adults or out of the reach from children.
14. No repair can by performed by the end user, if you experience trouble with this equipment, for repair or warranty information, please contact your supplier.

Table of Contents

1. **INTRODUCTION……………………………………………………………………. 4**
2. **SYSTEM OVERVIEW……………………………………………………………….. 5**
   - 2.1. GENERAL DESCRIPTION…………………………………………………………. 5
   - 2.2. SPECIFICATIONS………………………………………………………………… 5
3. **HARDWARE INSTALLATION……………………………………………………….. 7**
   - 3.1. PACKAGE CONTENT……………………………………………………………. 7
   - 3.2. HARDWARE SETUP PROCEDURE……………………………………………. 7
   - 3.3. CONNECTORIZATIONS…………………………………………………………. 8
   - 3.4. INDICATORS……………………………………………………………………… 9
4. **SOFTWARE CONFIGURATION……………………………………………………. 12**
   - 4.1. SET YOUR PC'S ETHERNET PORT…………………………………………... 12
   - 4.2. ACCESS THE WEB PAGE OF ROUTER………………………………………… 13
   - 4.3. LAN CONFIGURATION……………………………………………………………...14
   - 4.4. WIRELESS CONFIGURATION………………………………………………….....15
   - 4.5. WAN CONFIGURATION……………………………………………………………. 24
   - 4.6. SERVICES CONFIGURATION…………………………………………………….. 28
   - 4.7. FIREWALL…………………………………………………………………………. 39
   - 4.8. ADVANCE CONFIGURATION…………………………………………………….49
   - 4.9. DIAGNOSTIC………………………………………………………………………… 59
   - 4.10. ADMIN……………………………………………………………………………. 62
   - 4.11. STATISTICS……………………………………………………………………... 69

APPENDIX A. CHANNEL MODE CONFIGURATION…………………………………….. 71

APPENDIX B. PROTOCOL STACKS……………………………………………………. 76

APPENDIX C. MAPPING PVCS TO VLANS………………………………………………. 81

1. Introduction

The AW4062 is an ADSL2+ router that can be used to connect to a twisted copper pair ADSL2+ broadband network. The AW4062 is backwards compatible to all ADSL modulation technology including G.lite, G.dmt, T1.413, ADSL2 and ADSL2+. AW4062 also supports various Internet service provider networks via common WAN protocol such as PPPOE, PPPOA, Bridge/MER 1483 modes. With advanced features such as remote configuration, the AW4062 reduces provisioning, maintenance and deployment overheads and ensures a hassle free user experience. Leveraging adoption of Annex-M DSL technology, the AW4062 is capable to provide increased upstream rates to better fulfill growing demand from the SOHO/SMB user. Compliant to Annex L technology, the AW4062 can reach users in a larger service radius increasing the operators' Central Office user density. The AW4062 is a reliable and full-featured ADSL2+ router capable of supporting data traffic and IP services which allows for minimum overhead deployment.

This User's Manual mainly contains the guidance to install and configure this ADSL2+ Router using the Web GUI.

2. System Overview

2.1. General Description

This AW4062 Router is a high-speed ADSL Ethernet router that is specifically designed to connect to the Internet and to directly connect to your local area network (LAN) via high-speed 10/100 Mbps Ethernet, or wireless LAN (WLAN). The ADSL modem is compatible with the latest ADSL standards, including ADSL2 and ADSL2+, and supports up to 24 Mbps downstream and 1.5 Mbps upstream to deliver true broadband speed and throughput.

To ensure fully compatibility, the DSL device was tested with all major DSLAMs, and support standard 10/100 Mbps Base-T Ethernet interface Auto MDI / MDIX 10/100 Switch function allowing user easily to link to PC or other Switches/Hubs. The DSL device is an idea solution for multi-users utilizing build-in channel mode (PPPoE/A, IPoA, IPoE), IP routing, NAT functionalities sharing the ADSL link. The DSL device is also a perfect solution for the residential users, it supports the users with bridge mode in host based PPPoE Client.

2.2. Specifications

2.2.1. ADSL Standard

- ITU-T G.992.1(G.dmt)
- ANSI T1.413 Issue 2
- G.992.2 (G.lite)
- G.994.1 (G.hs)
- Auto-negotiating rate adaptation
- ADSL2 G.dmt.bis (G.992.3)
- ADSL2 G.lite.bis (G.992.4)
- ADSL2+ (G.992.5)

2.2.2. Software Features

- RFC-1483/2684 LLC/VC-Mux bridged/routed mode
- RFC-1577 Classical IP over ATM
- RFC-2516 PPPoE
- RFC-2364 PPPoA
- ITU-T 1.610 F4/F5 OAM send and receive loop-back
- 802.1d Spanning-Tree Protocol
- DHCP Client/Server/Relay
- NAT
- RIP v1/v2

- DNS Relay Agent
- DMZ support
- IGMP Proxy/Snooping
- Packet Inspection
- Protection against Denial of Service attacks
- IP Packet Filtering
- QoS
- Dynamic DNS
- Wi-Fi
- WPS

2.2.3. Management

- Web-based Configuration
- Menu-driven Command-line Interpreter
- Telnet Remote Management
- SNMP v1/v2/Trap
- Firmware upgrade through FTP, TFTP and HTTP
- Configuration backup/restore
- Diagnostic Tool
- TR069

3. Hardware Installation

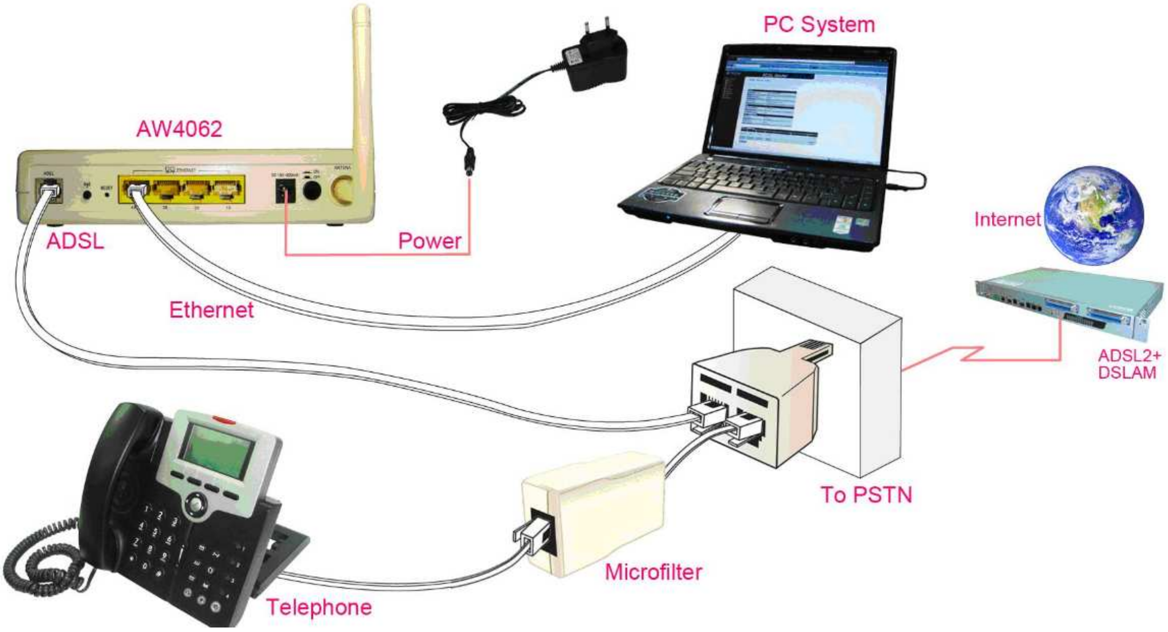
3.1. Package Content

Upon opening the gift box of AW4062 Router, you will find the following items.

- 1 x AW4062 Router Main Unit
- 1 x 15VDC/800mA power adaptor
- 1 x CD-ROM
- 1 x Quick Install Guide
- 1 x Warranty Card
- 1 x RJ-45 Ethernet cable
- 1 x RJ-11 ADSL line
- 1 x T-Connector
- 3 X Microfilters

3.2. Hardware Setup Procedure

Referring to the figure below and connect this ADSL router to the ISP ADSL line and PC.



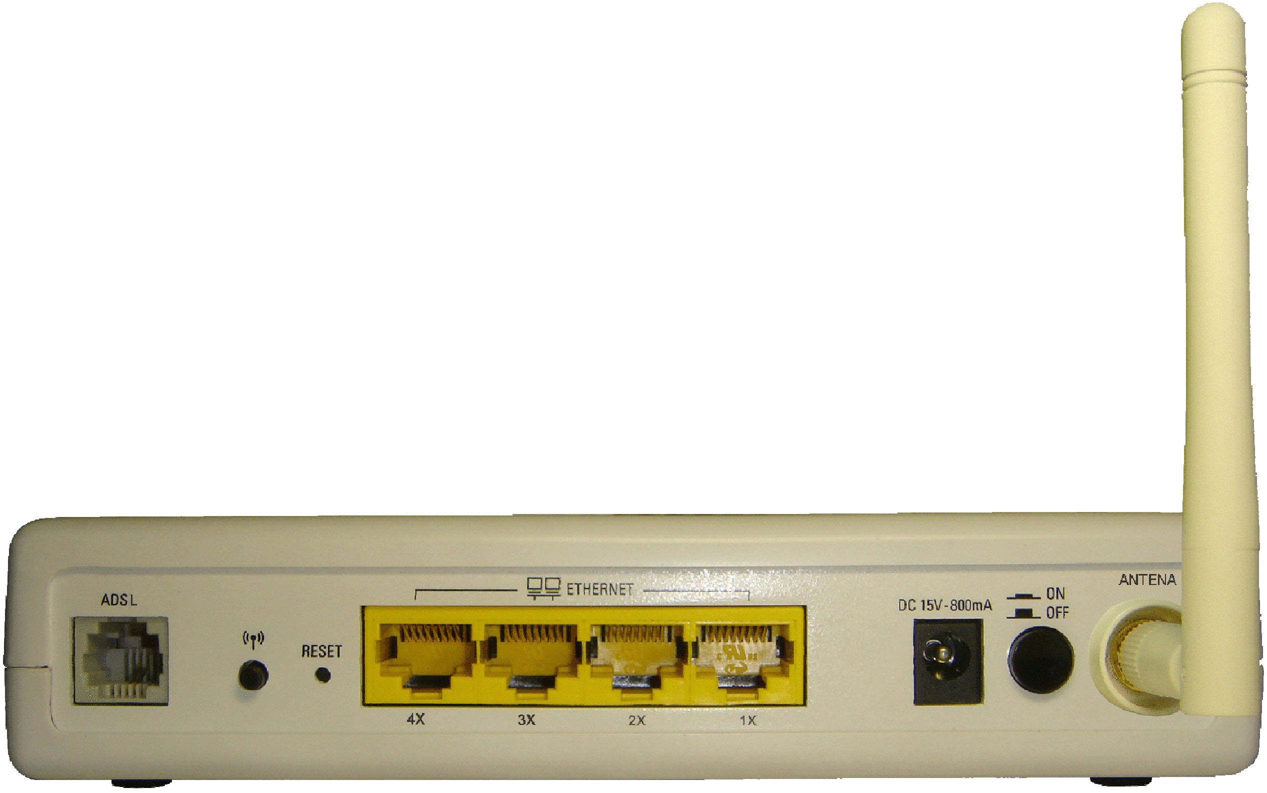
1. Connect RJ-11 Telephone wire from AW4062 Router ADSL port to the T-connector that connects the ADSL line to the DSLAM located at central office. Thus it is the gate to the world-wide Internet.
2. An analog telephone can be connected to ISP Microfilter. This phone can work as

it were connected directly to the PSTN Line (also called as ADSL line now)

3. Connect RJ-45 Ethernet Cable from your PC to AW4062 Router Ethernet port. If you have two or more PC systems, you have to prepare a low-density Ethernet switch or hub for expansion purpose.
4. Connect the AC Power Adaptor (15V) and then the AW4062 Router will start to run and connect the Home local network to the Broadband world.

3.3. Connectorizations

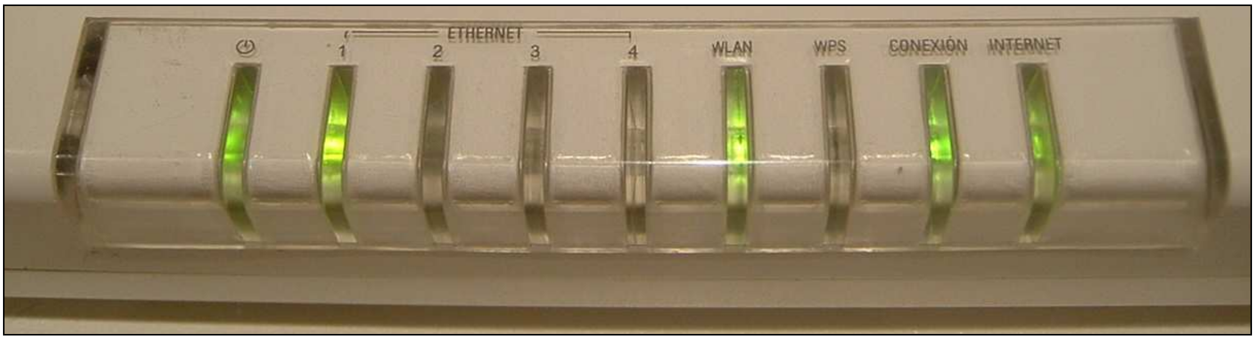
All the connectors, reset button power switch and power jack are on the rear panel. The drawing of the rear panel is shown below.



Label	Color	Function
ADSL	Gray	RJ-11 connector: Connect the device to the ADSL.
((•))	Black	Shortly press the Wi-Fi / WPS button to enable / disable Wi-Fi interface **(more than 1 and less than 8 seconds)** Long press the Wi-Fi / WPS button to enable WPS enrollee **(more than 8 seconds)**
RESET	Black	Long press RESET button to reset the configuration to factory default and restart the device **(more than 10 sec)**
ETHERNET 1-4	Yellow	RJ-45 connector: Connect the device to your PC's Ethernet port, or to the uplink port on your LAN's hub or home gateway, using the Ethernet cables.
DC 15V 800mA	Black	Connects to the power adaptor.
ON/OFF	Black	Turn on / off the power.
ANTENA	WHITE	Detachable antenna.

3.4. Indicators

The following table is a description of the meaning of the different LEDs on the AW4062:



Label	**Color**	**Function**
⏻	Red / Green	Steadily off: Power is off. Red solid on: Power on self test (POST) or fail to boot up. Green blinking: while booting. Green steadily on: Boot process is successful.
ETHERNET 1-4	Y-Green	Steadily off: Wired interface not established (Ethernet cable not detected or not connected properly). Blinking: Traffic is passing thru. Steadily on: Wired interface established (Ethernet cable detected).
WLAN	Y-Green	Steadily off: Wi-Fi is disabled. Blinking: Traffic is passing thru. Steadily on: Wi-Fi is activated.
WPS	Green Yellow Red	Blinking yellow: activation of WPS process (association started, in progress) Solid green: connected successfully; session established then off after 10 seconds. Blinking red: failure (whatever it is during the process)
CONEXIÓN	Y-Green	Steadily off: No ADSL connected. Blink slowly: DSL attempting sync when trying to detect carrier signal. (2Hz with 50% duty) Blinking fast: DSL attempting sync when the carrier has been detected and the modem is trying to train. (4Hz with 50% duty) Steadily On: DSL good sync. Link established.
INTERNET	Y-Green	Steadily off: ADSL connection is not present or modem is configured in bridge mode. Blink: IP connected and IP Traffic is passing thru the device (both ways). Steadily on: PPP connection established or Static WAN IP assigned successfully. Red: Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, etc).

NOTE 1:

SPECIAL LED's STATUS WHILE THE FIRMWARE IS BEING UPGRADED:

- While is being upgraded the Firmware, all the LEDs with the exception of the Ethernet led WILL BLINK IN GREEN AT THE SAME TIME DURING THIS PROCESS (if wireless net was disabled, the WLAN LED will not blink neither).
- After finishing the process all the LEDs will come back to the standard status with a normal behaviour.
- If during the firmware upgrading process the router detect a recoverable fail (punctual fail in the uploading which it is posible to come back with no damage in the system), all the LEDs with the exception of the Ethernet led will keep on in GREEN 15 seconds to inform you about the fail produced. After this period of time, all the LEDs will come back to the normal behaviour.
- If during the firmware upgrading process the router detect an unrecoverable fail (system fail impossible to come back: for example, corrupted file, or router disconnected from the power supply while the firmware upgrading was in process), the on LED (POWER) will keep in RED. In this case it is recommended to contact with the technical assistance support.

NOTE 2:

RESET THE ROUTER TO DEFAULT PARAMETERS

If in any case you want to reset the configuration to factory default parameters, please follow bellow steps:

- Put a paper clip or a pen in the hole back called "RESET".
- Keep pressing internal button more than 10 seconds.
- Stop pressing the internal button "RESET".
- Then, the router will be restarted.
- This process takes 20 seconds. Check LEDs behaviour comparing with figure of section "3.4. Indicators" to be sure the Reset process was finalized successfully.

4. Software Configuration

User can change settings via PC's WEB browser. The following sections describe the set up procedures. After successful setting, when you power on the AW4062 Router, it will boot up and connect to ADSL line automatically. The Router can provide PVC (Permanent Virtual Channel) 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
  - 8/32 for PPPoE
  - 8/36 for PPPoE with Imagnio service
- ADSL Line mode: Auto-detect.

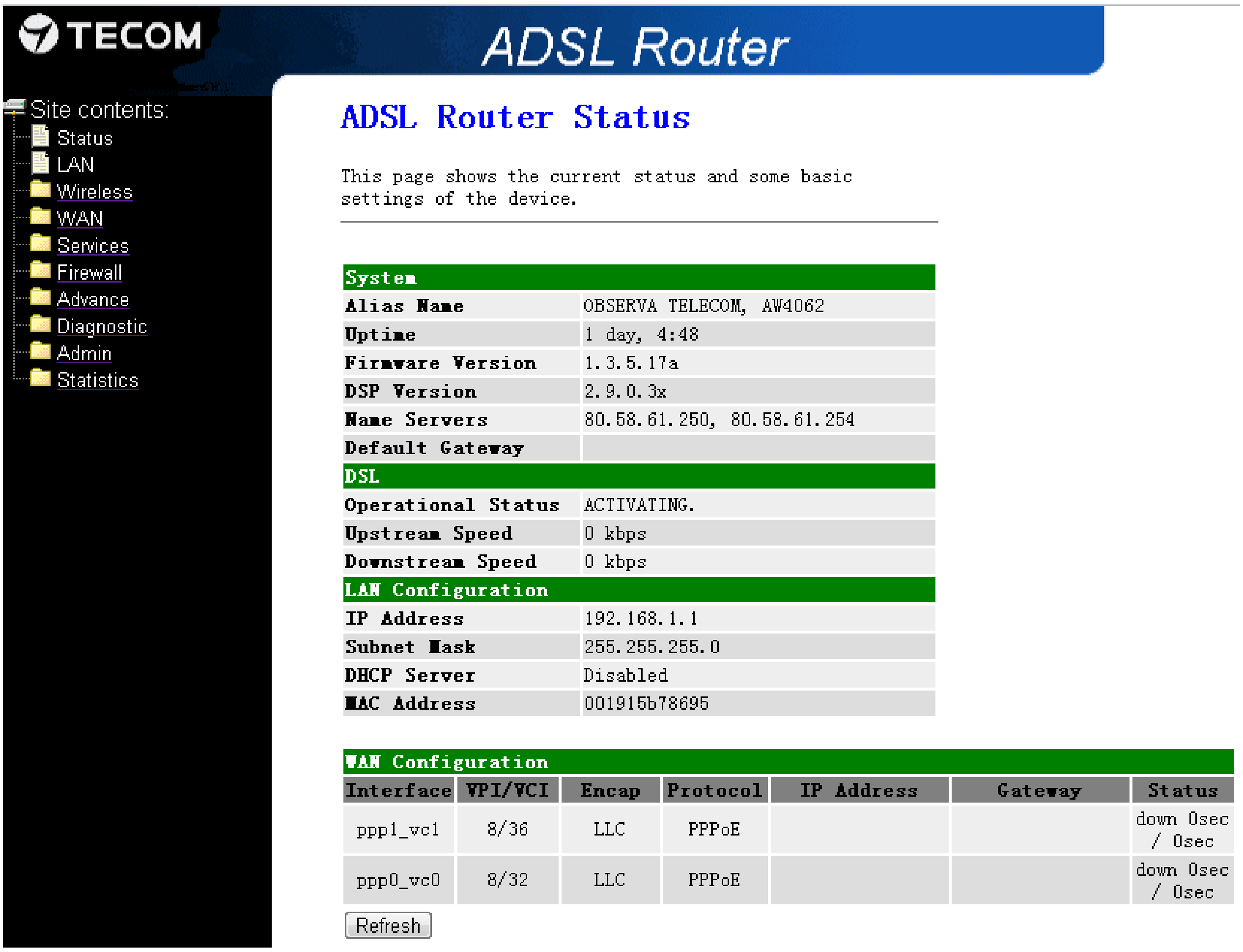
4.1. Set your PC's Ethernet port

AW4062 is an ADSL Router which support DHCP and default enable. You also can set your computer IP Address as **192.168.1.x** within the same subnet as AW4062 (default IP address is **192.168.1.1**) and netmask (default netmask is **255.255.255.0**). It can be done thru the following way.

1. Click start > Control Panel
2. In the Control Panel, double-click Network Connections
3. Right-click Local Area Connection the click Properties
4. Select Internet Protocol (TCP/IP) then click Properties
5. The TCP/IP Properties windows appear. You can select obtain an IP address automatically and click OK to have the AW4062 assign your computer an IP address. Or you can enter the IP within the same subnet as AW4062.
6. If your Internet Service Provider (ISP) gave you Domain Name System (DNS) settings, enter them in the Use the following DNS server addresses fields. If you are not sure of your DNS setting, contact your ISP.
7. Click OK to finish the setting.

4.2. Access the Web Page of Router

- 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 as follows:
  Username / Password: 1234 / 1234
- Once you have connected to ADSL router. You will see the status page.



ADSL Router Status

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

System	
Alias Name	OBSERVA TELECOM, AW4062
Uptime	1 day, 4:48
Firmware Version	1.3.5.17a
DSP Version	2.9.0.3x
Name Servers	80.58.61.250, 80.58.61.254
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	Disabled
MAC Address	001915b78695

WAN Configuration

Interface	VPI/VCI	Encap	Protocol	IP Address	Gateway	Status
ppp1_vc1	8/36	LLC	PPPoE			down 0sec / 0sec
ppp0_vc0	8/32	LLC	PPPoE			down 0sec / 0sec

This page displays the AW4062 Router 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

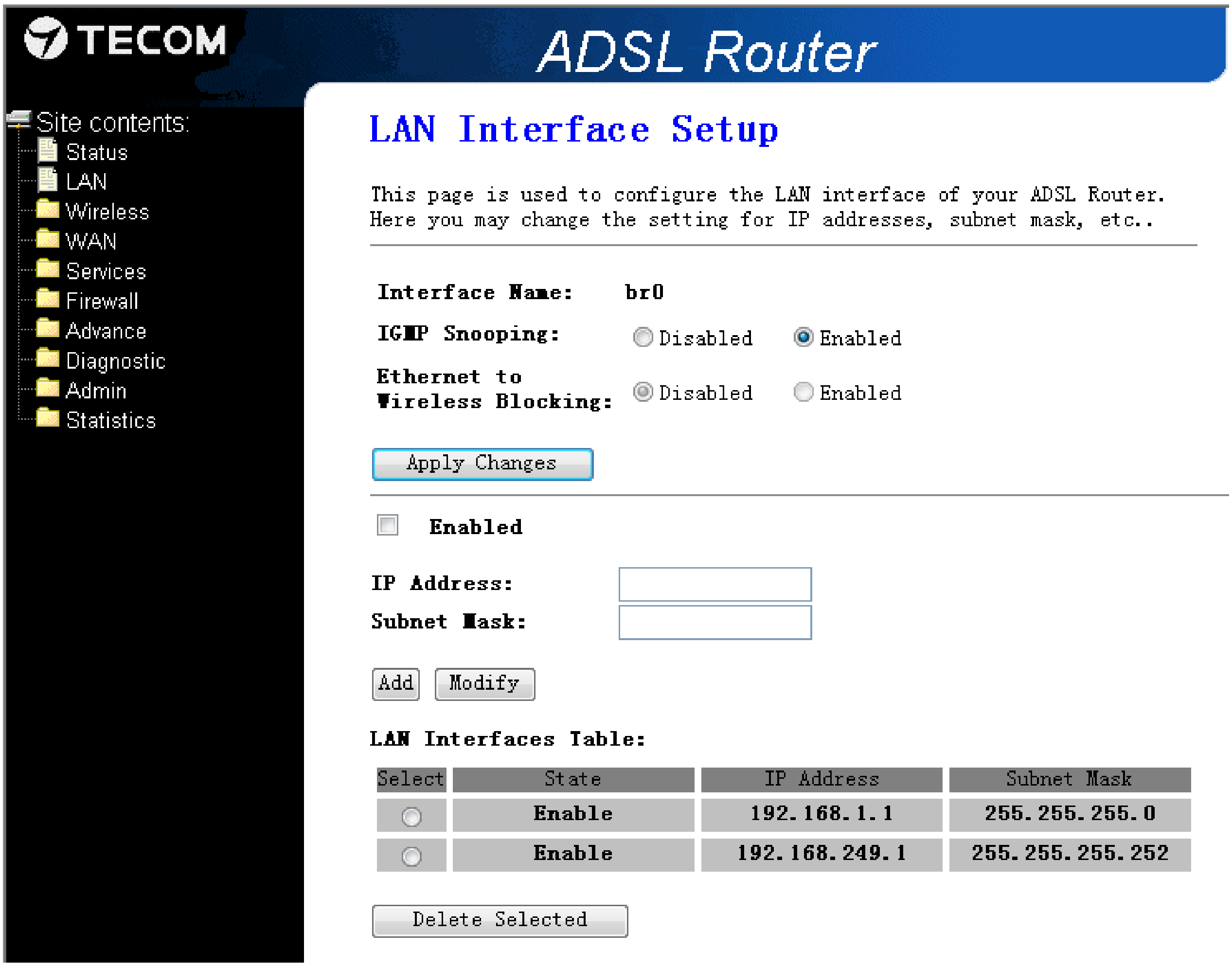
<u>Function buttons in this page:</u>

Refresh

Click Refresh button to update the status.

4.3. LAN Configuration

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



LAN Interface Setup

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

Interface Name: br0

IGMP Snooping: ○ Disabled ● Enabled

Ethernet to Wireless Blocking: ● Disabled ○ Enabled

□ Enabled

IP Address:

Subnet Mask:

LAN Interfaces Table:

Select	State	IP Address	Subnet Mask
○	Enable	192.168.1.1	255.255.255.0
○	Enable	192.168.249.1	255.255.255.252

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.

Function buttons in this page:

Add

Click to add a new LAN settings, new settings will tack effect after save into flash memory and no need to restart the system.

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.

Delete Selected

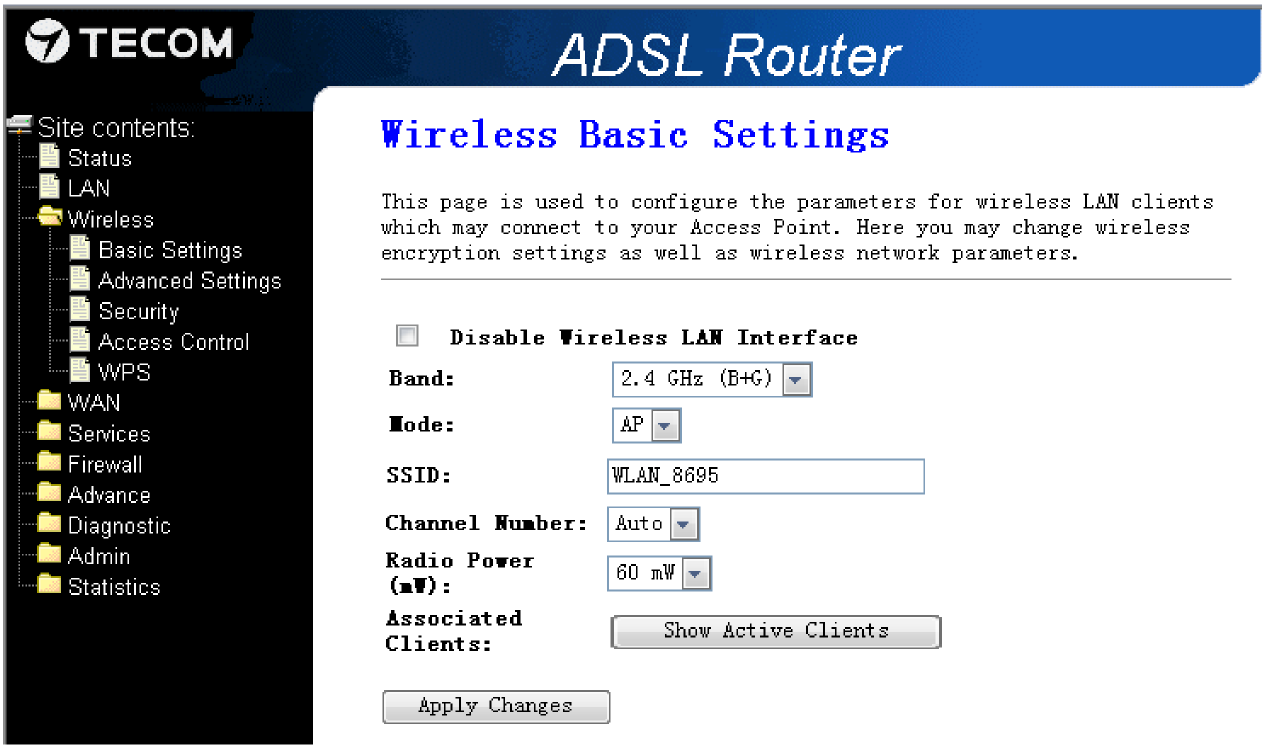
Select one LAN configuration and click to delete this setting.

4.4. Wireless Configuration

There are five sub-menus for Wireless configuration: [Basic Settings], [Advance Settings], [Security], [Access Control] and [WPS].

4.4.1. Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Please refer to the section – **Basic settings** for details.



Wireless Basic Settings

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

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

SSID: WLAN_8695

Channel Number: Auto

Radio Power (mW): 60 mW

Associated Clients: Show Active Clients

Apply Changes

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	**Access Point**—The gateway communicates with both clients and bridges.
SSID	Enter a name for your wireless network here. SSID stands for Service Set Identifier.
Channel Number	Drop-down menu that allows selection of specific channel.
Radio Power	The maximum output power: 15mW, 30mW or 60mW.

Function buttons in this page:

Associated Clients

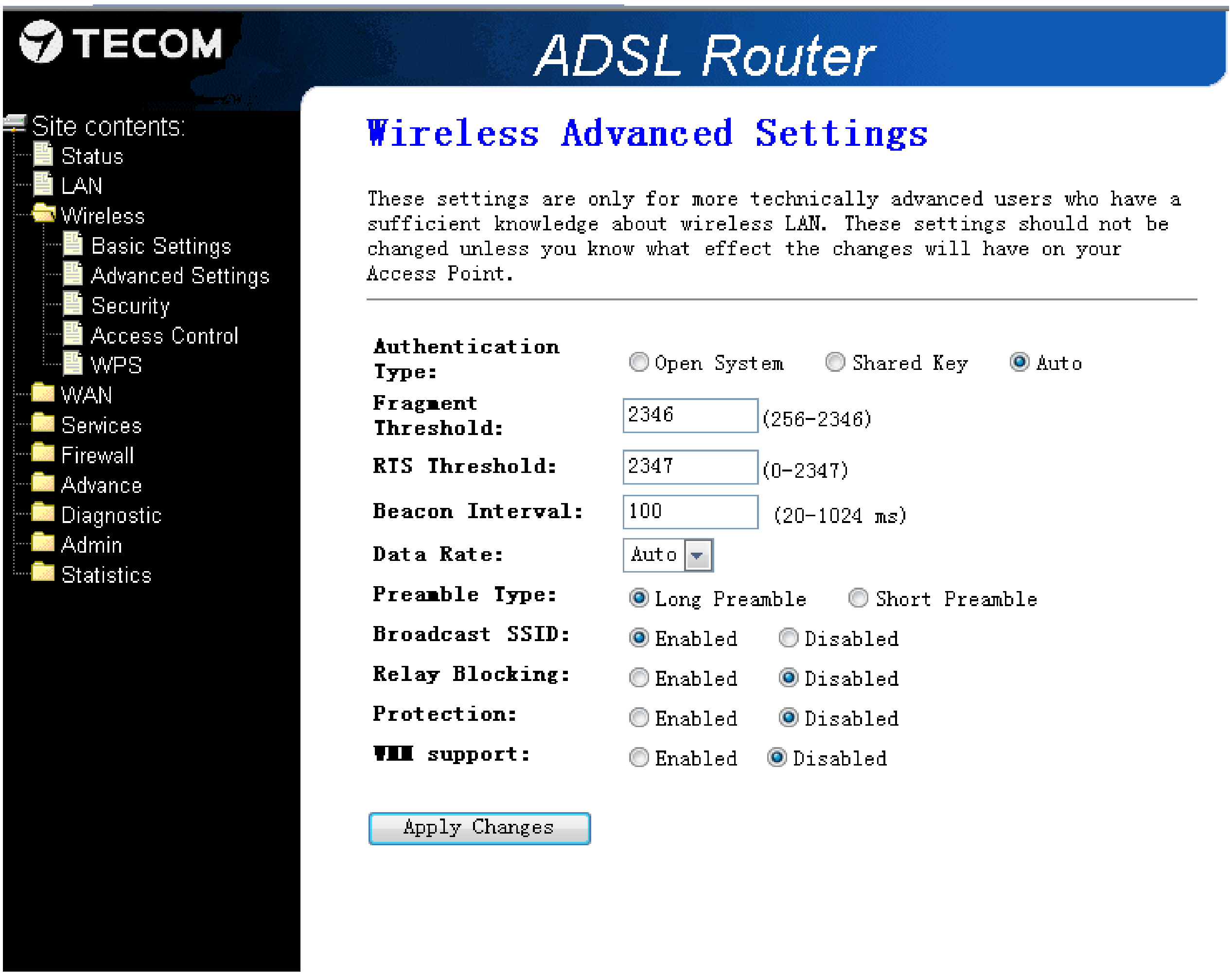
Click it will show the clients currently associated with the ADSL modem.

Apply Changes

Change the settings. New parameters will take effect after save into flash memory and reboot the system

4.4.2. 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. Please refer to the section – **Advance settings** for details.



Wireless Advanced Settings

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

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

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.
VMM support	WMM is a QoS solution with industry-wide support that offers strong interoperability, meets the requirements of all market segments, and has global reach. It is available now and will be interoperable with 802.11e. The Wi-Fi Alliance has launched a WMM certification program that establishes a solid foundation for the growth of the Wi-Fi multimedia market, and that facilitates the development of interoperable devices and applications with QoS capabilities. At the same time, WMM greatly improves the enduser experience and enables a wider, more efficient use of Wi-Fi networks everywhere.

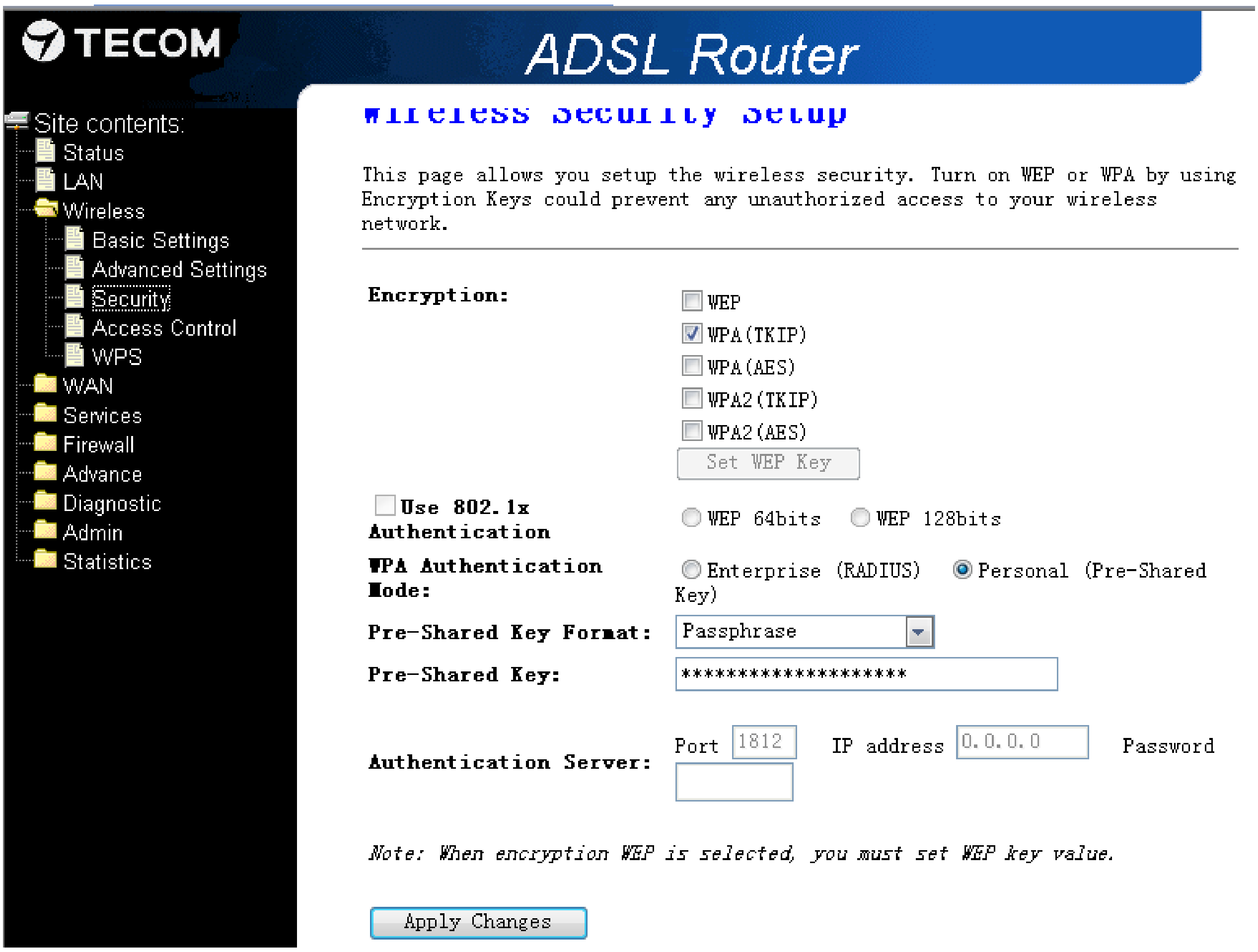
Function buttons in this page:

Apply Changes

Click to commit changes.

4.4.3. 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. Please refer to the section – **Security** for details.



Wireless Security Setup

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: ☐ WEP ☑ WPA(TKIP) ☐ WPA(AES) ☐ WPA2(TKIP) ☐ WPA2(AES)

☐ **Use 802.1x Authentication** ○ WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ********************

Authentication Server: Port 1812 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

Fields in this page:

Field	Description
Encryption	There are 5 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. **WPA(AES):** WPA uses Advanced Encryption Standard (AES) for data encryption, AES is hardware driven and it's better than TKIP **WPA2 (TKIP):** WPA2 was released and replaces WPA, but is not compatible with older routers and wireless cards. Uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP is software driven. **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. **Note**: The AP also can support WPA+WPA2, TKIP+AES for data encryption. The

	actual selection of the encryption methods will depend on the clients, but we **recommends** WPA2 with AES as the most advanced security protection available
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, he 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.

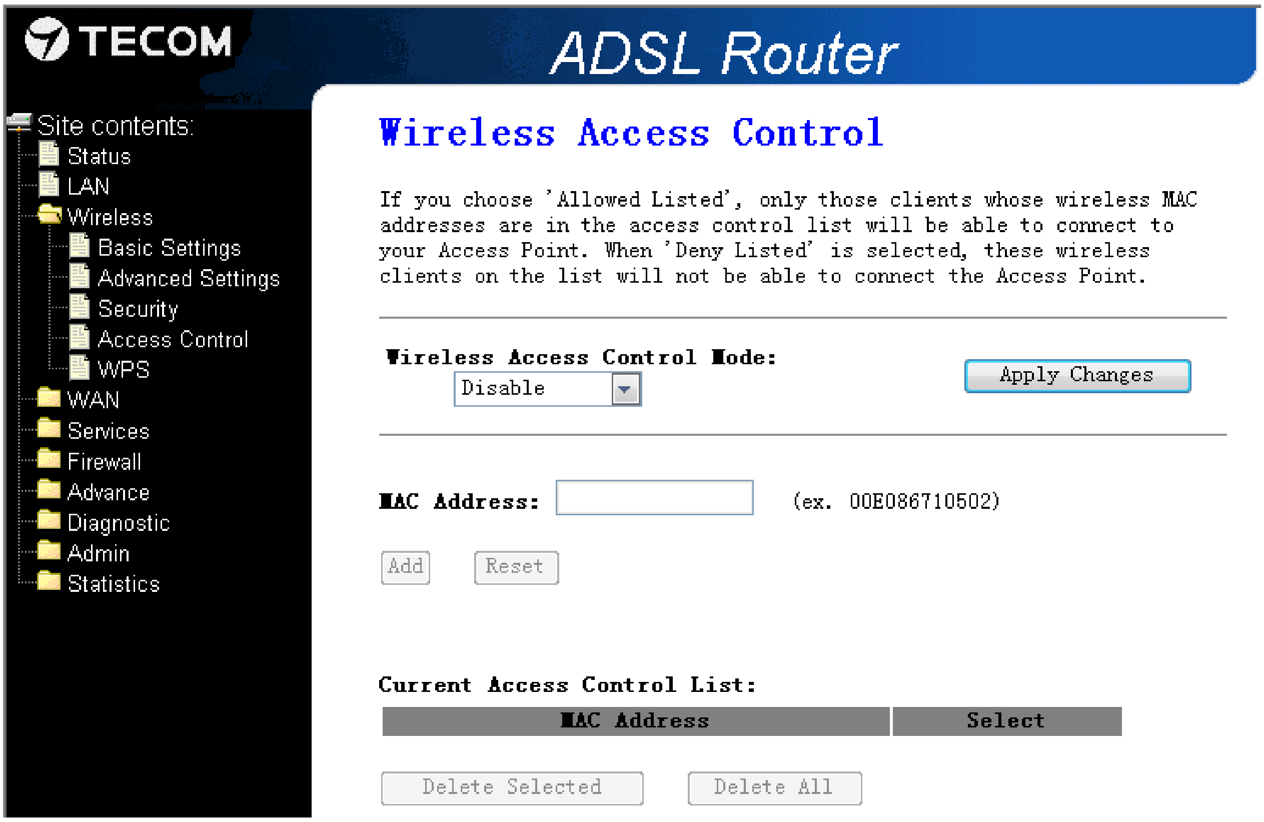
<u>Function buttons in this page:</u>

Apply Changes

Click to commit changes.

4.4.4. 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). Please refer to the section – **Access control** for details.



Wireless Access Control

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

Wireless Access Control Mode: Disable

MAC Address: (ex. 00E086710502)

Current Access Control List:

MAC Address	Select

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 in this page:

Apply Changes

Click to commit changes.

Add

Click to add this entry into the **Current Access Control List**.

Reset

It restores the original values

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

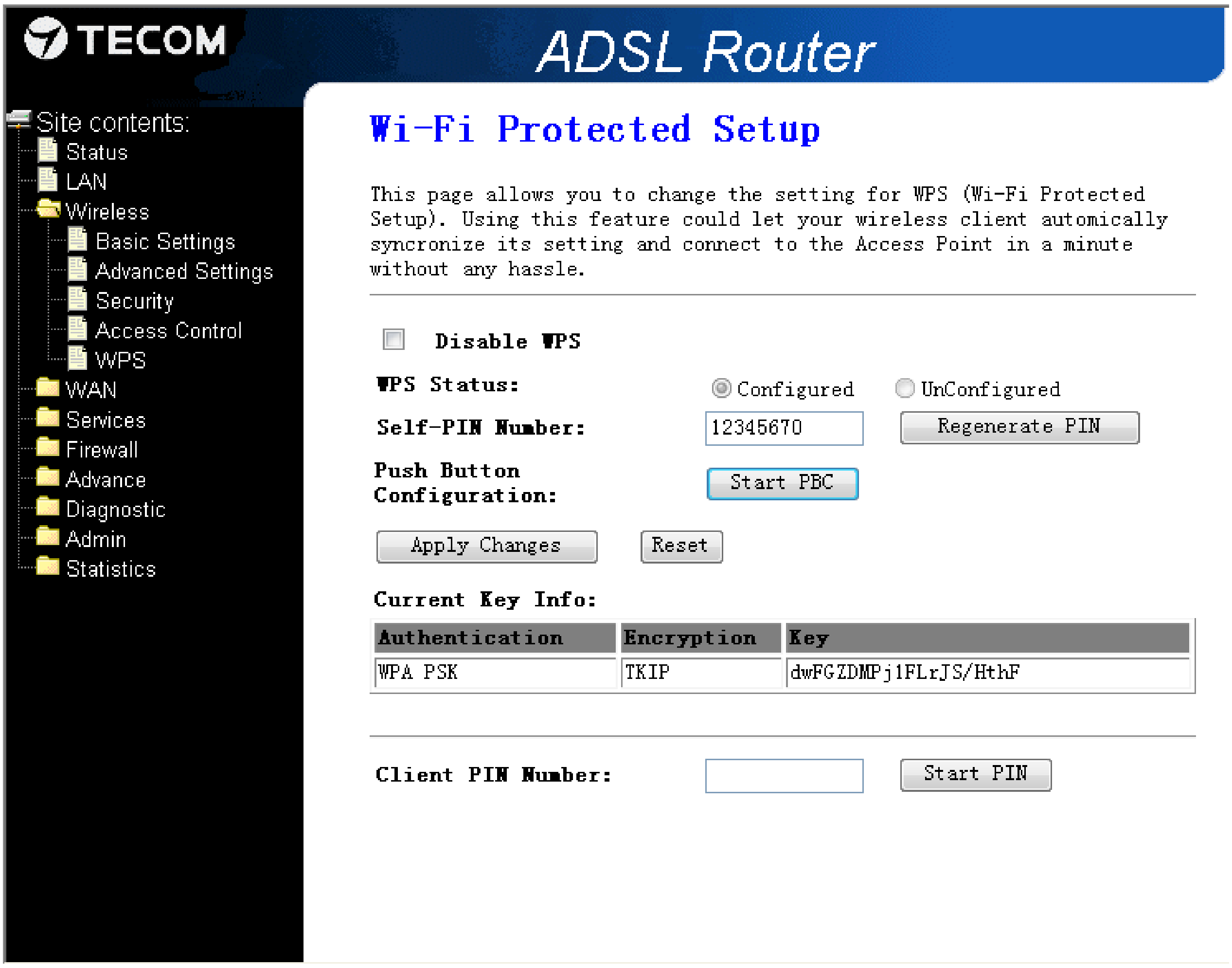
Flush the list.

4.4.5. WPS

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, The Wi-Fi Protected Setup (WPS) is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 8).

The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network.

This device supports Push Button method and PIN method for WPS. The following sub-paragraphs will describe the function of each item. The webpage is as below.



Wi-Fi Protected Setup

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

□ **Disable WPS**

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 12345670 [Regenerate PIN]

Push Button Configuration: [Start PBC]

[Apply Changes] [Reset]

Current Key Info:

Authentication	Encryption	Key
WPA PSK	TKIP	dwFGZDMPj1FLrJS/HthF

Client PIN Number: [Start PIN]

Fields in this page:

Field	Description
Disable WPS	Check to disable the Wi-Fi protected Setup.
WPS Status	When AP's settings are factory default (out of box), it is set to open security and un-configured state. "WPS Status" will display it as "UnConfigured". If it already shows "Configured", some registrars such as Vista WCN will not configure AP. Users will need to go to the "Backup/Restore" page and click "Reset" to reload factory default settings.
Self-PIN Number	"Self-PIN Number" is AP's PIN. Whenever users want to change AP's PIN, they could click "Regenerate PIN" and then click " Apply Changes". Moreover, if users want to make their own PIN, they could enter four-digit PIN without checksum and then click " Apply Changes". However, this would not be recommended since the registrar side needs to be supported with four-digit PIN.
Push Button Configuration	Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.
Client PIN Number	It is only used when users want their station to join AP's network. The length of PIN is limited to four or eight numeric digits. If users enter eight-digit PIN with

	checksum error, there will be a warning message popping up. If users insist on this PIN, AP will take it.

Function buttons in this page:

Regenerate PIN

Click to regenerate the Self-PIN Number.

Start PBC

Click to start the Push Button method of WPS.

Apply Changes

Click to commit changes.

Reset

It restores the original values.

Start PIN

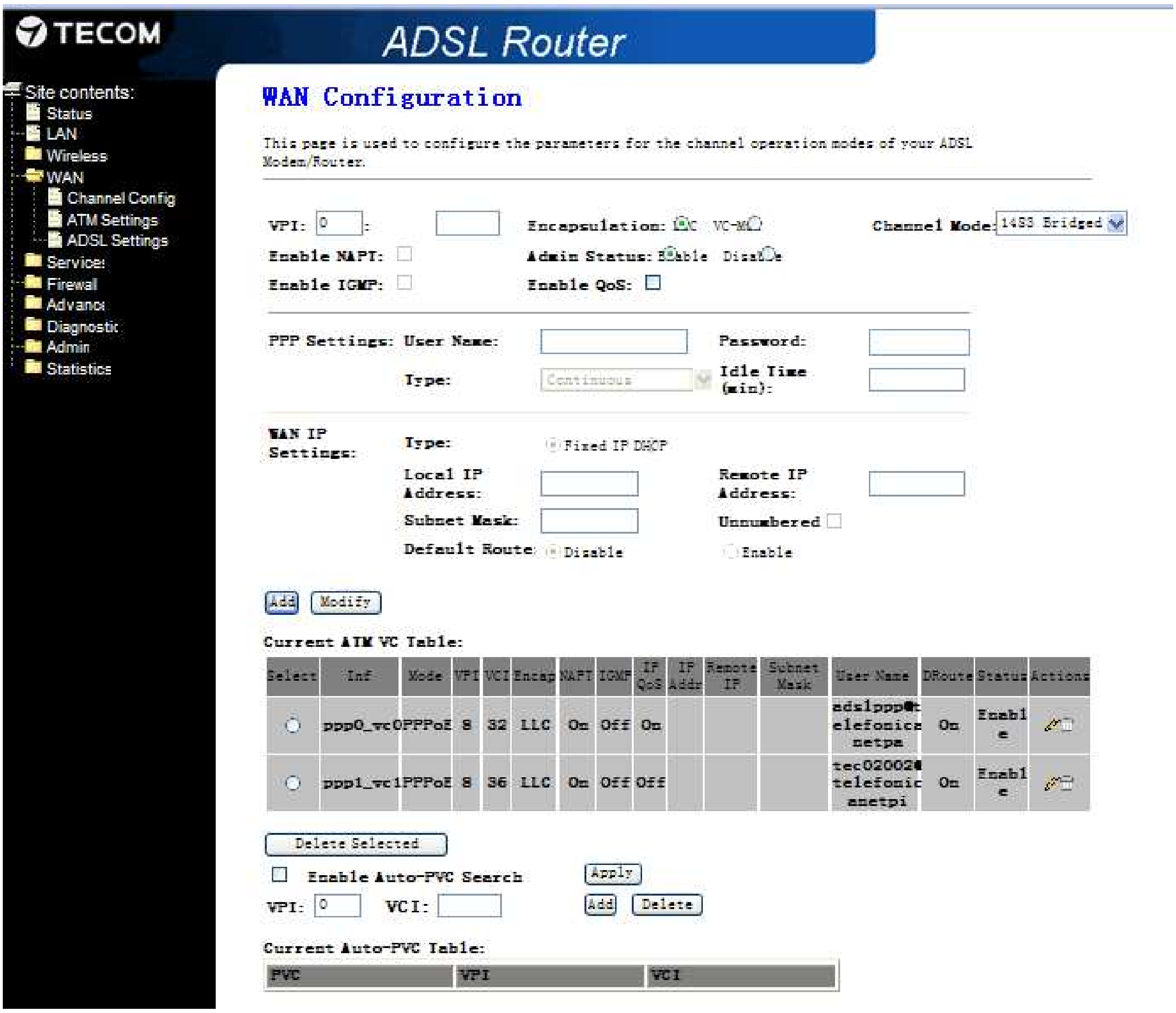
Click to start the PIN method of WPS.

4.5. WAN Configuration

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

4.5.1. 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 refer to the section – **Channel Mode Configuration** for details.



WAN Configuration

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

VPI: 0 :
Encapsulation: ● LLC ○ VC-Mux
Channel Mode: 1483 Bridged
Enable NAPT: □
Admin Status: ● Enable ○ Disable
Enable IGMP: □
Enable QoS: □

PPP Settings: User Name: Password:
Type: Continuous Idle Time (min):

WAN IP Settings: Type: ● Fixed IP ○ DHCP
Local IP Address: Remote IP Address:
Subnet Mask: Unnumbered □
Default Route: ● Disable ○ Enable

Add Modify

Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IGMP	IP QoS	IP Addr	Remote IP	Subnet Mask	User Name	DRoute	Status	Actions
○	ppp0_vc0	PPPoE	8	32	LLC	On	Off	On				adslppp@telefonicanetpa	On	Enable	
○	ppp1_vc1	PPPoE	8	36	LLC	On	Off	Off				tec02002@telefonicanetpi	On	Enable	

Delete Selected

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

Current Auto-PVC Table:

PVC	VPI	VCI

Function buttons in this page:

Add

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

Modify

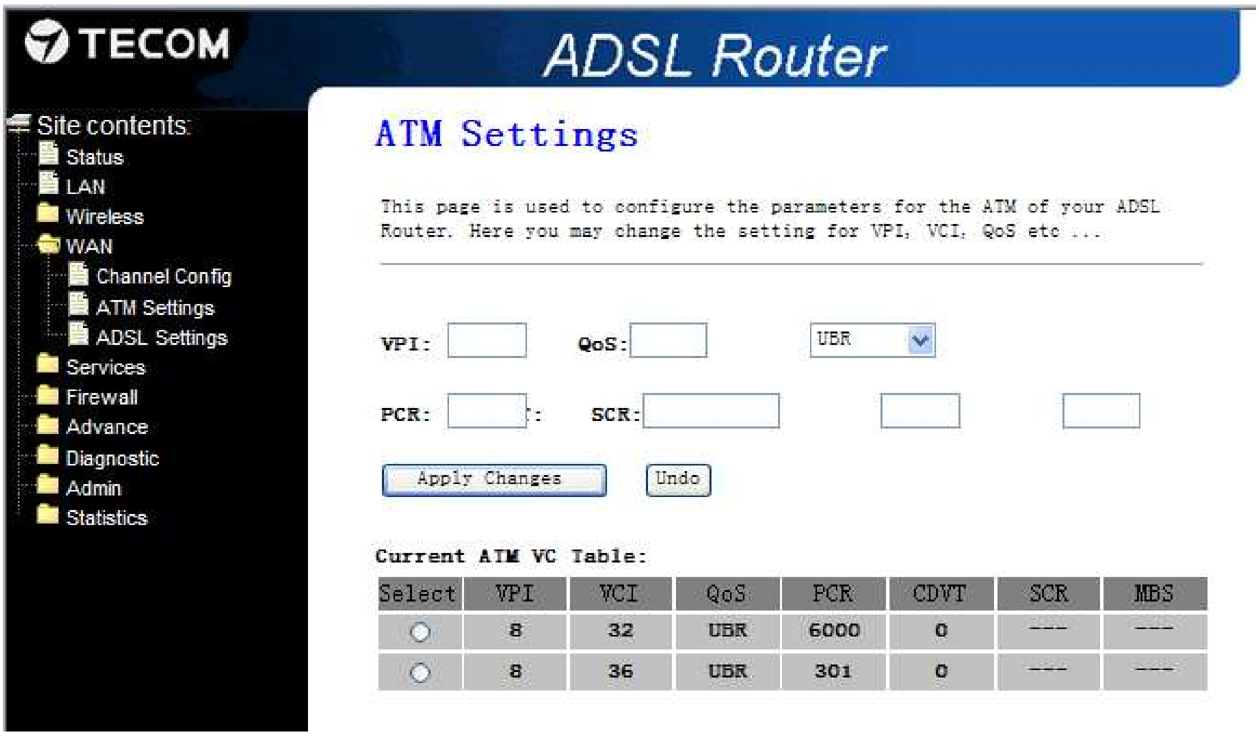
Select an existing PVC channel by clicking the radio button at the **Select** column of the **Current ATM VC Table** before we can modify the PVC channel. After selecting a PVC channel, we can modify the channel configuration at this page. Click **Modify** to complete the channel modification and apply 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.

4.5.2. ATM Setting

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



ATM Settings

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

VPI: QoS: UBR

PCR: : SCR:

Current ATM VC Table:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
○	8	32	UBR	6000	0	---	---
○	8	36	UBR	301	0	---	---

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

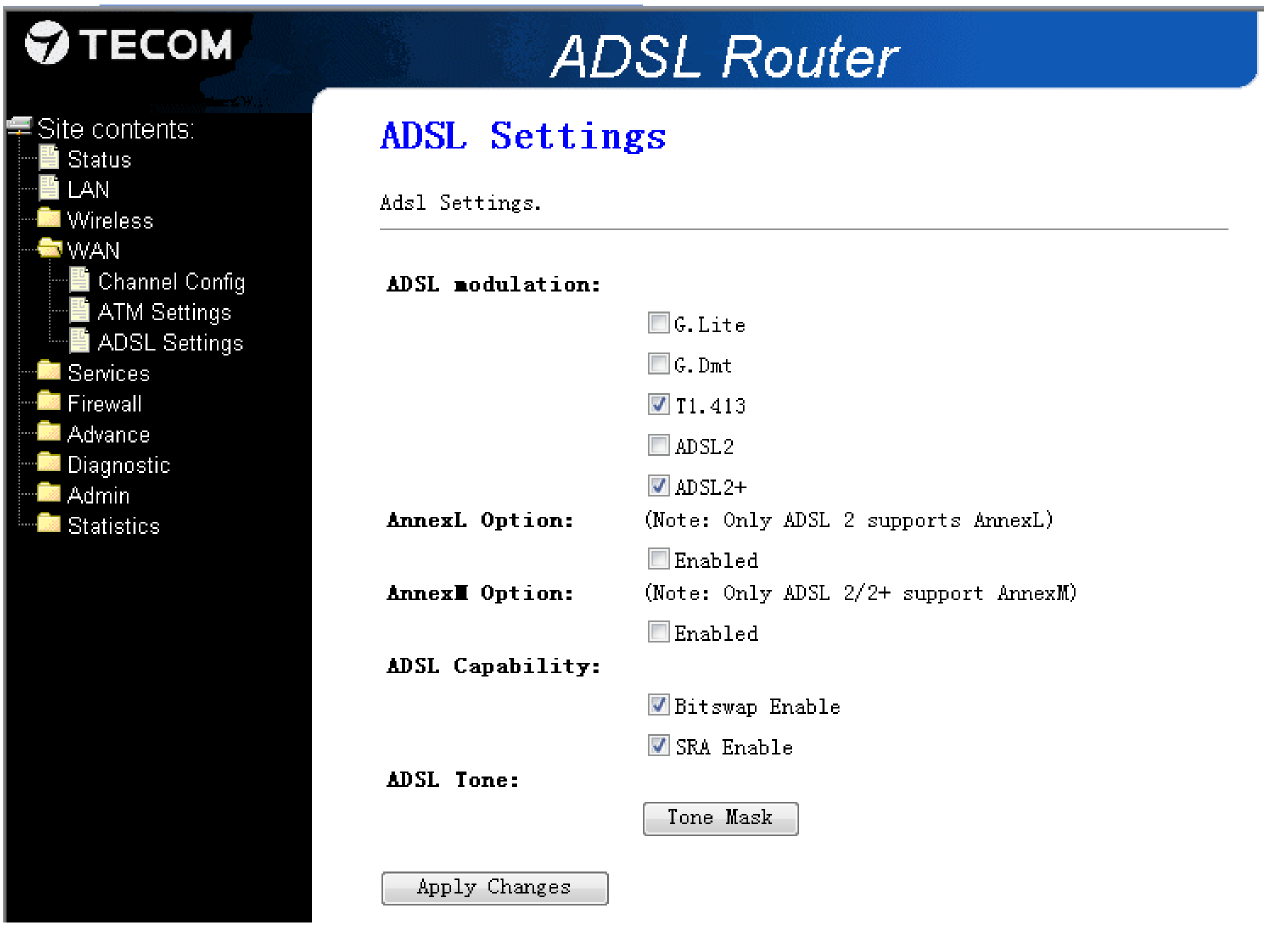
Set new PVC QoS mode for the selected PVC. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

Undo

Discard your settings.

4.5.3. ADSL Setting

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



ADSL Settings

Adsl Settings.

ADSL modulation:

□ G.Lite

□ G.Dmt

☑ T1.413

□ ADSL2

☑ ADSL2+

AnnexL Option: (Note: Only ADSL 2 supports AnnexL)

□ Enabled

AnnexM Option: (Note: Only ADSL 2/2+ support AnnexM)

□ Enabled

ADSL Capability:

☑ Bitswap Enable

☑ SRA Enable

ADSL Tone:

Fields in this page:

Field	**Description**
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	"Bit-swap Enable" : Enable/Disable bit-swap capability. "SRA Enable" : Enable/Disable SRA (seamless rate adaptation) capability.

Function buttons in this page:

Tone Mask

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

Apply Changes

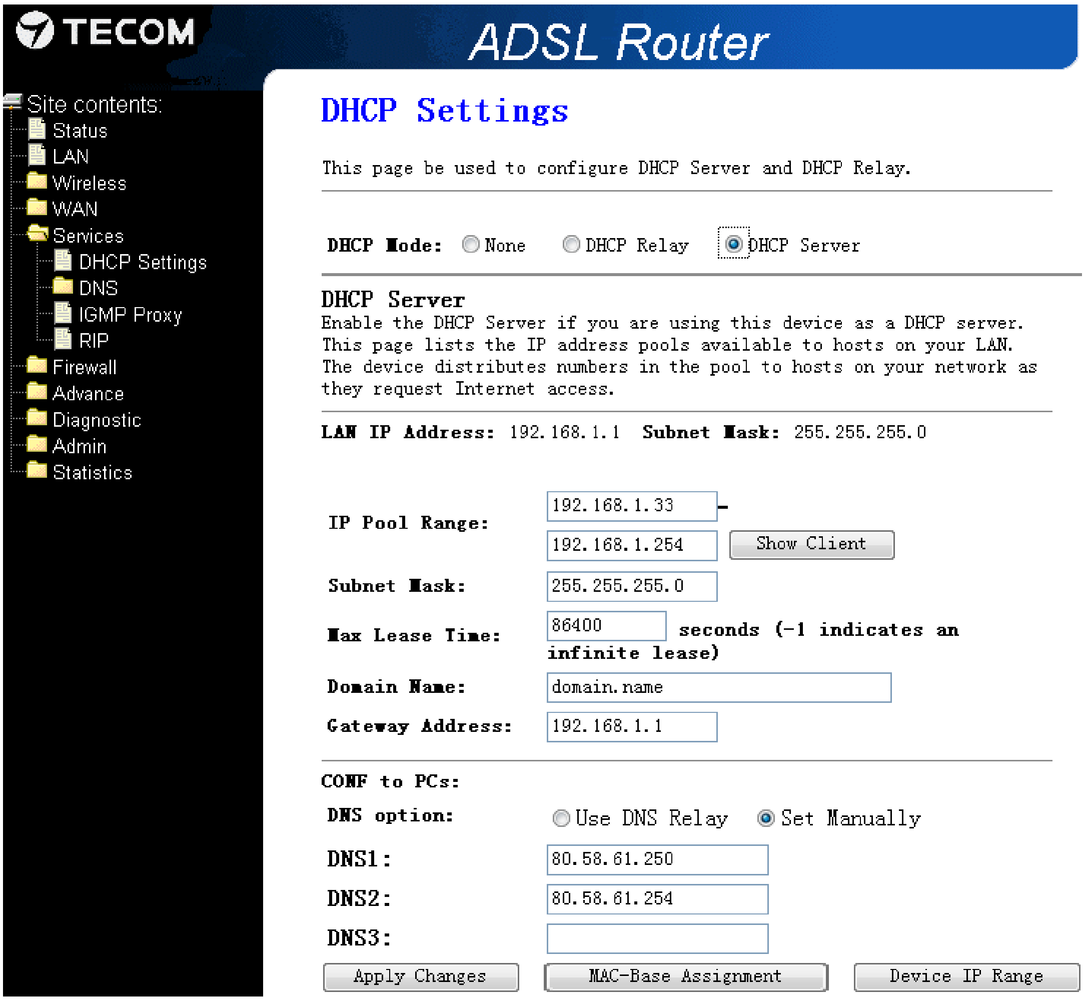
Click to save the setting to the configuration and the modem will be retrained.

4.6. Services Configuration

There are four sub-menus for Services: [DHCP Settings], [DNS], [IGMP Proxy] and [RIP].

4.6.1. DHCP Settings

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 Serve 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.



DHCP Settings

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

DHCP Mode: ○ None ○ DHCP Relay ● DHCP Server

DHCP Server

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

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

IP Pool Range: 192.168.1.33 - 192.168.1.254

Subnet Mask: 255.255.255.0

Max Lease Time: 86400 seconds (-1 indicates an infinite lease)

Domain Name: domain.name

Gateway Address: 192.168.1.1

CONF to PCs:

DNS option: ○ Use DNS Relay ● Set Manually

DNS1: 80.58.61.250

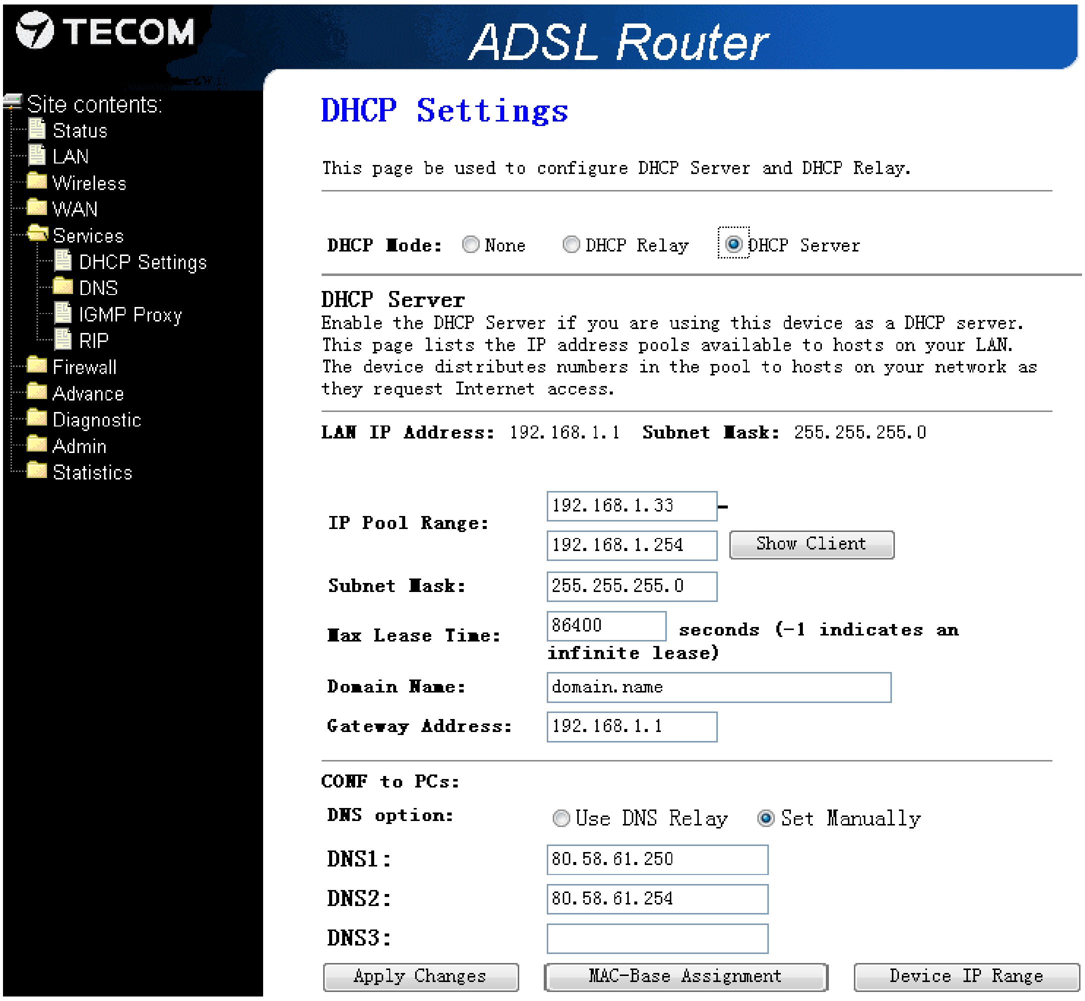
DNS2: 80.58.61.254

DNS3:

4.6.1.1. DHCP Server Configuration

By default, the device is configured as a DHCP server, with a predefined IP address pool of 192.168.1.33 through 192.168.1.254 (subnet mask 255.255.255.0).

4.6.1.2. Basic Settings



DHCP Settings

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

DHCP Mode: ○ None ○ DHCP Relay ● DHCP Server

DHCP Server

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

LAN IP Address: 192.168.1.1 **Subnet Mask:** 255.255.255.0

IP Pool Range: 192.168.1.33 - 192.168.1.254 [Show Client]

Subnet Mask: 255.255.255.0

Max Lease Time: 86400 **seconds (-1 indicates an infinite lease)**

Domain Name: domain.name

Gateway Address: 192.168.1.1

CONF to PCs:

DNS option: ○ Use DNS Relay ● Set Manually

DNS1: 80.58.61.250

DNS2: 80.58.61.254

DNS3:

[Apply Changes] [MAC-Base Assignment] [Device IP Range]

<u>Fields in this page:</u>

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.

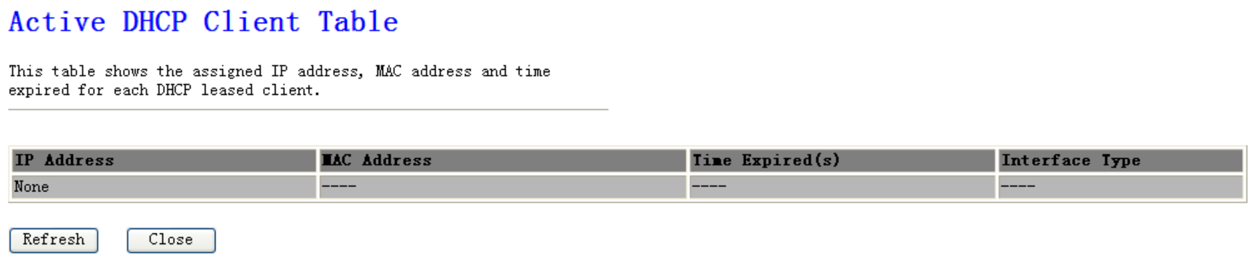
<u>Function buttons in this page:</u>

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.

4.6.1.3. Show Client

User can find the DHCP client which get IP from the device from **"Active DHCP Client Table"** page, to check those information please click the **"Show Client"** button on the **Basic Settings** page, then the "Active DHCP Client Table" page" will show.



Active DHCP Client Table

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

IP Address	MAC Address	Time Expired(s)	Interface Type
None	----	----	----

<u>Function buttons in this page:</u>

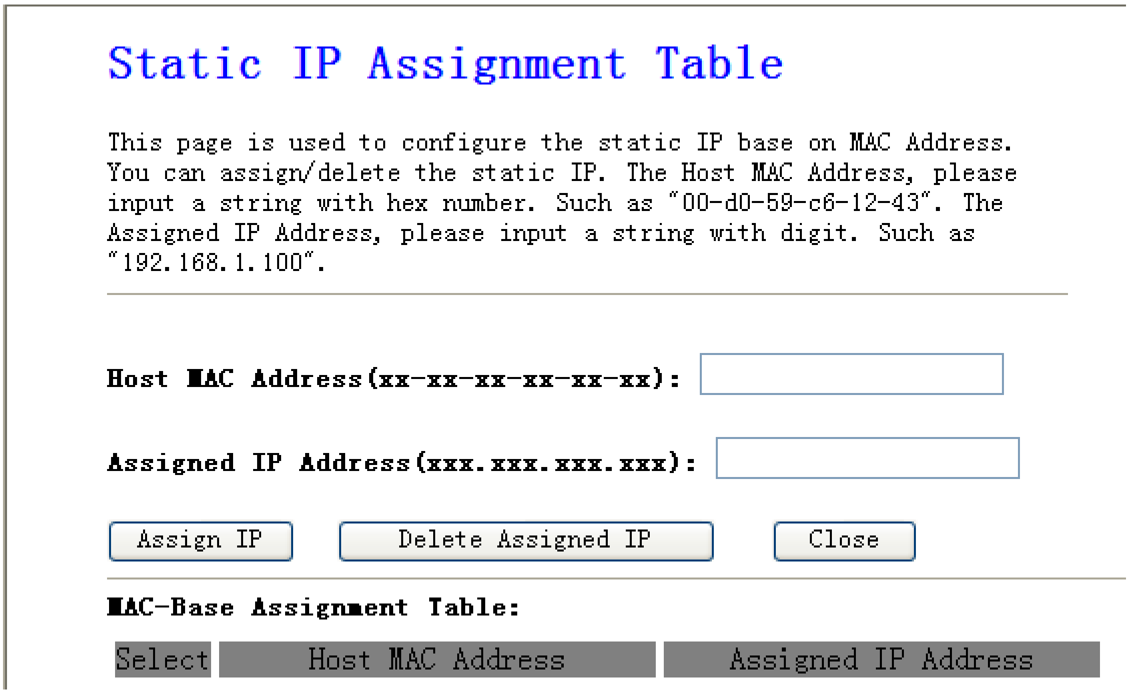
Refresh

Click to refresh this table to get the updating information for DHCP clients.

Close

Click to close the current page.

4.6.1.4. MAC-Based Assignment



Static IP Assignment Table

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

Host MAC Address(xx-xx-xx-xx-xx-xx):

Assigned IP Address(xxx.xxx.xxx.xxx):

MAC-Base Assignment Table:

Select	Host MAC Address	Assigned IP Address

<u>Fields in this page:</u>

Field	Description
Host MAC Address	Specify the unique identifier of a device in this field.
Assigned IP Address	Specify one IP for a given device.

Function buttons in this page:

Assign IP

Assign an IP to a specifically Device . New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

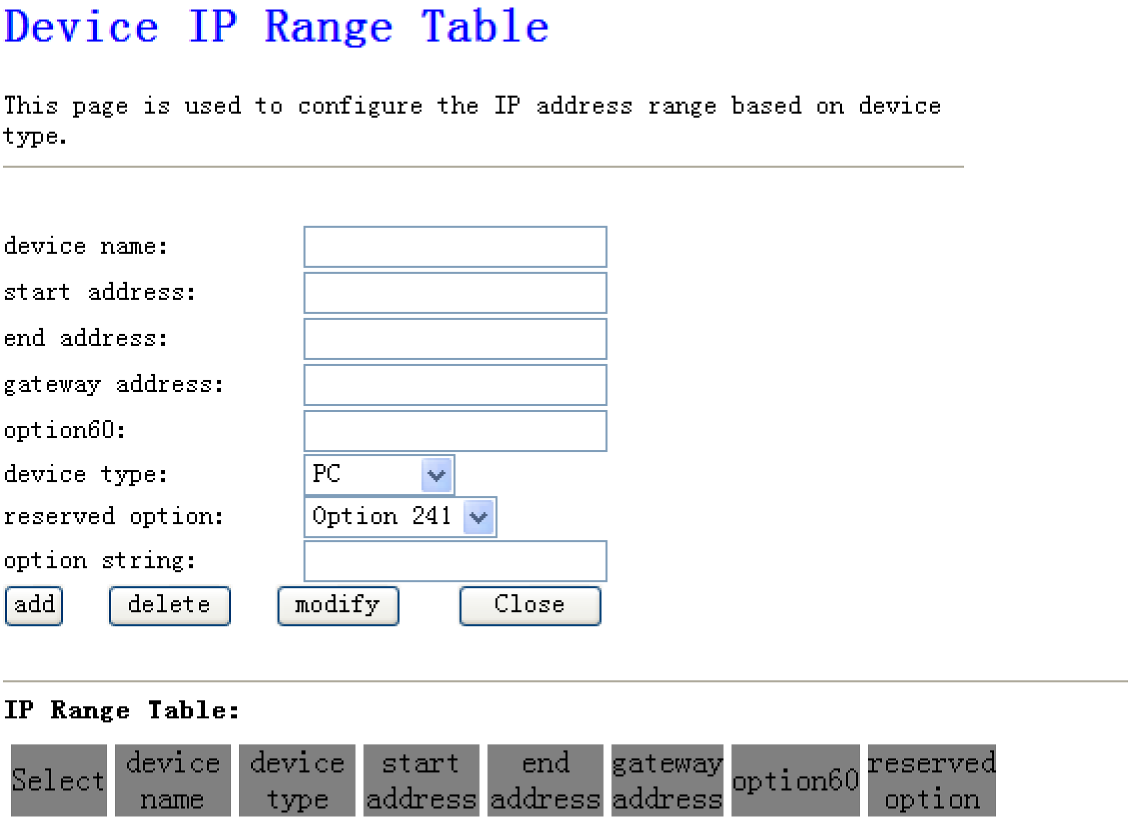
Delete Assigned IP

Delete selected Assigned IP from the MAC-base Assignment table. You can click the checkbox at the **Select** column to select the filtering rule.

Closed

Close this configuration page.

4.6.1.5. Device IP Range



Device IP Range Table

This page is used to configure the IP address range based on device type.

device name:	
start address:	
end address:	
gateway address:	
option60:	
device type:	PC
reserved option:	Option 241
option string:	

IP Range Table:

Select	device name	device type	start address	end address	gateway address	option60	reserved option

Fields in this page:

Field	Description
Option 60	To identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters or octets which has a meaning specified by the vendor of the DHCP client. One method that a DHCP client can utilize to communicate to the server that it is using a certain type of hardware or firmware is

	to set a value in its DHCP requests called the Vendor Class Identifier
Device type	User can define the client type such as PC, Camera, HGW, STB, Phone and Unknow device.
Reserved Option	It includes Option 241, 242, 243, 244, 245, which will be used to send information to the DHCP client.

Function buttons in this page:

Add

Click to save the rule entry to the configuration.

Delete

Delete selected setting from the IP range table. You can click the checkbox at the **Select** column to select the filtering rule.

Modify

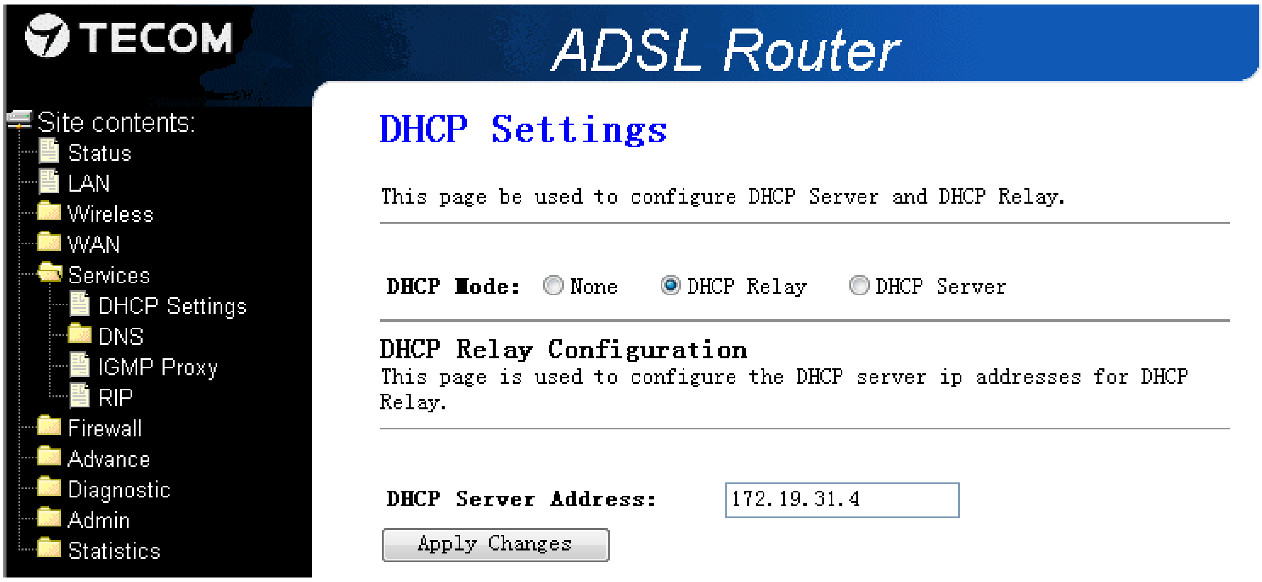
Change selected setting from the IP range table. You can click the checkbox at the **Select** column to select the filtering rule.

Closed

Close this configuration page.

4.6.1.6. 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.



DHCP Settings

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

DHCP Mode: ○ None ● DHCP Relay ○ DHCP Server

DHCP Relay Configuration

This page is used to configure the DHCP server ip addresses for DHCP Relay.

DHCP Server Address: 172.19.31.4

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

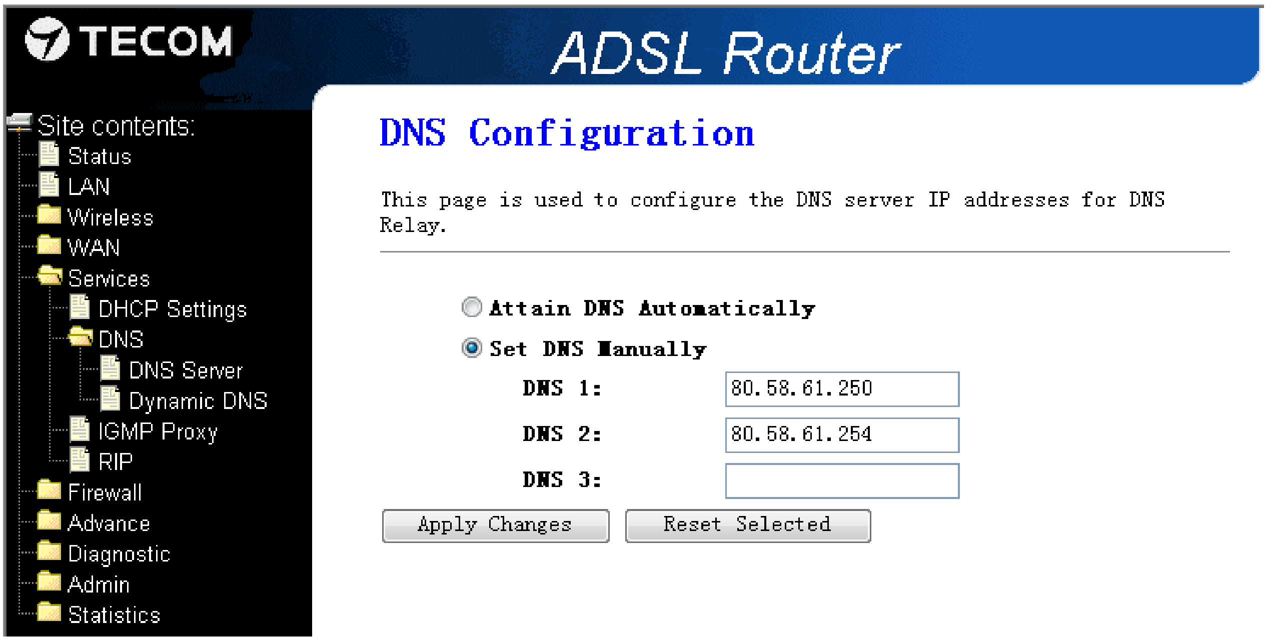
Click to save the setting to the configuration.

4.6.2. DNS Configuration

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.



DNS Configuration

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

○ Attain DNS Automatically

● Set DNS Manually

DNS 1: 80.58.61.250

DNS 2: 80.58.61.254

DNS 3:

Fields in this page:

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

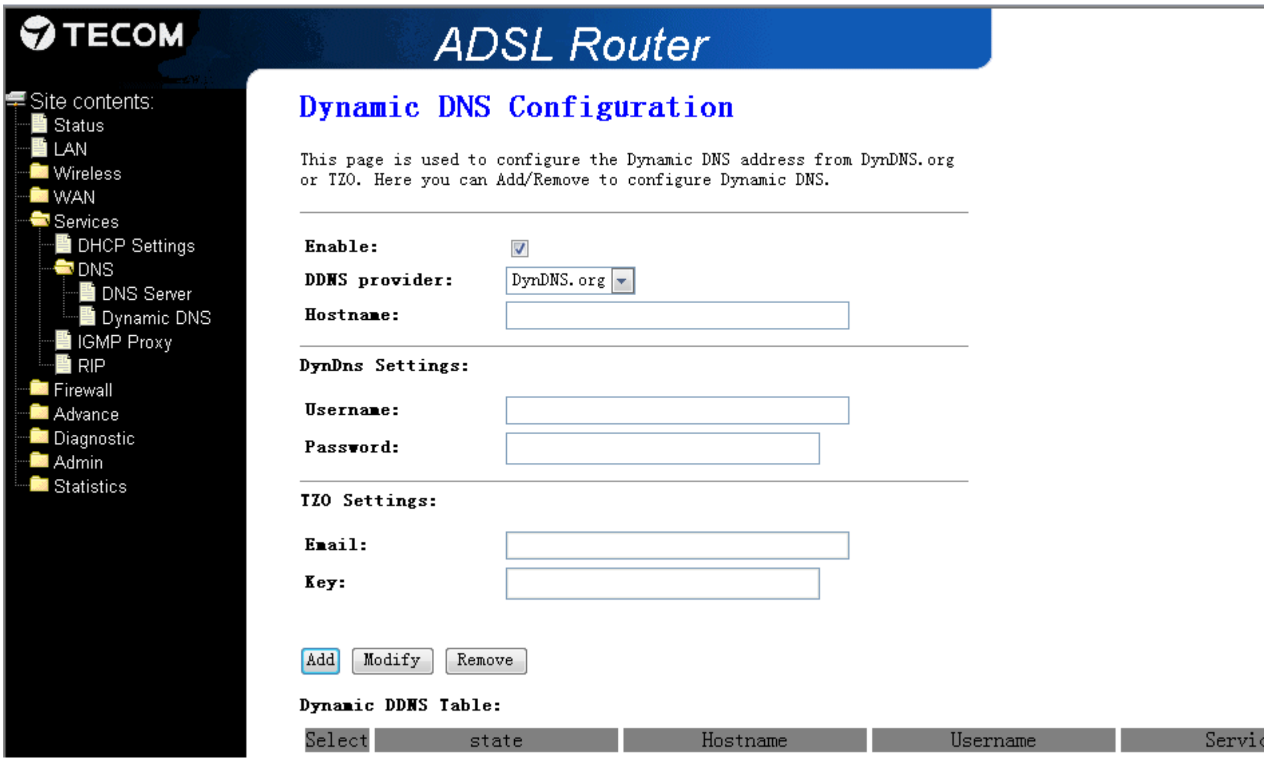
Set new DNS relay configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

Reset Selected

Discard your changes.

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.



Dynamic DNS Configuration

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

Enable:	☑
DDNS provider:	DynDNS.org
Hostname:	

DynDns Settings:

Username:	
Password:	

TZO Settings:

Email:	
Key:	

Dynamic DDNS Table:

Select	state	Hostname	Username	Servi

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 occur 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.

Modify

Select an entry in **Dynamic DNS Table**. Press "Modify" after change to apply settings.

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.

4.6.3. IGMP Proxy Configuration

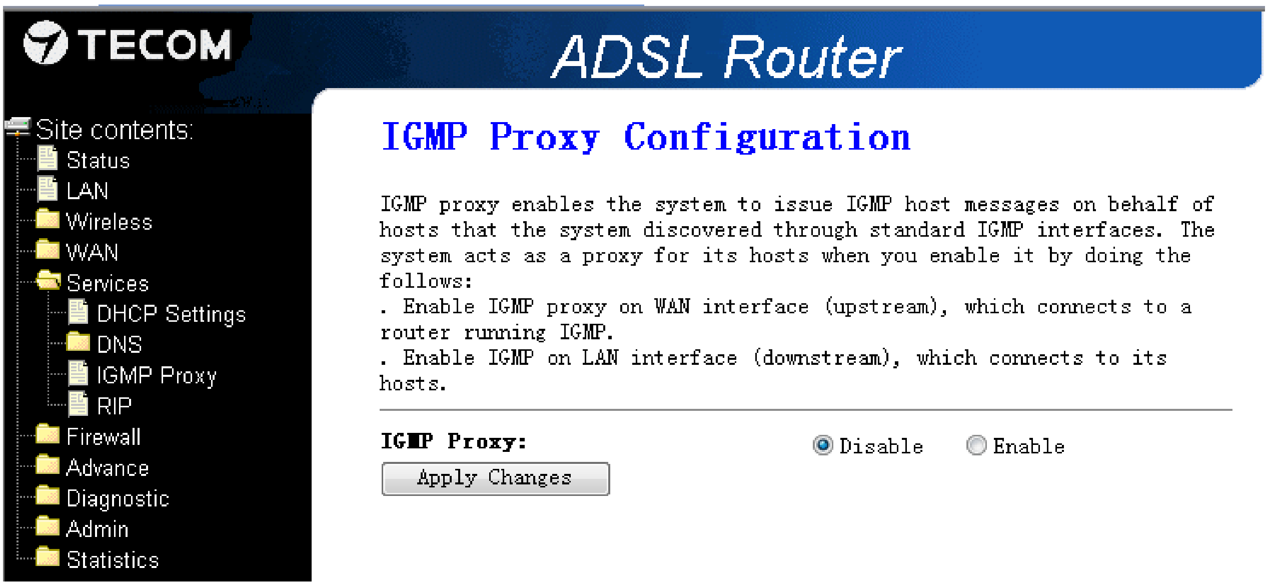
Multicasting is useful when the same data needs to be sent to more than one hosts. Using multicasting as opposed to sending the same data to the individual hosts uses less network bandwidth. The multicast feature also enables you to receive multicast video stream from multicast servers.

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 is sent to the multicast router. User can specify IGMP Proxy Upstream interface in the "WAN->Channel Config" page.
- Downstream: The interface data from the multicast router are sent to hosts in the multicast group database.



IGMP Proxy Configuration

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

IGMP Proxy: ● Disable ○ Enable

Fields in this page:

Field	Description
IGMP Proxy	Enable/disable IGMP proxy feature

Function buttons in this page:

Apply Changes

Click to save the setting to the configuration.

Undo

Discard your settings.

4.6.4. 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.

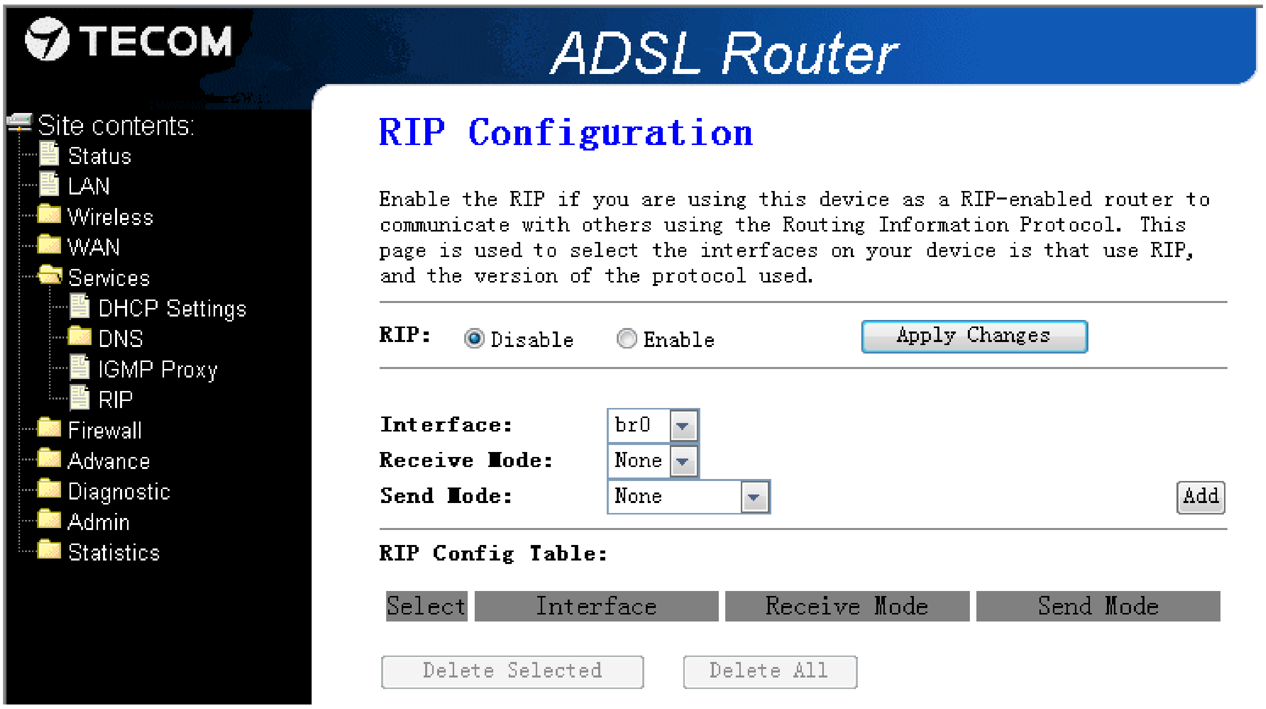
Most small home or office networks do not need to use RIP; they have only one router, such as the ADSL Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

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.



RIP Configuration

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

RIP: ● Disable ○ Enable

Interface: br0

Receive Mode: None

Send Mode: None

RIP Config Table:

Select	Interface	Receive Mode	Send Mode

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

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

Delete all

Delete all RIP entries on the RIP Configuration Table.

4.7. Firewall

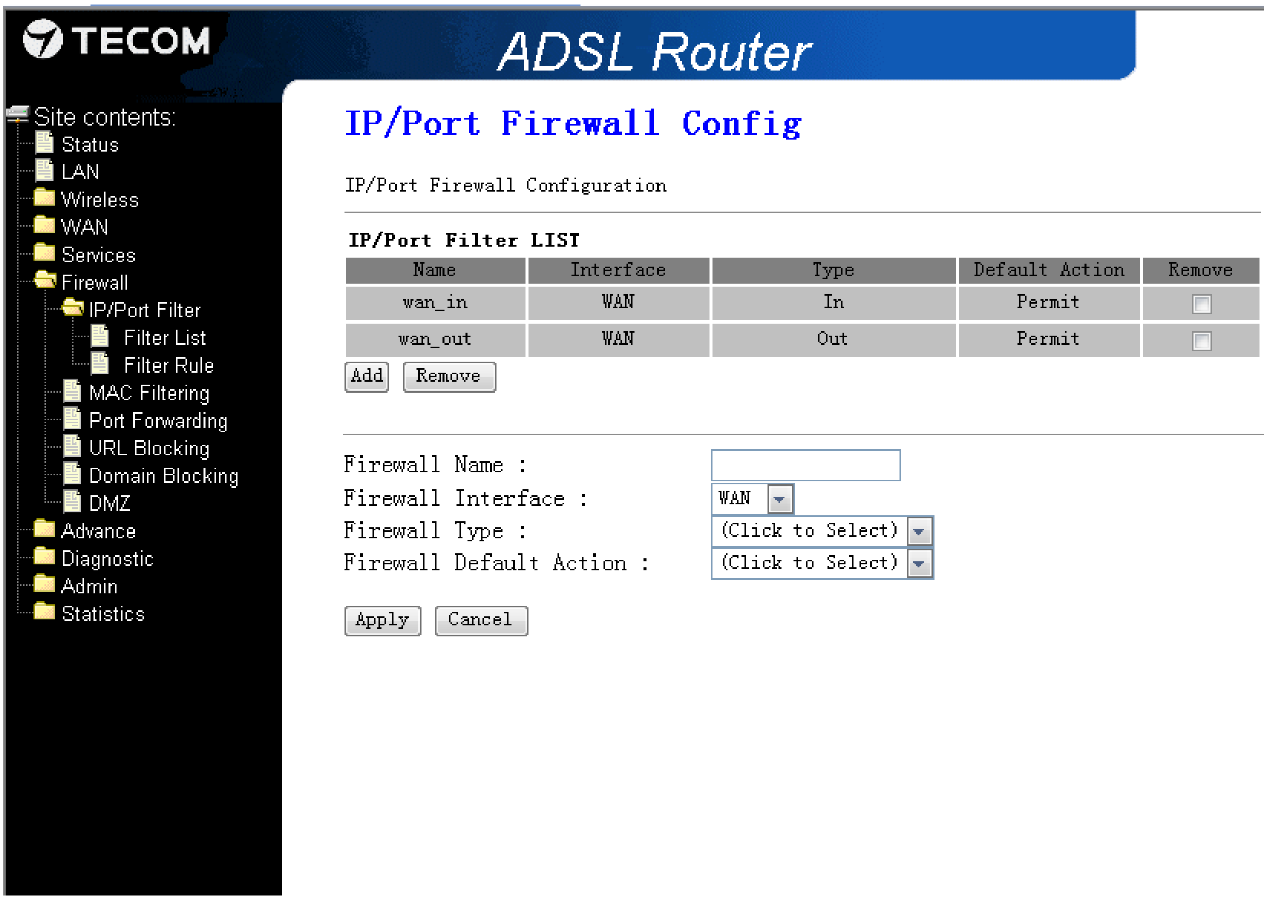
Firewall contains several features that are used to deny or allow traffic from passing through the device.

4.7.1. IP/Port Filter

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

4.7.1.1. Filter List

The Filter List feature allows you to set the IP/Port Firewall Configuration.



IP/Port Firewall Config

IP/Port Firewall Configuration

IP/Port Filter LIST

Name	Interface	Type	Default Action	Remove
wan_in	WAN	In	Permit	□
wan_out	WAN	Out	Permit	□

Add Remove

Firewall Name :
Firewall Interface : WAN
Firewall Type : (Click to Select)
Firewall Default Action : (Click to Select)

Apply Cancel

Fields in this page:

Field	Description
Firewall Name	Specify the filter name for this settings
Firewall Interface	Select the interface for this settings, user can set the interface to WAN, LAN.
Firewall Type	Specify this setting is for outgoing packets or incoming packets.
Firewall Default Action	Specify the default action for this settings, drop or permit.

Function button for this page:

Add

Click to add a new setting.

Remove

Click to delete the selected settings.

Apply

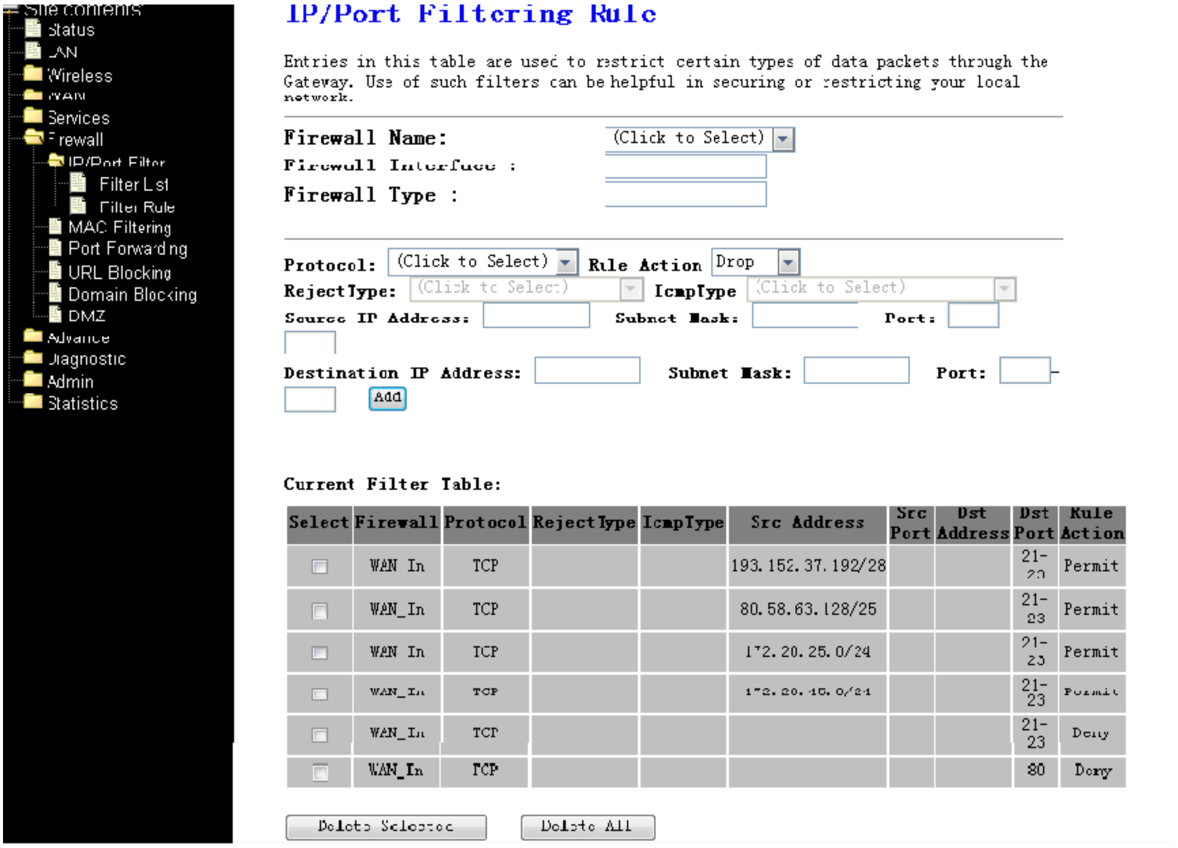
Click to save the setting of default actions to the configuration.

Cancel

Discard your settings.

4.7.1.2. Filter Rule

The Filter Rule that are used to restrict certain types of data packets through the Gateway.



IP/Port Filtering Rule

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

Firewall Name: (Click to Select)

Firewall Interface :

Firewall Type :

Protocol: (Click to Select) Rule Action Drop

RejectType: (Click to Select) IcmpType (Click to Select)

Source IP Address: Subnet Mask: Port: -

Destination IP Address: Subnet Mask: Port: -

Add

Current Filter Table:

Select	Firewall	Protocol	RejectType	IcmpType	Src Address	Src Port	Dst Address	Dst Port	Rule Action
□	WAN_In	TCP			193.152.37.192/28			21-23	Permit
□	WAN_In	TCP			80.58.63.128/25			21-23	Permit
□	WAN_In	TCP			172.20.25.0/24			21-23	Permit
□	WAN_In	TCP			172.20.45.0/24			21-23	Permit
□	WAN_In	TCP						21-23	Deny
□	WAN_In	TCP						80	Deny

Delete Selected Delete All

Fields on this page:

Field	**Description**
Firewall Name	The Firewall name is the same which you configured on the "Filter List" page. Click the comboBox to find all the settings which you set on "Filter List" page.
Protocol	There are 3 options available: TCP, UDP and ICMP.
Rule Action	There are 3 options available: Drop, Permit and Reject
Reject Type	If the **Rule Action** has been set to Reject, then this option can be set. Otherwise it will be black.
ICMP Type	If the **Protocol** has been set to **ICMP,** then this option can be set. Otherwise it will be black.
Source 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.
Destination 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 button for this page:

Add

Click to add a new setting.

Delete Selected

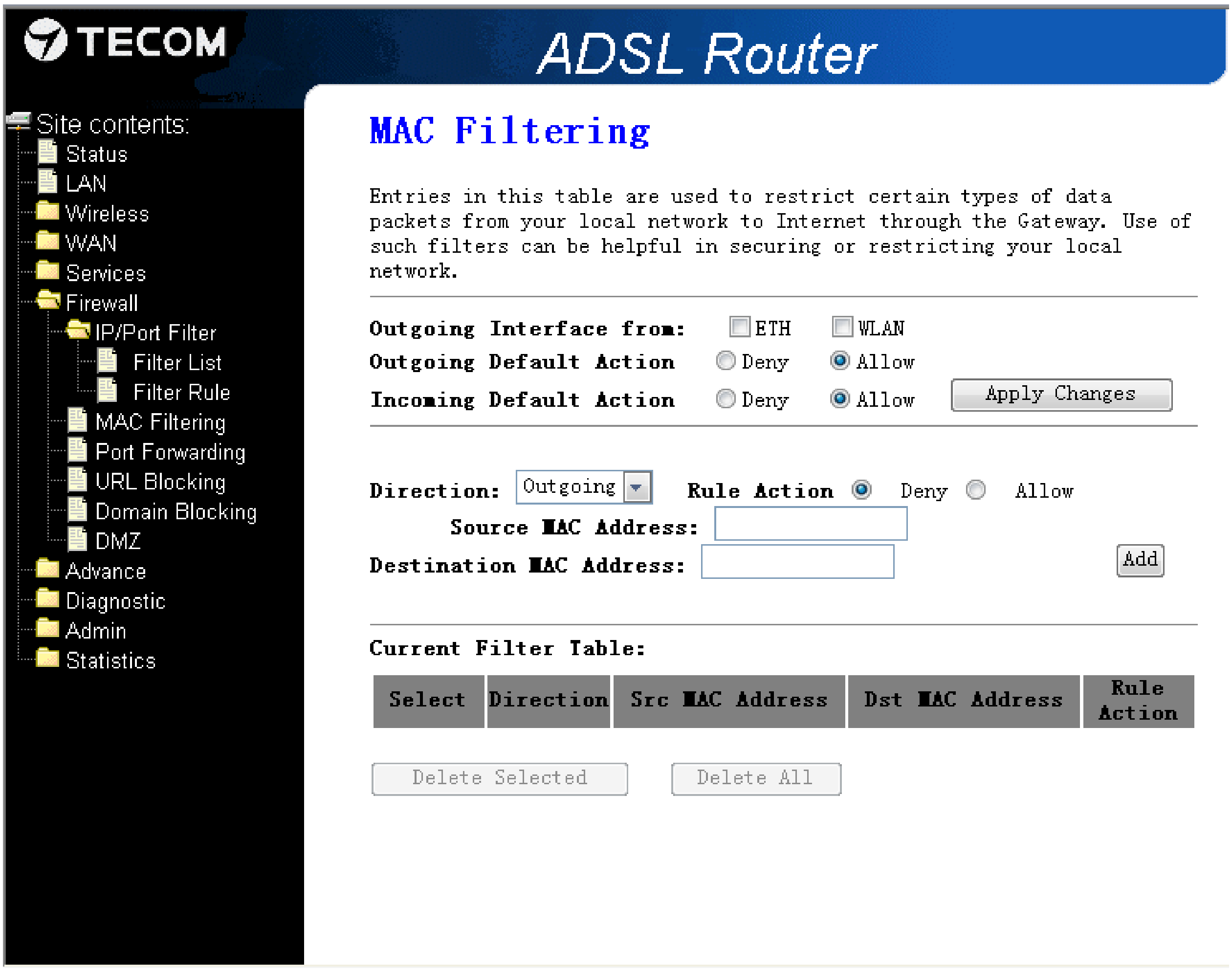
Delete a selected Filter rule in the current filter table.

Delete All

Delete all the Filter rules in the current filter table.

4.7.2. MAC Filter

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.



MAC Filtering

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

Outgoing Interface from: □ ETH □ WLAN

Outgoing Default Action ○ Deny ● Allow

Incoming Default Action ○ Deny ● Allow

Direction: Outgoing Rule Action ● Deny ○ Allow

Source MAC Address:

Destination MAC Address:

Current Filter Table:

Select	Direction	Src MAC Address	Dst MAC Address	Rule Action

Fields on the first setting block:

Field	Description
Outgoing Interface from	Select the interface to apply the filter: Ethernet (ETH) or Wifi (WLAN)

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	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.
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

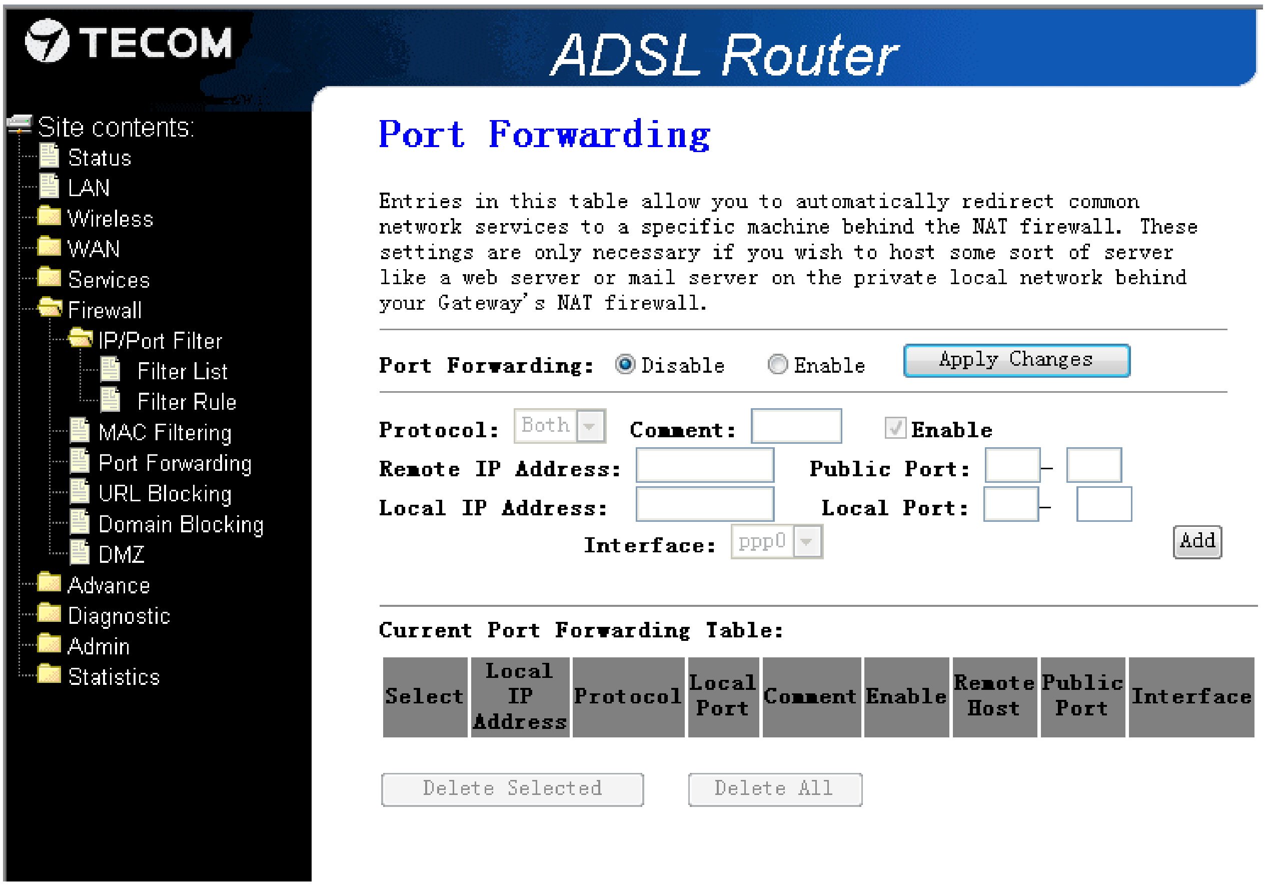
Delete selected filtering rules from the filter table. You can click the checkbox at the **Select** column to select the filtering rule.

Delete All

Delete all filtering rules from the filter table.

4.7.3. 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

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

Port Forwarding: ● Disable ○ Enable

Protocol: Both Comment: ☑ Enable

Remote IP Address: Public Port: -

Local IP Address: Local Port: -

Interface: ppp0

Current Port Forwarding Table:

Select	Local IP Address	Protocol	Local Port	Comment	Enable	Remote Host	Public Port	Interface

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.
Comment	Specify the rule name.
Enable	Check this item to enable this entry.
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
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.
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

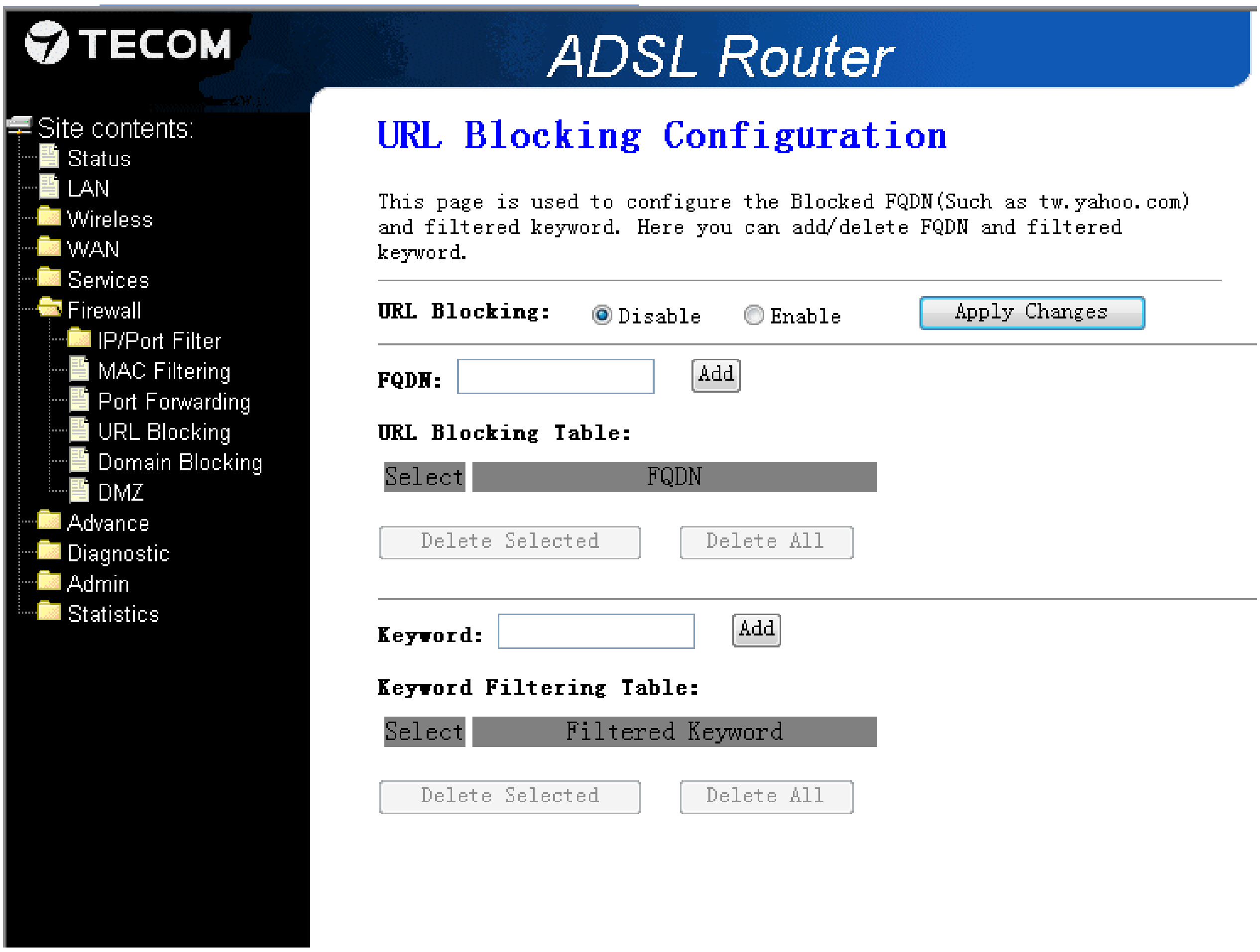
Delete the selected port forwarding rules from the forwarding table. You can click the checkbox at the **Select** column to select the forwarding rule.

Delete All

Delete all forwarding rules from the forwarding table.

4.7.4. URL Blocking

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



URL Blocking Configuration

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: ● Disable ○ Enable [Apply Changes]

FQDN: [ ] [Add]

URL Blocking Table:

Select	FQDN

[Delete Selected] [Delete All]

Keyword: [ ] [Add]

Keyword Filtering Table:

Select	Filtered Keyword

[Delete Selected] [Delete All]

Fields in this page:

Field	Description
URL Blocking	Check this item to enable the URL Blocking feature.
FQDN	A fully qualified domain name (or FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely, such as tw.yahoo.com. The FQDN will be blocked to access.
Keywords	The filtered keyword such as yahoo. If the URL includes this keyword. The URL will be blocked to access.

Function buttons in this page:

Apply Changes

Click to disable/enable the URL blocking capability.

Add FQDN

Add FQDN into URL Blocking table.

Add Keyword

Add filtered keyword into Keyword Filtering table.

Delete Selected

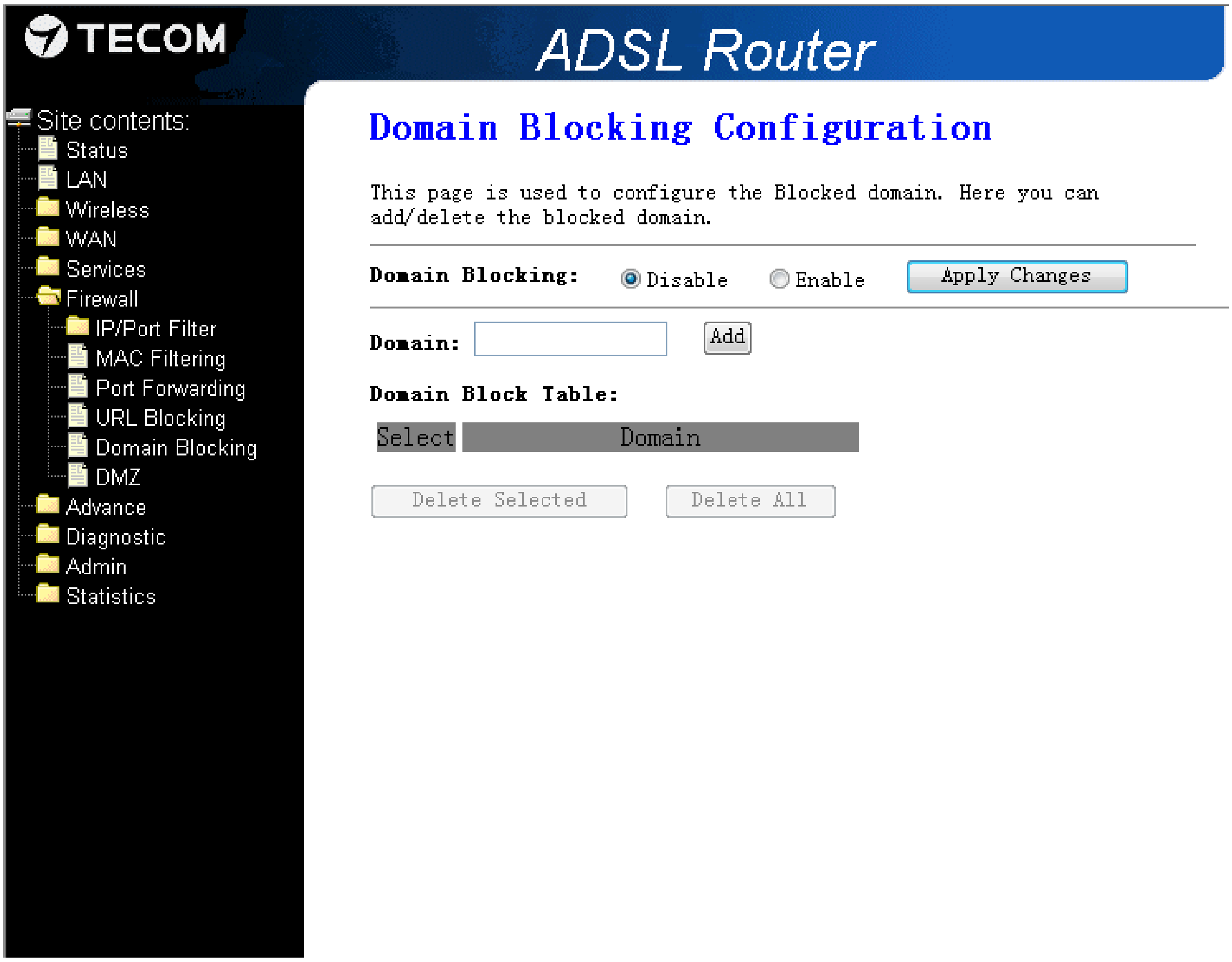
Delete the selected settings; You can click the checkbox at the **Select** column to select the current rule.

Delete All

Delete all rules from the current table.

4.7.5. Domain Blocking

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



Domain Blocking Configuration

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

Domain Blocking: ● Disable ○ Enable

Domain:

Domain Block Table:

Select	Domain

Fields in this page:

Field	Description
Domain Blocking	Check this item to enable the Domain Blocking feature.
Domain	The blocked domain. If the URL of Taiwan Yahoo web site is tw.yahoo.com, the domain can be yahoo.com.

Function buttons in this page:

Apply Changes

Click to disable/enable the Domain Block capability

Add

Add domain into Domain Block table.

Delete Selected

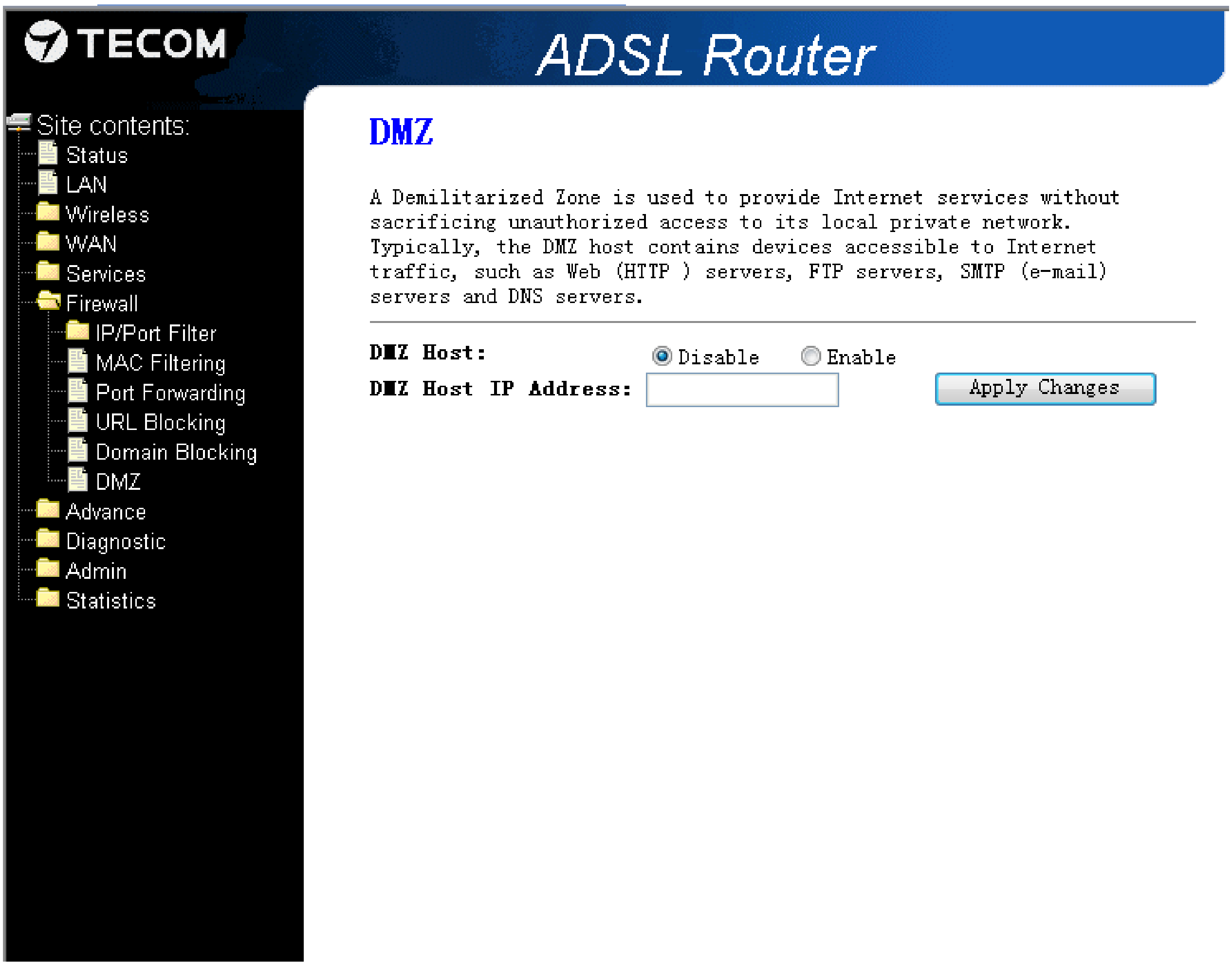
Delete the selected domain from the Domain Block table. You can click the checkbox at the Select column to select the Blocked domain.

Delete All

Delete all rules from the current table.

4.7.6. 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

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

DMZ Host: ● Disable ○ Enable

DMZ Host IP Address:

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:

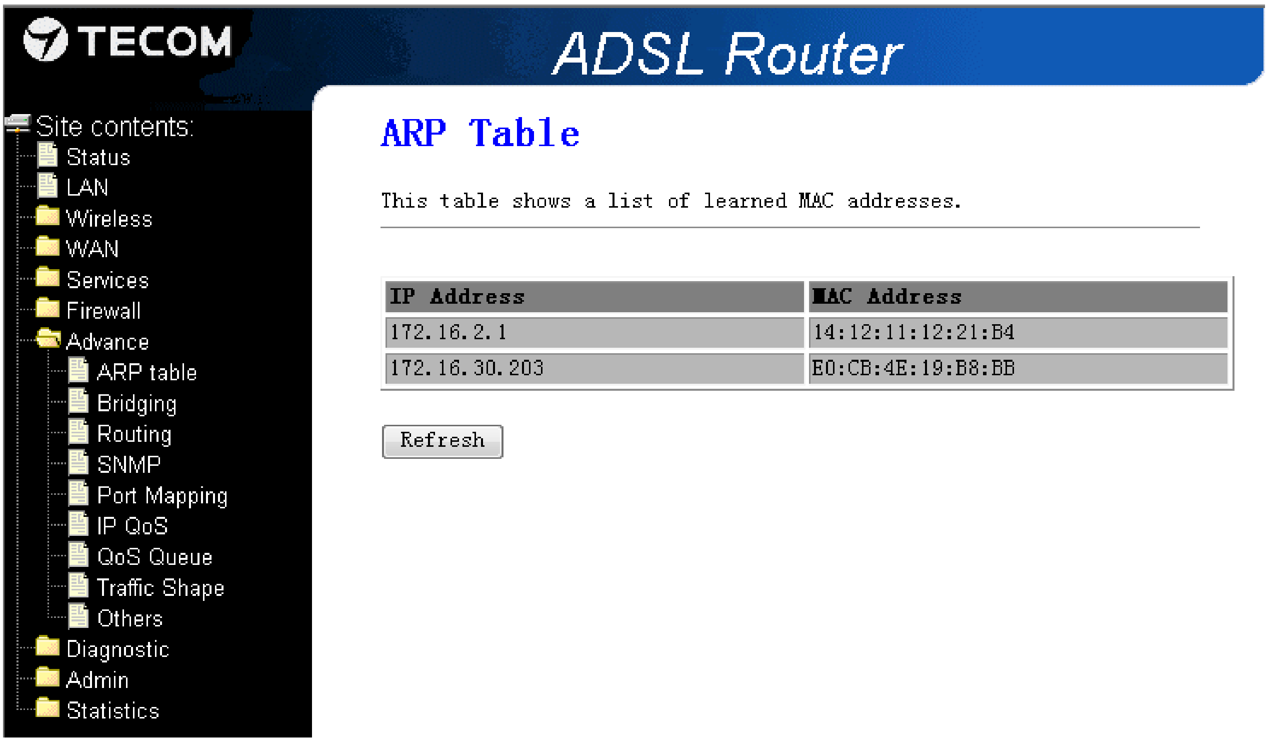
Apply Changes

Click to save the setting to the configuration.

4.8. Advance Configuration

4.8.1. ARP table

You can see the show list of learned MAC addresses through ARP in this page.



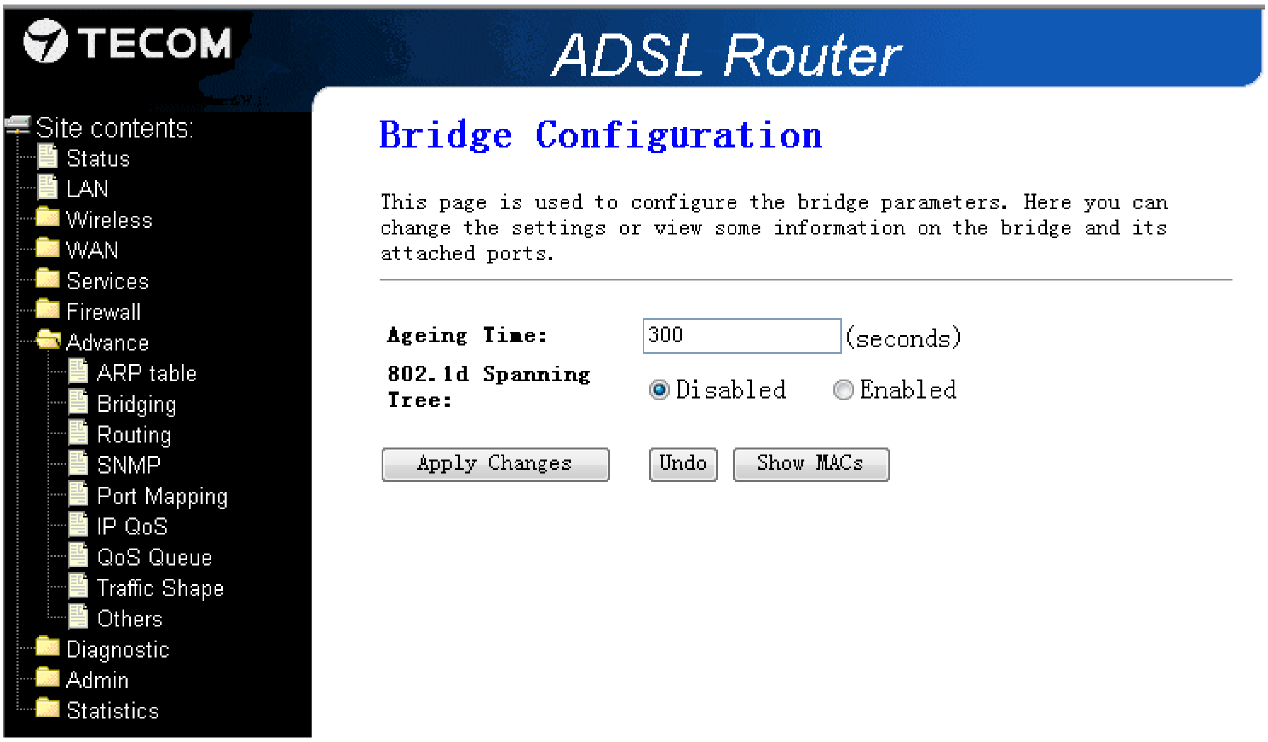
ARP Table

This table shows a list of learned MAC addresses.

IP Address	MAC Address
172.16.2.1	14:12:11:12:21:B4
172.16.30.203	E0:CB:4E:19:B8:BB

4.8.2. Bridging

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



Bridge Configuration

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

Ageing Time: 300 (seconds)

802.1d Spanning Tree: ● Disabled ○ Enabled

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.

Undo

Undo changes

Show MACs

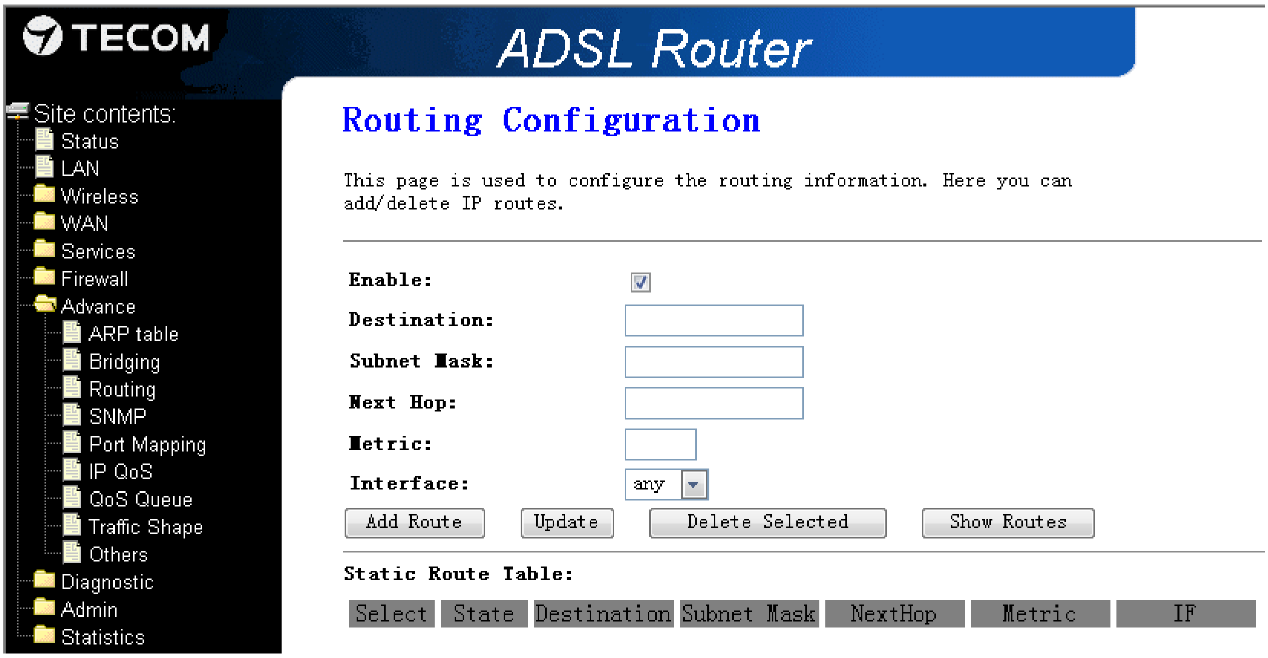
List MAC address in the table.

4.8.3. 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.



Routing Configuration

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

Enable: ☑

Destination:

Subnet Mask:

Next Hop:

Metric:

Interface: any

Add Route | Update | Delete Selected | Show Routes

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	IF

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

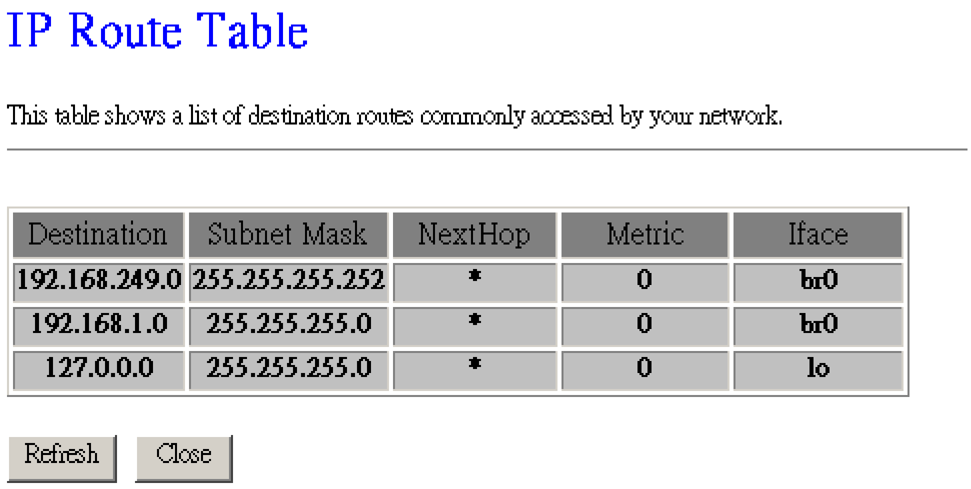
Update the selected destination route on the **Static Route Table**.

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.



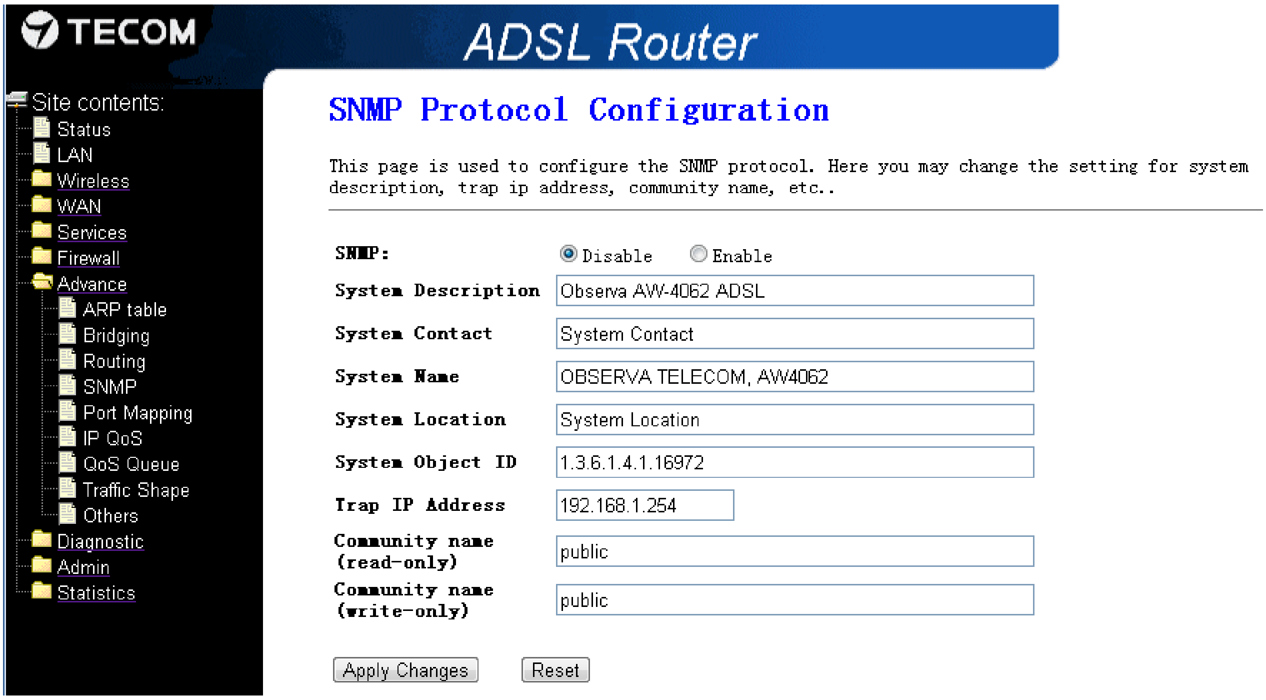
IP Route Table

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

Destination	Subnet Mask	NextHop	Metric	Iface
192.168.249.0	255.255.255.252	*	0	br0
192.168.1.0	255.255.255.0	*	0	br0
127.0.0.0	255.255.255.0	*	0	lo

4.8.4. 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



SNMP Protocol Configuration

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

SNMP:	● Disable ○ Enable
System Description	Observa AW-4062 ADSL
System Contact	System Contact
System Name	OBSERVA TELECOM, AW4062
System Location	System Location
System Object ID	1.3.6.1.4.1.16972
Trap IP Address	192.168.1.254
Community name (read-only)	public
Community name (write-only)	public

Fields in this page:

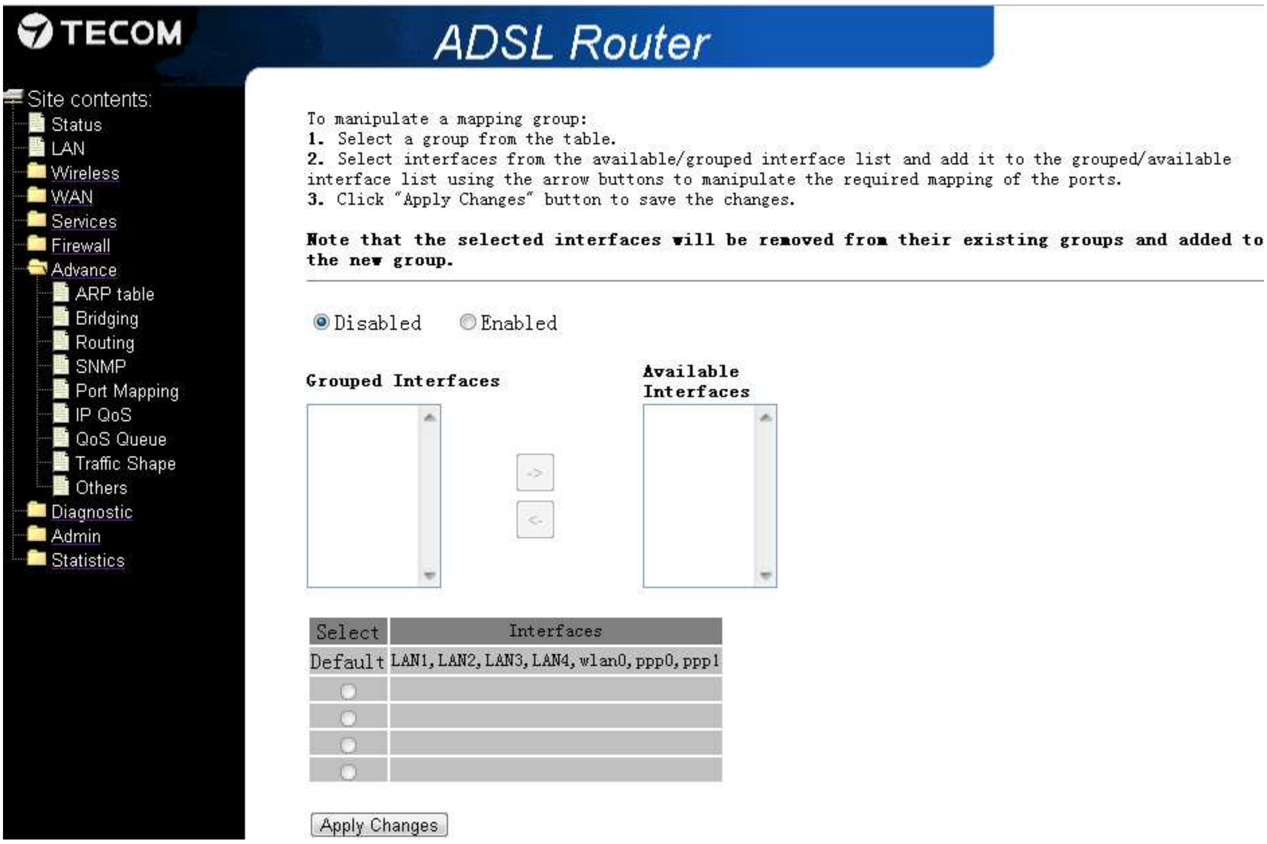
Field	Description
SNMP	Click this feature to disable/enable the SNMP function.
System Description	System description of the DSL device.
System Contact	Contact person and/or contact information for the DSL device.
System Name	An administratively assigned name for the DSL device.
System Location	The physical location of the DSL device.
System Object ID	Vendors 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.

4.8.5. 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.

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

● Disabled ○ Enabled

Grouped Interfaces **Available Interfaces**

Select	Interfaces
Default	LAN1,LAN2,LAN3,LAN4,wlan0,ppp0,ppp1
○	
○	
○	
○	

Fields in this page:

Field	**Description**
Enable	Check to enable the selected route or route to be added.
Available Interfaces	All Ethernet interface,PVC interface and wireless interface will show.
Grouped Interfaces	Group any interface in Available Interface column to this field.

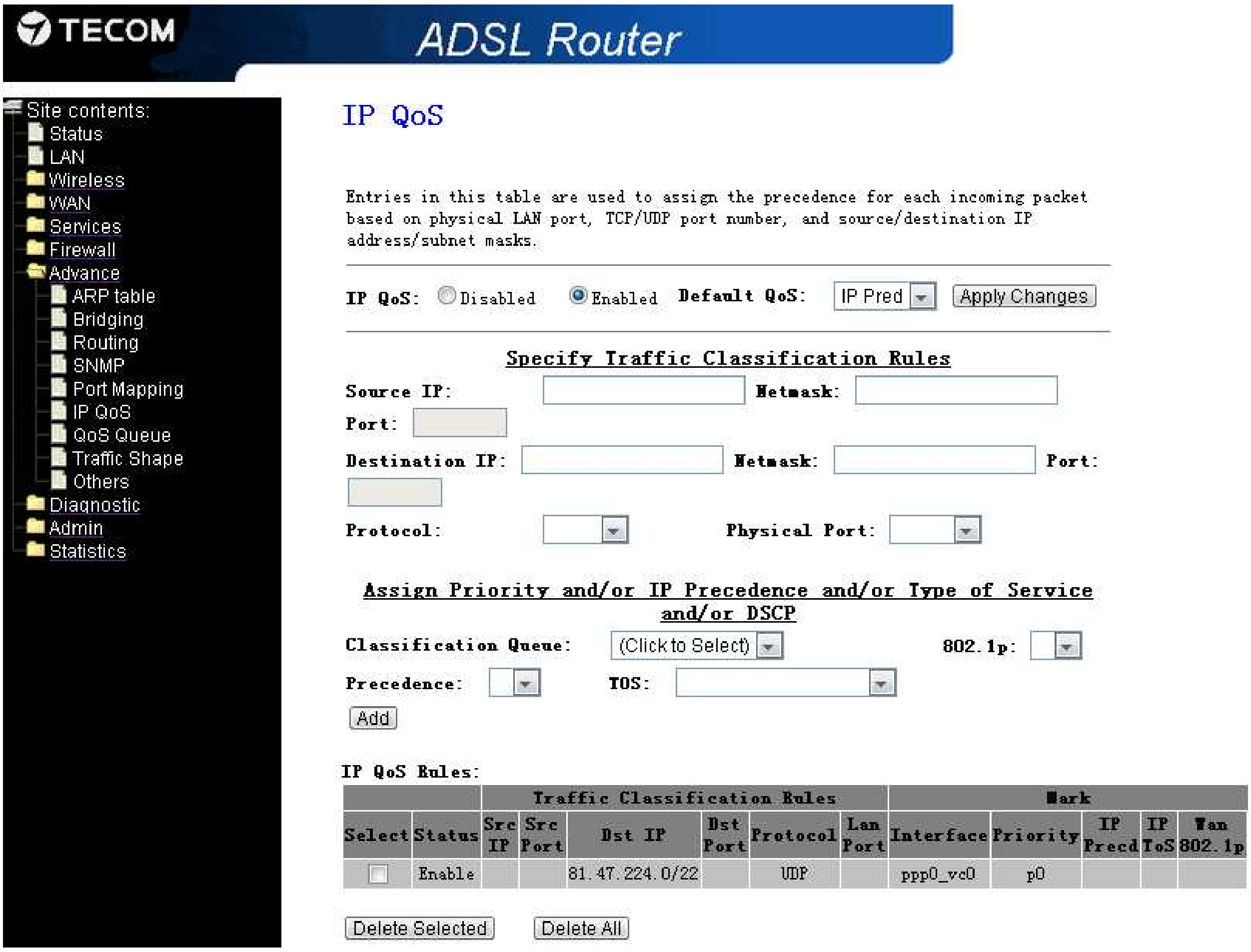
Buttons in this page:

Apply Changes

Push to apply changes

4.8.6. IP QoS

QoS (Quality of service) is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. User can configure QoS parameters in the following page:



IP QoS

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

IP QoS: ○ Disabled ● Enabled **Default QoS:** IP Pred [Apply Changes]

Specify Traffic Classification Rules

Source IP: **Netmask:**

Port:

Destination IP: **Netmask:** **Port:**

Protocol: **Physical Port:**

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

Classification Queue: (Click to Select) **802.1p:**

Precedence: **TOS:**

[Add]

IP QoS Rules:

		Traffic Classification Rules						Mark				
Select	Status	Src IP	Src Port	Dst IP	Dst Port	Protocol	Lan Port	Interface	Priority	IP Precd	IP ToS	Wan 802.1p
□	Enable			81.47.224.0/22		UDP		ppp0_vc0	p0			

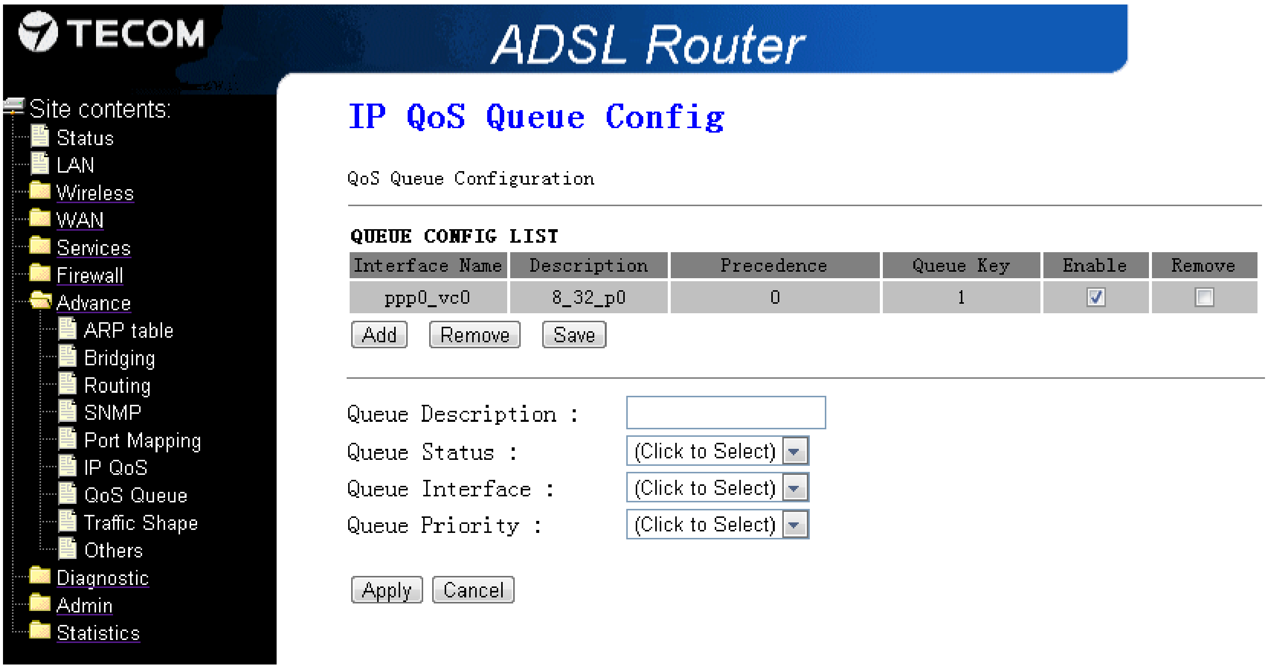
[Delete Selected] [Delete All]

Fields in this page:

Field	Description
IP QoS	Check to enable the IP Qos function.
Default QoS	IP Pred or 802.1p is to apply.
Source IP	Source IP for IP packet incoming from Ethernet
Destination IP	Source IP for IP packet incoming from Ethernet
Netmask	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
Port	Port number is filled in this column.
Protocol	Which Protocol to apply? Protocol TCP, UDP and ICMP.
Physical Port	Which LAN interfaces to apply? LAN interface have LAN 1, LAN 2, LAN 3, LAN 4
Clasiffication Queue	Select the QoS classification Queue
802.1p	Mark 802.1p for incoming IP Packet.
Precedence	Mark IP precedence for incoming IP Packet.
TOS	Mark type of services for incoming IP Packet.

4.8.7. QoS Queue

User can set the QoS Queue in the QoS Queue page, when press the Add button, the below page will be shown to user:



IP QoS Queue Config

QoS Queue Configuration

QUEUE CONFIG LIST

Interface Name	Description	Precedence	Queue Key	Enable	Remove
ppp0_vc0	8_32_p0	0	1	☑	☐

Queue Description :

Queue Status : (Click to Select)

Queue Interface : (Click to Select)

Queue Priority : (Click to Select)

Fields in this page:

Field	Description
Queue Description	This description will generate automatically when user set the other option for QoS Queue.
Queue Status	Enable/Disable the Queue status
Queue Interface	Select one interface for this rule.
Queue Priority	Set the queue priority for this rule, the priority rage is from 0 to 3.

Function buttons in this page:

Add

Click to add one rule for QoS Queue.

Apply

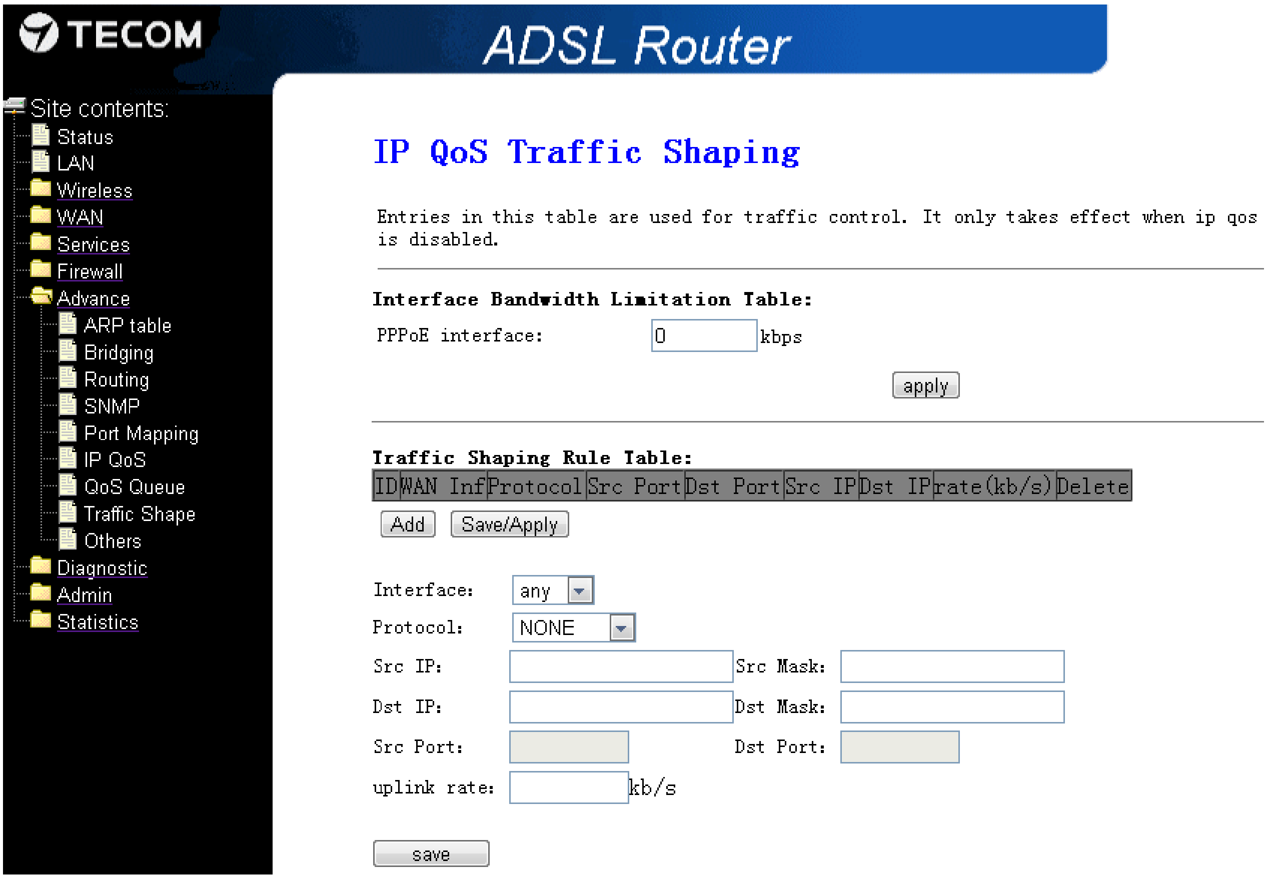
Click to save the setting to the configuration.

Cancel

Discard your settings.

4.8.8. Traffic Shape

Traffic shaping allows you to control the traffic going out an interface in order to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to policies contracted for it. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches. Configure traffic shaping on an interface if you have a network with differing access rates, press Add button on Traffic Shape page you can find the flowing configuration page:



IP QoS Traffic Shaping

Entries in this table are used for traffic control. It only takes effect when ip qos is disabled.

Interface Bandwidth Limitation Table:

PPPoE interface: 0 kbps

apply

Traffic Shaping Rule Table:

ID	WAN Inf	Protocol	Src Port	Dst Port	Src IP	Dst IP	rate(kb/s)	Delete

Add Save/Apply

Interface: any

Protocol: NONE

Src IP: Src Mask:

Dst IP: Dst Mask:

Src Port: Dst Port:

uplink rate: kb/s

save

Fields in this page:

Field	Description
Interface	Select one interface for this rule.
Protocol	There are 5 options available: NONE, ICMP, TCP, UDP and TCP/UDP.
Uplink rate	Set the max uplink rate for one rule.

Function buttons in this page:

Add

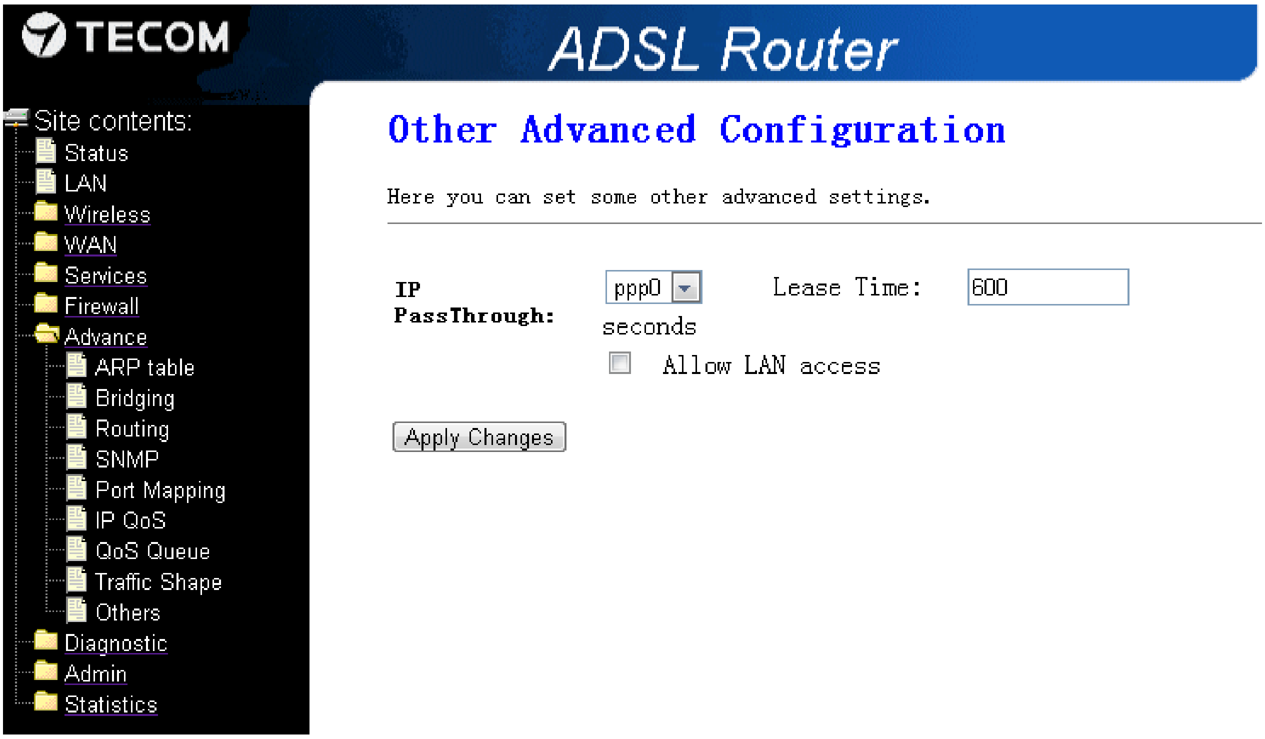
Click to add one rule for Traffic Shape.

Save

Click to save the setting to the configuration.

4.8.9. Others

This advanced configuration allows user pass the WAN IP to the LAN side. For example, if the IP PassThrough function has been enabled for PPP0 interface, then the LAN PC which set as DHCP mode will get the IP which provided by ISP as the PPP0.



Other Advanced Configuration

Here you can set some other advanced settings.

IP PassThrough: ppp0 Lease Time: 600 seconds

□ Allow LAN access

Fields in this page:

Field	Description
IP PassThrough	Enable/Select the WAN interface for IP PassTrough, and the interface can only be PPPOA or PPPoE.
Lease Time	Set the Lease time.
Allow LAN Access	Enable this function; other LAN PC can communicate with this PC which gets IP as PPP0.

Function buttons in this page:

Apply changes

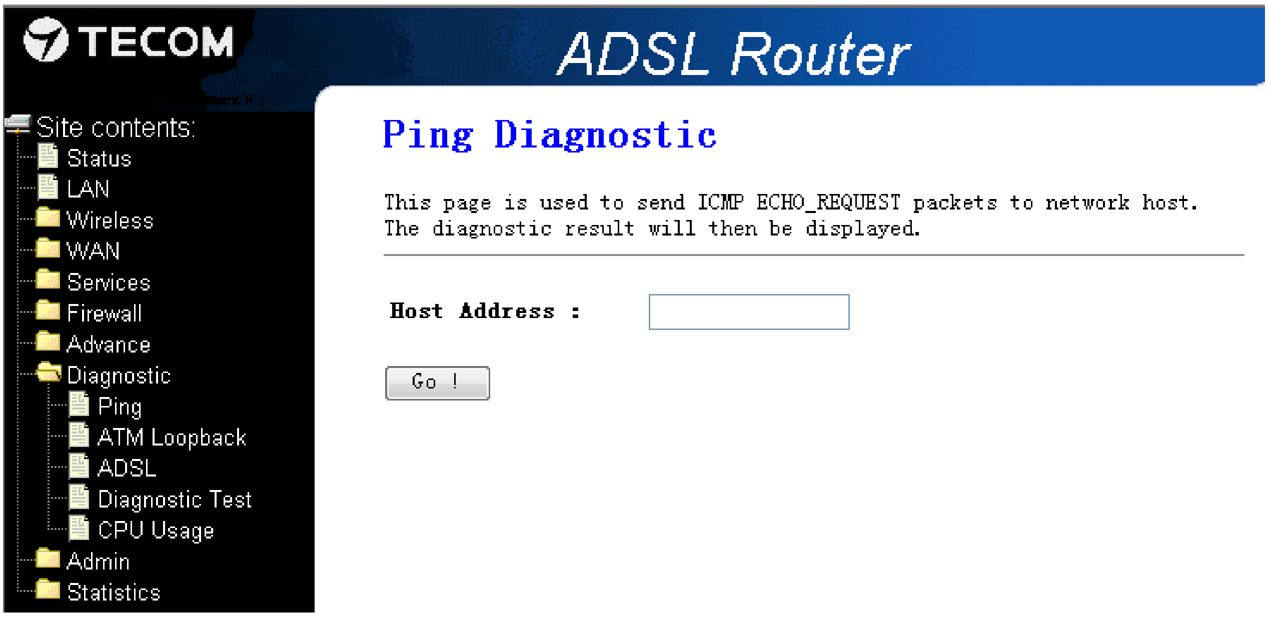
Click to save the changes to the configuration.

4.9. Diagnostic

The DSL device supports some useful diagnostic tools.

4.9.1. 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.



Ping Diagnostic

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

Host Address :

Go !

Fields in this page:

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

Function buttons in this page:

Go

Click to start the test.

4.9.2. 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:

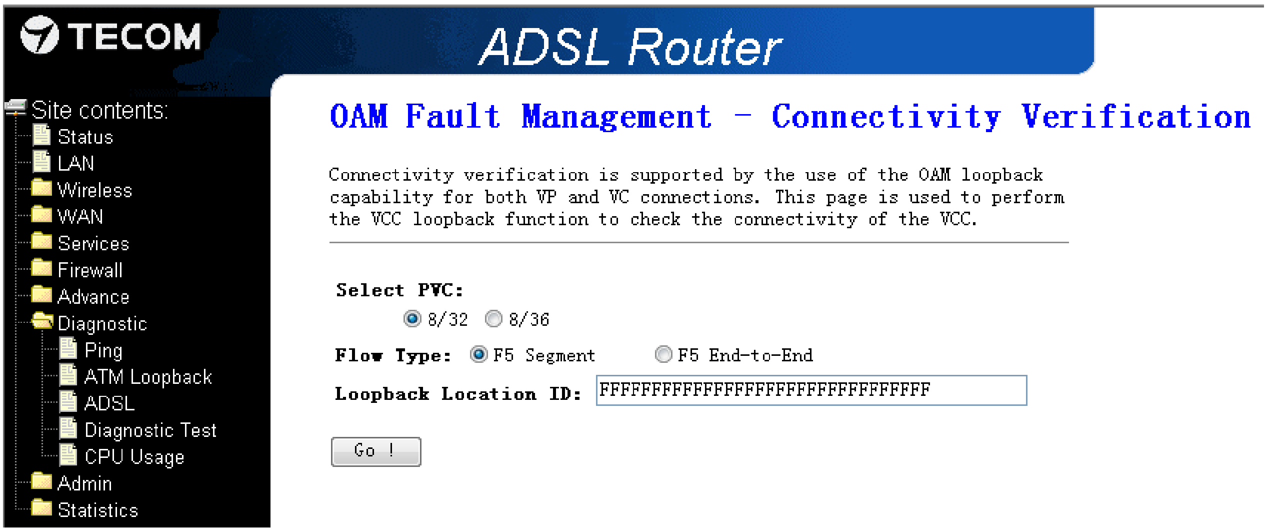
- F4: used in VPs

- 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 reachability of a segment endpoint or a connection endpoint.



OAM Fault Management - Connectivity Verification

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

Select PVC:
● 8/32 ○ 8/36

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

Loopback Location ID: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

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.

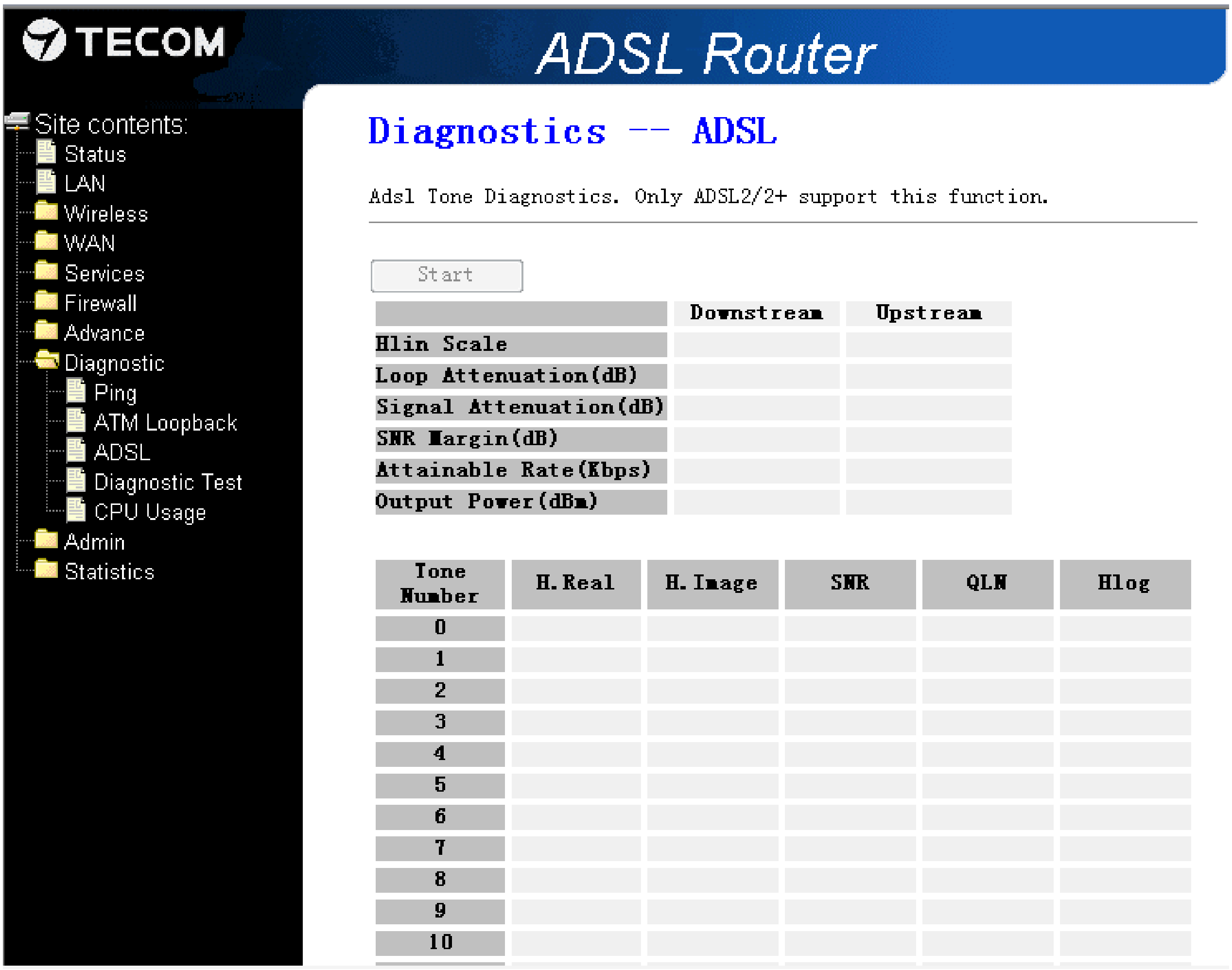
Function buttons in this page:

Go!

Click to start the test.

4.9.3. ADSL

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



Diagnostics -- ADSL

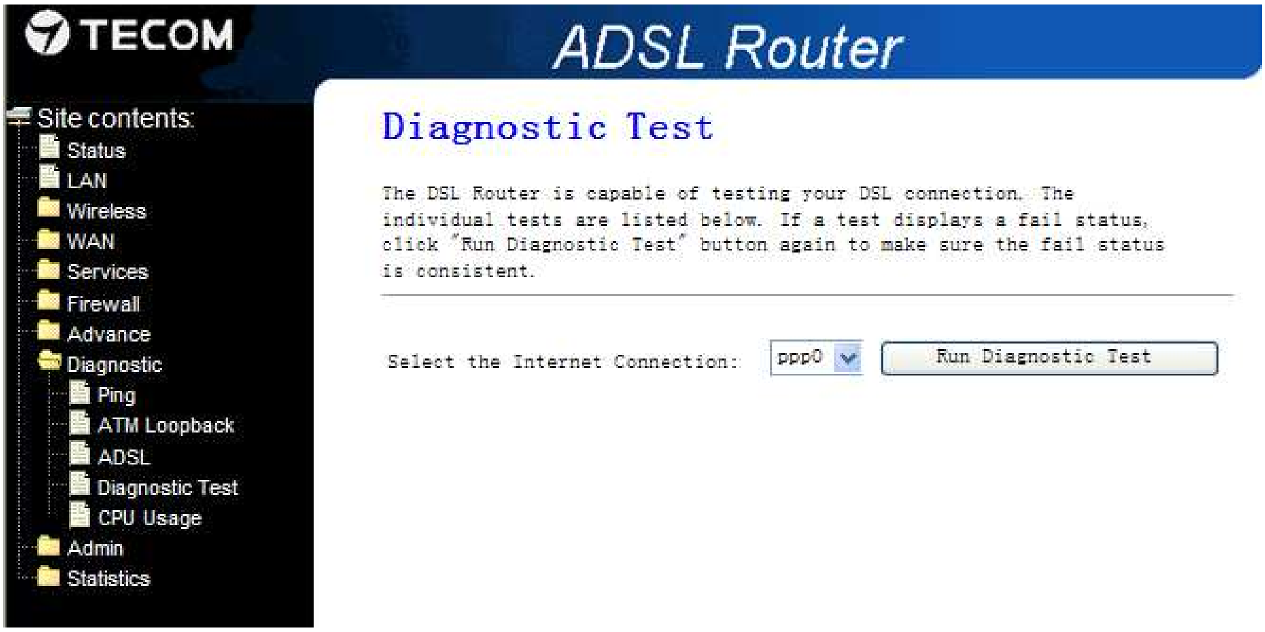
Adsl Tone Diagnostics. Only ADSL2/2+ support this function.

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

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

4.9.4. 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.



Diagnostic Test

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

Select the Internet Connection: ppp0

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.

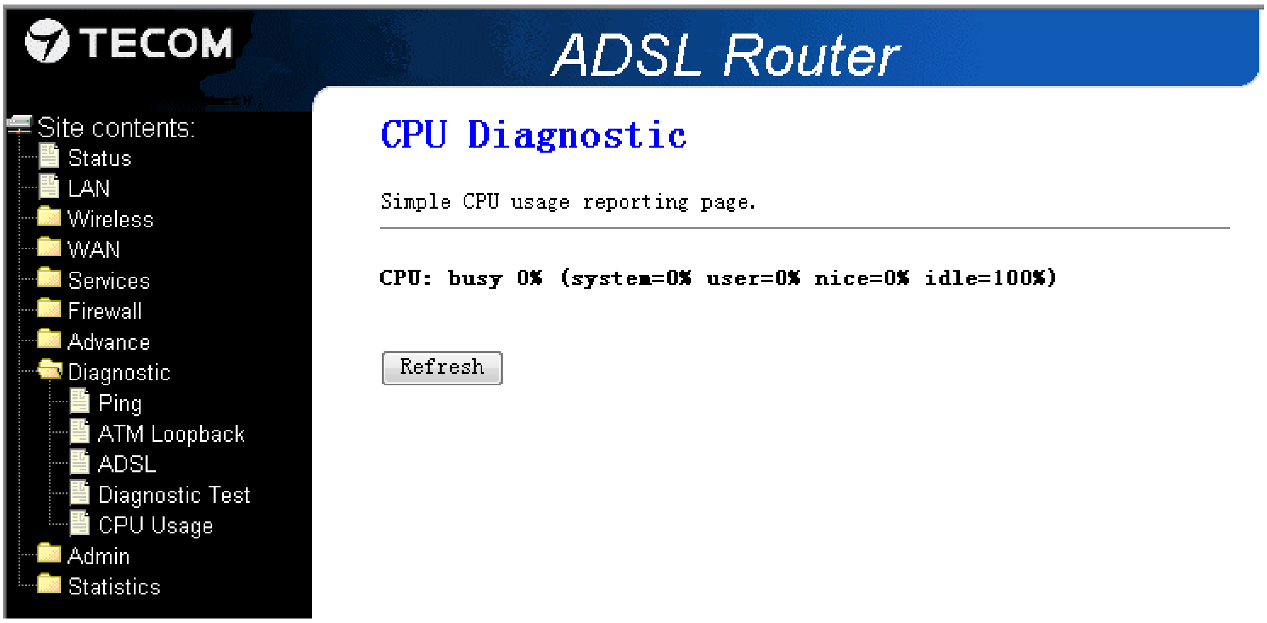
Function buttons in this page:

Run Diagnostic Test

Click to start the diagnostic test for this WAN interface.

4.9.5. CPU Usage

This page shows CPU Usage result. Click **Refresh** button to start the CPU Usage detection.



CPU Diagnostic

Simple CPU usage reporting page.

```
CPU: busy 0% (system=0% user=0% nice=0% idle=100%)
```

Function buttons in this page:

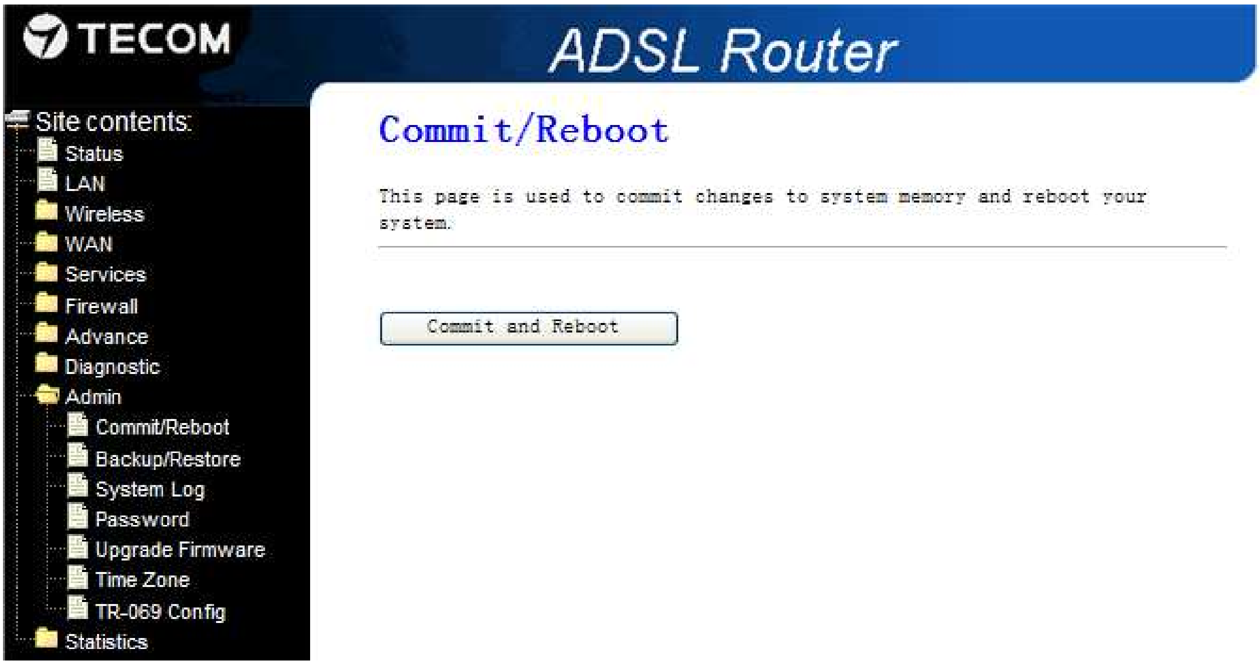
Refresh

Click to **Refresh** the test result for CPU.

4.10. Admin

4.10.1. 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/Reboot

This page is used to commit changes to system memory and reboot your system.

Function buttons in this page:

Commit and Reboot

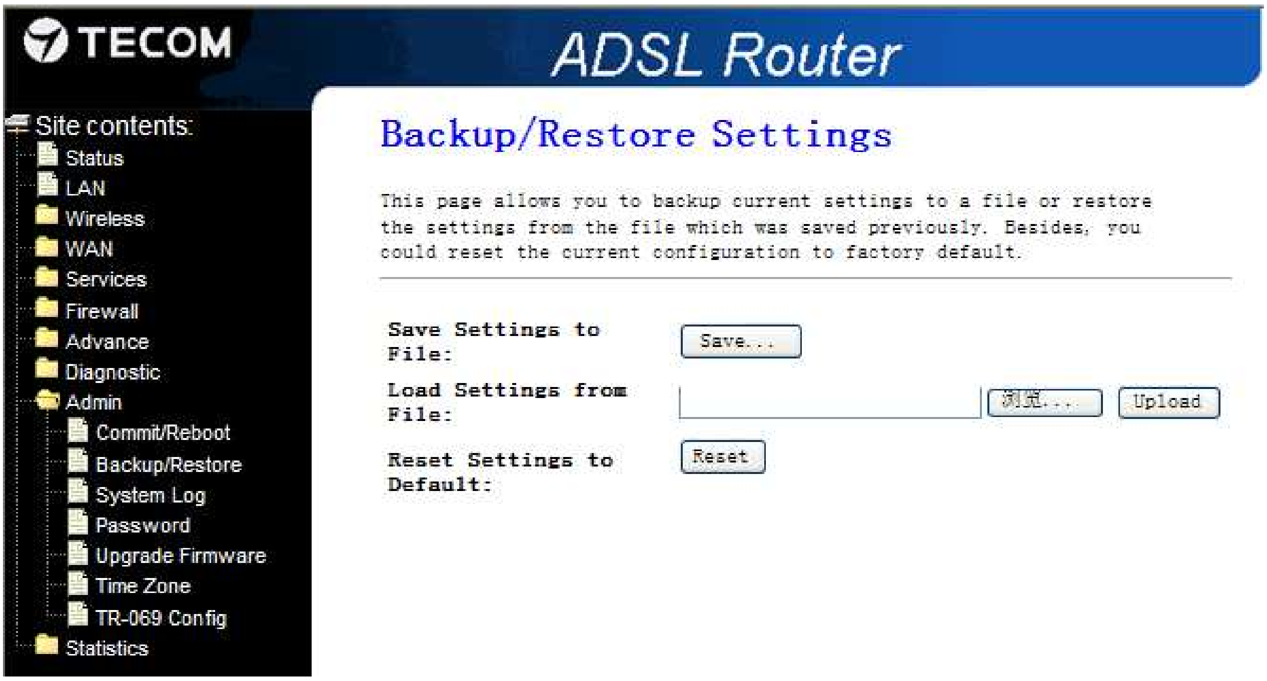
Whenever you use the web console to change system settings, the changes are initially placed in temporary storage. To save your changes for future use, you can use the Commit/Reboot function. This function saves your changes from RAM to flash memory and reboot the system.

IMPORTANT!

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

4.10.2. Backup/Restore

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



Backup/Restore Settings

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

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

<u>Function buttons in this page:</u>

Save

Click to save the current configuration file.

Upload

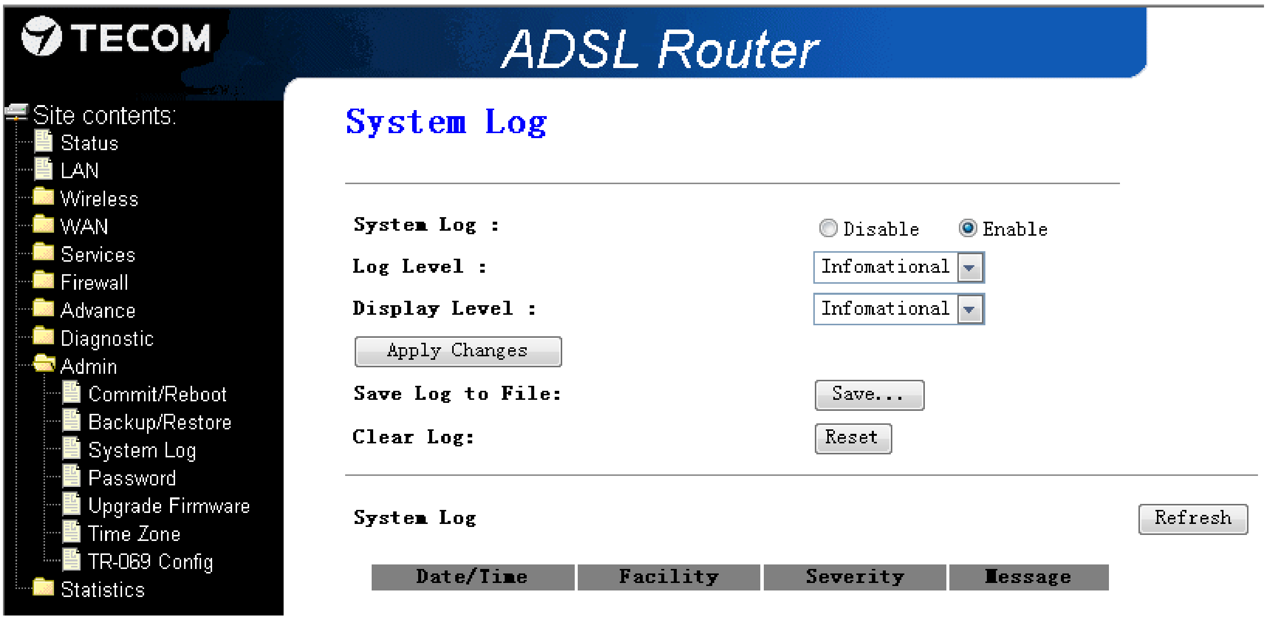
Click to upload the configuration file.

Reset

Click to reset the device to factory settings.

4.10.3. System Log

This page will show the system log.



System Log

System Log :	○ Disable ● Enable
Log Level :	Infomational
Display Level :	Infomational
Apply Changes	
Save Log to File:	Save...
Clear Log:	Reset

System Log Refresh

Date/Time	Facility	Severity	Message

Fields in this page:

Field	Description
System Log	Enable/Disable the system log feature.
Log Level	Set the system log level.
Display Level	Select that which level log will be shown on the log page.

Function buttons in this page:

Apply Changes

Click to save the setting of system log level to the configuration.

Save

Click to save the system log to the local PC.

Reset

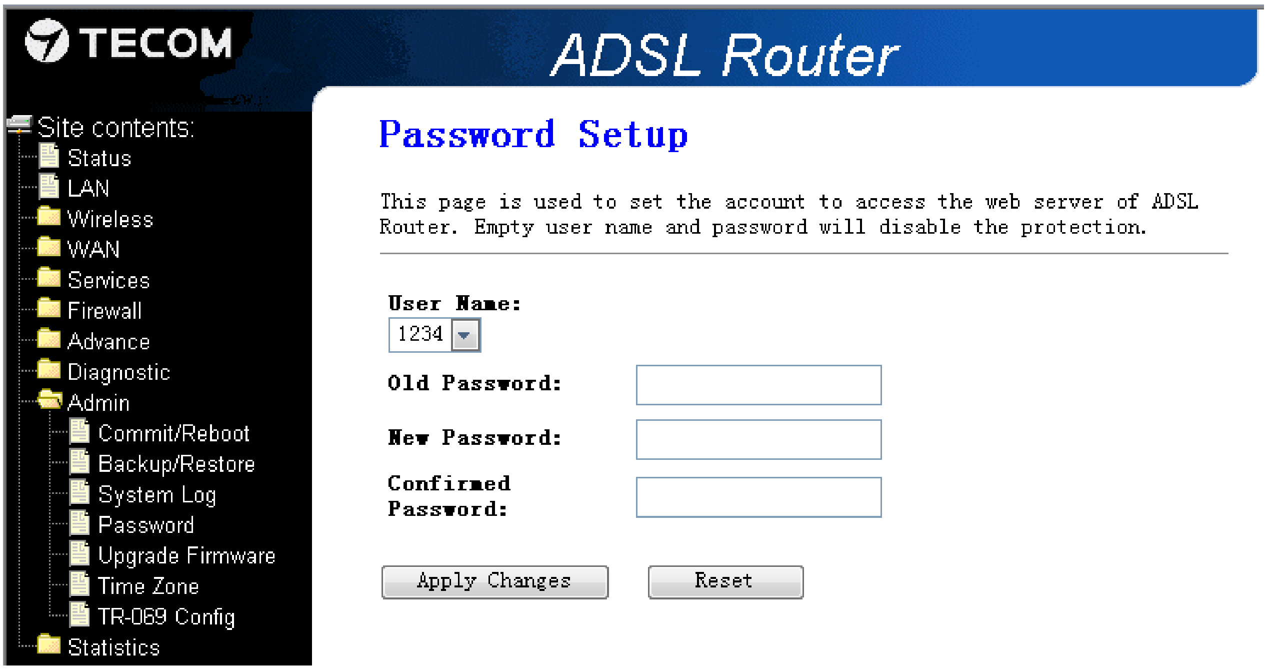
Click to reset all the settings for system log, remove all the logs on the system log page.

Refresh

Click to refresh all the system logs.

4.10.4. Password

The first time you log into the system, you use the default password. There are two-level logins: **1234** and **user**. The **1234** and **user** password configuration allows you to change the password for administrator and user.



Password Setup

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

User Name:	1234
Old Password:	
New Password:	
Confirmed Password:	

Fields in this page:

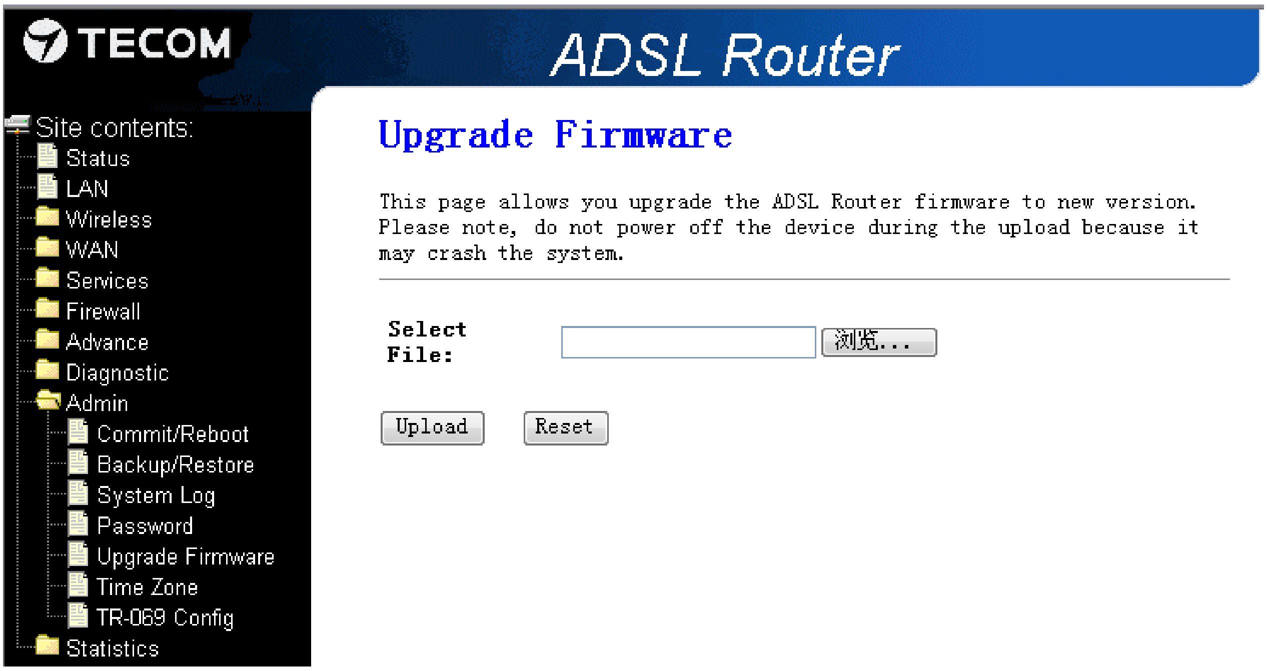
Field	Description
User Name	Selection of user levels are: admin and user.
Old Password	Enter the old password for this selected login.
New Password	Enter the new password here.
Confirmed Password	Enter the new password here again to confirm.

4.10.5. 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.



Upgrade Firmware

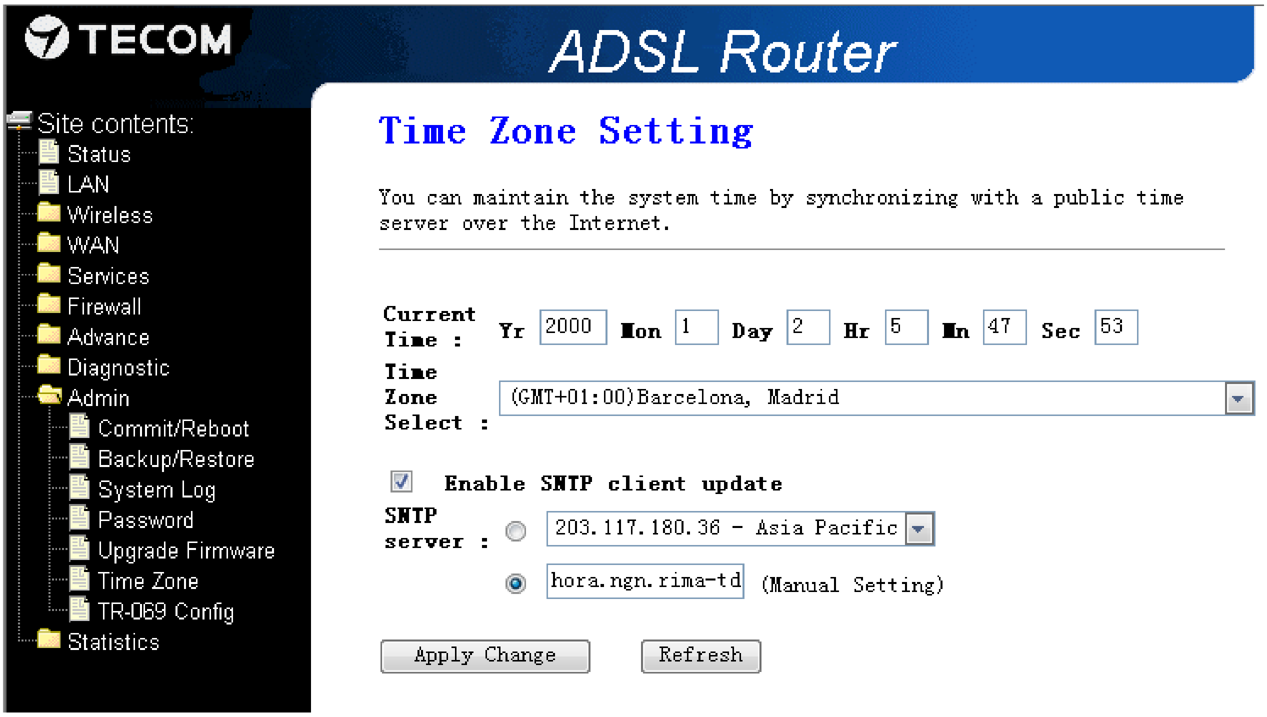
This page allows you upgrade the ADSL Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File: 浏览...

Upload Reset

4.10.6. 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



Time Zone Setting

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

Current Time : Yr 2000 Mon 1 Day 2 Hr 5 Mn 47 Sec 53

Time Zone Select : (GMT+01:00)Barcelona, Madrid

☑ Enable SNTP client update

SNTP server : ○ 203.117.180.36 - Asia Pacific

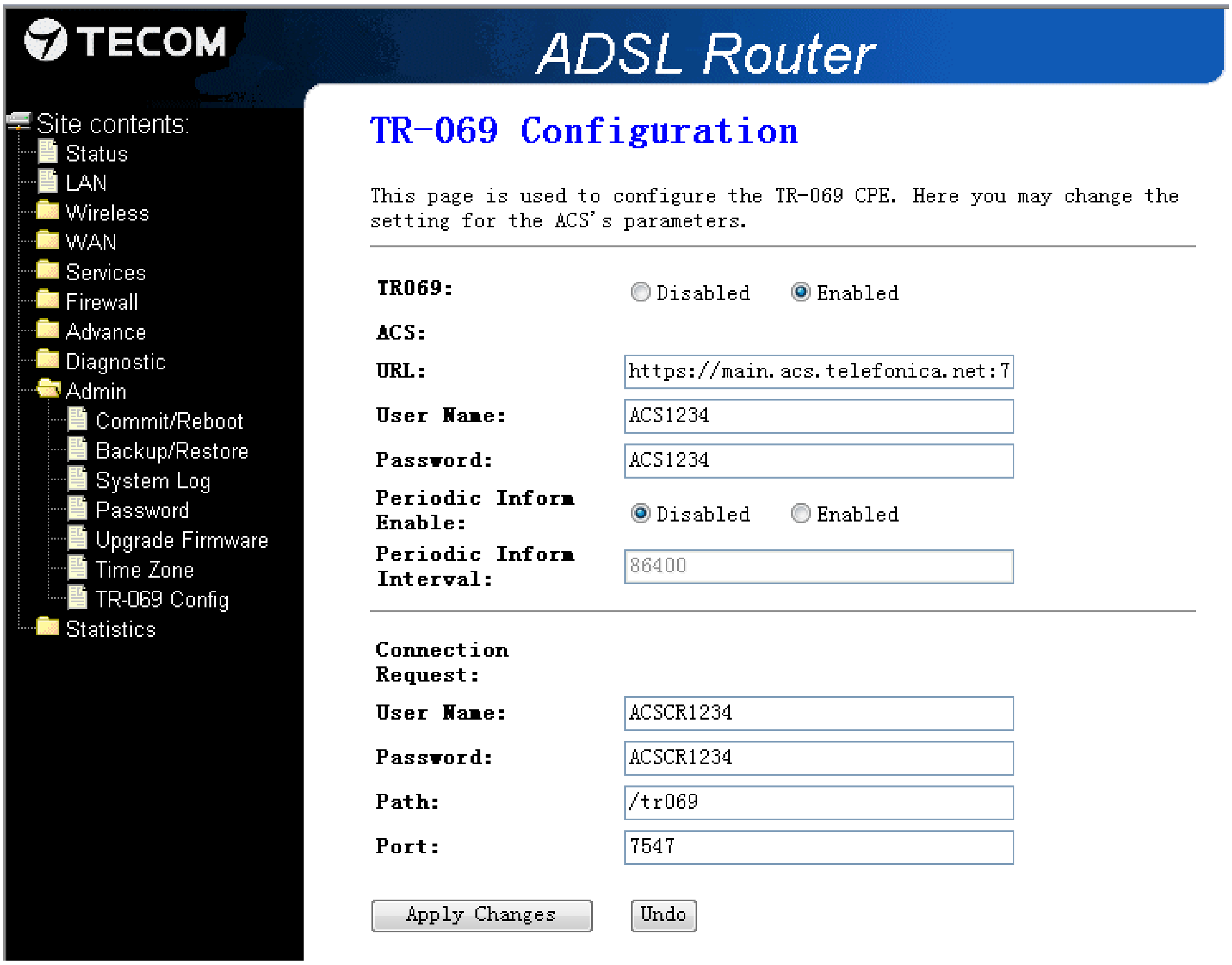
● hora.ngn.rima-td (Manual Setting)

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.

4.10.7. TR-069 Config.

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



TR-069 Configuration

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

TR069: ○ Disabled ● Enabled

ACS:

URL: https://main.acs.telefonica.net:7

User Name: ACS1234

Password: ACS1234

Periodic Inform Enable: ● Disabled ○ Enabled

Periodic Inform Interval: 86400

Connection Request:

User Name: ACSCR1234

Password: ACSCR1234

Path: /tr069

Port: 7547

Fields in this page:

ACS Field	Description
URL	ACS URL. For example, http://10.0.0.1:80 https://10.0.0.1:443
User Name	The username the DSL device should use when connecting to the ACS.
Password	The password the DSL device should use when connecting to the ACS.
Periodic Inform Enable	When this field is enabled, the DSL device will send an Inform RPC to the ACS server at the system startup, and will continue to send it periodically at an interval defined in **Periodic Inform Interval** field; When this field is disabled, the DSL device will only send Inform RPC to the ACS server once at the system startup.
Periodic Inform Interval	Time interval in second to send Inform RPC.
Connection Request Field	Description
User Name	The username the remote ACS should use when connecting to this device.
Password	The password the remote ACS should use when connecting to this device.
Path	The path of the device ConnectionRequestURL. The device ConnectionRequestURL should be configured based on the Device_IP, Path and Port as follows:

	http://Device_IP:Port/Path
Port	The port of the device ConnectionRequestURL.

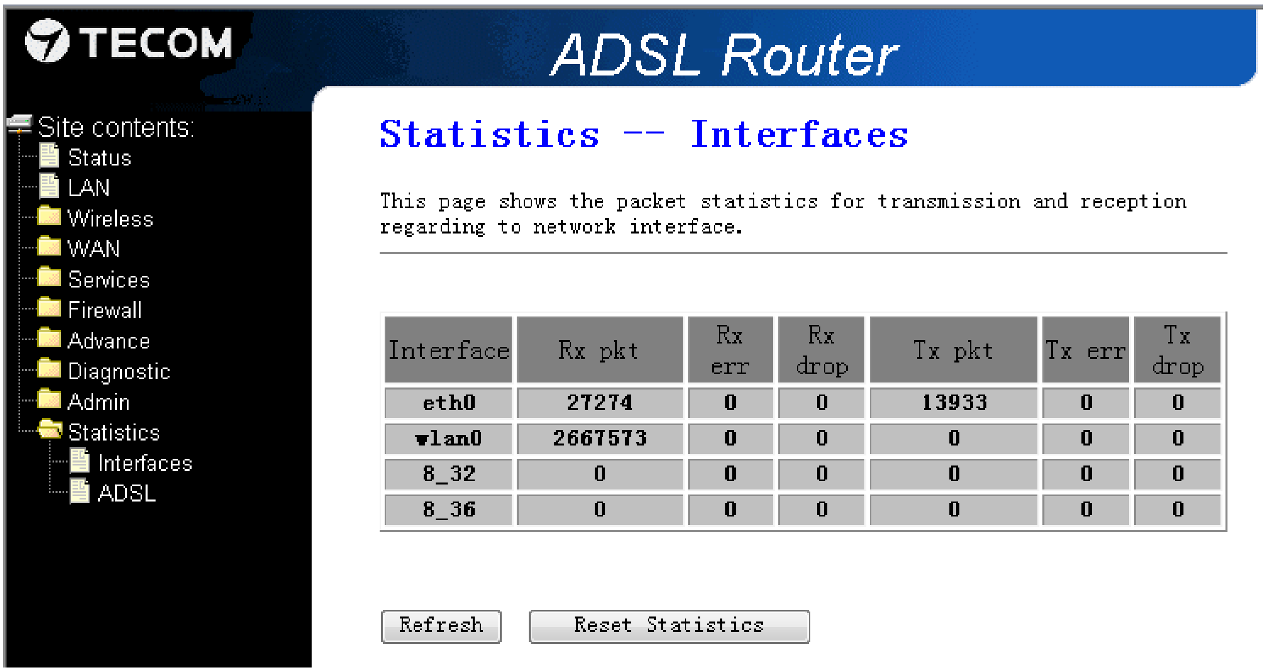
Note: Please enable the Auto-Execution to enable the TR-069 process

4.11. Statistics

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

4.11.1. 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.



Statistics -- Interfaces

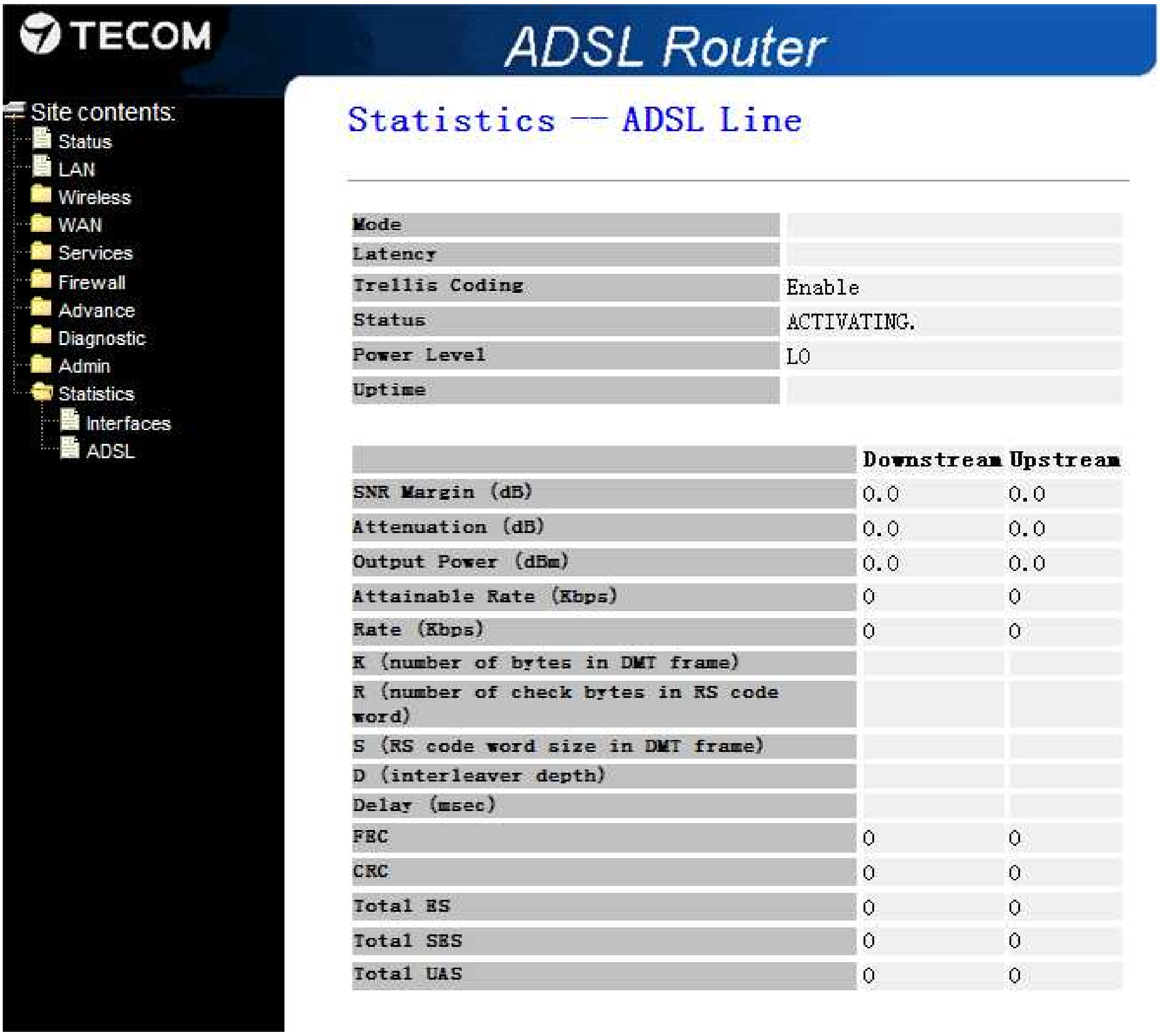
This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0	27274	0	0	13933	0	0
wlan0	2667573	0	0	0	0	0
8_32	0	0	0	0	0	0
8_36	0	0	0	0	0	0

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

4.11.2. ADSL

This page shows the ADSL line statistic information.



Statistics -- ADSL Line

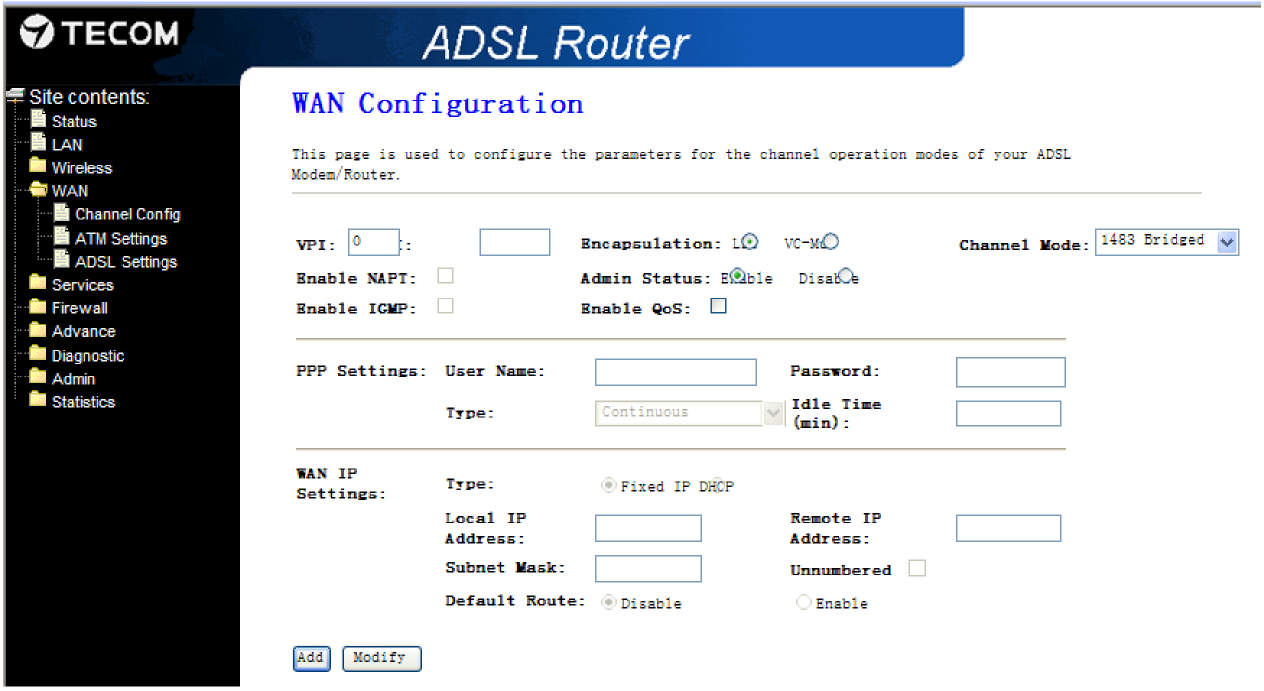
Mode	
Latency	
Trellis Coding	Enable
Status	ACTIVATING.
Power Level	L0
Uptime	

	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

APENDIX A: Channel Mode Configuration

ADSL router supports multiple channel operation modes. This section will show procedures to configure the router.

Bridge Mode



WAN Configuration

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

VPI: 0 VCI:

Encapsulation: ● LLC ○ VC-Mux

Channel Mode: 1483 Bridged

Enable NAPT: □

Admin Status: ● Enable ○ Disable

Enable IGMP: □

Enable QoS: □

PPP Settings: User Name: Password:

Type: Continuous Idle Time (min):

WAN IP Settings: Type: ● Fixed IP ○ DHCP

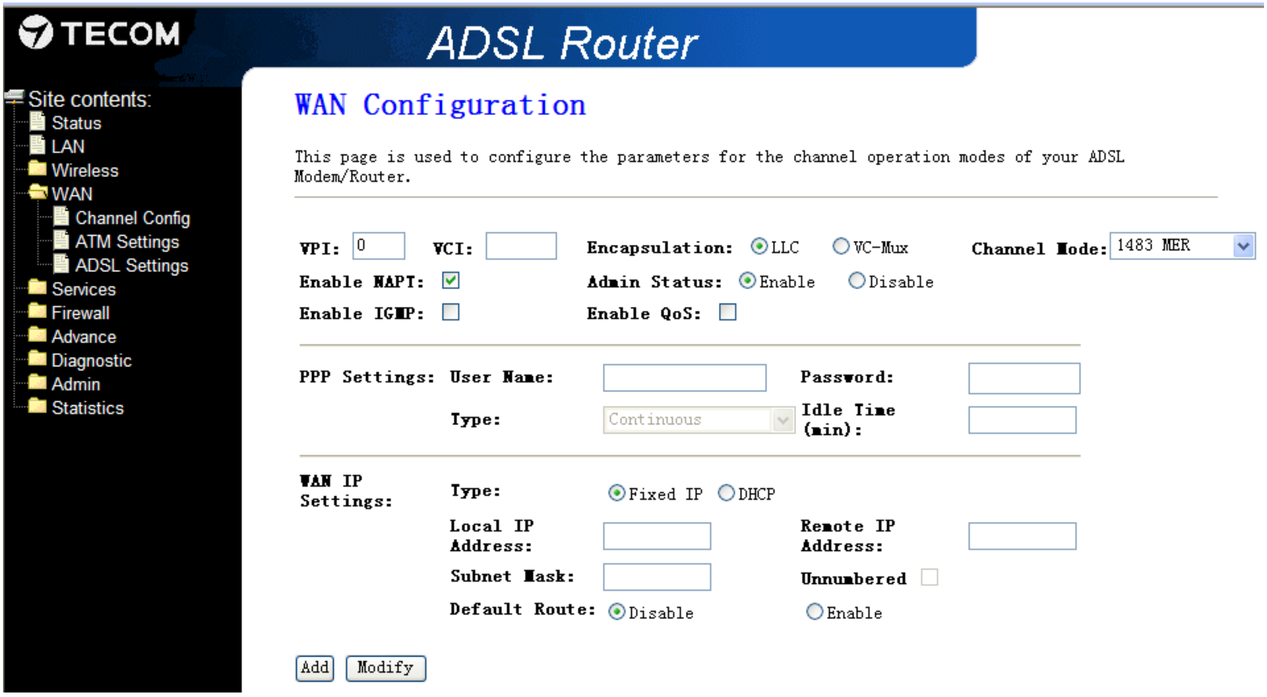
Local IP Address: Remote IP Address:

Subnet Mask: Unnumbered □

Default Route: ● Disable ○ Enable

1. Open the WEB page at "WAN interface/Channel Configuration".
2. Select the Channel Mode to "1483 Bridged". Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM setting.
3. Click "Add" button to add this channel into VC table.
4. Open the WEB page at "Admin/ Commit/Reboot". Press "Commit" to save the settings into flash memory.
5. The new settings will take effect after reboot the system.

MER(Mac Encapsulating Routing) Mode



WAN Configuration

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

VPI: 0 VCI: Encapsulation: ● LLC ○ VC-Mux Channel Mode: 1483 MER

Enable NAPT: ☑ Admin Status: ● Enable ○ Disable

Enable IGMP: □ Enable QoS: □

PPP Settings: User Name: Password:

Type: Continuous Idle Time (min):

WAN IP Settings: Type: ● Fixed IP ○ DHCP

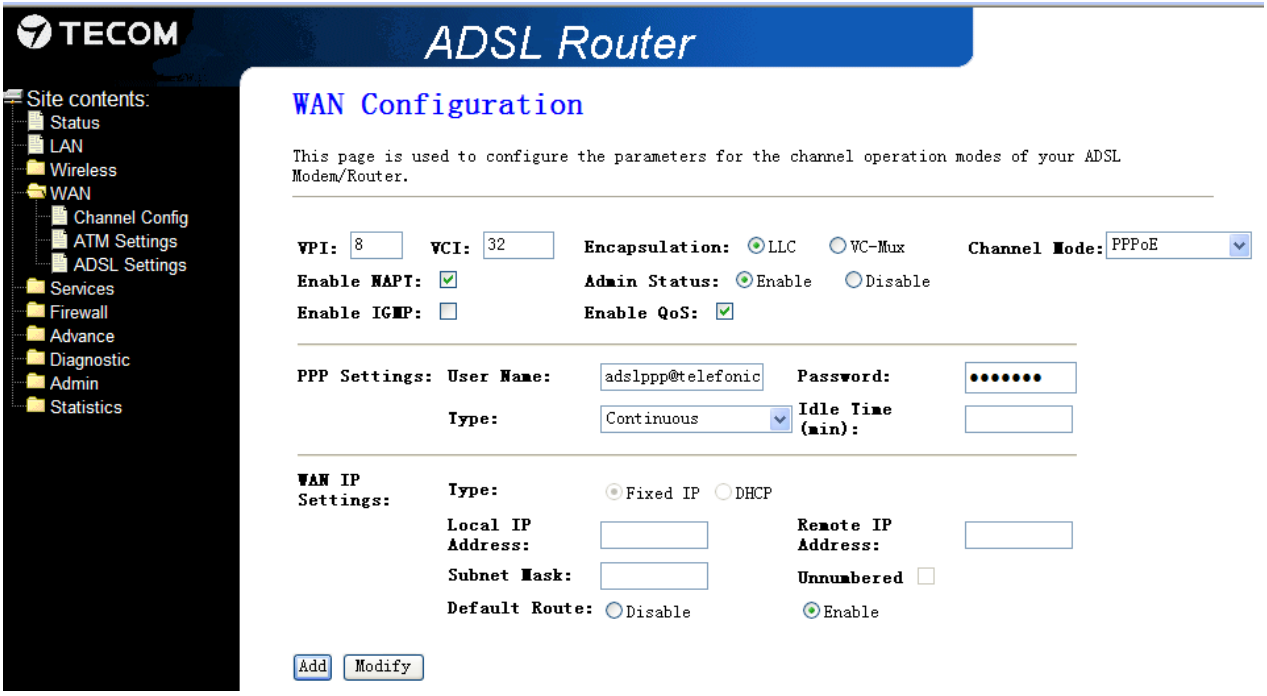
Local IP Address: Remote IP Address:

Subnet Mask: Unnumbered □

Default Route: ● Disable ○ Enable

1. Open the WEB page at "WAN interface/Channel Configuration".
2. Select the Channel Mode to "1483 MER". Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM setting.
3. Set "Local IP Address:" according to the IP that ISP assign for your router. Set "Remote IP Address" to the ISP's gateway.
4. Click "Add" button to add this channel into VC table.
5. Open the WEB page at "Admin/ Commit/Reboot". Press "Commit" to save the settings into flash memory.
6. The new settings will take effect after reboot the system.

PPPoE Mode



WAN Configuration

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

VPI: 8 VCI: 32 Encapsulation: ● LLC ○ VC-Mux Channel Mode: PPPoE

Enable NAPT: ☑ Admin Status: ● Enable ○ Disable

Enable IGMP: ☐ Enable QoS: ☑

PPP Settings: User Name: adslppp@telefonic Password: ●●●●●●●

Type: Continuous Idle Time (min):

WAN IP Settings: Type: ● Fixed IP ○ DHCP

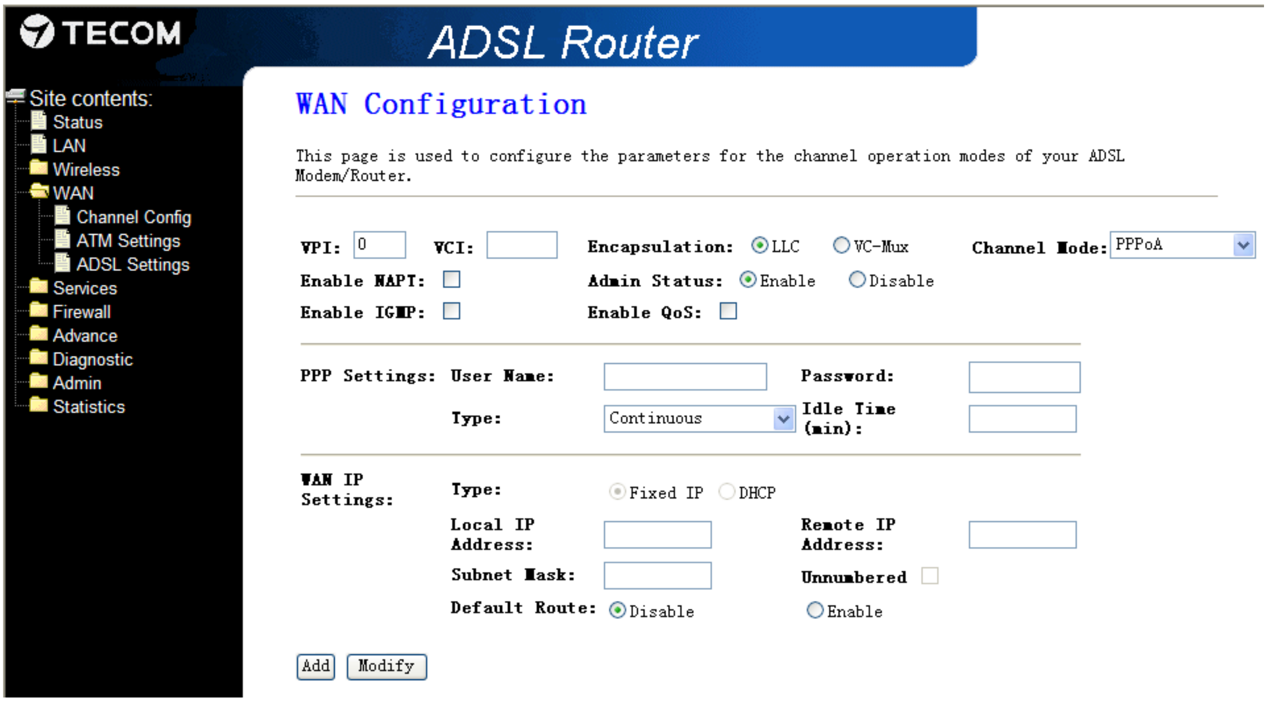
Local IP Address: Remote IP Address:

Subnet Mask: Unnumbered ☐

Default Route: ○ Disable ● Enable

1. Open the WEB page at "WAN interface/Channel Configuration".
2. Select the Channel Mode to "PPPoE". Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM setting.
3. Enter user/password from your ISP.
4. Click "Add" button to add this channel.
5. Enable DHCP server to allow the local PCs share the PPP connection. Reference to section 4.6.1 DHCP Server Configuration.
6. Set DNS address from your ISP. Reference to section 4.6.2 DNS Configuration.
7. Open the WEB page at "Admin/ Commit/Reboot". Press "Commit" to save the settings into flash memory.
8. The new settings will take effect after reboot the system.

PPPoA Mode



WAN Configuration

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

VPI: 0 VCI: Encapsulation: ● LLC ○ VC-Mux Channel Mode: PPPoA

Enable NAPT: □ Admin Status: ● Enable ○ Disable

Enable IGMP: □ Enable QoS: □

PPP Settings: User Name: Password:

Type: Continuous Idle Time (min):

WAN IP Settings: Type: ● Fixed IP ○ DHCP

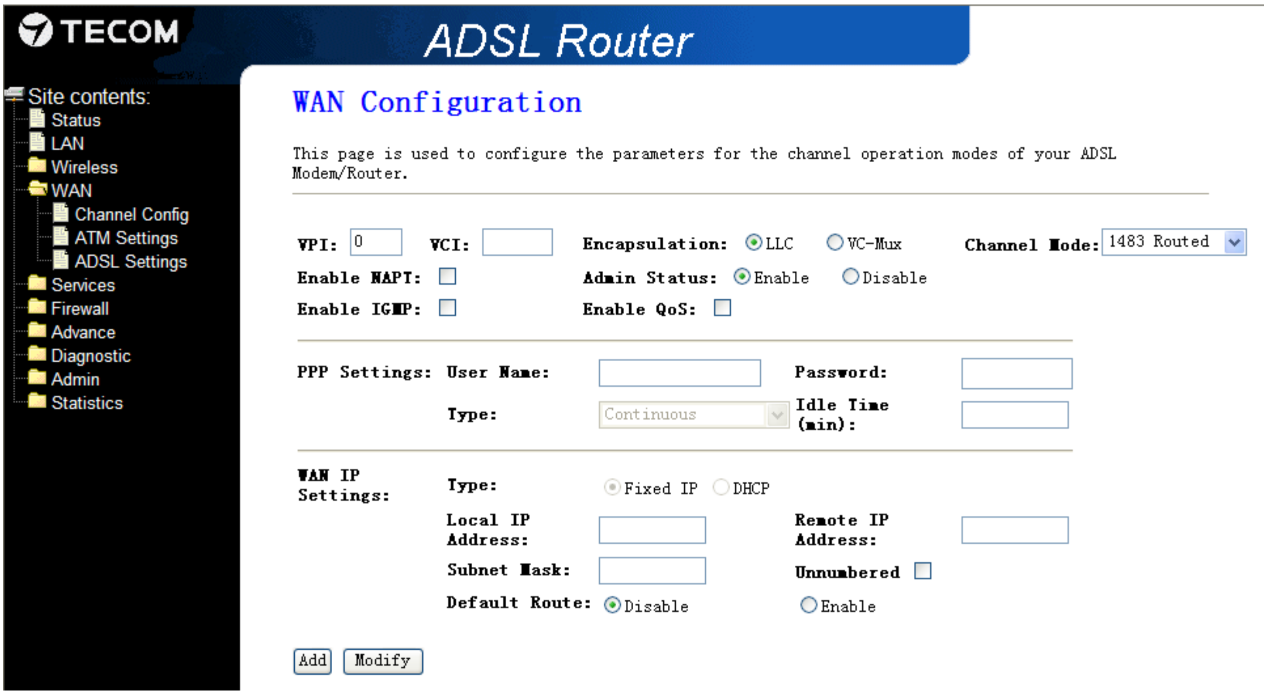
Local IP Address: Remote IP Address:

Subnet Mask: Unnumbered □

Default Route: ● Disable ○ Enable

1. Open the WEB page at “WAN interface/Channel Configuration”.
2. Select the Channel Mode to “PPPoA”. Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM setting.
3. Enter user/password from your ISP.
4. Click “Add” button to add this channel.
5. Enable DHCP server to allow the local PCs share the PPP connection. Reference to section 4.6.1 DHCP Server Configuration.
6. Set DNS address from your ISP. Reference to section 4.6.2 DNS Configuration.
7. Open the WEB page at “Admin/ Commit/Reboot”. Press “Commit” to save the settings into flash memory.
8. The new settings will take effect after reboot the system.

1483 Routed Mode



WAN Configuration

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

VPI: 0 VCI: Encapsulation: ● LLC ○ VC-Mux Channel Mode: 1483 Routed

Enable NAPT: □ Admin Status: ● Enable ○ Disable

Enable IGMP: □ Enable QoS: □

PPP Settings: User Name: Password:

Type: Continuous Idle Time (min):

WAN IP Settings: Type: ● Fixed IP ○ DHCP

Local IP Address: Remote IP Address:

Subnet Mask: Unnumbered □

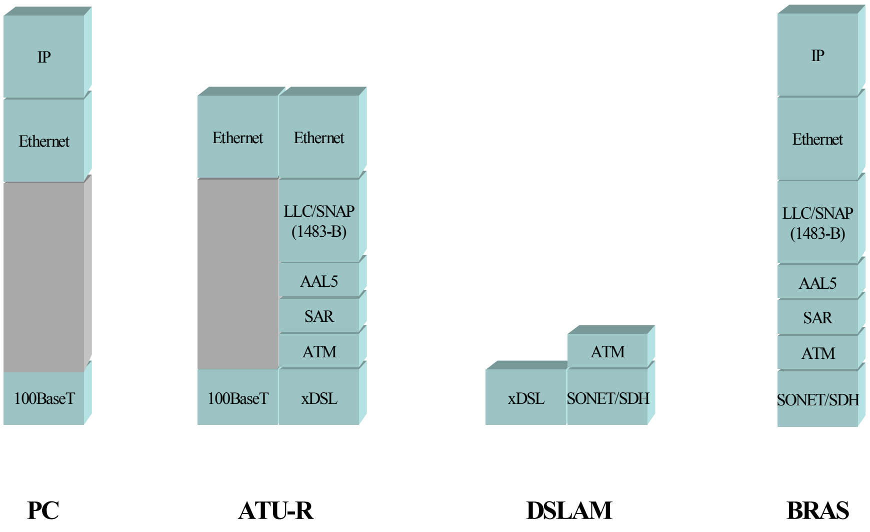
Default Route: ● Disable ○ Enable

1. Open the WEB page at “WAN interface/Channel Configuration”.
2. Select the Channel Mode to “1483 Routed”. Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM setting.
3. In WAN IP settings, give the local and remote IP address from your ISP or use DHCP to get them automatically if your ISP support it. Local IP is the address of ADSL router. Remote IP is the ISP’s gateway address.
4. Click “Add” button to add this channel.
5. Open the WEB page at “Admin/ Commit/Reboot”. Press “Commit” to save the settings into flash memory.
6. The new settings will take effect after reboot the system.

For more information or any question, please consult to your supplier for details.

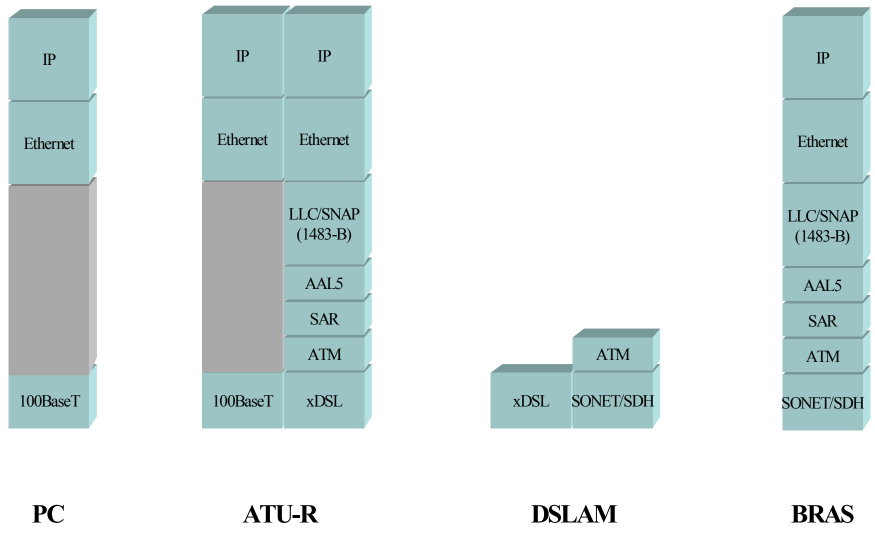
APENDIX B: Protocol Stacks

A.1 1483 Bridged Model



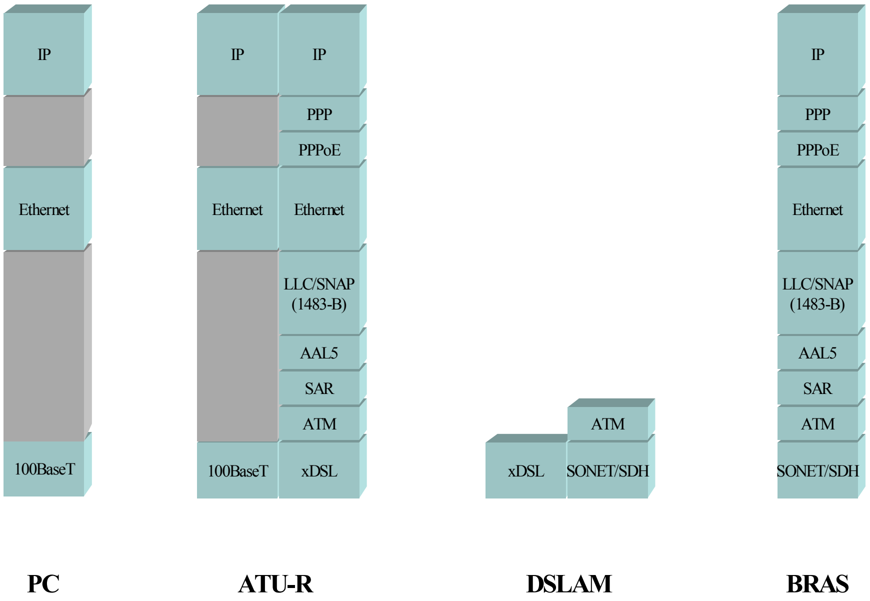
1483 Bridged Channel Mode Scenario

A.2 1483 MER Model



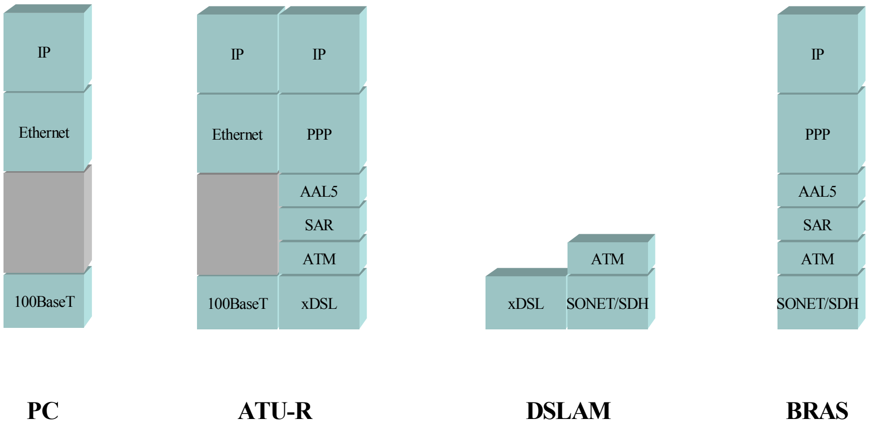
1483 MER Channel Mode Scenario

A.3 PPPoE Model



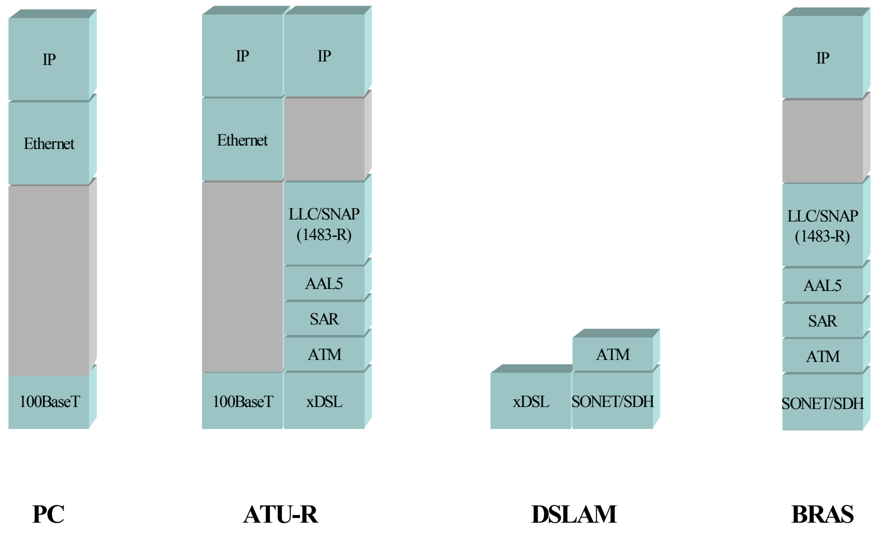
PPPoE Channel Mode Scenario

A.4 PPPoA Model



PPPoA Channel Mode Scenario

A.5 1483 Routed Model



1483 Routed Channel Mode Scenerio

APENDIX C: Mapping PVCs to VLANs

The AW4062 Router supports mapping ATM Permanent Virtual Circuits (PVCs) to VLANs, based on the ATM bridging standards of RFC2684. This feature allows an ATM PVC to be configured as a bridging interface and used in conjunction with a VLAN.

Figure B.1 illustrates the how the AW4062 Router adds a VLAN ID and tag to packets subject to PVC-VLAN mapping. In this example, vc3 is mapped to VLAN 20. The AW4062 Router adds VLAN ID 20 and tag 8100 to packets from vc3.

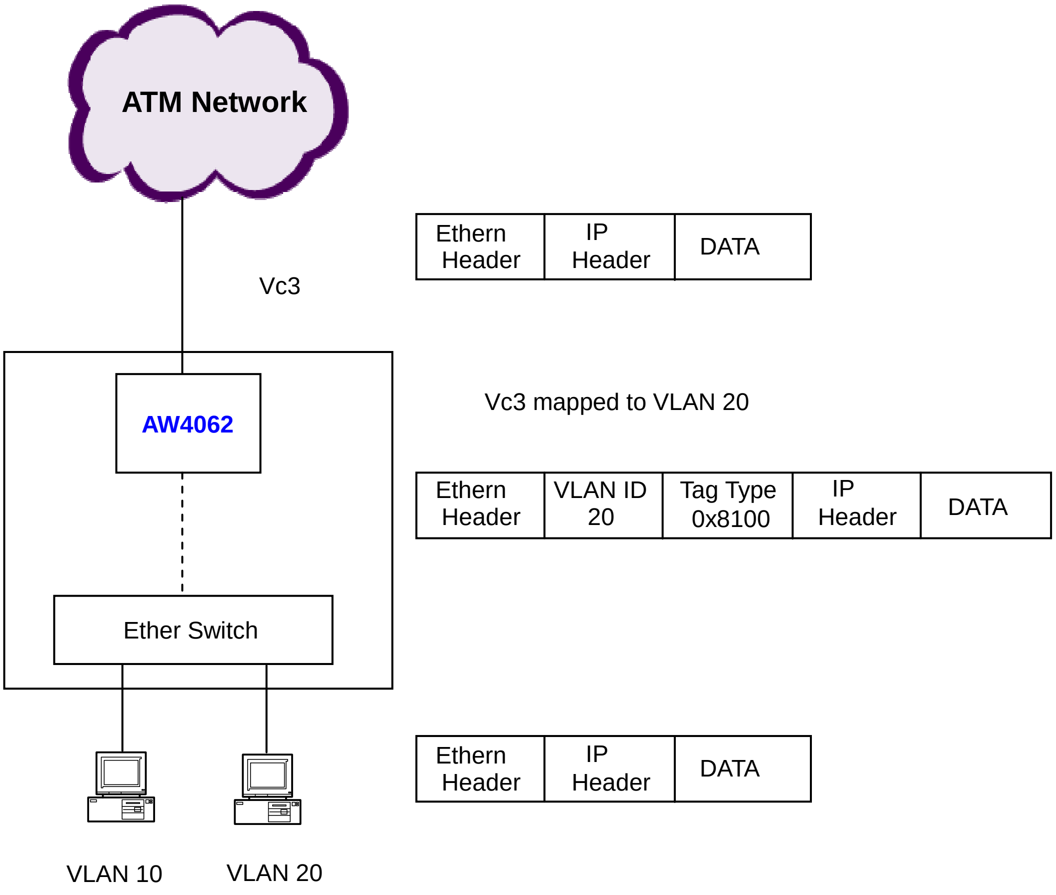


Figure B.1 Adding a VLAN ID and tag to packets from a PVC