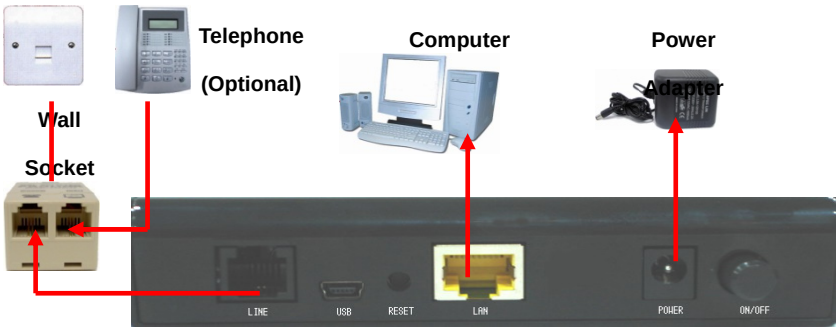
Hurricane 5200C/H5201

ADSL2+ Modem / Router

User Manual

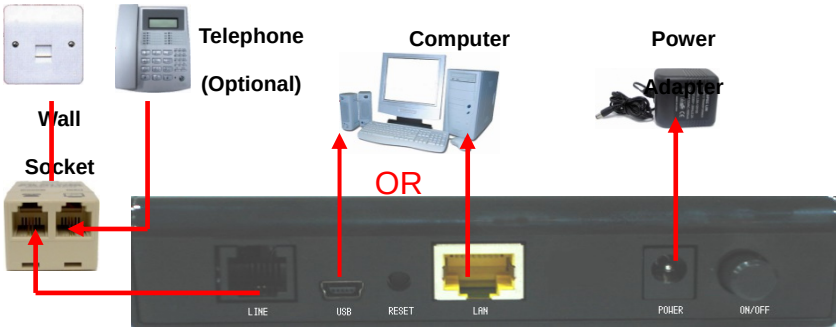
Version 1.0

Hardware connection for H5201



Line **LAN** **Power Switch**

Hardware connection for H5200C



Line **USB** **LAN** **Power Switch**

Contents

1 Introduction

The ADSL2+ Modem/Router user manual contains the guidance to install and configure PROLiNK Hurricane 5200C/5201 ADSL2+ Modem/Router using the Web GUI.

1.1 INTENDED AUDIENCE

This manual is intended for end users to access ADSL broadband service.

1.2 DEFINITIONS OF TERMS USED IN THIS DOCUMENT

None.

1.3 ACRONYMS USED THROUGHOUT THIS DOCUMENT

None.

1.4 USAGE INSTRUCTIONS

None.

1.5 QUESTIONS OR COMMENTS ON THIS DOCUMENT

Please contact us and visit our website at http://www.prolink2u.com should you have any questions or comments on this document.

2 System Overview

2.1 GENERAL DESCRIPTION

Hurricane 5200C/H5201 modem/router is a high-speed ADSL2+ 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. The ADSL2+ 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 full 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 to link to PC or other Switches/Hubs easily. The DSL device is an ideal solution for multi-users utilizing build-in channel mode (PPPoE/A, IPoA, IPoE), IP routing and NAT functionalities to share the ADSL link. The DSL device is also a perfect solution for residential users, as it supports users with bridge mode in host based PPPoE Client.

2.2 SPECIFICATIONS

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)

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
- Stateful Packet Inspection
- Protection against Denial of Service attacks
- IP Packet Filtering
- QoS
- Dynamic DNS
- UPnP support
- VoIP/VPN Pass-through

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
- TR069 supported
- Diagnostic Tool

3 Hardware Installation

3.1 HARDWARE REQUIREMENTS

- 12V power adapter
- RJ-45 Ethernet (LAN/network) cable
- RJ-11 ADSL (phone) line
- DSL Splitter (optional)

3.2 HARDWARE SETUP PROCEDURES

1. Connect the phone line (RJ-11) from Hurricane 5200C/5201 to the wall phone socket.
2. Connect the network cable (RJ-45) from your PC LAN port (network card) to Hurricane 5200C/5201 Ethernet (LAN) port.
3. Connect the 12V power adapter.

4 Software Configuration

When you switch ON the modem/router, the system will boot up and connect to ADSL automatically. The system provides PVC for bridge test by default. These default configurations for the system are listed as below.

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

You can change the settings via WEB browser. The following sections will describe the set-up procedures.
Please configure your PC's LAN port as followed:

- IP address: **192.168.1.xxx** ***(e.g. 192.168.1.10)***
- Net Mask: **255.255.255.0**

Then, access the Web Console using the steps below:

- Start your web browser.
- Type the LAN IP address of the modem/router on the address bar of the browser. The default IP address is 192.168.1.1.

Once you are connected to the ADSL2+ router, you will see the status page.

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

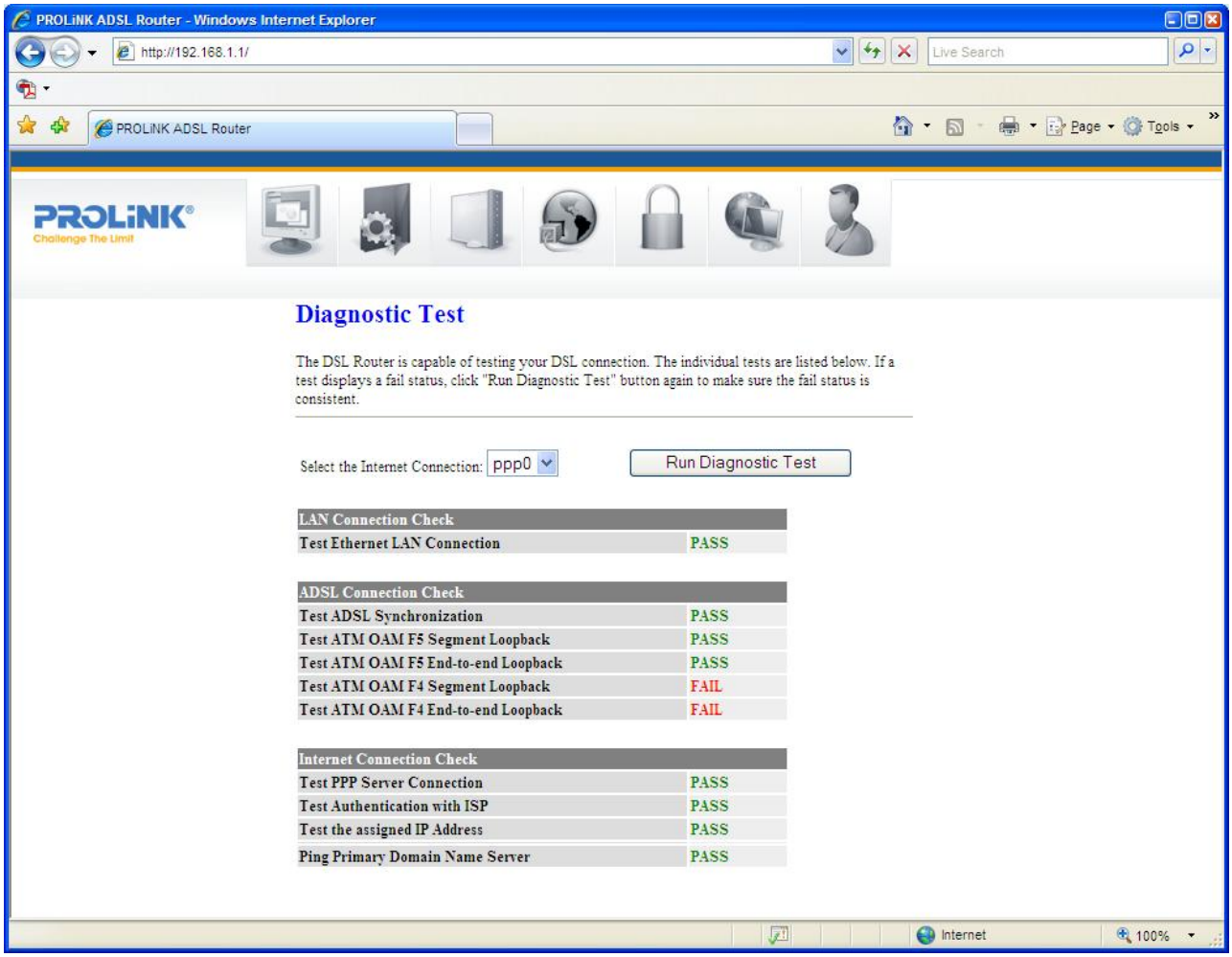
Function buttons in this page:

Connect / Disconnect

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

4.1 DIAGNOSTIC TEST

The Diagnostic Test page shows the test results for the connectivity of the physical and protocol layers.



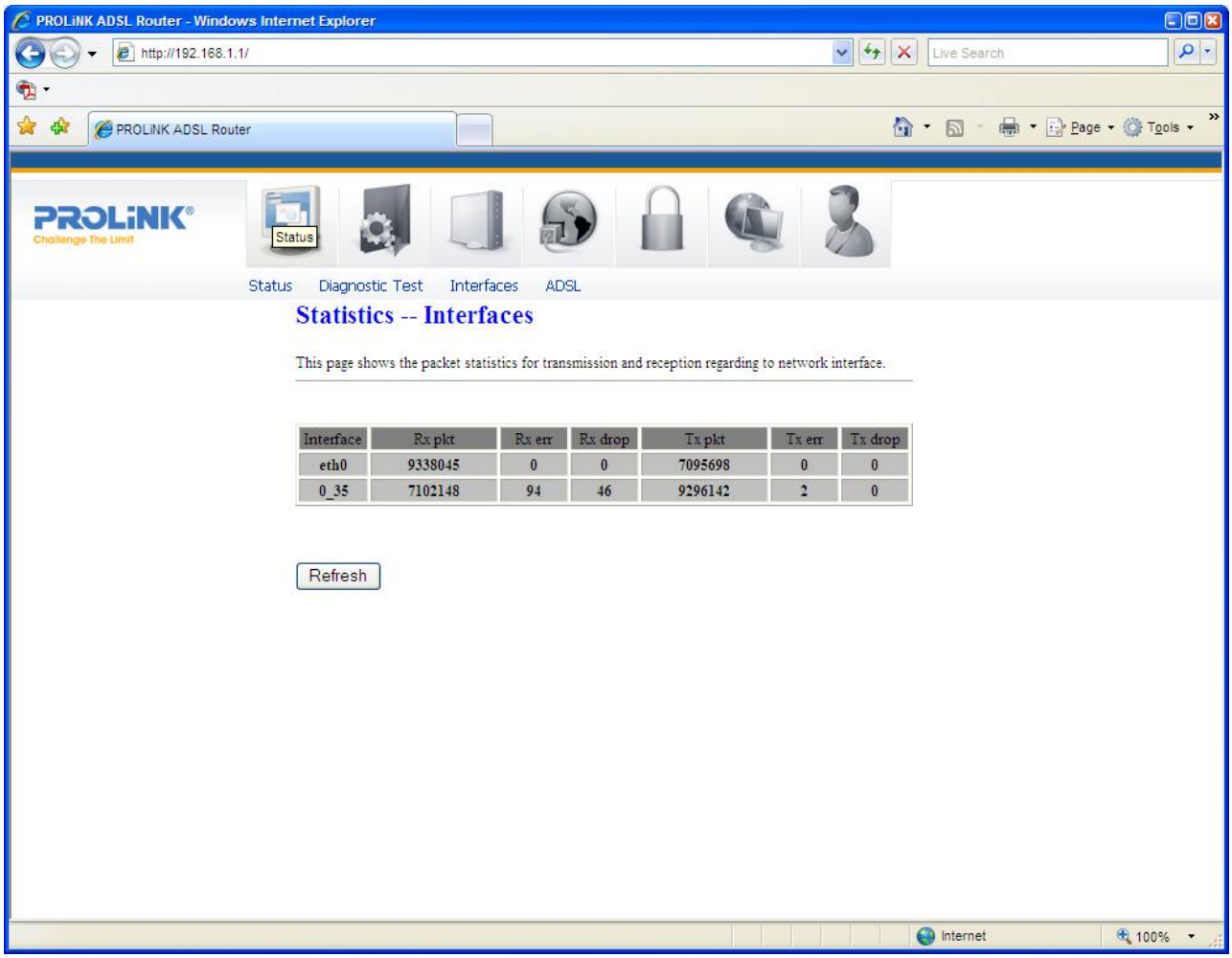
Fields in this page:

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

4.2 STATISTICS – INTERFACES

The modem/router shows the different layer of network statistics information.

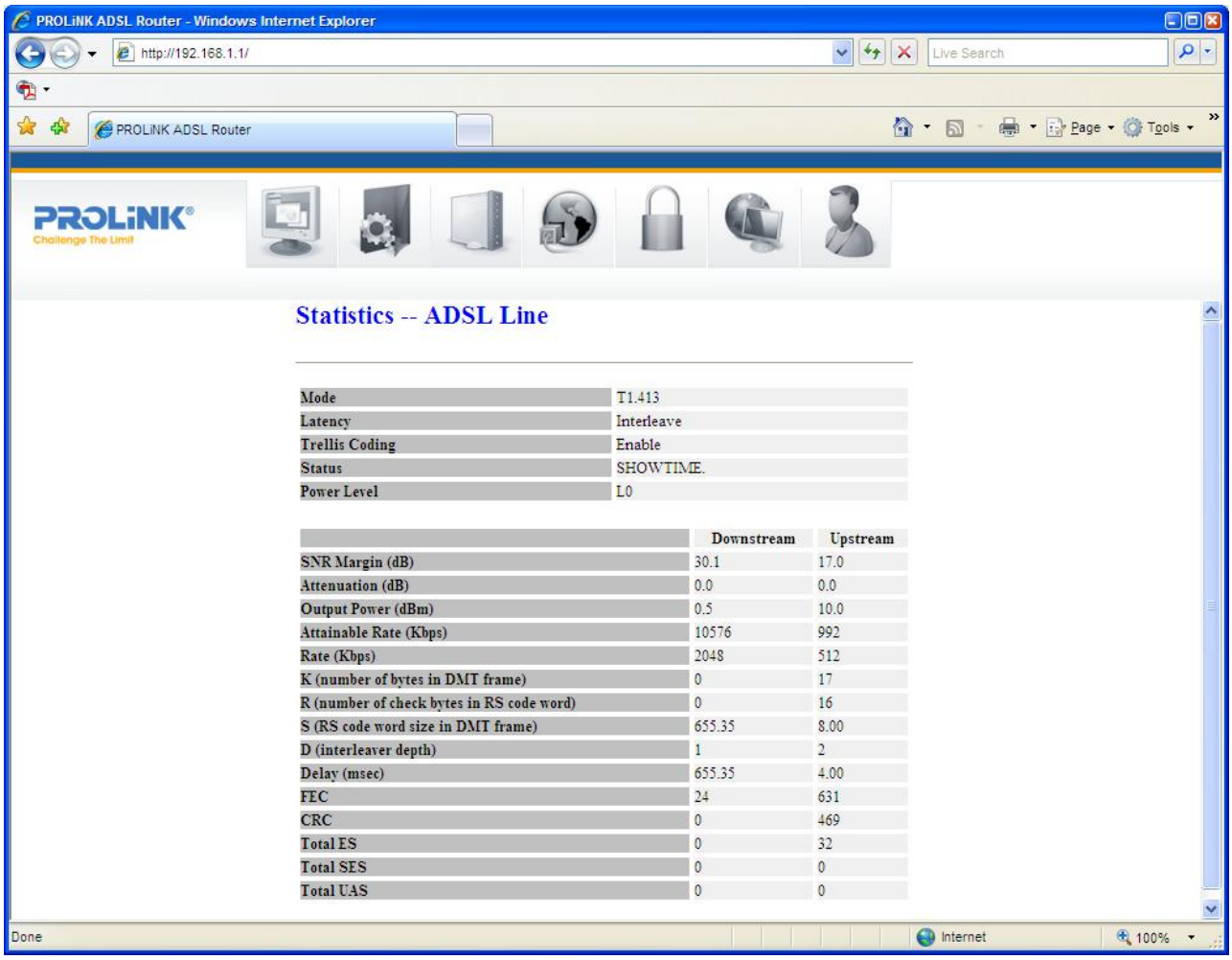
You can view statistics on the processing of IP packets on your networking interfaces. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.



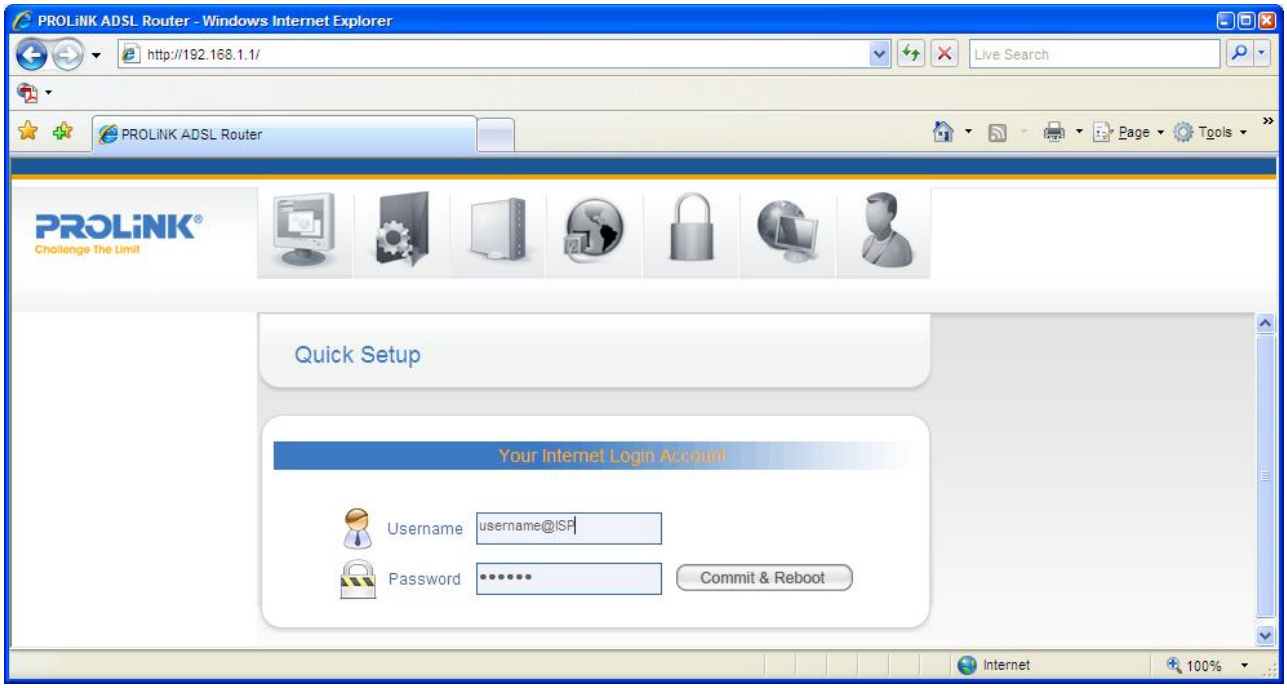
Click **Refresh** to display updated statistics showing any new data.

4.4 STATISTICS – ADSL LINE

This page shows the ADSL line statistic information.



5 Quick Setup



Fields in this page:

Field	Description
Username	Enter your login username provided by your ISP (Internet Service Provider).
Password	Enter your password provided by ISP.

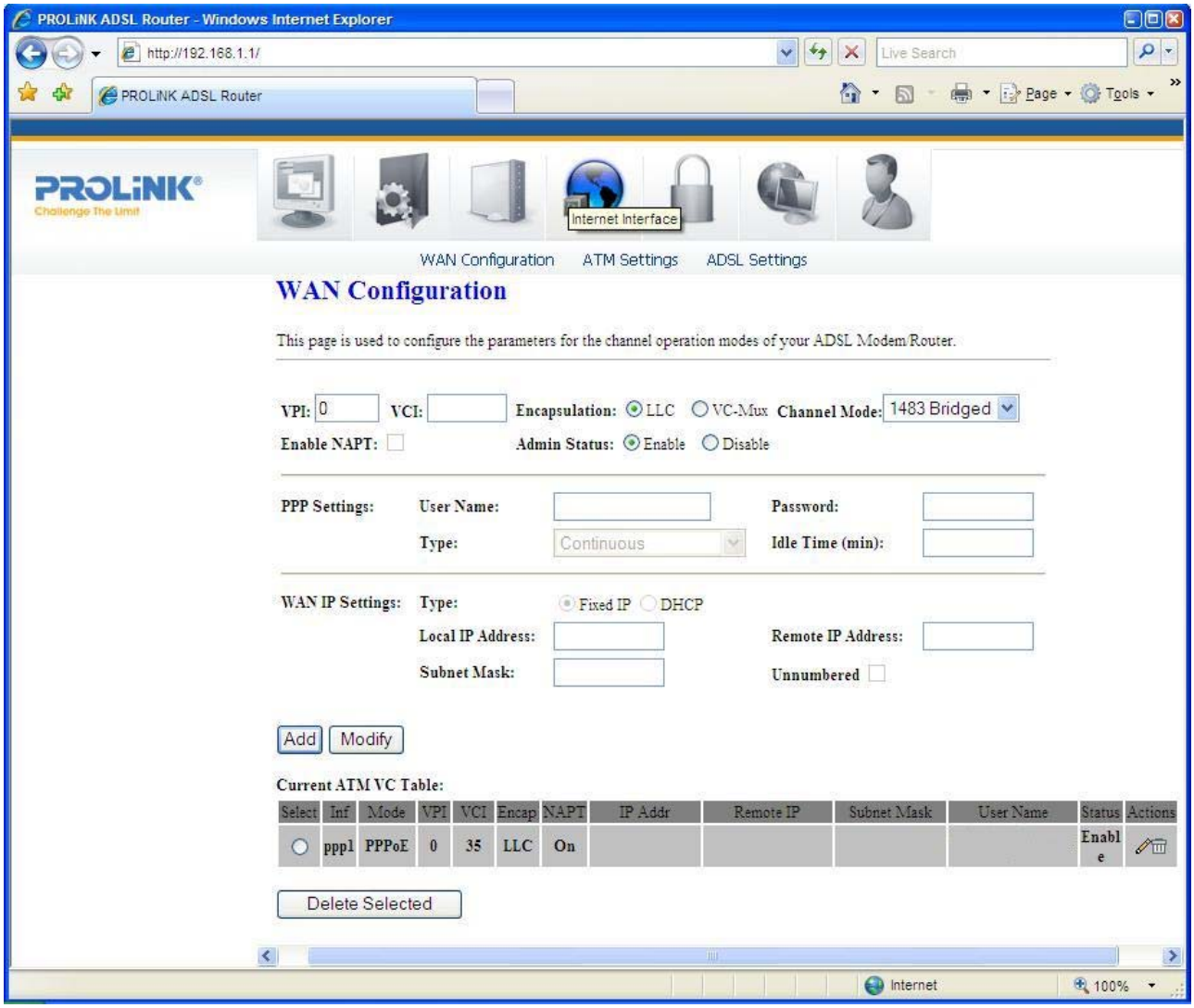
Function buttons in this page:

Commit & Reboot

To apply and save changes to flash memory.

6 Internet Interface

6.1 WAN CONFIGURATION



Function buttons in this page:

Add

Click **Add** to complete the WAN Configuration setup and add this PVC channel into the **Current ATM VC Table**.

Modify

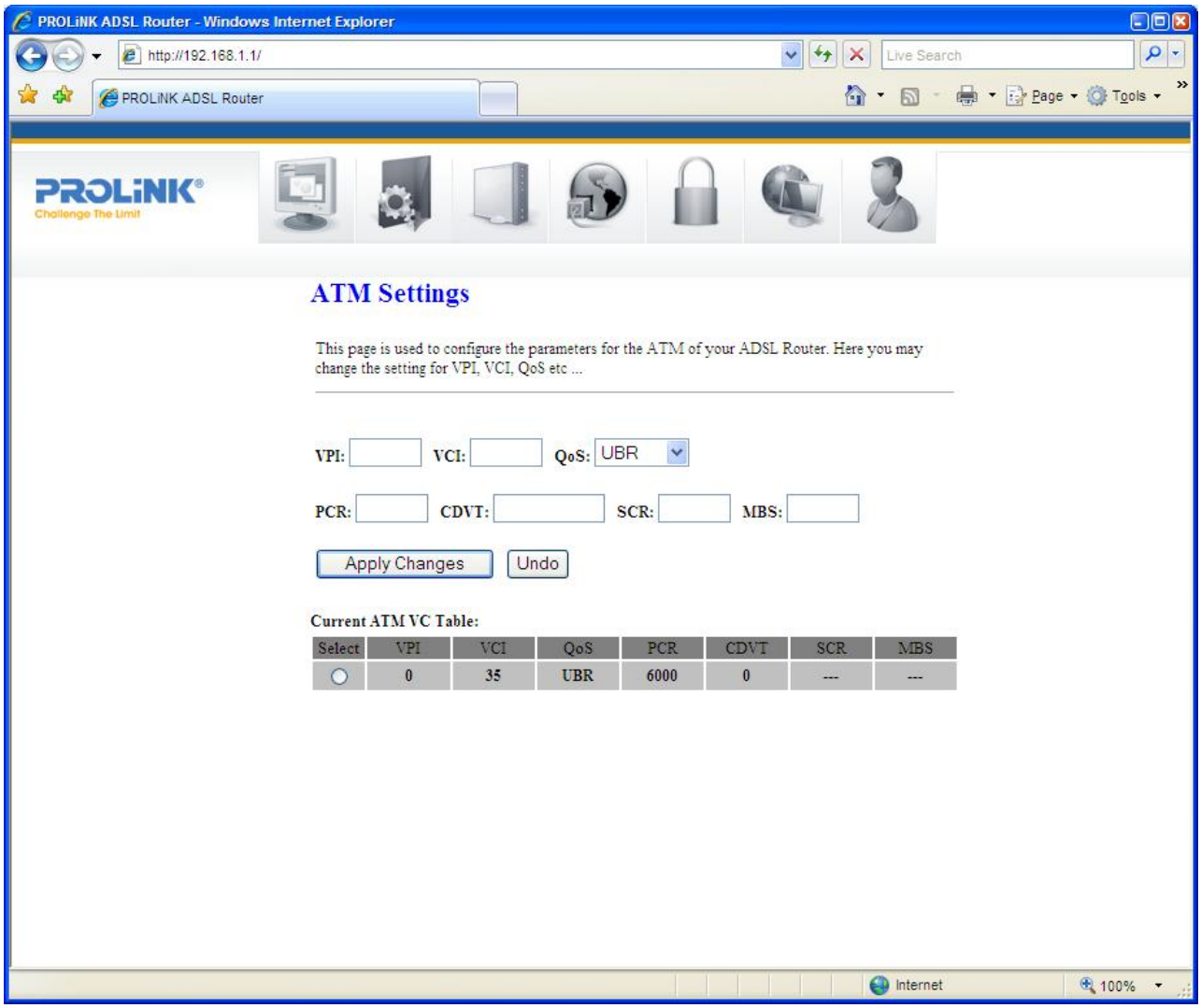
Select an existing PVC channel by clicking the radio button at the **Select** column of the **Current ATM VC Table** before you can modify the PVC channel. After selecting a PVC channel, you can modify the channel configuration at this page. Click **Modify** to complete the channel modification and apply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

Delete Selected

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.

6.2 ATM SETTING

This page is used for ATM PVC QoS parameters setting. The modem supports 4 QoS mode —CBR/rt-VBR/nrt-VBR/UBR.



Fields in this page:

Field	Description
VPI	Virtual Path Identifier. This is a read-only field and is selected on the **Select** column in the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is a 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

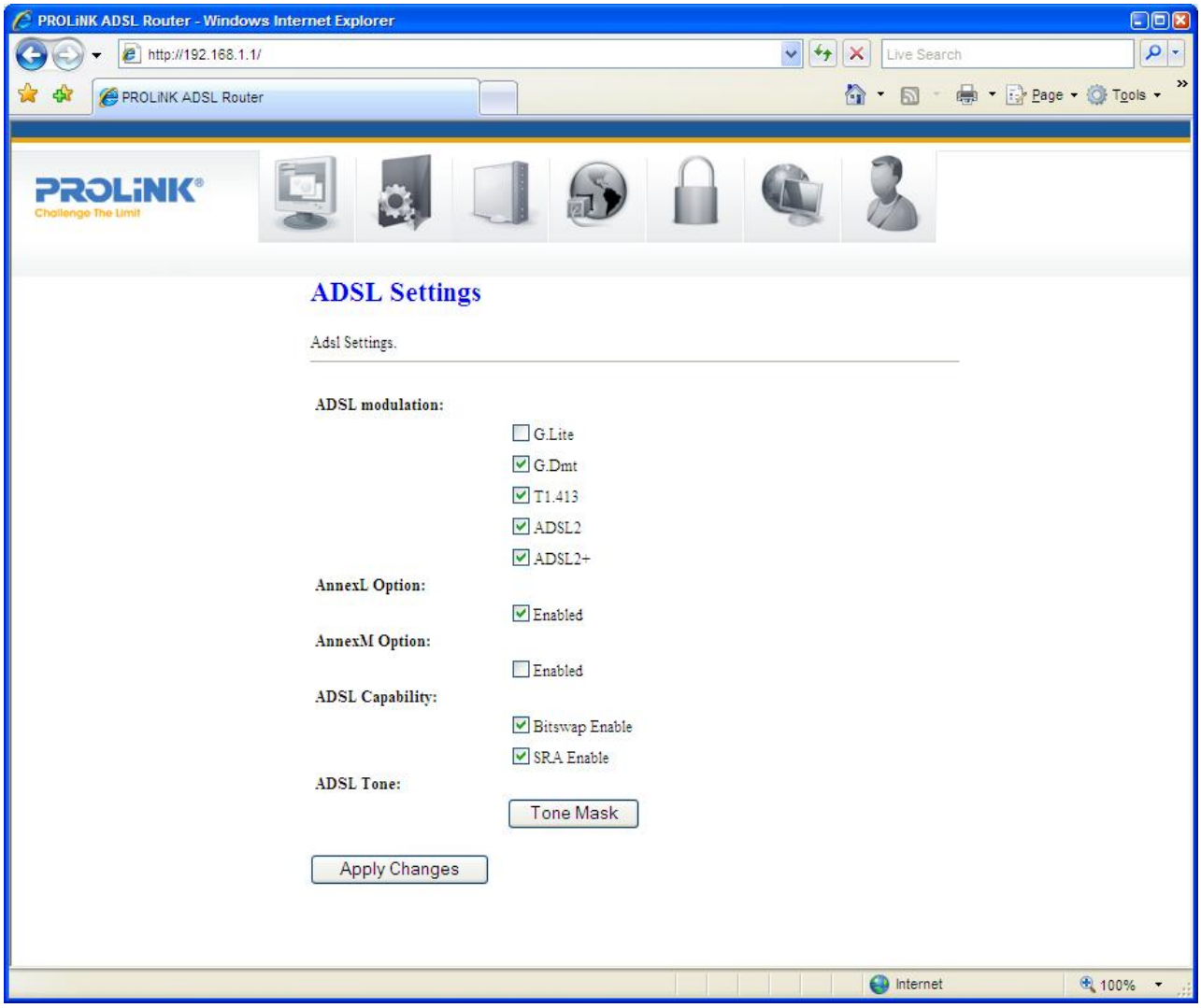
Set new PVC QoS mode for the selected PVC. New parameters will take effect after the setting is saved into flash memory and the system is rebooted *(see section "Admin" for save details)*.

Undo

Discard your settings.

6.3 ADSL SETTINGS

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



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	“Bitswap Enable” : Enable/Disable bitswap capability.

	“SRA Enable” : Enable/Disable SRA (seamless rate adaptation) capability.

Function buttons in this page:

Tone Mask

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

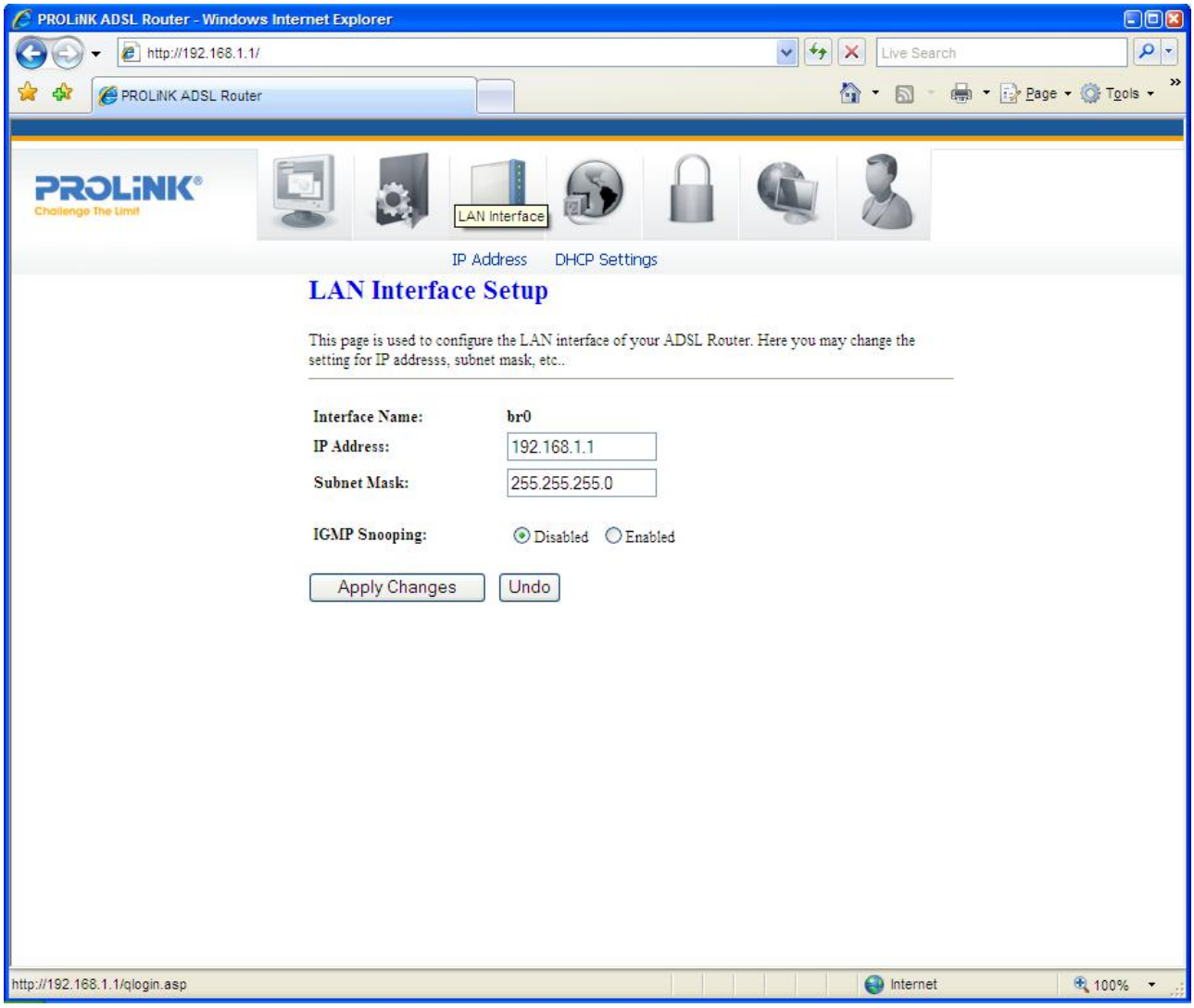
Apply Changes

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

7 LAN INTERFACE

7.1 IP ADDRESS

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



Fields in this page:

Field	Description
IP Address	The IP address that your LAN hosts (or PCs) use to identify the modem/router's LAN port. In short, this is the modem/router's LAN IP address.
Subnet Mask	LAN subnet mask.
IGMP Snooping	Enable/disable the IGMP snooping function for multiple bridged LAN ports.

Function buttons in this page:

Apply Changes

Click to save the settings into flash memory. New parameters will take effect after system is rebooted *(automatically).*

Undo

Discard your changes.

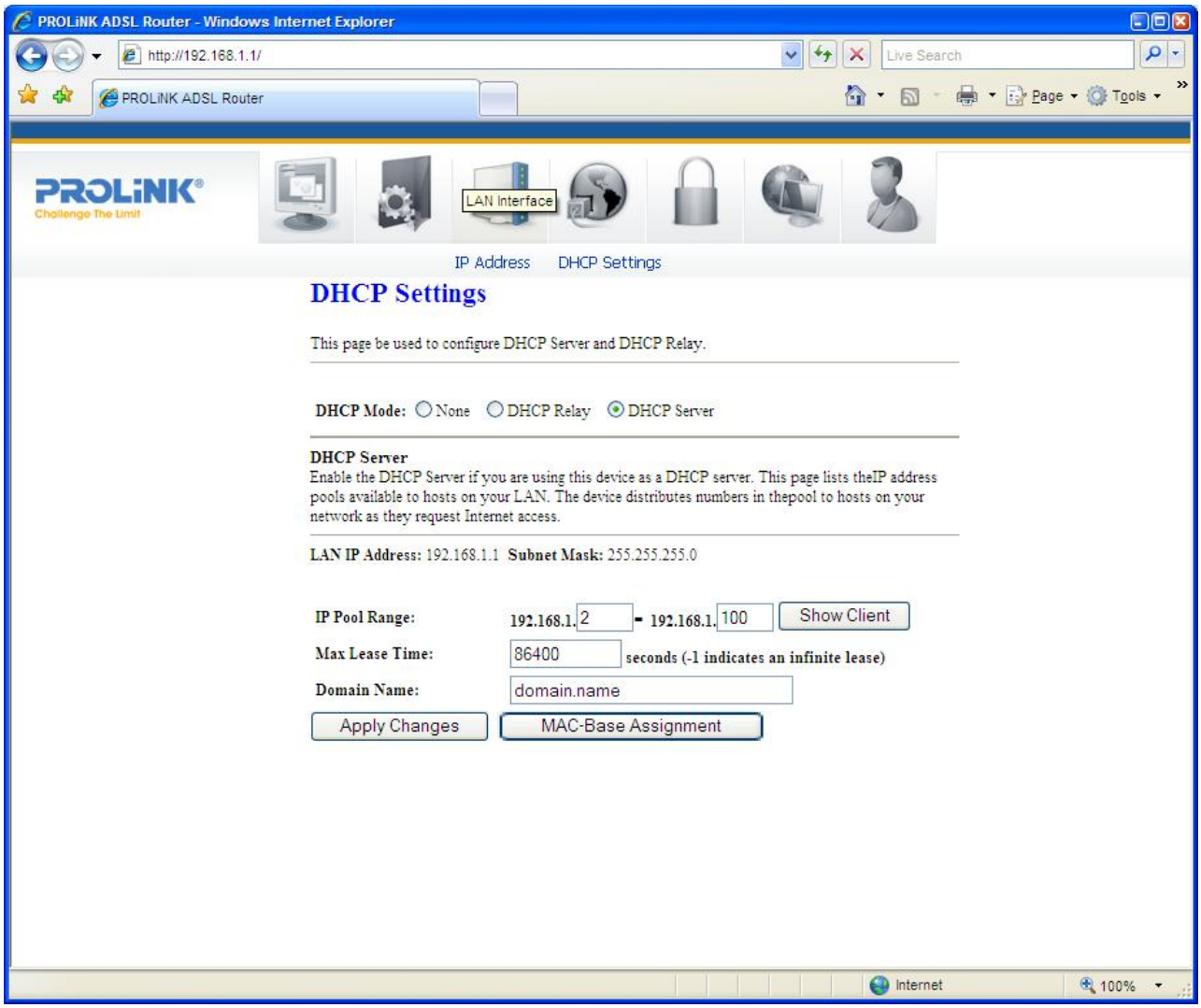
7.2 DHCP SETTINGS

DHCP Mode

You can configure your network and the modem/router 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 modem/router wants to play. There are two different DHCP roles that this modem/router can act as: DHCP Server and DHCP Relay. When acting as a DHCP server, you can setup the server parameters at the **DHCP Server** page *(by selecting this option as DHCP mode)*; while acting as DHCP Relay, you can setup the relay at the **DHCP Relay** page.

DHCP Server Configuration

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



Fields in this page:

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

Function buttons in this page:

Show Client

The pop-up window will list a table of each connected DHCP client PCs in the local network *(in terms of assigned IP address, MAC address and leased time)*.

Apply Changes

Set new DHCP server configuration. New parameters will take effect after the setting is saved into flash memory and the system is rebooted *(see section "Admin" for save details)*.

MAC-Base Assignment

This page is used to assign static IP address based on MAC address. Please enter your respective MAC address and IP address in the following format:

Host MAC Address : xx-xx-xx-xx-xx-xx (e.g. 00-d0-59-c6-12-43)

Assigned IP Address : xxx.xxx.xxx.xxx (e.g. 192.168.1.100)

Assign IP

Click on **Assign IP** button to apply your settings.

Delete Assigned IP

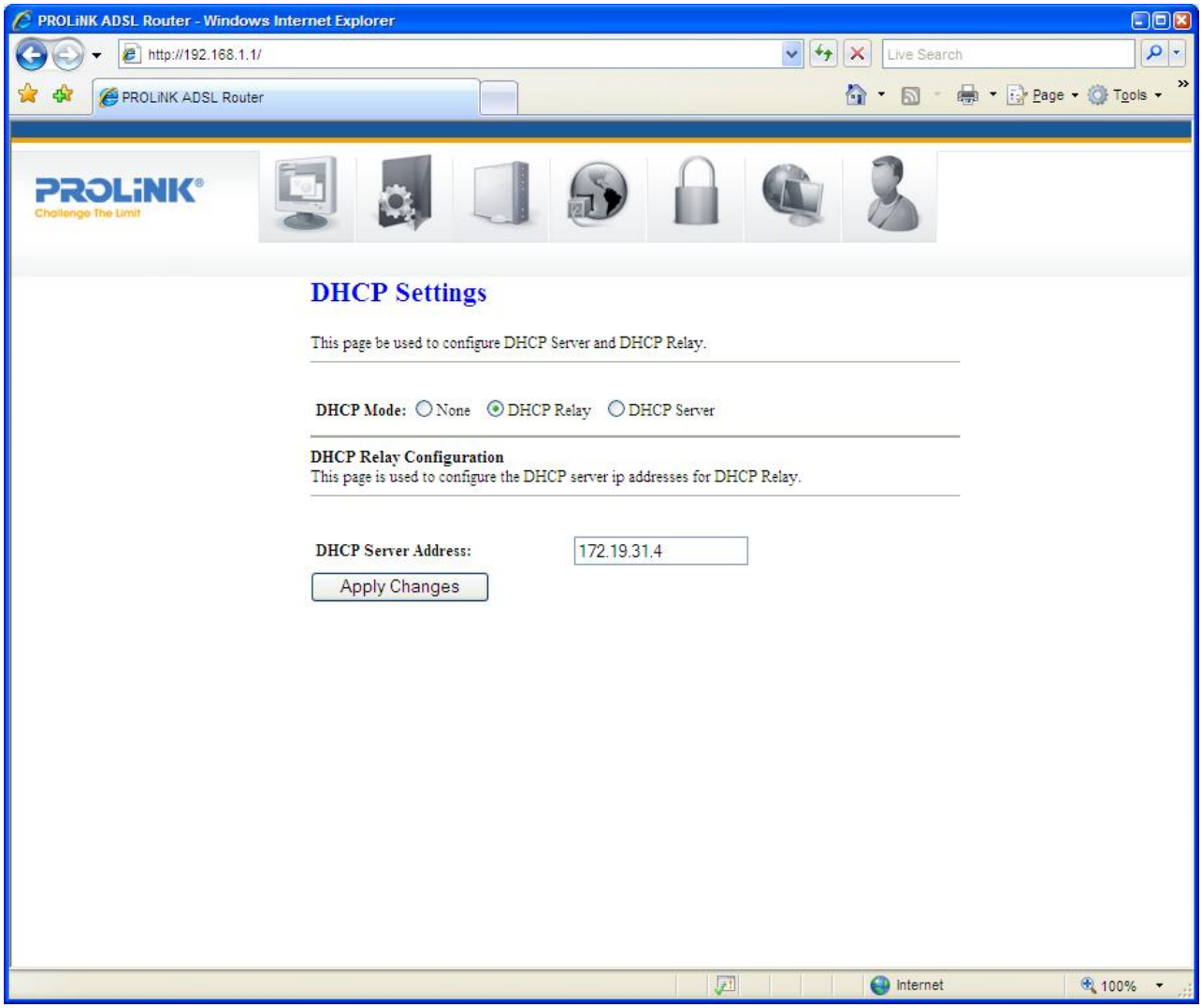
Select an existing entry to be deleted by clicking the radio button at the **Select** column of the **MAC-Base Assignment Table**. Click **Delete Assigned IP** to delete this entry from configuration.

Close

Exit from this page.

DHCP Relay Configuration

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



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

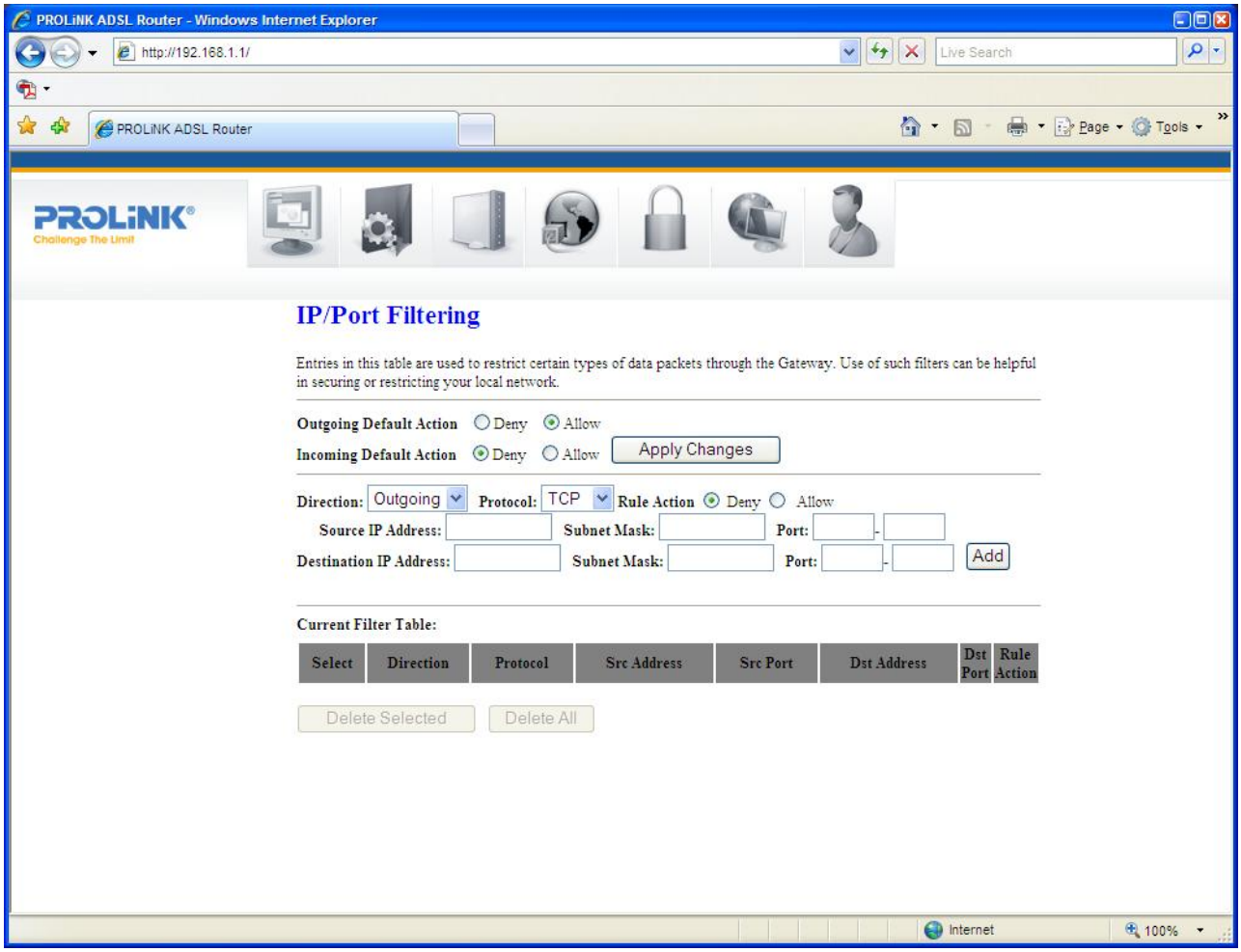
Apply Changes

Click to save the setting to the configuration.

8 Firewall Configuration

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

8.1 IP/PORT FILTERING



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

Fields settings on the first block:

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

Function button for the first block:

Apply Changes

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

Fields settings on the second block:

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

Function buttons for the second block:

Add

Click to save the rule entry and add to the Current Filter Table.

Function buttons for the Current Filter Table:

Delete Selected

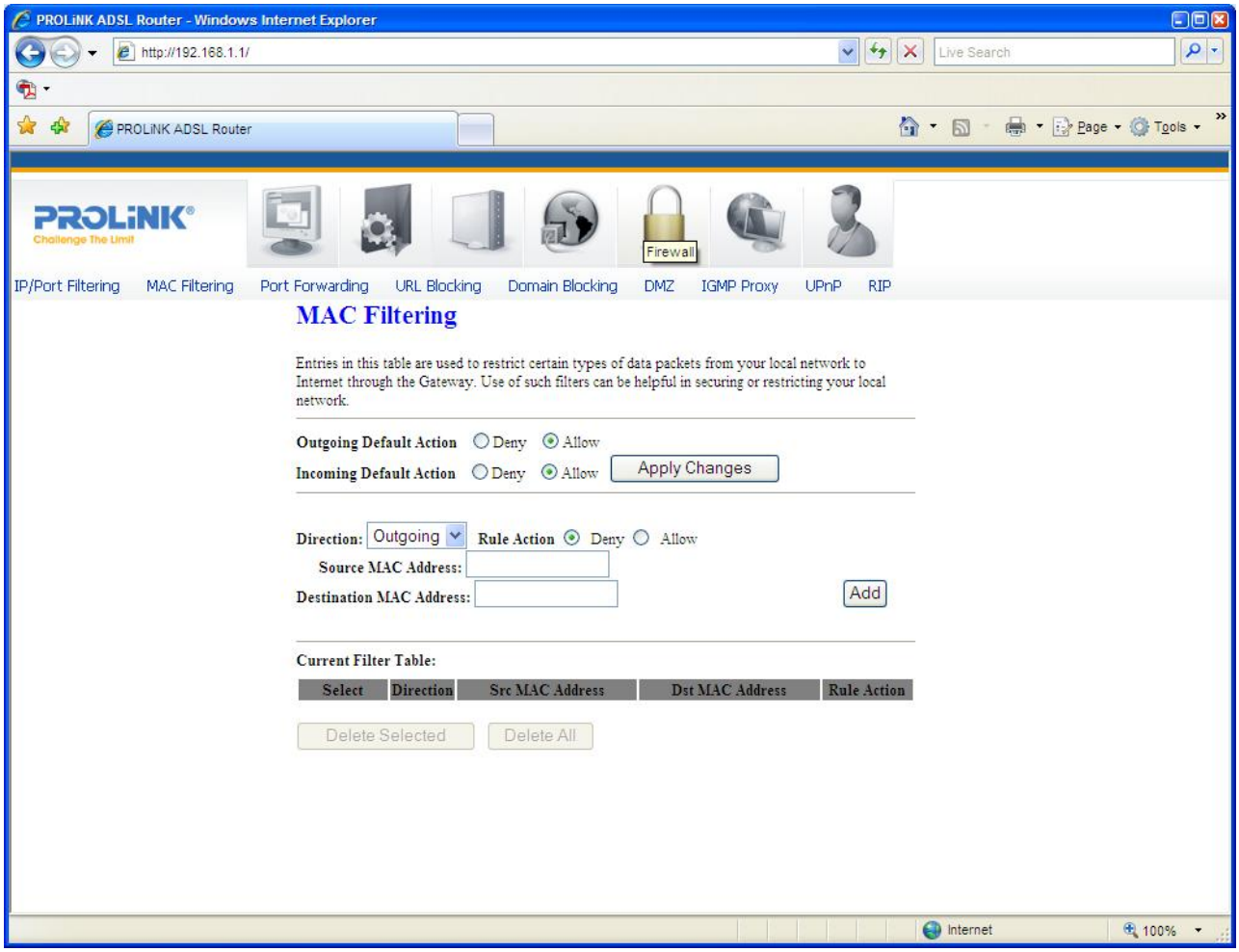
Delete selected filtering rules from the Current Filter Table. You can click the checkbox at the **Select** column to select the filtering rule.

Delete All

Delete all filtering rules from the Current Filter Table.

MAC FILTERING

The MAC filtering feature allows you to deny/allow frames through the modem/router based on source MAC address, destination MAC address, and traffic direction.



Fields settings on the first block:

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

Function button for the first block:

Apply Changes

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

Fields settings on the second 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 will be 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 will be considered as "*don't care*".

Function buttons for the second block:

Apply Changes

Click to apply the rule entry to the configuration.

Function buttons for the Current Filter Table:

Delete Selected

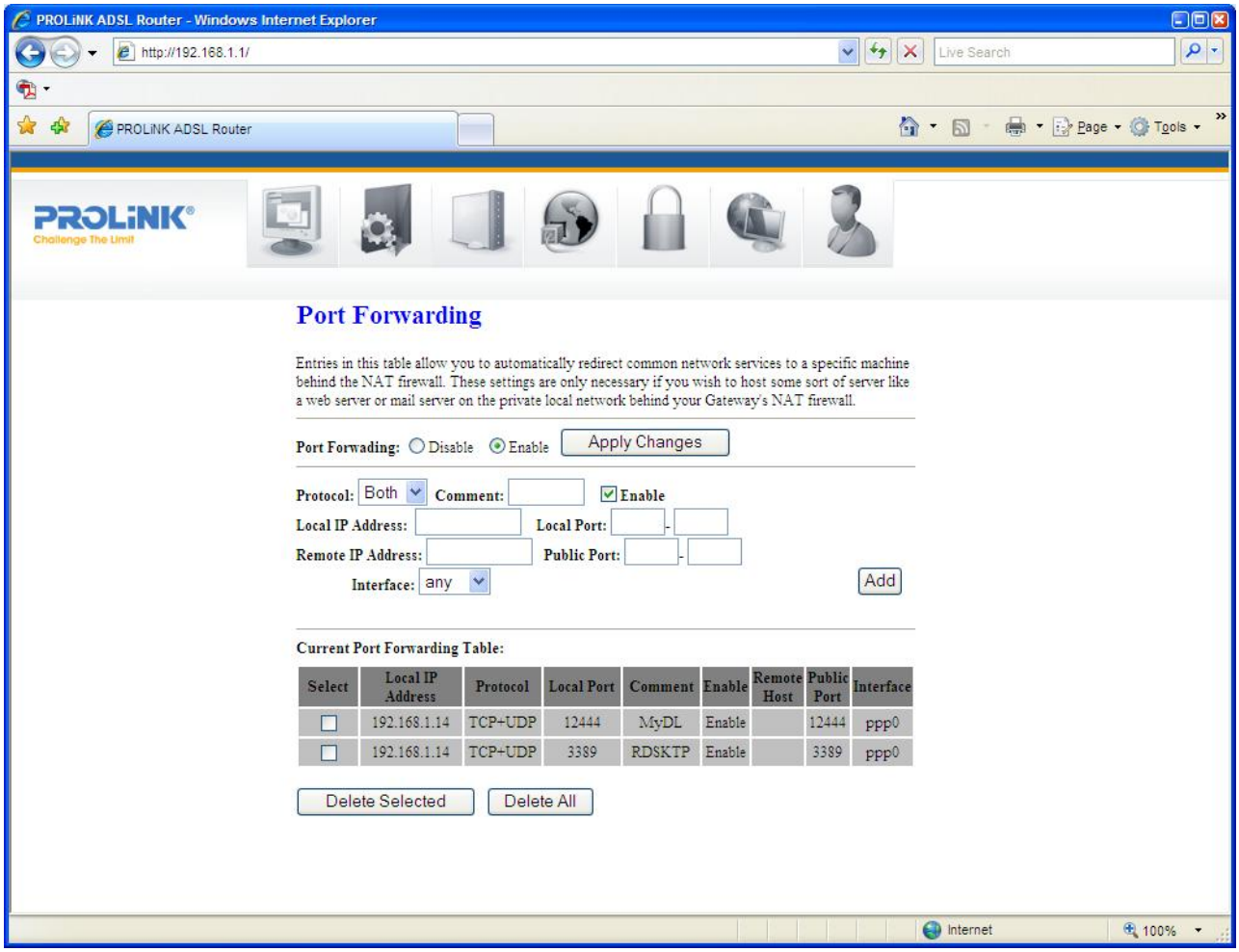
Delete selected filtering rules from the Current Filter Table. You can click the checkbox at the **Select** column to select the filtering rule.

Delete All

Delete all filtering rules from the Current Filter Table.

8.3 PORT FORWARDING

Firewall keeps unwanted traffic in the Internet away from your LAN computers. By adding a Port Forwarding entry, a tunnel will be created through your firewall so that users on the Internet can initiate communication to one of the computers in your local network.



Fields in this page:

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

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

Function buttons for the setting block:

Apply Changes

Click to save the rule entry to the configuration.

Function buttons for the Current Port Forwarding Table:

Delete Selected

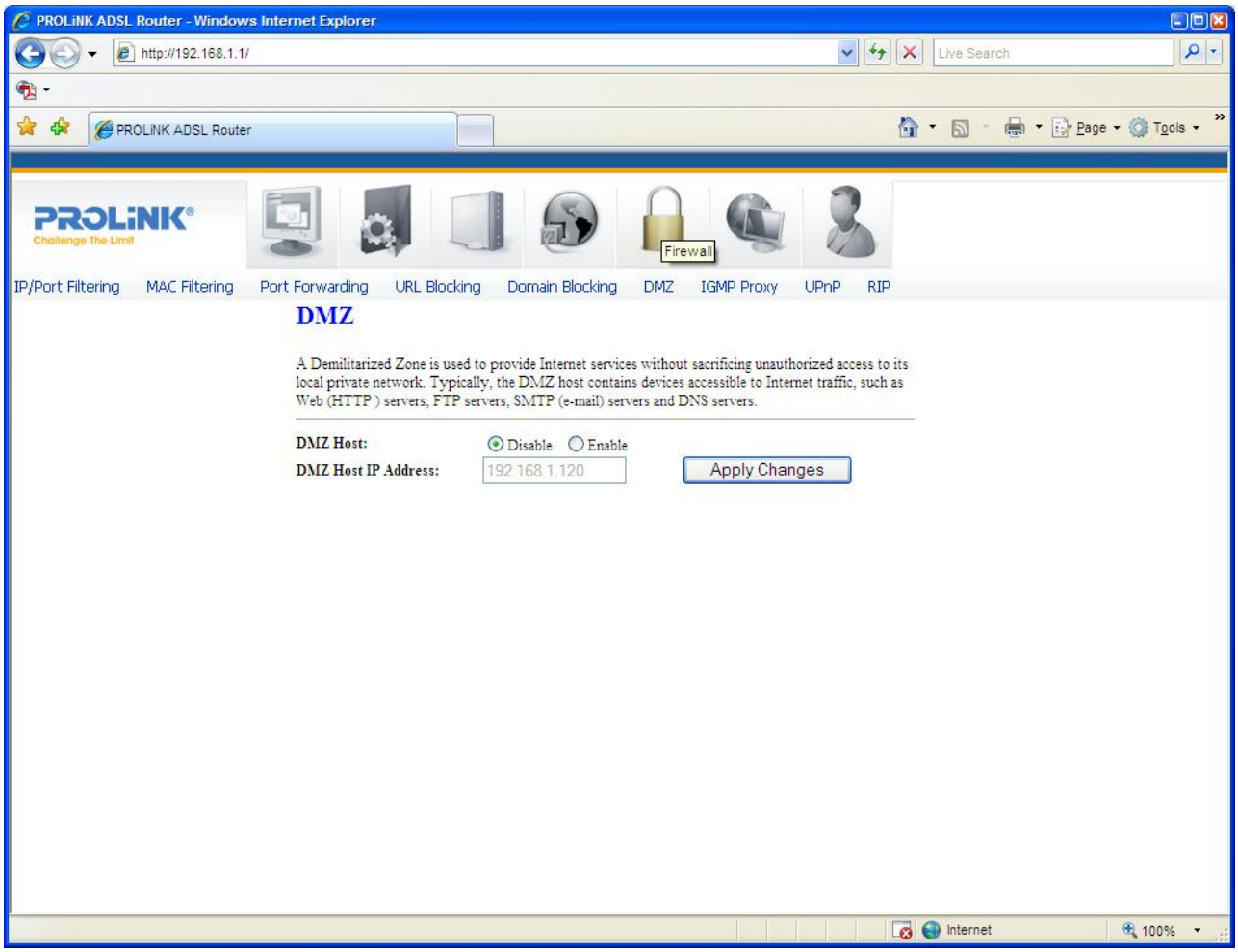
Delete the selected port forwarding rules from the forwarding table. You can click the checkbox at the **Select** column to select the forwarding rule.

Delete All

Delete all forwarding rules from the forwarding table.

8.6 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.



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.

8.7 IGMP PROXY CONFIGURATION

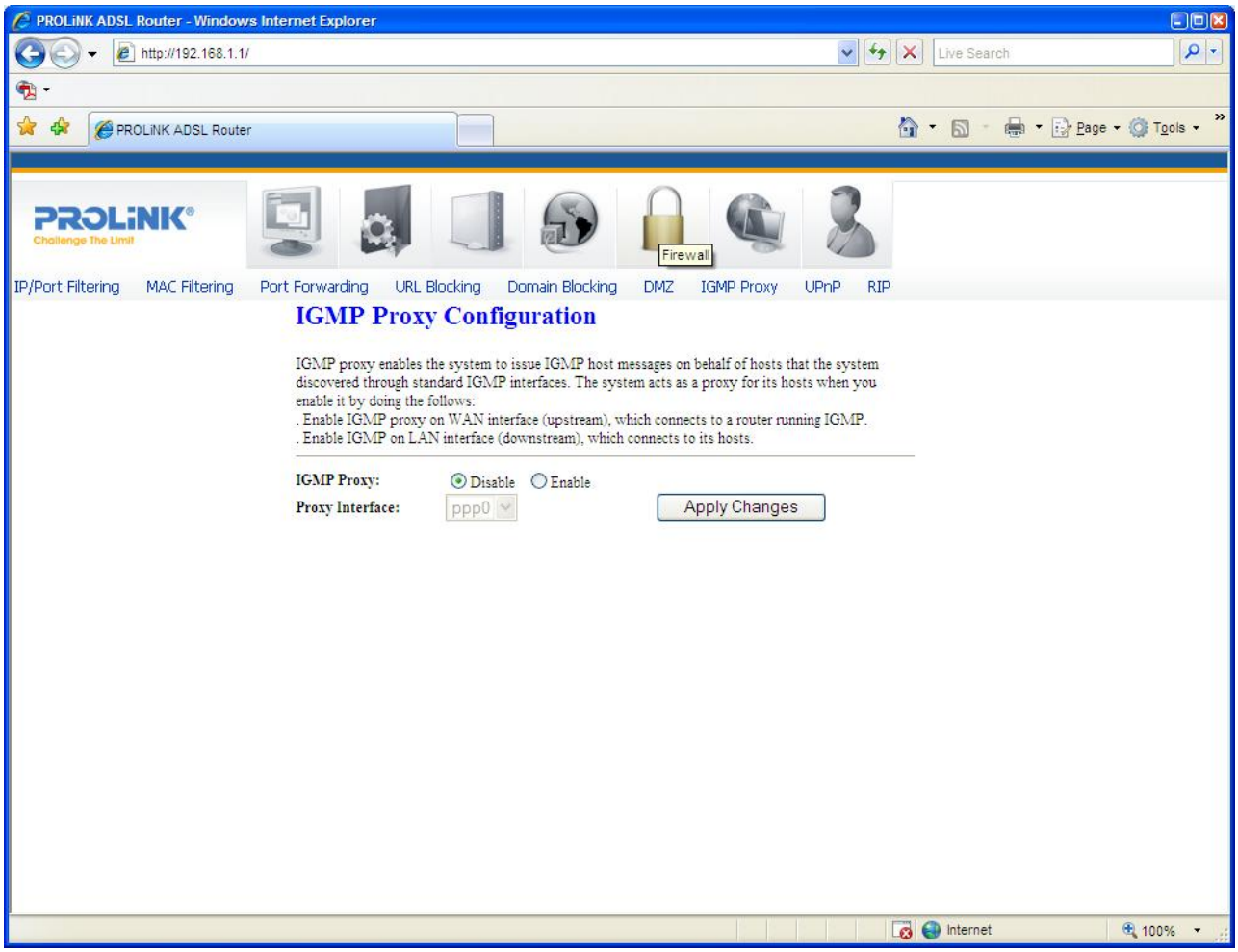
Multicasting is useful when the same data needs to be sent to more than one hosts. Using multicasting, as opposed to sending the same data to the individual hosts uses less network bandwidth. The multicast feature also enables you to receive multicast video stream from multicast servers.

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. Hurricane 5200C/5201 supports IGMP proxy that handles IGMP messages. When enabled, this modem/router 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 Hurricane 5200C'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 a 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 (LAN) is sent to the multicast router.
- **Downstream**: The interface data from the multicast router are sent to hosts (LAN) in the multicast group database.



Fields in this page:

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

Function buttons in this page:

Apply Changes

Click to save the setting to the configuration.

Undo

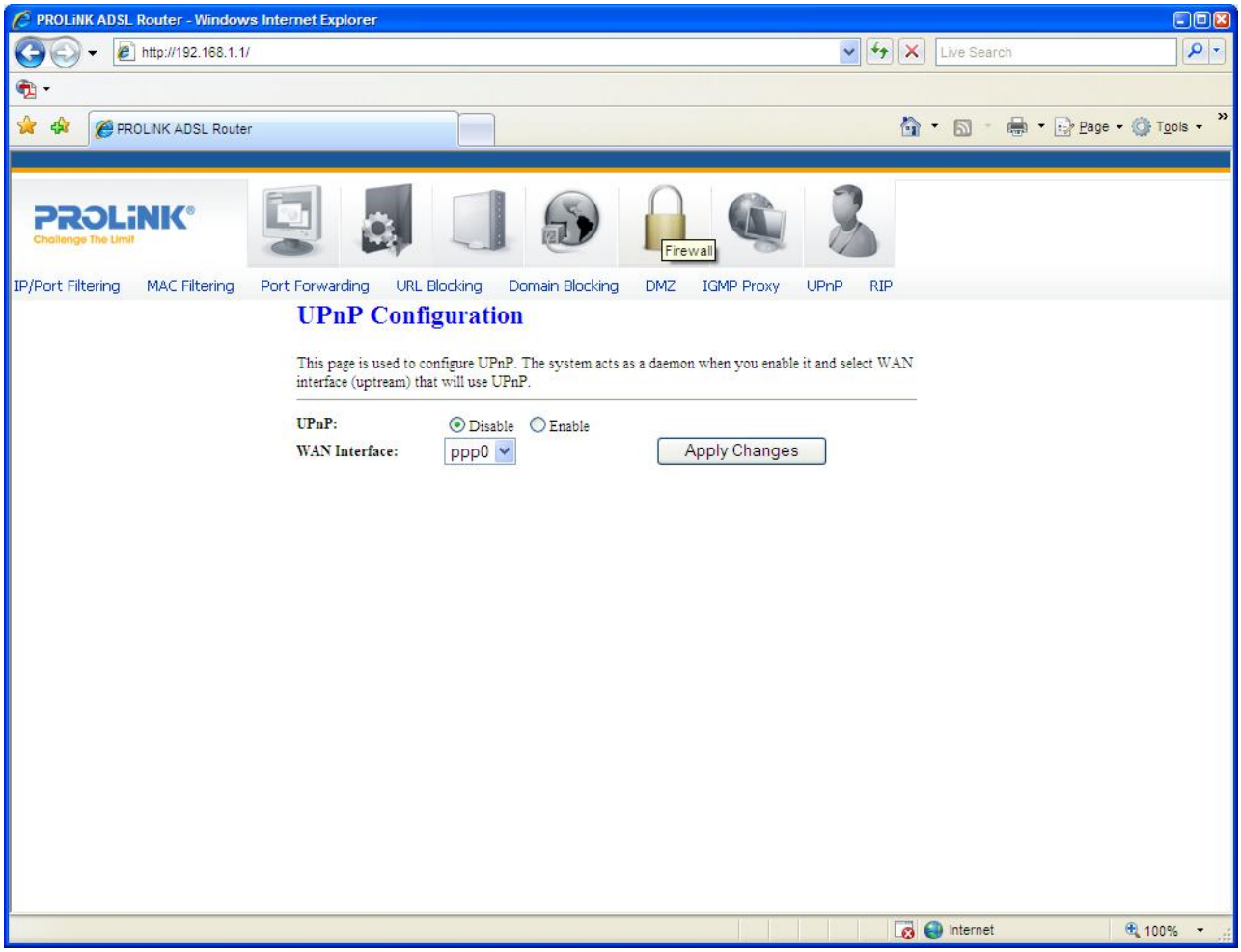
Discard your settings.

8.8 UPnP CONFIGURATION

The modem/router supports a control point for Universal Plug and Play (UPnP) version 1.0, and supports two key features: **NAT Traversal** and **Device Identification**. This feature requires one active WAN interface. In addition, the host should support this feature. In the presence of multiple WAN interfaces, select an interface on which the incoming traffic is present.

With NAT Traversal, when UPnP command is received to open ports in NAT, the application translates the request into system commands to open the ports in NAT and the firewall.

For Device Identification, the application will send a description of the modem/router as a control point back to the host making the request.



Fields in this page

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

Function buttons in this page:

Apply Changes

Click to save the setting to the system configuration.

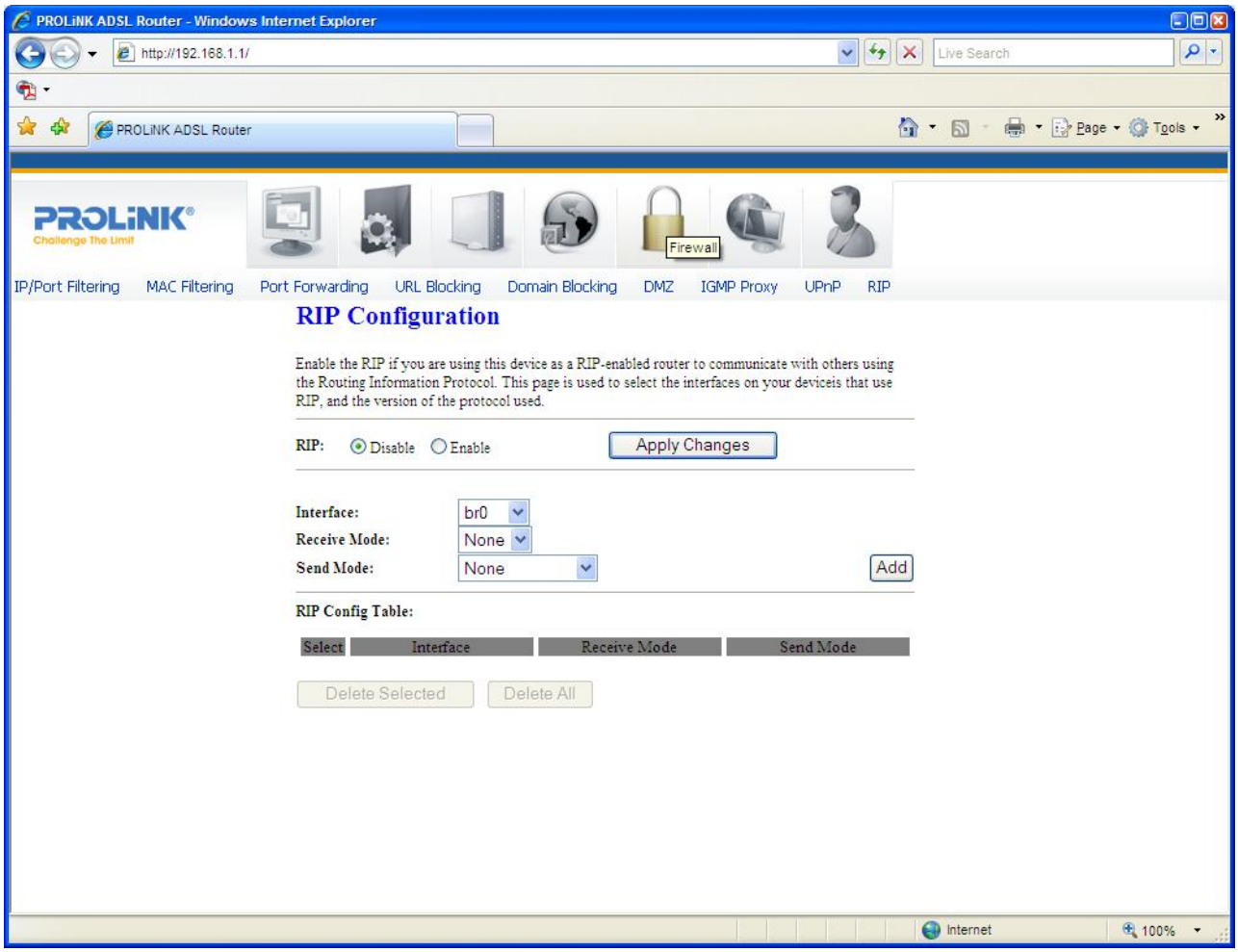
8.9 RIP CONFIGURATION

RIP (Routing Information Protocol) is an Internet protocol that 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 LAN via ADSL line.

Most home or small 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 this case, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

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

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



Fields settings on the first 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 block to the system configuration

Fields settings on the second 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 modem/router in order for it to be accepted into its routing table.
Send Mode	Indicate the RIP version this interface will use when it sends its route information to other devices.

Function buttons for the second setting block in this page:

Add

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

Delete Selected Entry

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

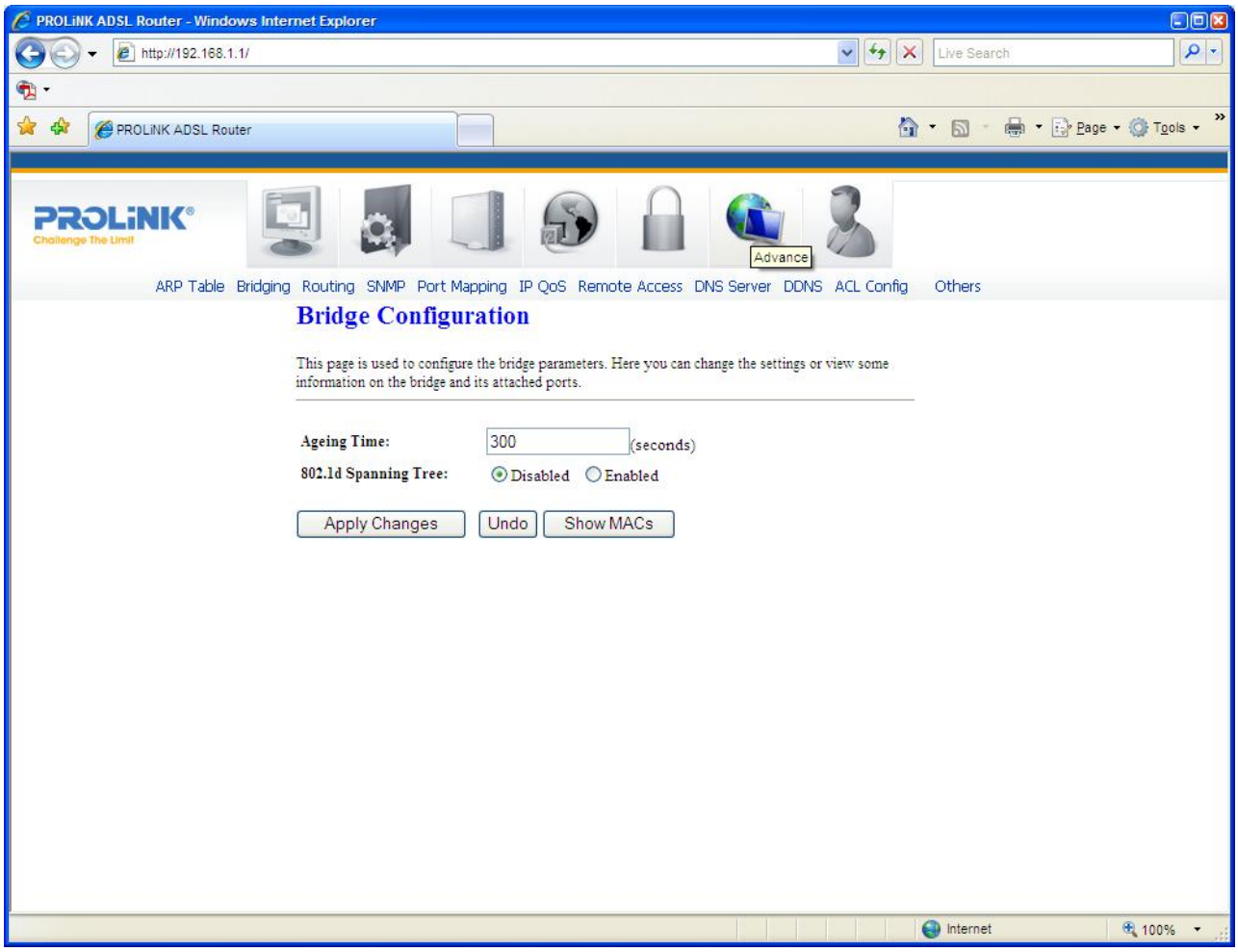
Delete All

Delete all entries in **RIP Config Table**.

9 Advance Configuration

9.1 BRIDGING

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



Fields in this page:

Field	Description
Ageing Time	Set the Ethernet address ageing time, in seconds. After [Ageing Time] seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from Forwarding Database (fdb).
802.1d Spanning Tree	Enable/disable the spanning tree protocol

Function buttons in this page:

Apply Changes

Save this bridge configuration. New configuration will take effect after saving into flash

memory and rebooting the system *(See section "Admin" for details).*

Show MACs

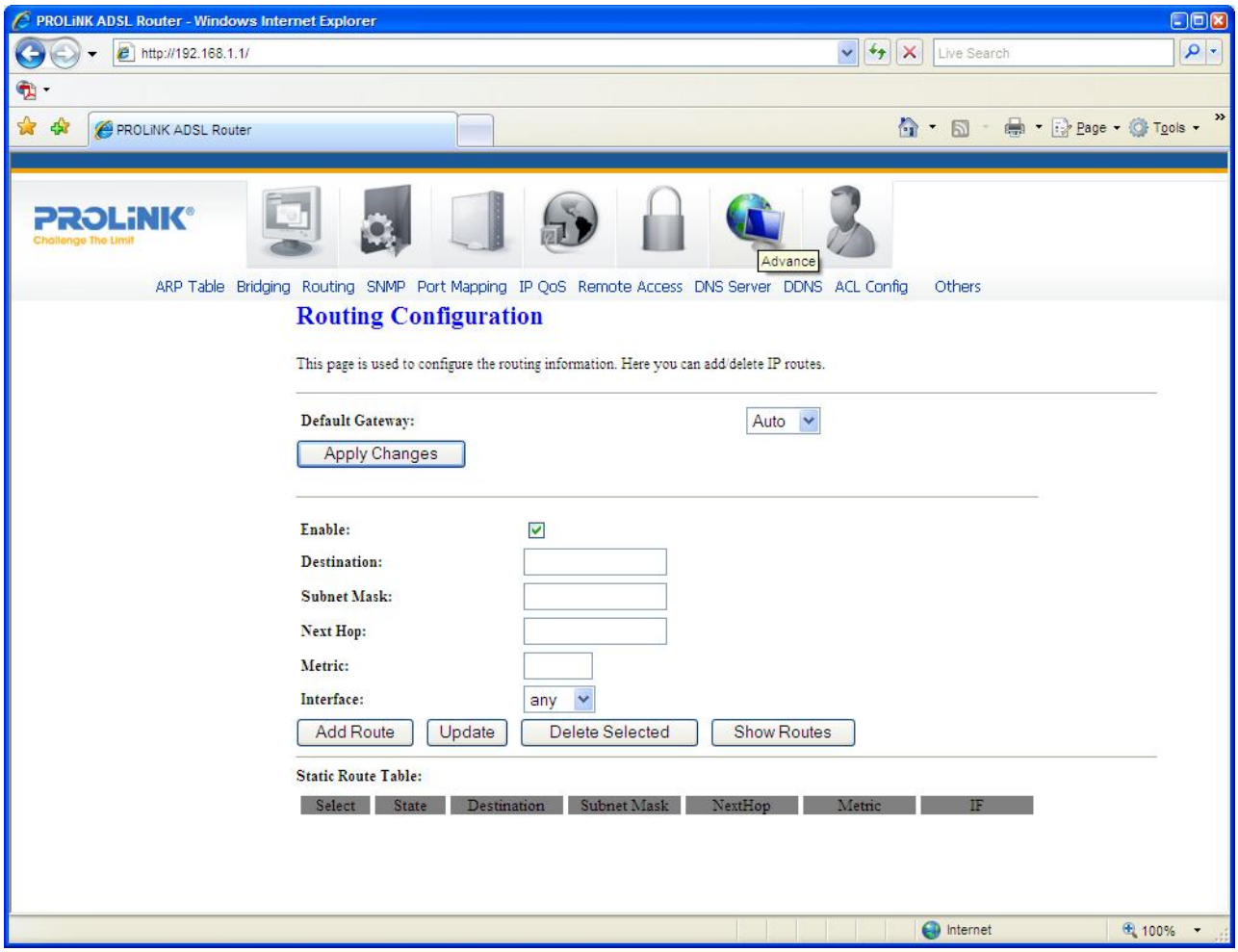
List MAC addresses in forwarding table.

9.2 ROUTING

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

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

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



Fields in this page:

Field	Description
Enable	Check to enable the selected route or route to be added.
Destination	The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined *(this is the route that creates the default gateway)*.
Subnet Mask	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
Next Hop	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.
Interface	The WAN interface to which a static routing subnet is to be applied.

Function buttons in this page:

Add Route

Add a user-defined destination route.

Update

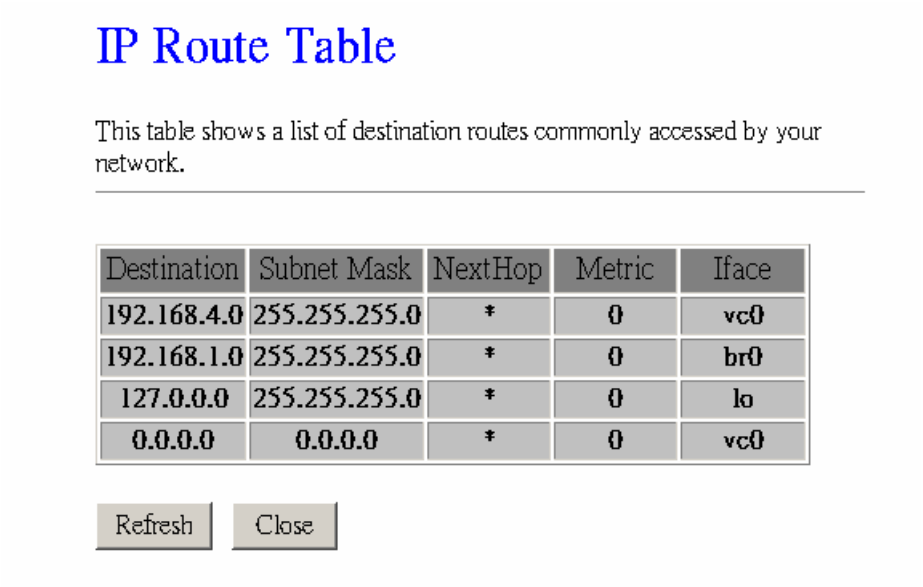
Update the selected destination route on the **Static Route Table**.

Delete Selected

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

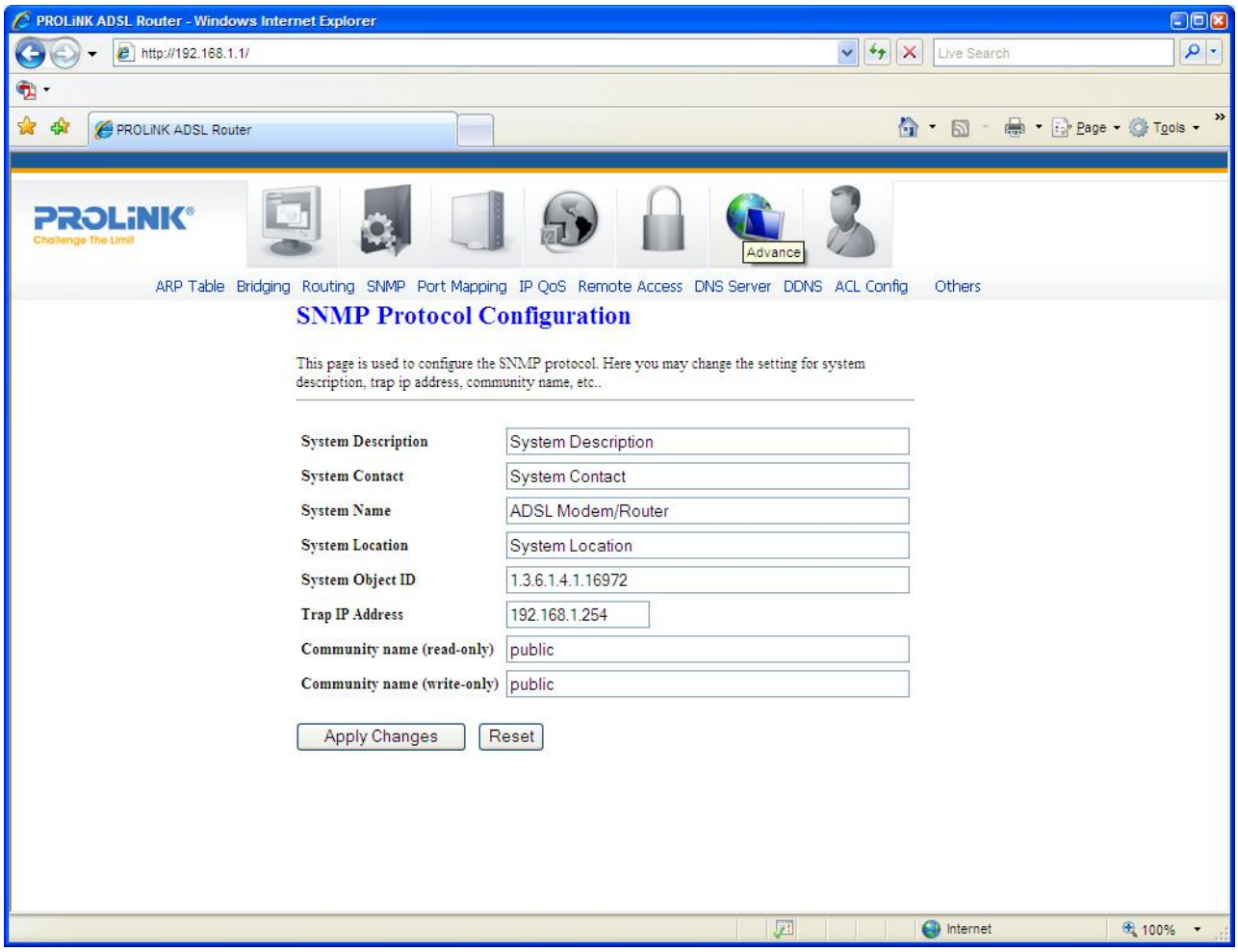
Show Routes

Click this button to view the modem/router's routing table. The IP Route Table displays, as shown in Figure below.



9.3 SNMP CONFIGURATION

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



Fields in this page:

Field	Description
System Description	System description of the modem/router.
System Contact	Contact person or contact information for the modem/router.
System Name	An administratively assigned name for the modem/router.
System Location	The physical location of the modem/router.
System Object ID	Vendor-object identifier. The vendor's authoritative identification of the network management subsystem contained in the entity.
Trap IP Address	Destination IP address of the SNMP trap.
Community name (read-only)	Name of the read-only community. This read-only community allows read operation to all objects in the MIB.
Community name	Name of the write-only community. This write-only community allows write

(write-only)	operation to the objects defines as read-writable in the MIB.

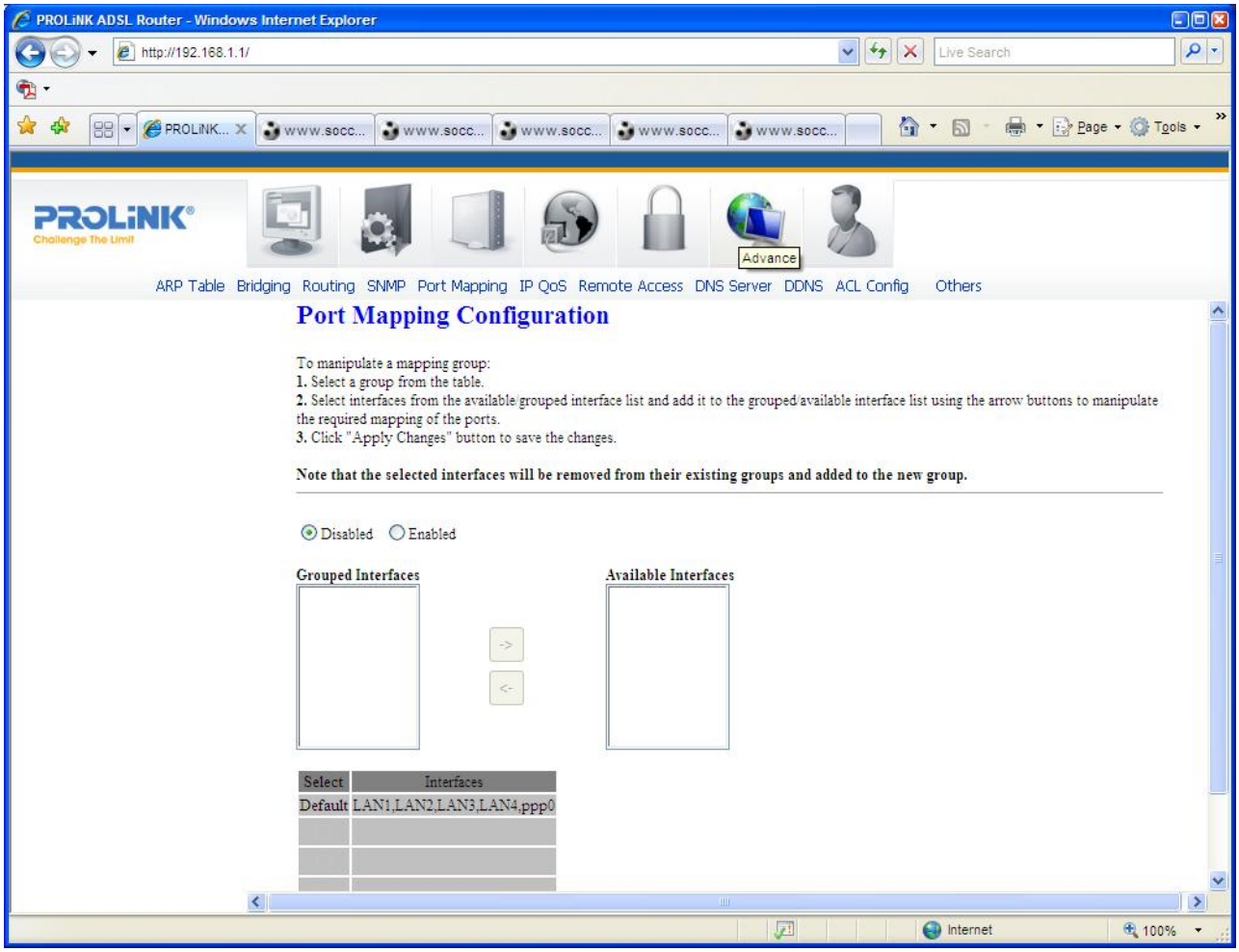
Function buttons in this page:

Apply Changes

Save SNMP configuration. New configuration will take effect after saving into flash memory and rebooting the system *(See section "Admin" for details).*

9.4 PORT MAPPING

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



Fields in this page:

Field	Description
Enabled/Disabled	Radio buttons to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.
Interface groups	To manipulate a mapping group: a. Select a group from the table. b. Select interfaces from the ***Available Interface List*** and add it to the ***Grouped Interface List*** or vice versa, using the arrow buttons to manipulate the required mapping of the ports. c. Click on "***Apply Changes***" button to save the changes.

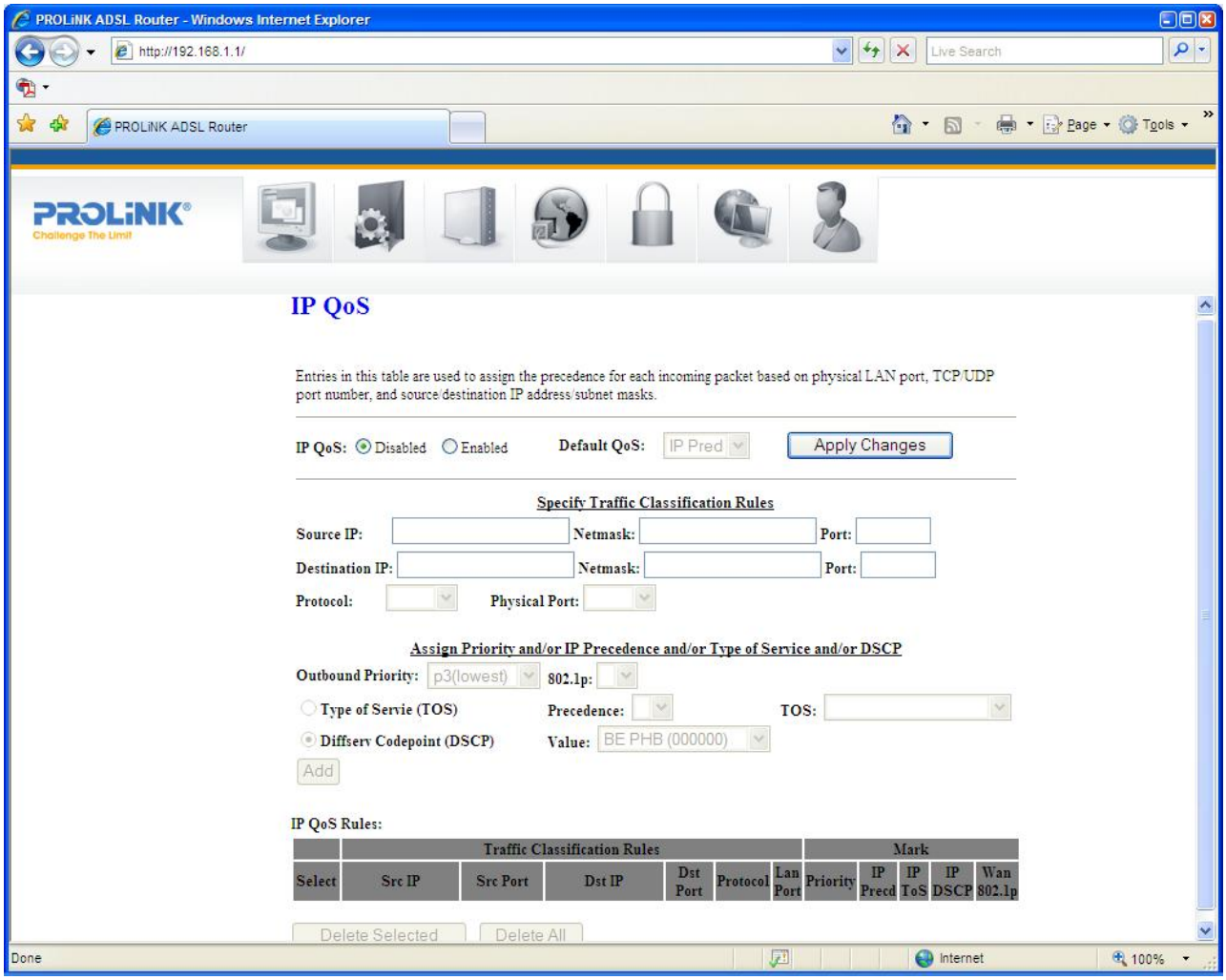
Function buttons in this page:

Apply Changes

Save configuration to system. New configuration will take effect after saving into flash memory and rebooting the system *(See section "Admin" for details).*

9.5 IP QoS

The modem/router provides a control mechanism that can provide different priority to different users or data flows. The QoS (Quality of Service) is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: **Traffic Classification** and **Action**. The Traffic Classification feature enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The Action feature enables you to assign priority level for fields in the packet that matches the Traffic Classification rule. You can configure any or all field as needed in these two QoS blocks for a single QoS rule.



Fields settings on the first block:

Field	Description
IP QoS	Enable/disable the IP QoS function.
Source IP	The IP address of the traffic source.
Source Netmask	The source IP netmask. This field is ***required*** if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Destination Netmask	The destination IP netmask. This field is ***required*** if the destination IP has been entered.
Protocol	The selections are TCP, UDP, ICMP or blank for none. This field is ***required*** if the source port or destination port has been entered.
Source Port	The source port of the selected protocol. You ***cannot*** configure this field without entering the protocol first.
Destination Port	The destination port of the selected protocol. You ***cannot*** configure this field without entering the protocol first.
Physical Port	The incoming ports. The selections including LAN ports, Wireless, or blank

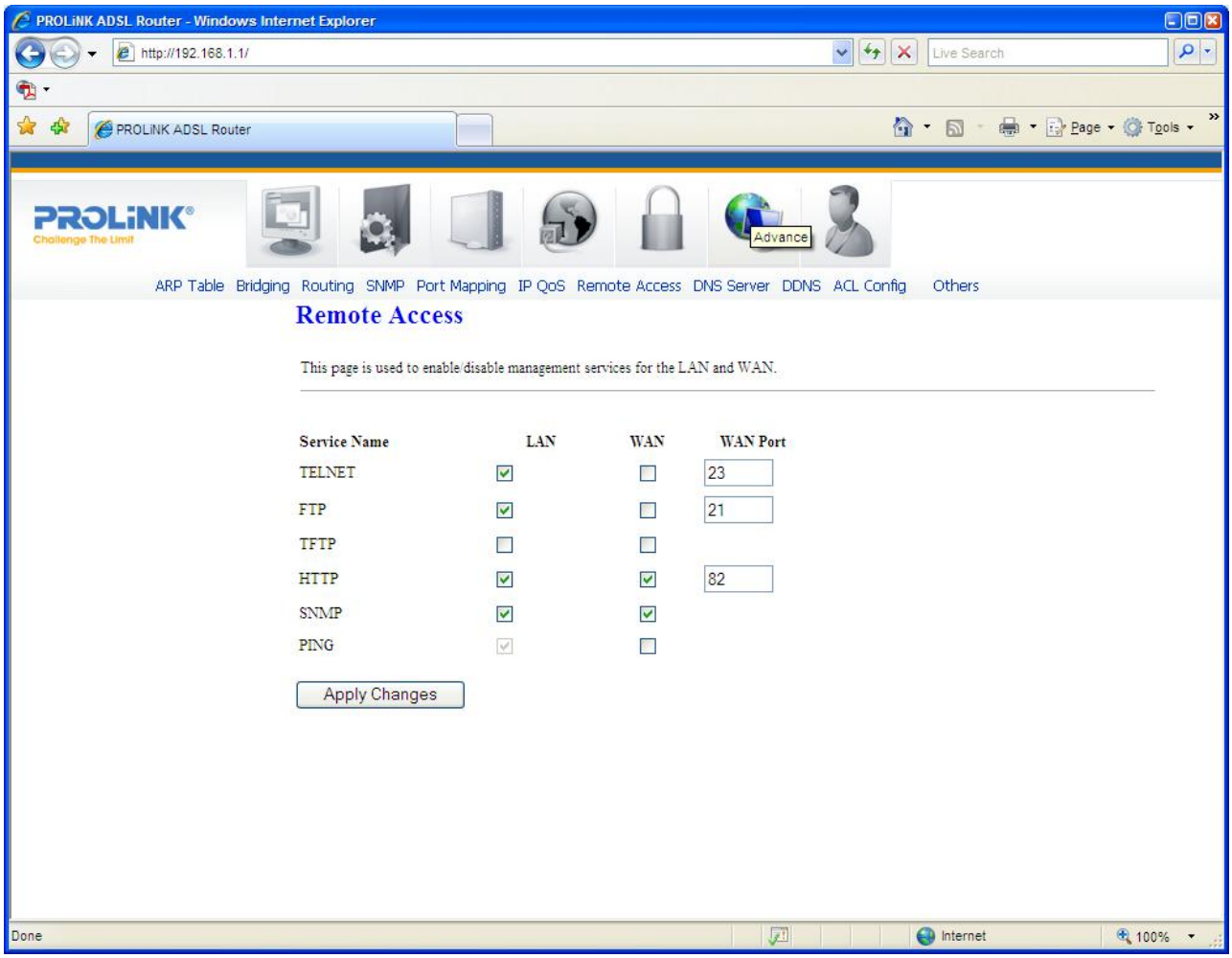
	for non-applicable.

Fields settings on the second block:

Field	Description
Outbound Priority	The priority level for the traffic that matches this classification rule. The possible selections are (in descending priority): p0, p1, p2, p3.
IP Precedence	Select this field to mark the IP precedence bits in the packet that match this classification rule.
IP Type of Service	Select this field to mark the IP TOS bits in the packet that match this classification rule.
802.1p	Select this field to mark the 3-bit user-priority field in the 802.1p header of the packet that matches this classification rule. Note that this 802.1p marking is workable on a given PVC channel only if the VLAN tag is enabled in this PVC channel.

9.6 REMOTE ACCESS

The Remote Access function can secure remote host access to your modem/router from LAN and WAN interfaces.

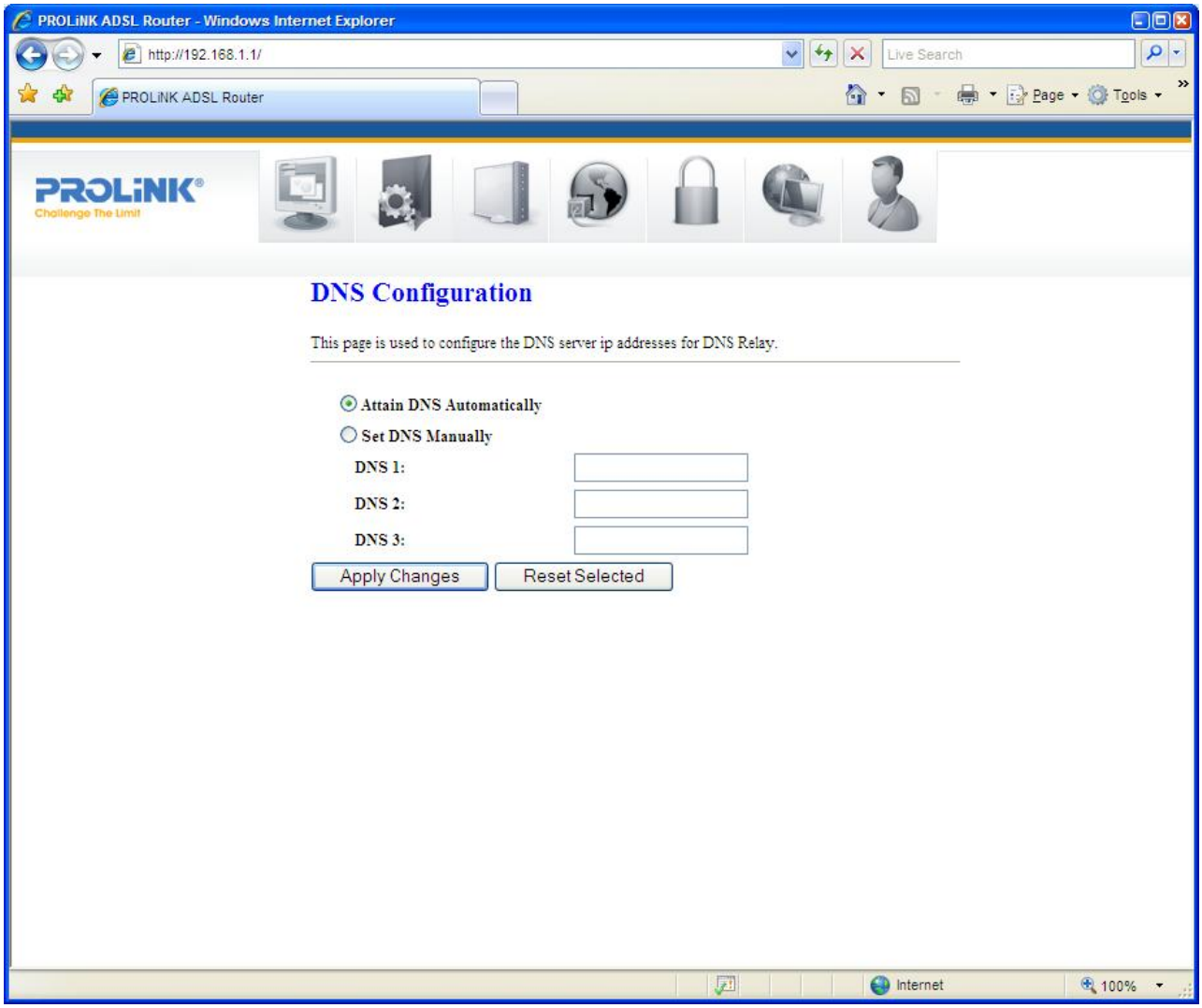


Fields in this page:

Field	Description
LAN	Check the services on the LAN column to allow access from LAN and vice-versa.
WAN	Check the services on the WAN column to allow access from WAN and vice-versa.
WAN Port	This field allows user to specify the port of the corresponding service. For example, when HTTP service is changed to port 82, the HTTP server address for WAN access is http://dsl_addr:82, where the ***dsl_addr*** is the WAN IP address of modem/router.

9.7 DNS CONFIGURATION

This page is used to select the way to obtain IP addresses of the DNS (Domain Name Servers).



Field	Description
Attain DNS Automatically	Select this item if you want to use the DNS servers obtained by the WAN interface via the auto-configuration mechanism.
Set DNS Manually	Select this item to configure up to three DNS IP addresses.

Function buttons in this page:

Apply Changes

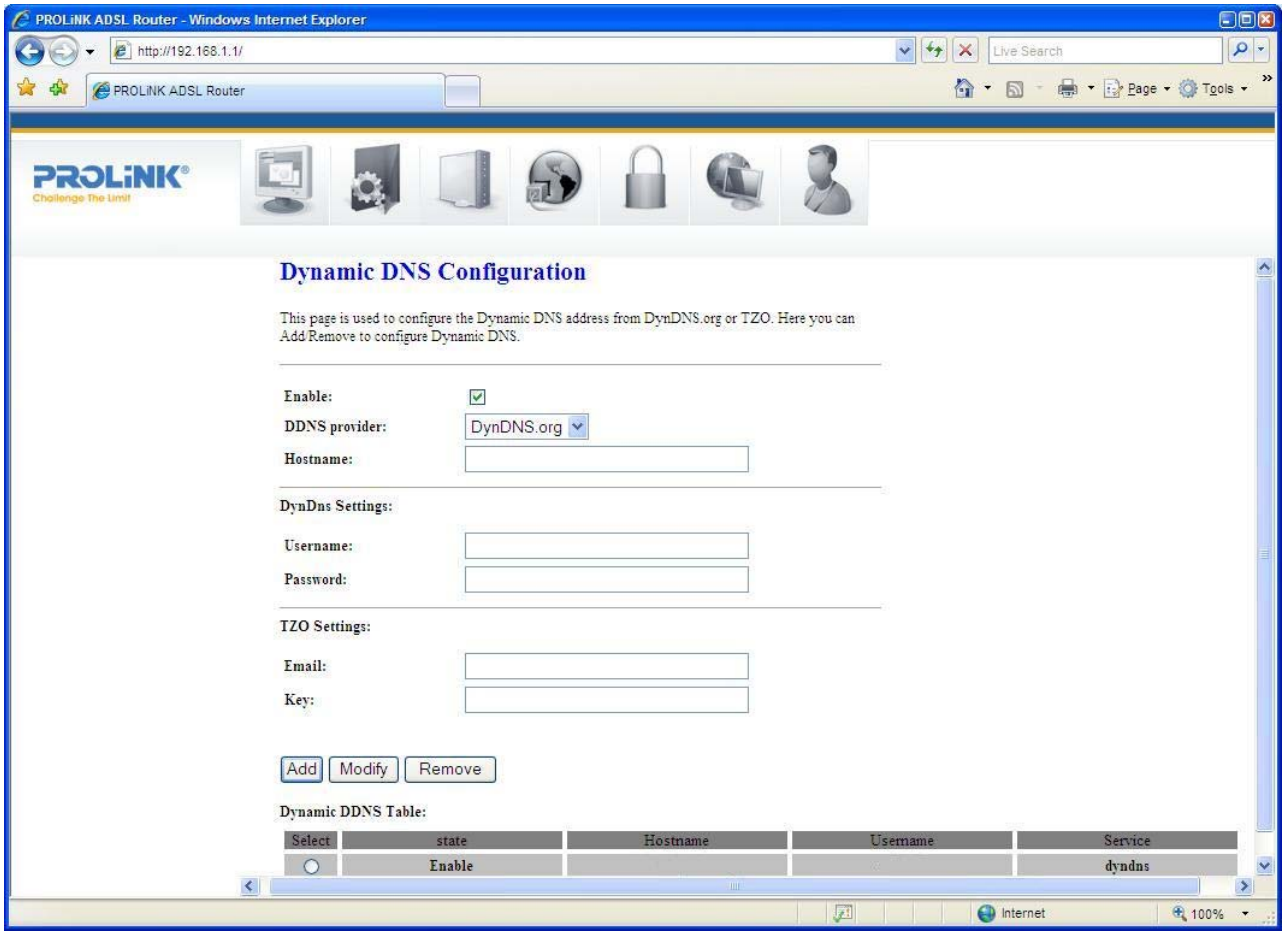
Set new DNS configuration. New parameters will take effect after the setting is saved into flash memory and the system is rebooted *(see section "Admin" for save details)*.

Reset Selected

Discard your changes.

9.8 Dynamic DNS

Each time the modem/router connects to Internet, your ISP assigns a different IP address to the modem. In order to remote access your modem from the Internet, you need to manually track the WAN IP that is currently used. The Dynamic DNS feature allows you to register your modem/router with a DNS server so that you can access your modem/router remotely, each time using the same host name. The **Dynamic DNS** page allows you to enable/disable the Dynamic DNS feature.



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

Field	Description
Enable	Check this item to enable the DNS server registration account for the modem/router.
DDNS provider	There are two options of DDNS providers: DynDNS and TZO. Changes may occur depends on the services that you select.
Hostname	The Domain name that you registered with the DDNS server.
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

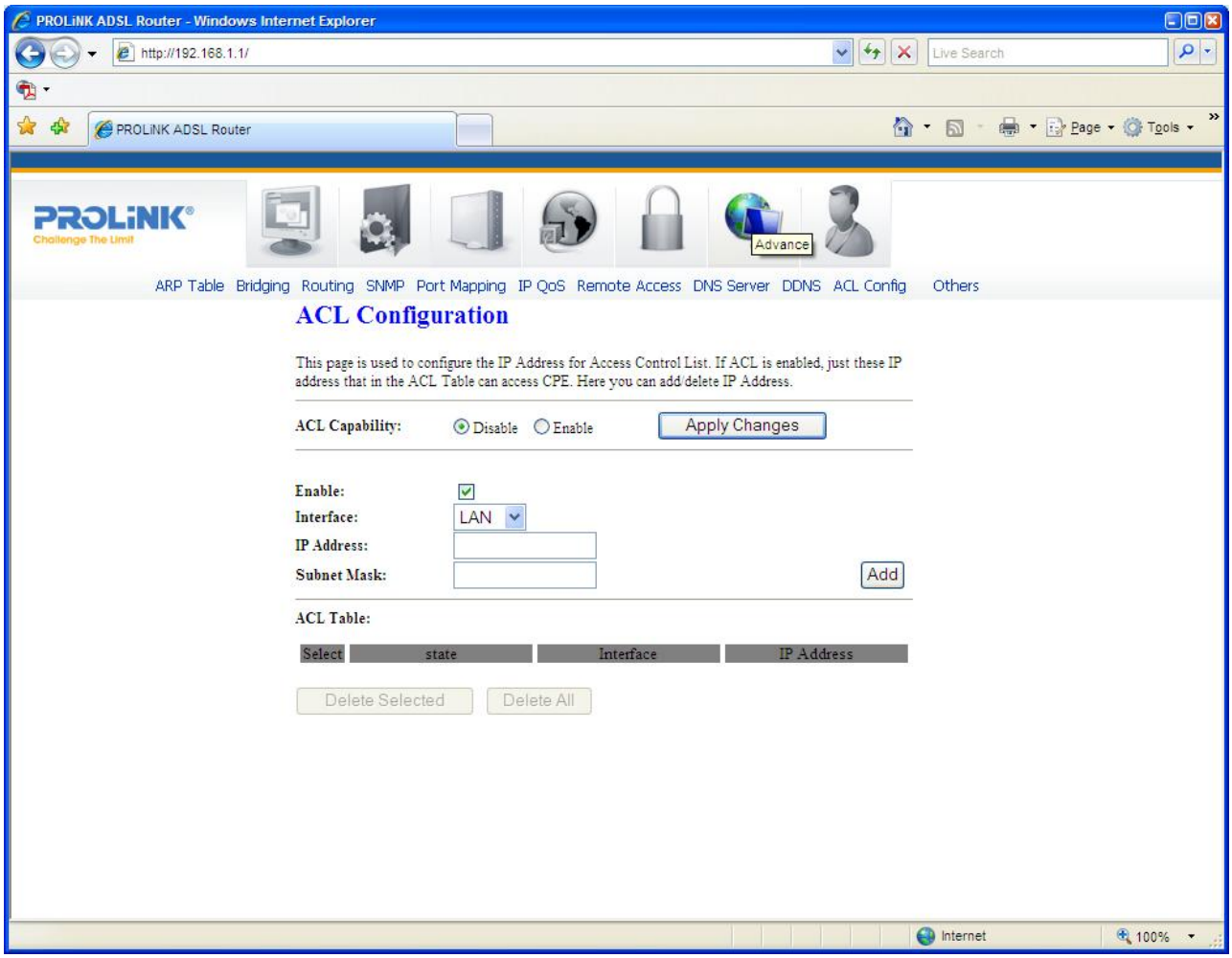
Select an existing DDNS registration by clicking the radio button at the **Select** column of the **Dynamic DNS Table**. Amend new settings to the selected registration and click Modify to save new changes.

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.

9.9 ACL CONFIGURATION

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



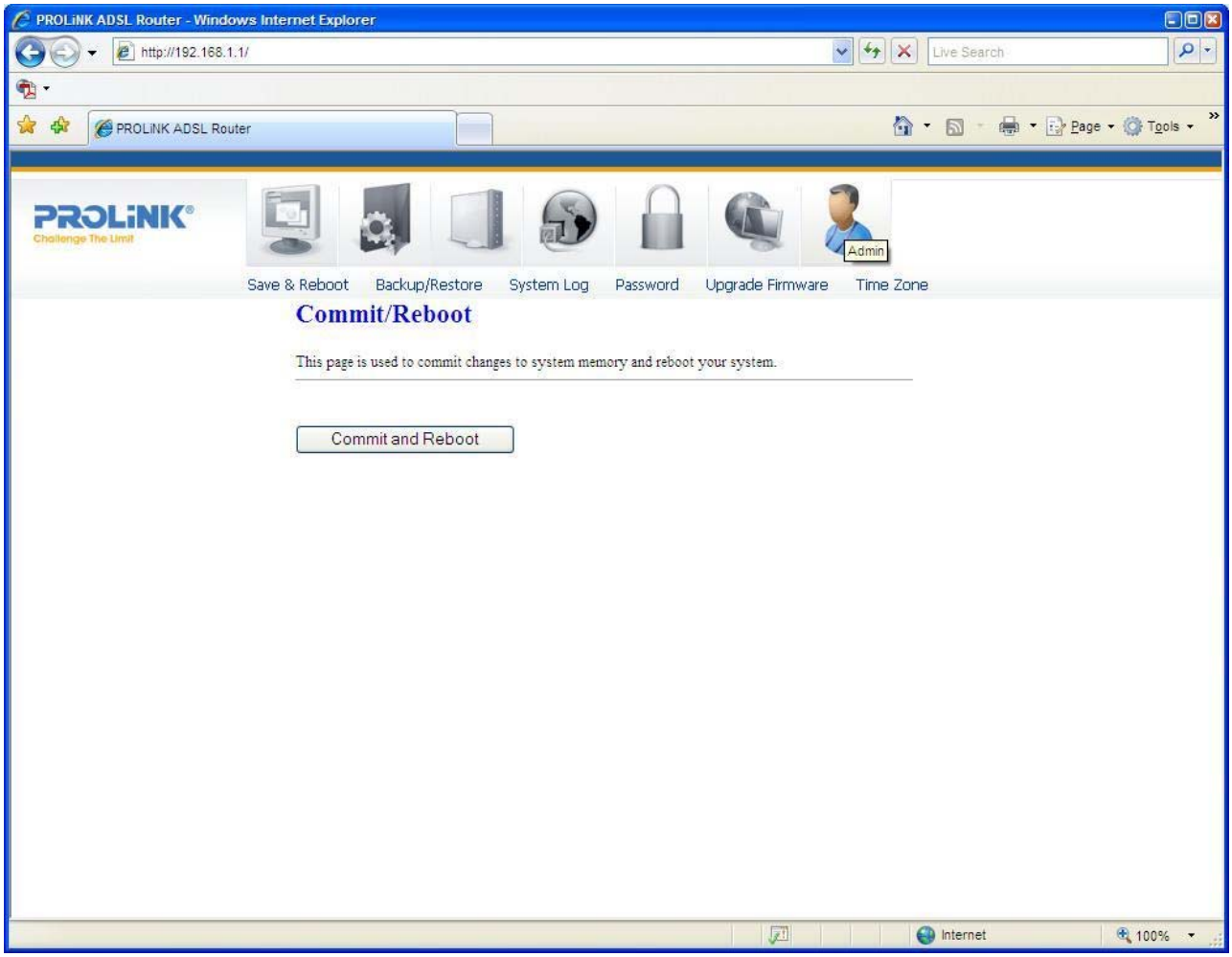
Fields in this page:

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

10 Admin

10.1 SAVE & REBOOT

Whenever you use the Web configuration to change system settings, the changes are initially stored in temporary storage. These changes will be lost if the modem/router is reset or turn off. To save your changes permanently, you can use the Commit function.



Function buttons in this page:

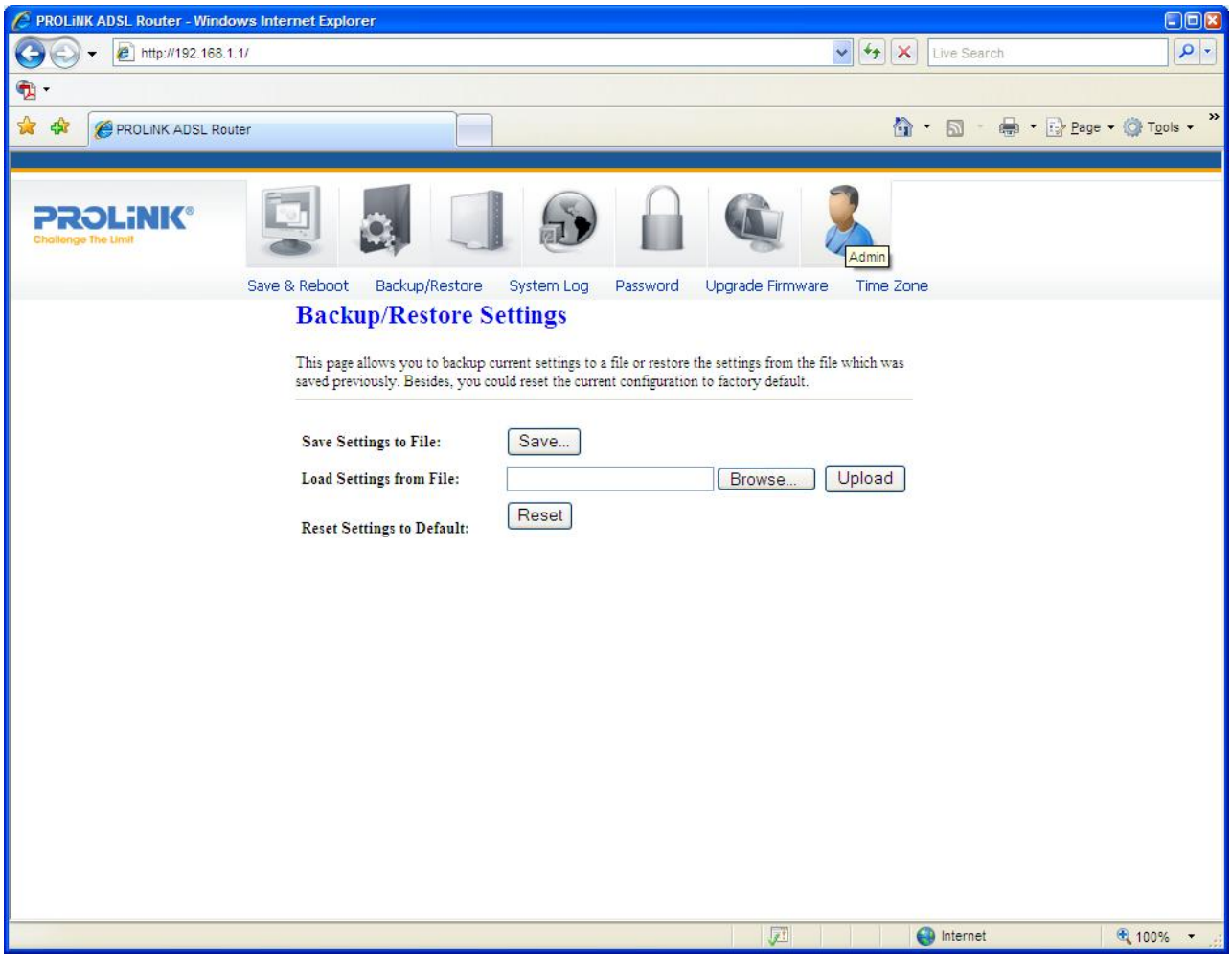
Commit and Reboot

This function saves your changes permanently, from RAM to flash memory and reboot the modem.

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

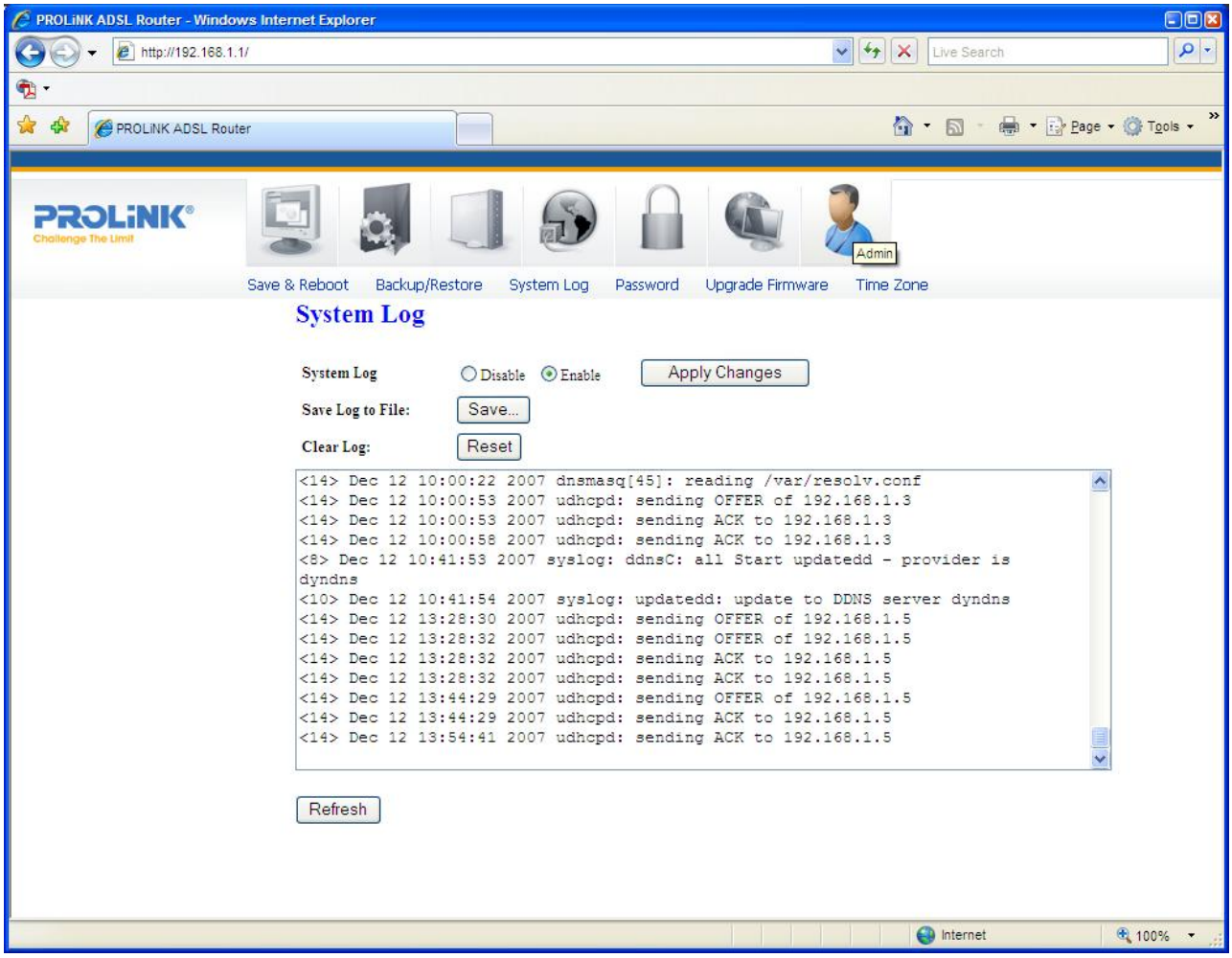
10.2 BACKUP/RESTORE SETTINGS

This page allows you to backup and restore your configuration from files in your host PC (LAN).



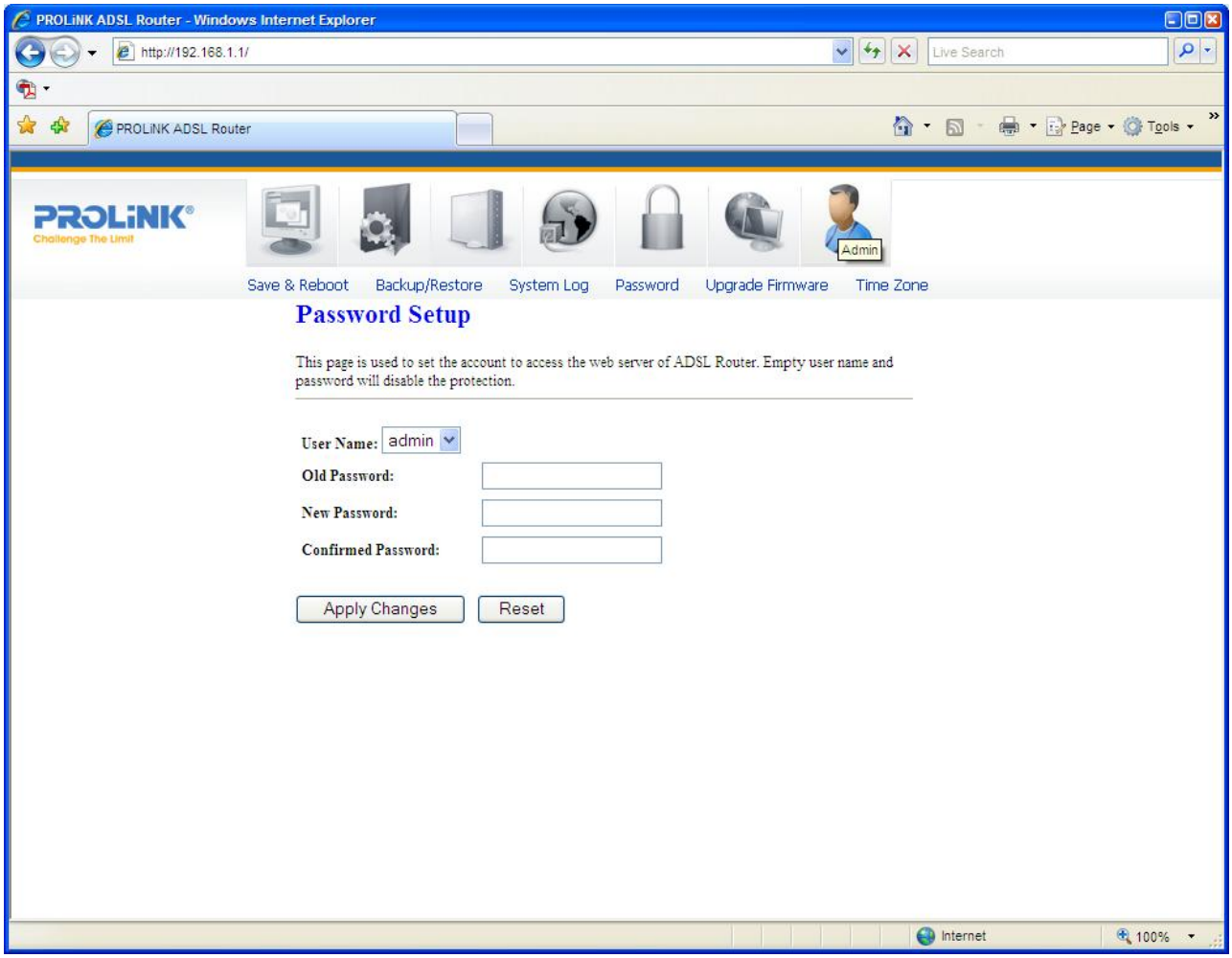
10.3 SYSTEM LOG

This page shows the System Log.



10.4 PASSWORD SETUP

There are two-level of logins: **admin** and **user**. The **admin** and **user** password configuration allows you to change the password for administrator and user.



Fields in this page:

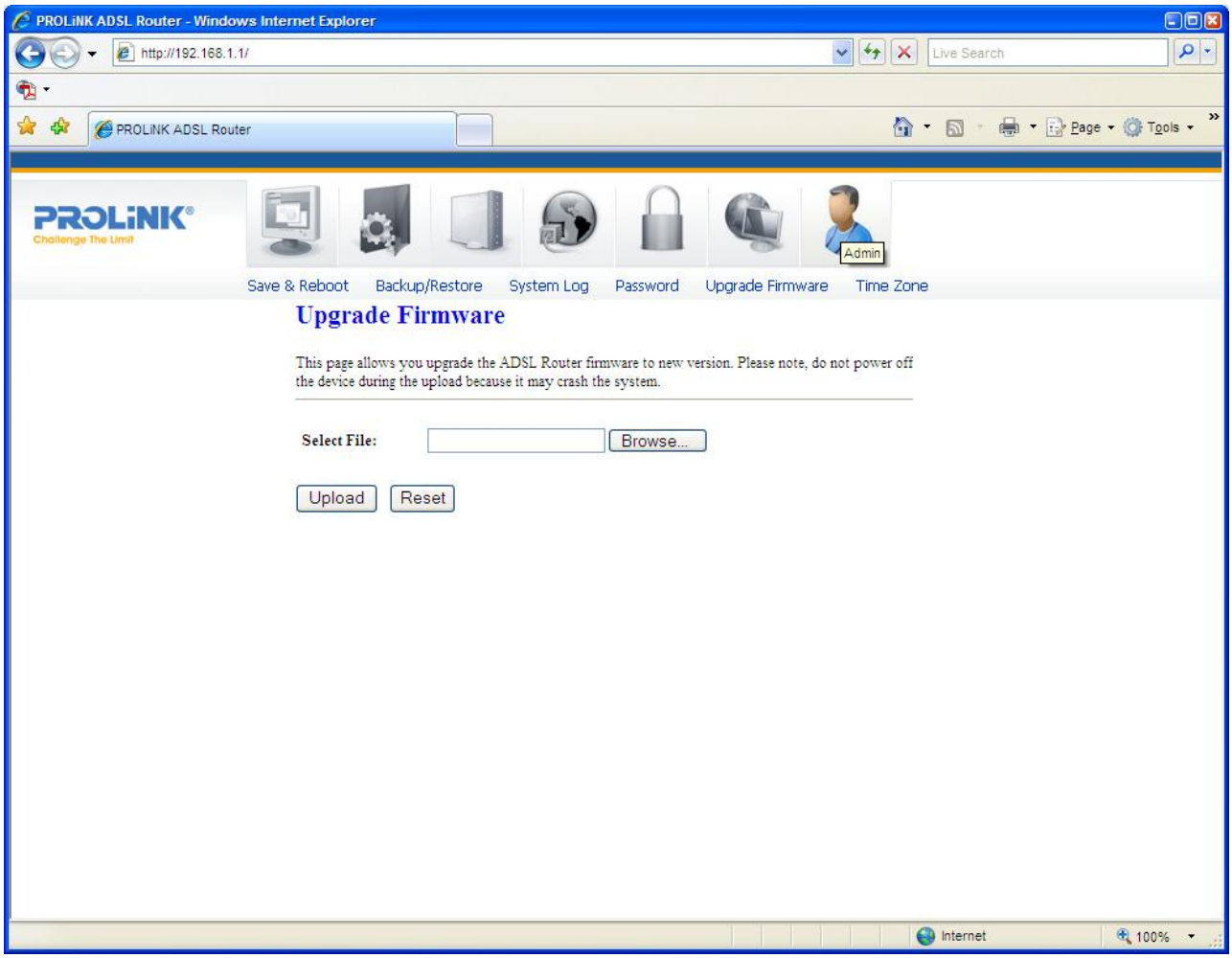
Field	Description
User Name	Select user levels: *admin* or *user*.
Old Password	Enter the current/default password for this selected login.
New Password	Enter the new password here.
Confirmed Password	Enter the new password again to confirm.

10.5 Upgrade Firmware

To upgrade the firmware for Hurricane 5200C/5201:

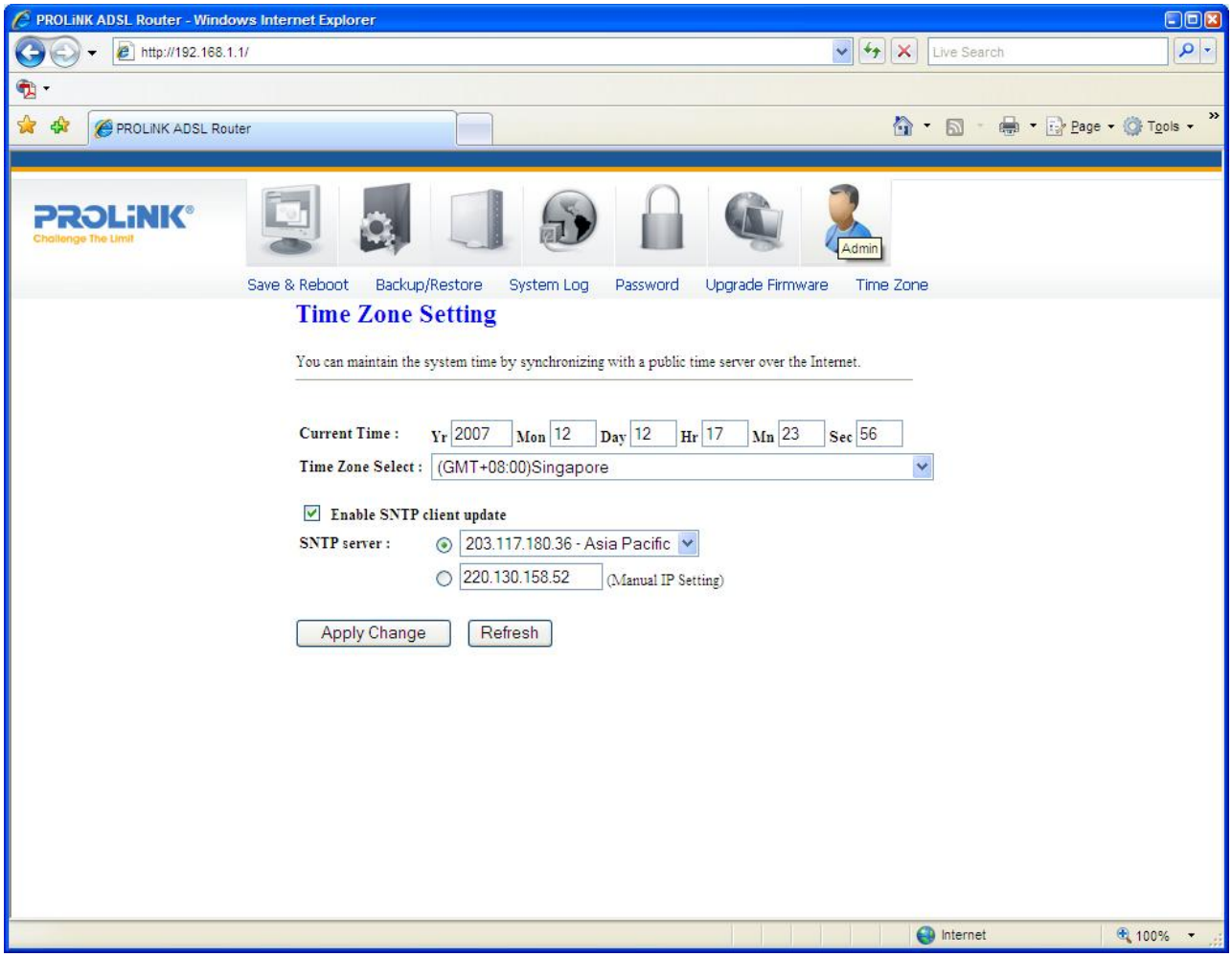
- Click on the **Browse** button to select the firmware file.
- Confirm your selection.
- Click on the **Upload** button to start upgrading.

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



10.6 TIME ZONE SETTING

Simple Network Timing Protocol (SNTP) is the protocol used to synchronize the system time to the public SNTP servers. The modem/router supports SNTP client functionality in compliance with IETF RFC2030.



Fields in this page:

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

Appendix

PRODUCT SUPPORT AND CONTACT INFORMATION

At PROLiNK, we are committed to provide you with the best quality of products as well as the best technical support. While if your computer is infected by virus, we may suggest you to find a solution in order to remove the virus, because we are unable to assist you until the virus is eradicated.

Singapore Service Center

Tel: (65) 6357 0668

Fax: (65) 6357 0669

Email: support@fida.com

Address: Blk 16 Kallang Place, #06-02 Kallang Basin Industrial Estate, Singapore 339156.

Operating Hours: Mon-Fri : 0900-1745 hrs Wed : 0900-2030 hrs

Malaysia Service Center

Tel: (603) 8023 9151

Fax: (603) 8024 9161

Email: support_my@fida.com

Address: 29, Jalan USJ 1/31, 47600 Subang Jaya, Selangor Darul Ehsan. Malaysia

Operating Hours: Mon-Fri: 0900-1745 hrs Sat: 0900-1300 hrs

Indonesia Service Center

Tel: (62) 021 628 3205

Fax: (62) 021 628 3206

Email: support_id@fida.com

Address: P. Jayakarta Komplek 85 BR/AJ Jakarta Pusat – Indonesia

Operating Hours: Mon-Fri: 0900-1800 hrs

www.prolink2u.com