ADSL2+ 4-Port Switch Wireless Router
Freeway DSL Series
User's Manual

Revision 0.2
Feb. 2009

Table of Contents

1. Introduction

The FREEWAY DSL is an ADSL2+ router which integrates a 4-port Fast Ethernet Switch, Wireless AP and File Server. FREEWAY DSL provides high speed ADSL2+ broadband connection and sharing it with up to four computers via the LAN ports and 32 computers via the WLAN. The Router is compatible with ADSL, ADSL2, and ADSL2+ lines for worldwide ADSL deployment. FREEWAY DSL supports robust QoS and IGMP features to ensure high quality triple play. Consider the application of home networking and sharing of file and printer, FREEWAY DSL supports easy-to-use file server.

FREEWAY DSL adopts easy-to-use web-GUI management interface. Its user friendly interface will amaze you with total difference experience. FREEWAY DSL also supports TR-069 (CPE WAN Management Protocol) which enables central management from the central offices and benefits the ISP much.

1.1 Features

- Comply with ITU ADSL, ADSL 2 and ADSL2+ standards
- Comply with IEEE802.3/802.3u 10/100 BASE-T standards
- Comply with IEEE802.11b/g Wireless LAN standards
- Integrate ADSL router and wireless AP (Access Point) together
- Enables sharing of broadband Internet connection
- Easy to use Samba file server for mass storage file sharing
- Security supports WPA/WPA2-PSK, & 64/128-bit WEP Encryption
- Double firewalls: NAT and SPI
- Built-in DHCP server
- MAC address filtering
- VPN pass-through
- Web-based advanced user interface
- Universal Plug and Play (UPnP)
- Support TR-069 for central management
- Remote / Local configuration & management through Web / Telnet configuration & management

1.2 System Requirement

In order to use the Freeway DSL, you must have the following:

- ADSL service up and running on your telephone line
- One or more computers each containing an Ethernet network interface card (NIC)
- For system configuration using the supplied web-based program: a web browser such as Internet Explorer v 5.0 or later, or Netscape v 6.1 or later.

2. Freeway DSL Overview

Your Freeway DSL has many ports, switches and LEDs. The features are listed below.

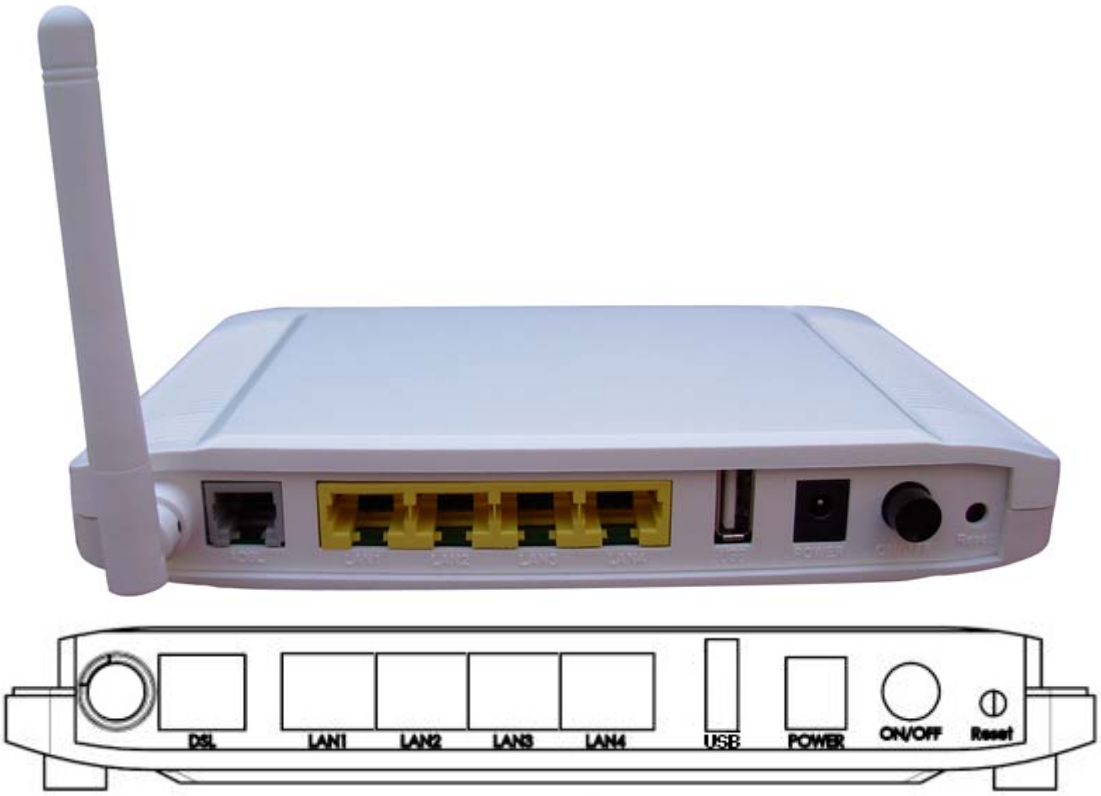
2.1 LED Description

LED	Color	Status	Description
Power	**Green**	**On**	Power on
		Off	Power off
	Red	**Flashing**	Not bootable (POST failure) or Device malfunction
DSL	**Green**	**On**	DSL Good sync.
		Off	Modem power off
		Flashing	DSL attempting sync.
LAN	**Green**	**On**	Device connected to LAN port
		Off	No Activity
		Flashing	LAN Activity present
Internet	**Green**	**On**	IP connected
		Off	Modem power off, in bridged mode or ADSL connection not present
	Red	**Flashing**	Device attempted to become IP connected and failed
USB	**Green**	**On**	Device connected to USB port
		Off	No Activity
		Flashing	USB Activity present
WLAN	**Green**	**On**	Ready to connect clients
		Off	Wireless Disable
		Flashing	Sending/Receiving Data
WPS	**Green**	**On**	Client already join the Wireless
		Off	No any WPS client
		Flashing	Client is joining the Wireless

Button	Description
WPS	Push this button for about 4 seconds, the WPS LED will then light up and flashing. At this moment, click the PBC button in the wireless client software, the wireless client will then scan and connect to the AP (Freeway DSL) automatically.

2.2 Ports and Buttons

The rear panel contains the ports for the Freeway DSL's data and power connections.



DSL: Connecter for accessing the Internet through ADSL line.

LAN1-4: Connector for Ethernet network devices, such as a PC, hub, switch or router.

USB: Connector for USB drive or Flash drive.

POWER: Connecter for a power adapter. Using a power supply with a different voltage rating will damage this product. Make sure to observe the proper power requirements. The requirement of adapter is 12 AC/ 1A.

ON/OFF: Power on/off your Freeway DSL.

Reset: Restore the default settings. You may need to place the Freeway DSL into its factory defaults if the configuration is changed, you loose the ability to enter the Freeway DSL via the web interface, or following a software upgrade, and you loose the ability to enter the Freeway DSL. To reset the Freeway DSL, simply press the reset button for more than 8 seconds. The Freeway DSL will be reset to its factory defaults and after about 30 seconds the Freeway DSL will become operational again.

2.3 Installing your Freeway DSL

1. Locate an optimum location for the Freeway DSL.
2. For connections to the Ethernet and DSL interfaces, refer to the Quick Start Guide.
3. Connect the Power Adapter. Depending upon the type of network, you may want to put the power supply on an uninterruptible supply. Only use the power adapter supplied with the Freeway DSL. A different adapter may damage the product.

Now that the hardware installation is complete, continue on to set up your Freeway DSL.

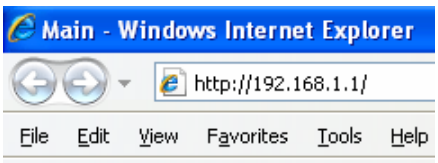
3. Setting up Your Freeway DSL

This section guides you through configuring your Freeway DSL. You should have your computers configured for DHCP mode and have proxies disabled on your browser. If you do not get the page as shown below, you may need to delete your temporary Internet files by flushing the cached web pages.

3.1 Log into Your Freeway DSL

Use the following procedures to log in to your Freeway DSL.

1. Open your web browser. Type the default IP address of the Freeway DSL **http://192.168.1.1** and press **Enter**.
The Log In page appears.



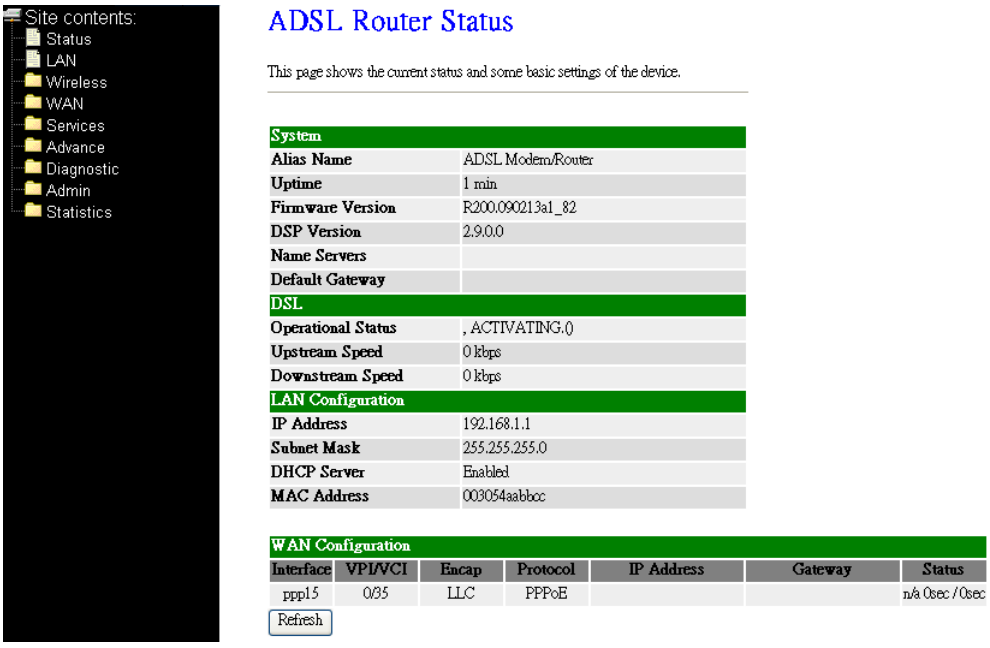
2. Enter user name as **Admin** and password as **Admin** (case sensitive).

3. Click **OK**.
The main page appears.

Note

*You can change the password in **System->Password** page at any time.*

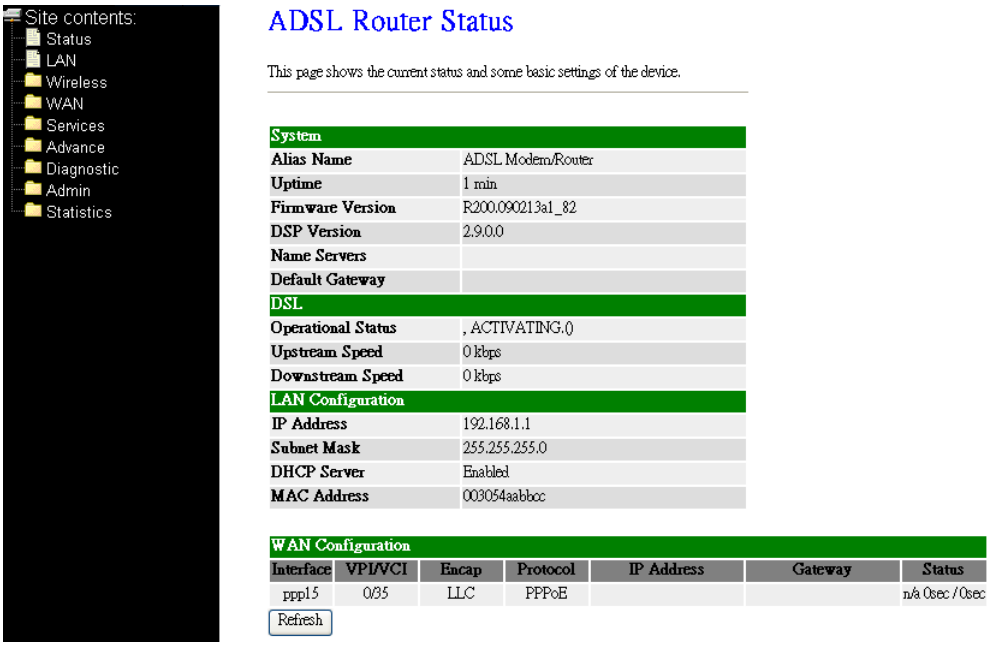
The Web Application is displayed as shown below. This page displays the Freeway DSL's current status.



4. Web Configuration

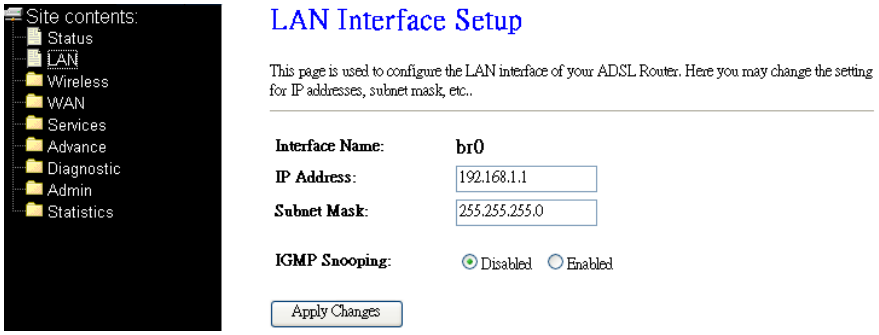
4.1 Status

This page displays the firmware version, DSP version, interface status and Internet connection. This information will vary depending on the Internet connection status.



4.2 LAN

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.

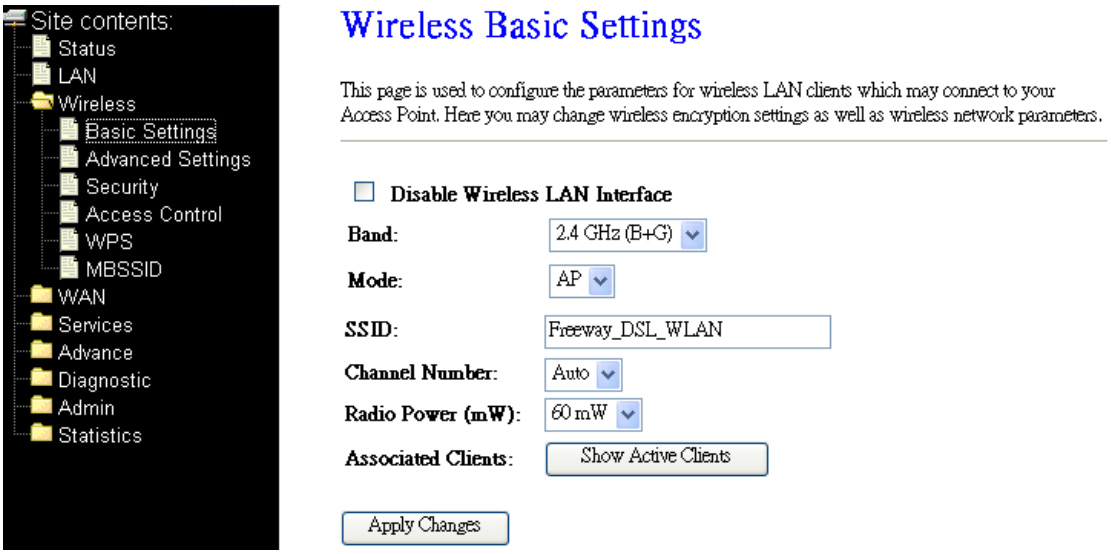


Field	Description
IP Address	Enter the IP address of Freeway DSL.
Subnet Mask	Enter the subnet mask for this network.
IGMP Snooping	Select the radio button to enable/disable IGMP Snooping.

4.3 Wireless

4.3.1 Basic Settings

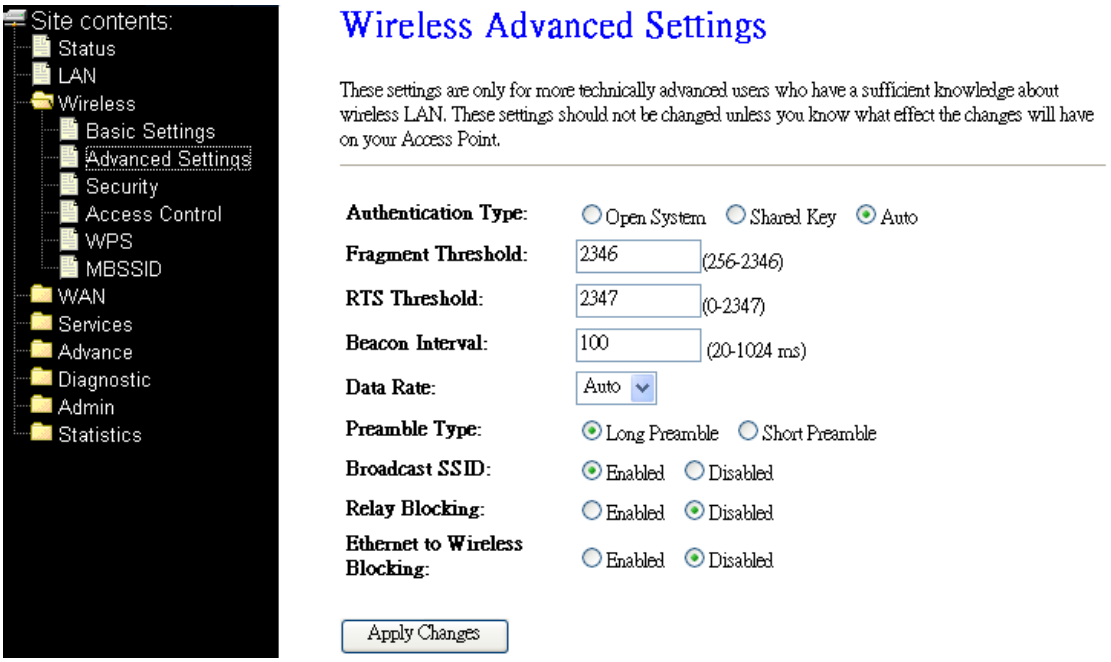
This page is used to configure the parameters for wireless LAN clients which may connect to your AP (Access Point). Here you may change wireless encryption settings as well as wireless network parameters.



Field	Description
Disable Wireless LAN Interface	Check it to disable the wireless function for Freeway DSL.
Band	Select the appropriate band from the list provided to correspond with your network setting.
Mode	Select the mode to be AP or AP+WDS. Used to specify the wireless mode to be: • **AP:** Configure the Freeway DSL as a standard wireless AP (access point). • **AP+WDS:** This mode allows you to connect the Freeway DSL with up to four WDS-capable wireless routers to expand the network.
SSID	The Service Set Identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. The mobile wireless stations shall select the same SSID to be able to communicate with the Freeway DSL (AP).
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP and Freeway DSL to avoid signal interference.
Radio Power (mW)	Select the output power of wireless radio to 100%, 50% or 25%. Unless you are using this Freeway DSL in a really wide space, you may not have to set radio power to 100%. The wider coverage the more security risk (malicious or unknown users in distance will be able to reach the Freeway DSL).
Associated Clients	Click this button to show the clients currently associated with the Freeway DSL.

4.3.2 Advanced Settings

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

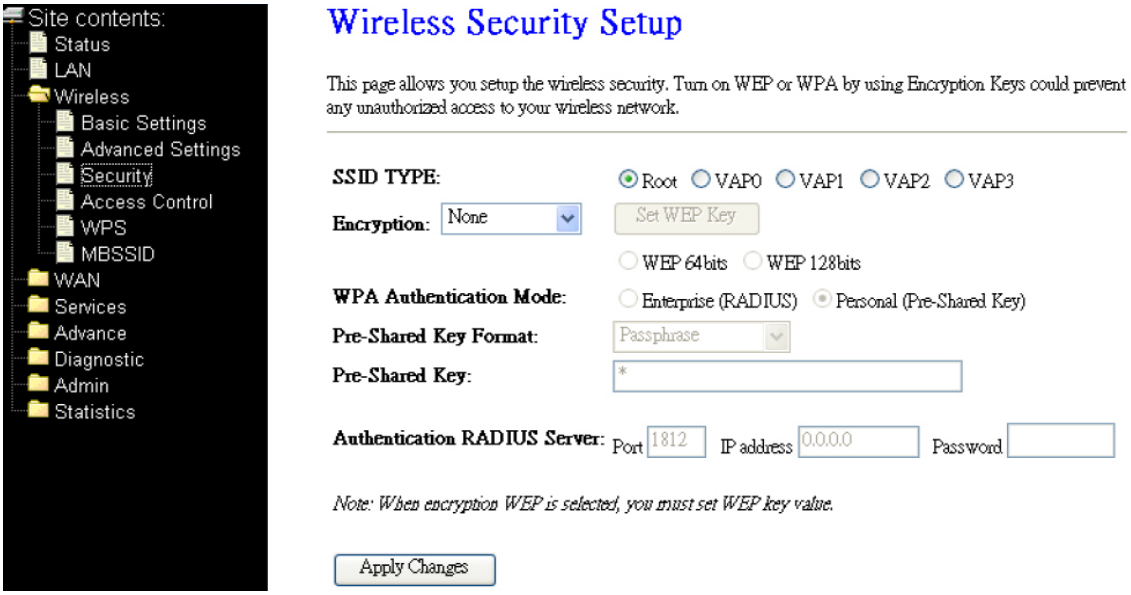


Field	Description
Authentication Type	Used to specify the wireless authentication type which can be: • **Open System**: Enables your client adapter, regardless of its WEP settings, to attempt to authenticate and communicate with an access point. Open Authentication is the default setting. • **Shared Key**: Enables your client adapter to communicate only with access points that have the same WEP key. This option is available only if Use Static WEP Keys is selected. • **Auto**: This allows either Open System or Shared Key authentication to be used.
Fragment Threshold	Defines the largest RF packet that the client adapter sends without splitting the packet into two or more smaller fragments. If a single fragment experiences interference during transmission, only that fragment must be resent. Fragmentation generally reduces throughput because the packet overhead for each fragment consumes a higher portion of the RF bandwidth.
RTS Threshold	Specifies the data packet size beyond which the low-level RF protocol invokes RTS/CTS flow control. A small value causes RTS packets to be sent more often, which consumes more of the available bandwidth and reduces the throughput of other network packets. However, small values help the system recover from interference or collisions, which can occur in environments with obstructions or metallic surfaces that create complex multipath signals. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.

Beacon Interval	Specifies the interval between beacon packets, which IEEE 802.11 systems use to synchronize clients. Beacon packets contain timing and other information that is broadcast over the airwaves. Any station that receives the beacon packet can then synchronize with the system broadcasting beacons. The default value of the beacon period is 100 milliseconds.
Data Rate	The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.
Preamble Type	Preamble is part of the wireless signal that synchronizes network traffic. Select the appropriate preamble type, Long Preamble (default) or Short Preamble. High network traffic areas should use the shorter preamble type.
Broadcast SSID	When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, Enable. If you do not want to broadcast the Router's SSID, then select Disable.
Relay Blocking	Enables you to prevent your server from being used as a relay host.
Ethernet to Wireless Blocking	Enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other.

4.3.3 Security

This page allows advanced users who have sufficient knowledge of wireless LAN to configure advanced settings for the wireless connection. The default settings shall not be changed unless you know exactly what will happen for the changes you made to your Freeway DSL. This screen allows you to setup the wireless security. Enable WEP or WPA by configuring encryption keys can prevent unauthorized access to your WLAN.

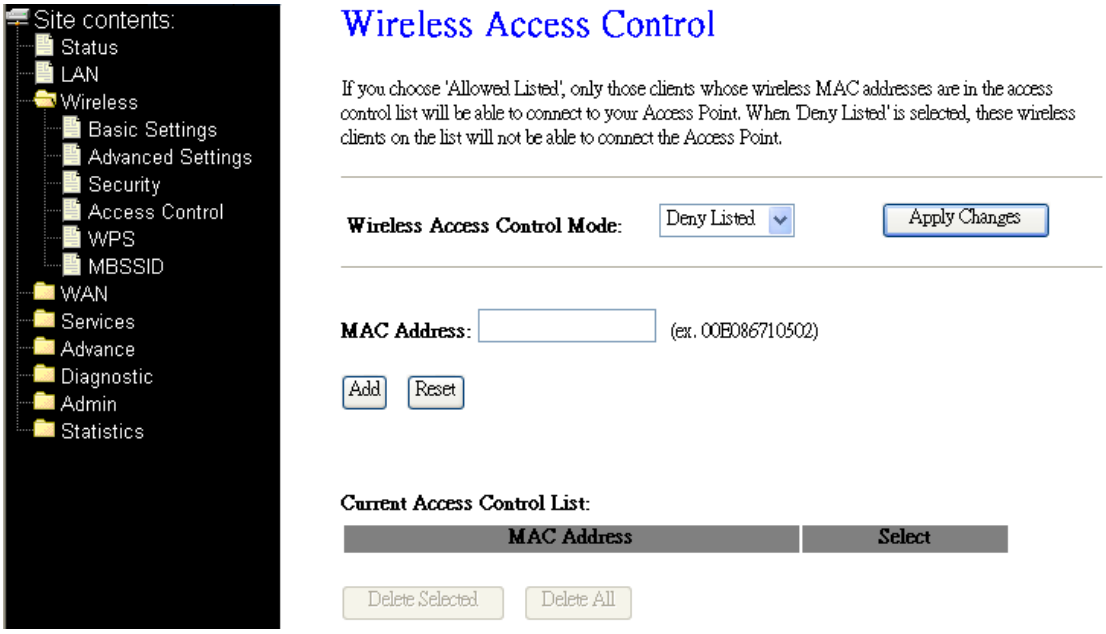


Field	Description
SSID Type	A VAP (Virtual Access Point) is a logical entity which exits within a physical Access Point (AP). A physical AP can support several VAPs. Each VAP might advertise either different SSID and capability set or same SSID with different capability set. In general terms, VAPs can be seen as totally independent APs. That is, with different capabilities, SSID, MAC addresses, IP addresses, client configurations and connected to different VLANs.
Encryption	There are 4 types of security to be selected. To secure your wireless network, it's strongly recommended to enable this feature. • **WEP:** Make sure that all wireless devices on your network are using the same encryption level and key. Click **Set WEP Key** button to set the encryption key. • **WPA (TKIP):** WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilized a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. • **WPA2 (AES):** WPA2 uses Advanced Encryption Standard (AES) for data encryption. AES utilized a symmetric 128bit block data encryption. • **WAP2 Mixed**: The AP supports WPA (TKIP) and WPA2 (AES) for data encryption.
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. • **Enterprise (WPA-RADIUS):** WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Please refer to "Authentication RADIUS Server" setting below for RADIUS setting. • **Personal (Pre-Shared Key):** Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the *Pre-Shared Key Format* and *Pre-Shared Key* setting respectively.
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**, it indicates a passphrase of 8 to 63 alphanumerical characters. If the *Pre-Shared Key Format* is specified as **Hex (64 characters)**, it indicates a 64-hexadecimal characters of 0-9, a-f and A-F.
Authentication RADIUS Server	Specify the IP address, port number and password of external RADIUS server if the **Enterprise (RADIUS)** is selected at *WPA Authentication Mode*.

4.3.4 Access Control

This page allows you to manage whether a wireless client is allowed to access the AP or not based on the MAC address of device.
If you choose "Allowed Listed", only those clients whose wireless MAC addresses are in the access control list will be able to connect to the AP. When "Deny Listed" is selected, these wireless clients on the list will not be able to connect the AP.



Field	Description
Wireless Access Control Mode	The Selections are: • **Disable:** Disable the wireless ACL function. • **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 the Freeway DSL). • **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 the Freeway DSL).
MAC Address	Enter client MAC address and press "Apply Changes" button to add client MAC address into current access control list.
Current Access Control List	It lists the client MAC addresses can/cannot connected to the Freeway DSL. You can select the entries at the **Select** column and apply to the following function buttons.

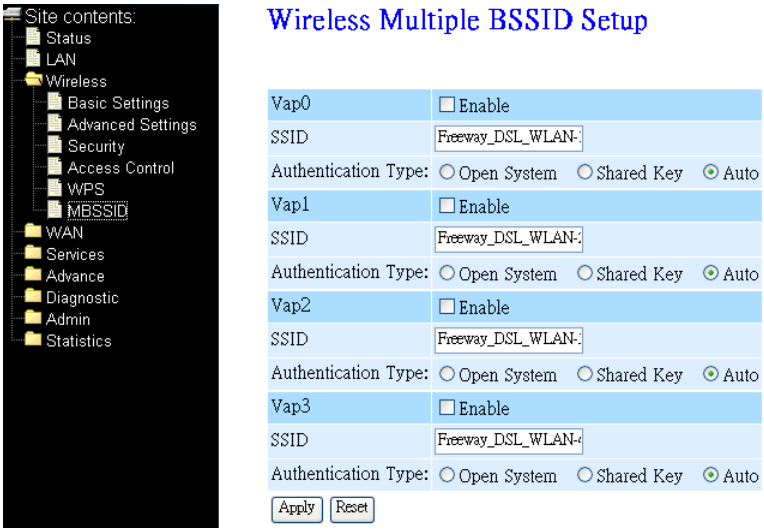
4.3.5 WPS

This page is used to configure the settings for WPS (Wi-Fi Protected Setup). It uses a push-button or a 4- or 8-digit personal identification number (PIN) to simplify the secure network setup. The PIN can be generated by software or preprogrammed into a client device and printed on an included card. With WPS, Freeway DSL can automatically set the SSID or network name as part of the setup process and provide strong encryption keys to client devices. You do not need to configure SSID, wireless security setting, etc., in the client software. In order to use WPS, the wireless client software must also support WPS.

Field	Description
Disable WPS	Check this box to disable WPS function.
WPS Status	If the wireless security (encryption) function of the Freeway DSL is properly set, you will see "Configured" radio button in action mode, otherwise, "UnConfigured" is in action mode.
Self-PIN Number	The the PIN Number of this Freeway DSL. This number is useful when you need to build wireless connection by WPS with other WPS-enabled wireless devices.
Regenerate PIN	Click this button to generate a set of new PIN number.
Start PBC	Click this button to start PBC (Push-Button Configuration) setup procedure. The **WPS** LED on the Freeway DSL will blink slowly for 2 minutes when the Freeway DSL is waiting for incoming WPS request.
Client PIN Number	Enter the PIN number of the wireless client you wish to connect.
Start PIN	Click this button to start PIN setup procedure. The **WPS** LED on the Freeway DSL will blink slowly for 2 minutes when the Freeway DSL is waiting for incoming WPS request.

4.3.6 MBSSID (Multiple Base Service Set Identifier)

This page allows you to configure one AP as several Basic Service Sets (BSSs) simultaneously. You can then assign different levels of privilege to different SSIDs (Service Set IDentifiers). Wireless clients can use different BSSIDs to associate with the same AP.

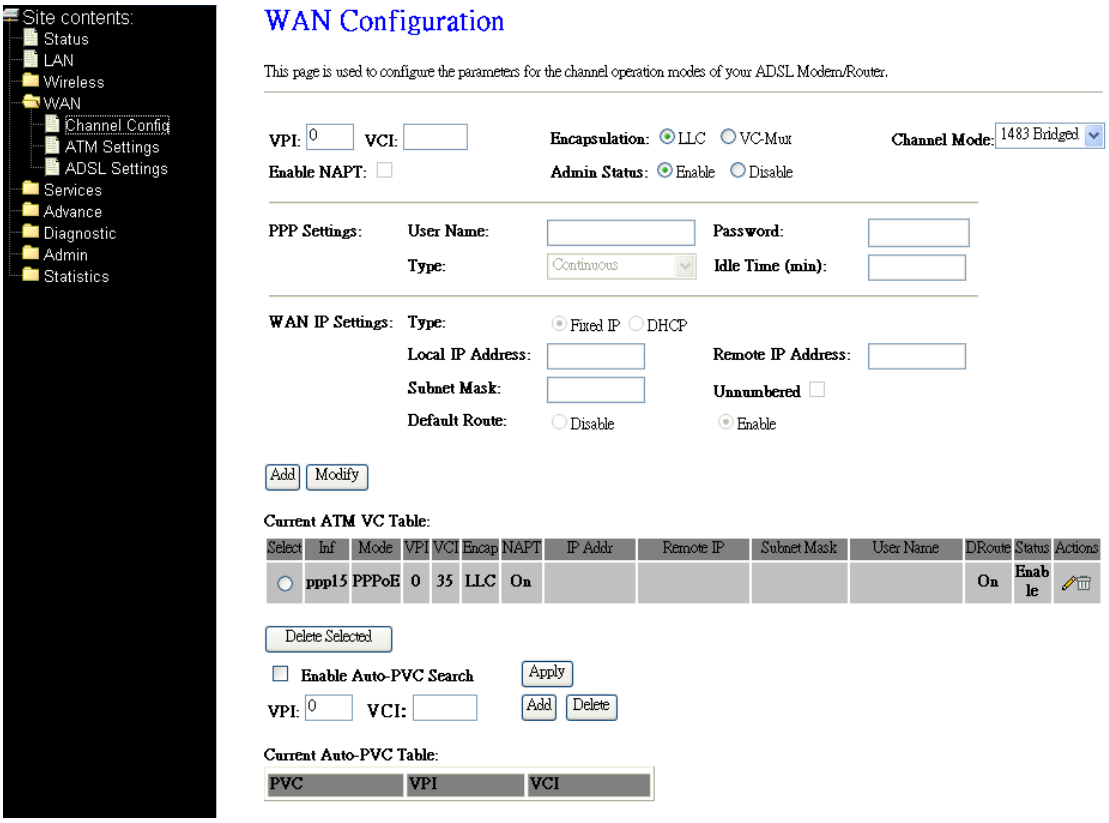


Field	Description
VAP0-3	Check to this VAP profile.
SSID	The Service Set Identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. The mobile wireless stations shall select the same SSID to be able to communicate with the Freeway DSL (AP).
Authentication Type	Used to specify the wireless authentication type which can be: • **Open System**: Enables your client adapter, regardless of its WEP settings, to attempt to authenticate and communicate with an access point. Open Authentication is the default setting. • **Shared Key**: Enables your client adapter to communicate only with access points that have the same WEP key. This option is available only if Use Static WEP Keys is selected. • **Auto**: This allows either Open System or Shared Key authentication to be used.

4.4 WAN

4.4.1 Channel Configuration

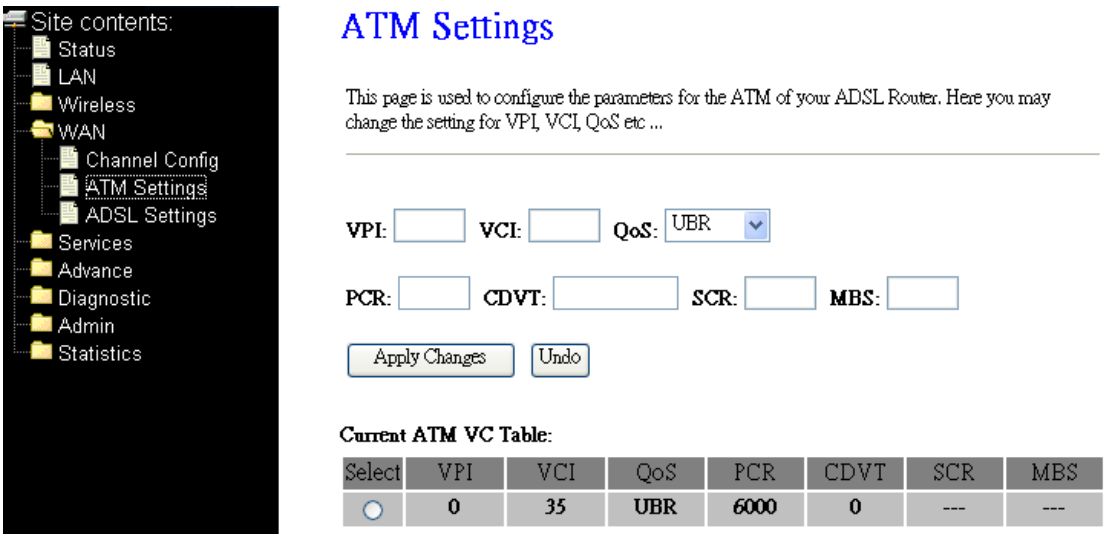
This page is used to configure the parameters for the channel operation modes of your ADSL Router.



Field	Description
VPI/VCI	Enter the PVC identifier (VPI and VCI) provided by your ISP.
Encapsulation	Select the encapsulation mode for the connection. Your ISP should inform you which mode to use.
Channel Mode	Select the channel type for the connection. Your ISP should inform you which type to use.
Enable NAPT	Select the radio button to enable NAPT (Network Address Port Translation).
Admin Status	Select the radio button to enable/disable administration status.
PPP User Name	To enter a name to use the PPP session.
PPP Password	To enter a password of the login user.
WAN IP Settings Type	Select the WAN IP to be fixed IP or assigned form the ISP.
Local IP Address	Enter the local IP Address provided by the ISP.
Remote IP Address	Enter the remote IP Address provided by the ISP.
Subnet Mask	To enter the subnet mask provided by the ISP.
Default Route	Select the radio button to enable/disable default route.
Enable Auto-PVC Search	Check to allow the Freeway DSL to search for PVC settings automatically.

4.4.2 ATM Settings

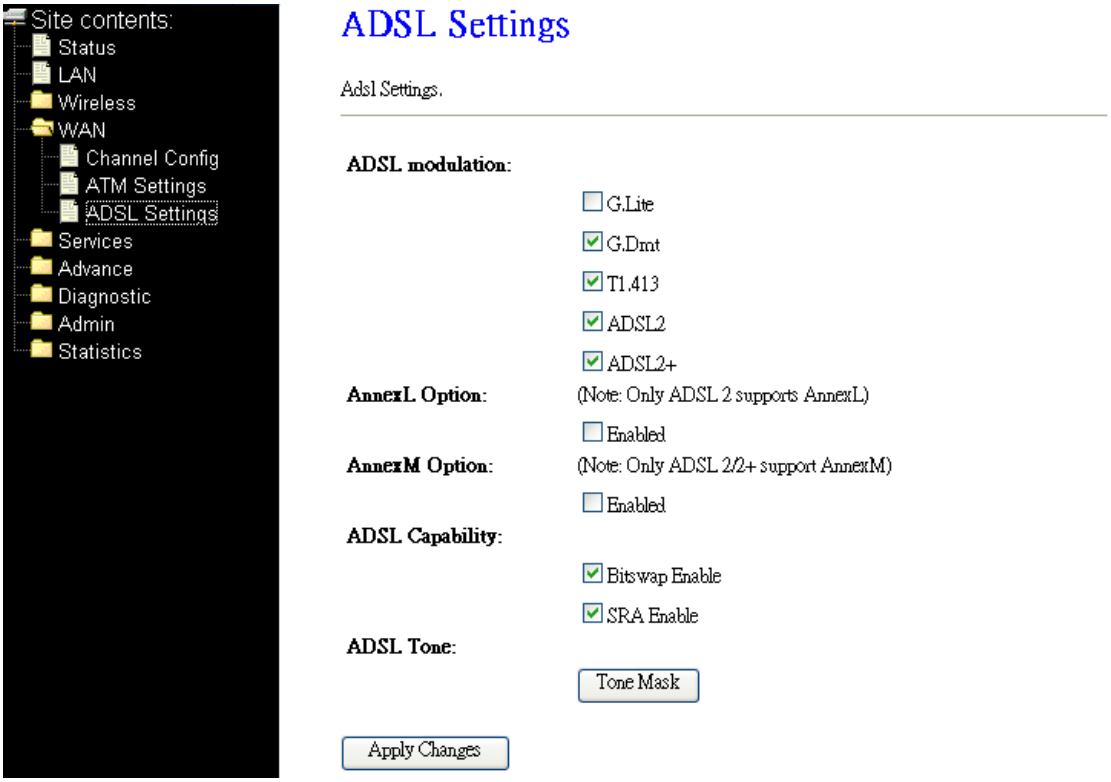
This page is used to configure the parameters for the ATM of your ADSL Router. You may change the setting for VPI, VCI, QoS, etc.



Field	Description
VPI/VCI	Enter the PVC identifier (VPI and VCI) provided by your ISP.
QoS	Select the QoS from the drop-down list.
PCR	Configure the PCR (Peak Cell Rate) parameter for ATM.
CDVT	Configure the CDVT (Cell Delay Variation Tolerance) parameter for ATM.
SCR	Configure the SCR (Substainable Cell Rate) parameter for ATM.
MBS	Configure the MBS (Maximum Burst Size) parameter for ATM.

4.4.3 ADSL Settings

This page allows you to select the modulation, phone line type and capability specified by your ISP. The default configuration in this page can work with most ADSL implementations. DO NOT change any setting unless you are instructed to do so.

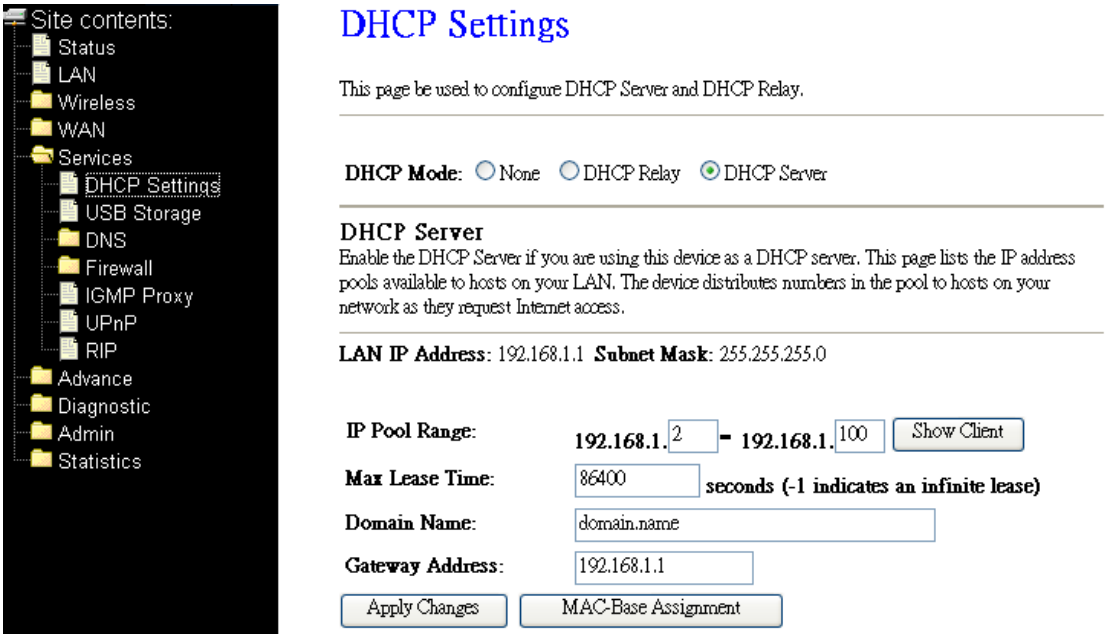


4.5 Services

4.5.1 DHCP Settings

The Freeway DSL supports the Dynamic Host Configuration Protocol (DHCP). This page is used to configure the Freeway DSL to be a DHCP server or a DHCP Relay agent. 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.

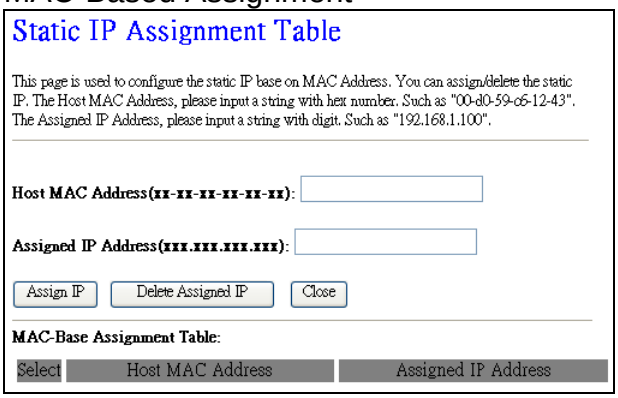
DHCP Server Configuration
By default, the Freeway DSL is configured as a DHCP server, with a predefined IP address pool from 192.168.1.2 to 192.168.1.100 (subnet mask 255.255.255.0).



Field	Description
IP Pool Range	Enter the start and end addresses in the pool.
Show Client	Click this button to display the clients that is connected to the Freeway DSL.
Max Lease Time	The Lease Time is the amount of time hat a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 86400 seconds (1 day). The value -1 stands for the infinite lease.
Domain Name	A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.
Gateway Address	Enter the Gateway's Address of the Freeway DSL.
MAC-Base Assignment	Click this button to configure the static IP base on MAC Address. You can assign/delete the static IP. To configure the host MAC address, enter a string with hex number, e.g. "00-d0-59-c6-12-43". To configure the assignment IP address, enter a string with digit, e.g. "192.168.1.100".

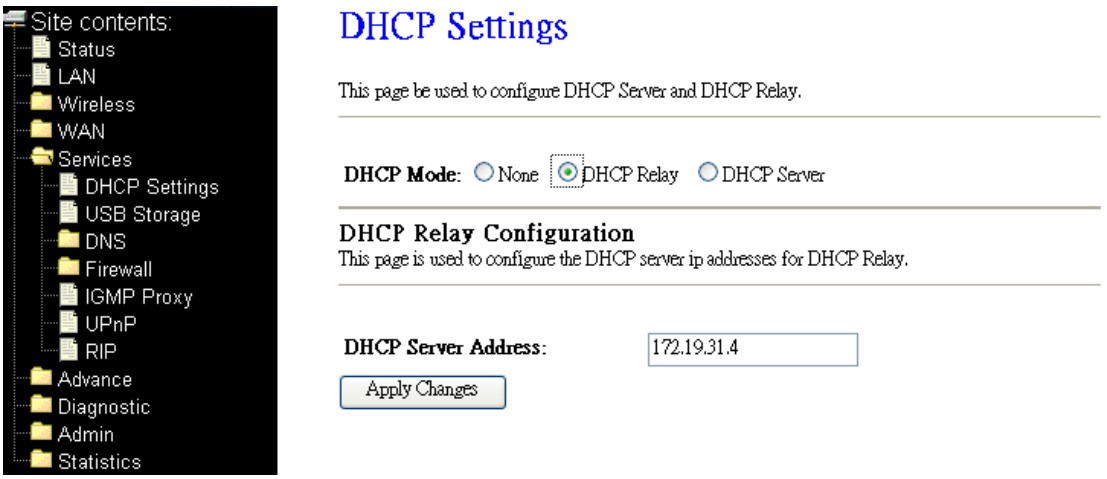
This pop-up page is used to configure the static IP base on MAC address. You can assign or delete the static IP. Input a string in hex number format, such as 00-d0-59-c6-12-43 to be the assigned IP address; input a string in digit format, such as 192.168.1.100, to be the Host MAC address.

MAC-Based Assignment



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.



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.

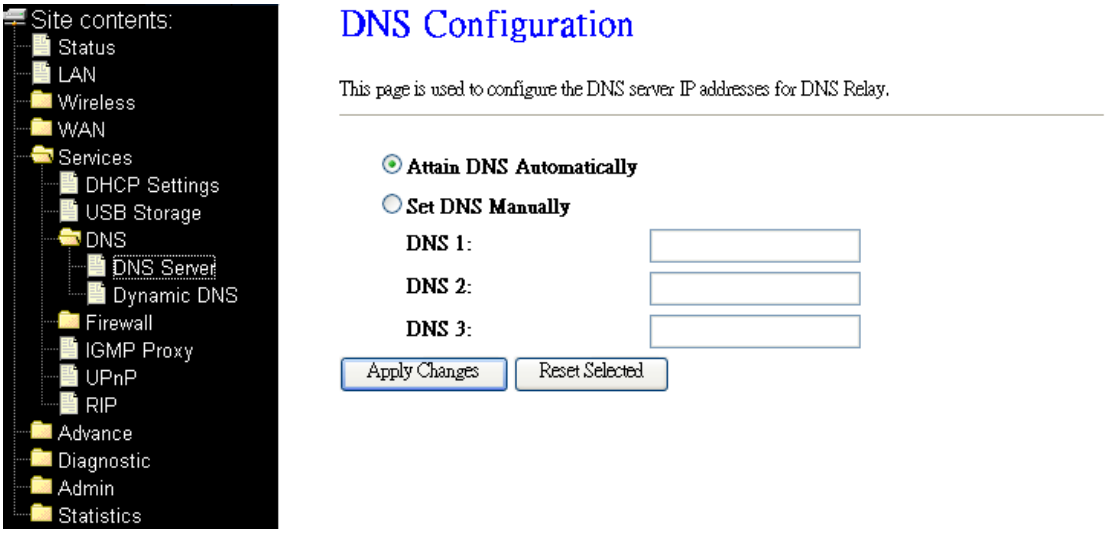
4.5.2 USB Storage

This page shows the information of USB mass storage. Open a file explorer window and type in the address field:
\\192.168.1.1\DeviceName
where "DeviceName" is the name that was assigned to the storage device.

4.5.3 DNS

4.5.3.1 DNS Server

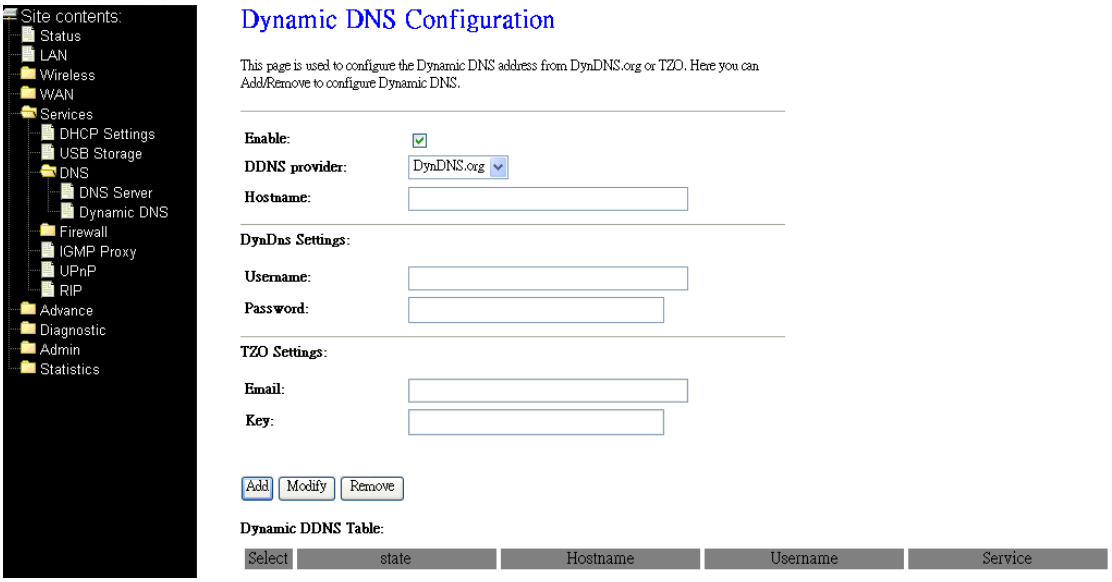
This page is used to configure the DNS server IP addresses for DNS Relay.



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 radio button to configure up to three DNS IP addresses manually.

4.5.3.2 Dynamic DNS

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

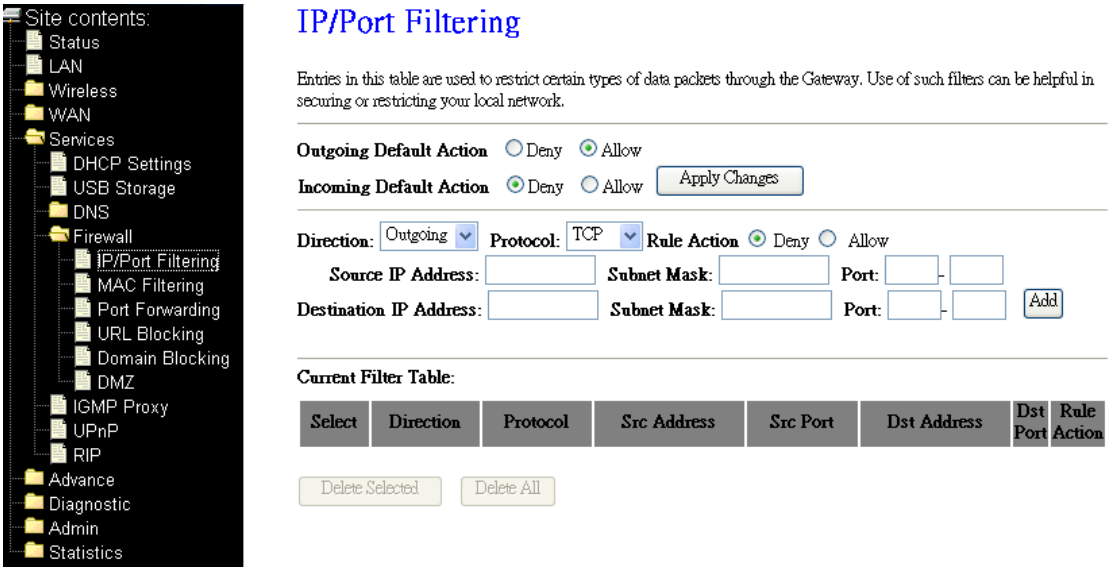


Field	Description
Enable	Check to enable this registration account for the DNS server.
DDNS Provider	There are two DDNS providers to be selected in order to register your device with: DynDNS and TZO. A charge may occur depends on the service you select.
Hostname	Enter the domain name to be registered with the DDNS server.
DynDNS Username / Password	Enter the user name and password of your registered account in DDNS service provider DynDNS.
TZO Email / Key	Enter the e-mail address and key (password) of your registered account in DDNS service provider TZO.

4.5.4 Firewall

4.5.4.1 IP/Port Filtering

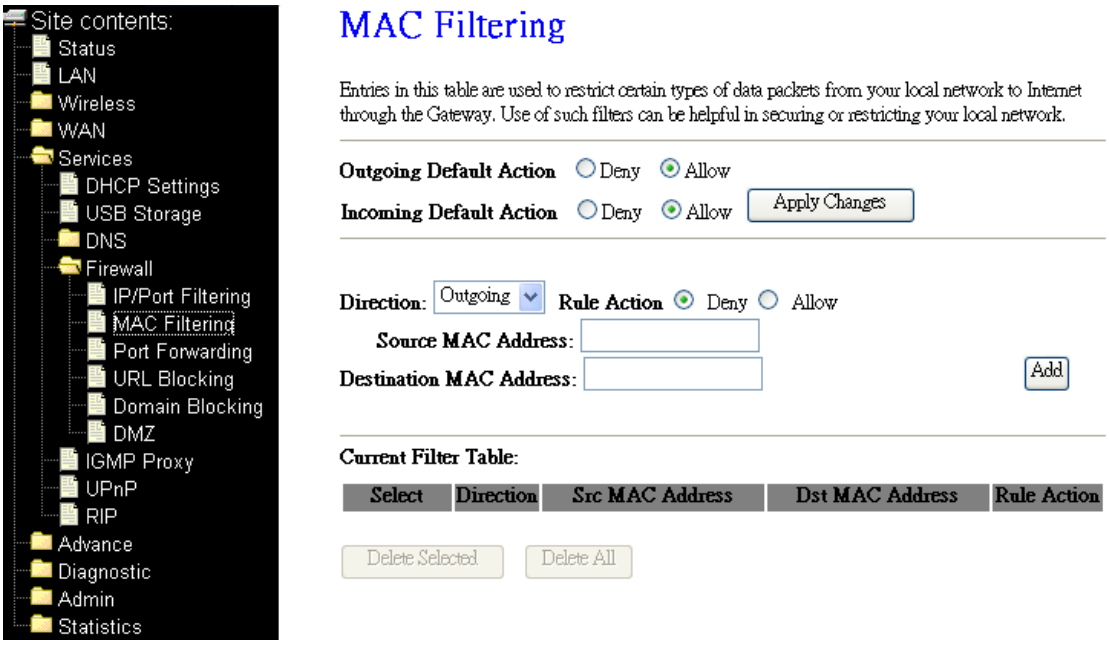
This page allows you to create entries to identify outgoing and incoming IP traffic by specifying the source and destination IP addresses. Entries in the below table are used to restrict certain types of data packets through the ADSL Router. Use of such filters can be helpful in securing or restricting your local network.



Field	Description
Outgoing Default Action	Select to deny or allow the default action on the LAN to WAN forwarding path.
Incoming Default Action	Select to deny or allow the default action on the WAN to LAN forwarding path.
Direction	Select the traffic forwarding direction.
Protocol	There are 3 options available: TCP, UDP and ICMP.
Rule Action	Select to deny or allow traffic when matching this rule.
Source IP Address	The source IP address assigned to the traffic on which filtering is applied.
Source Subnet Mask	Enter the subnet mask of the source IP.
Source Port	Enter the starting and ending source port numbers.
Destination IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Destination Subnet Mask	Enter the subnet mask of the destination IP.
Destination Port	Enter the starting and ending destination port numbers.

4.5.4.2 MAC Filtering

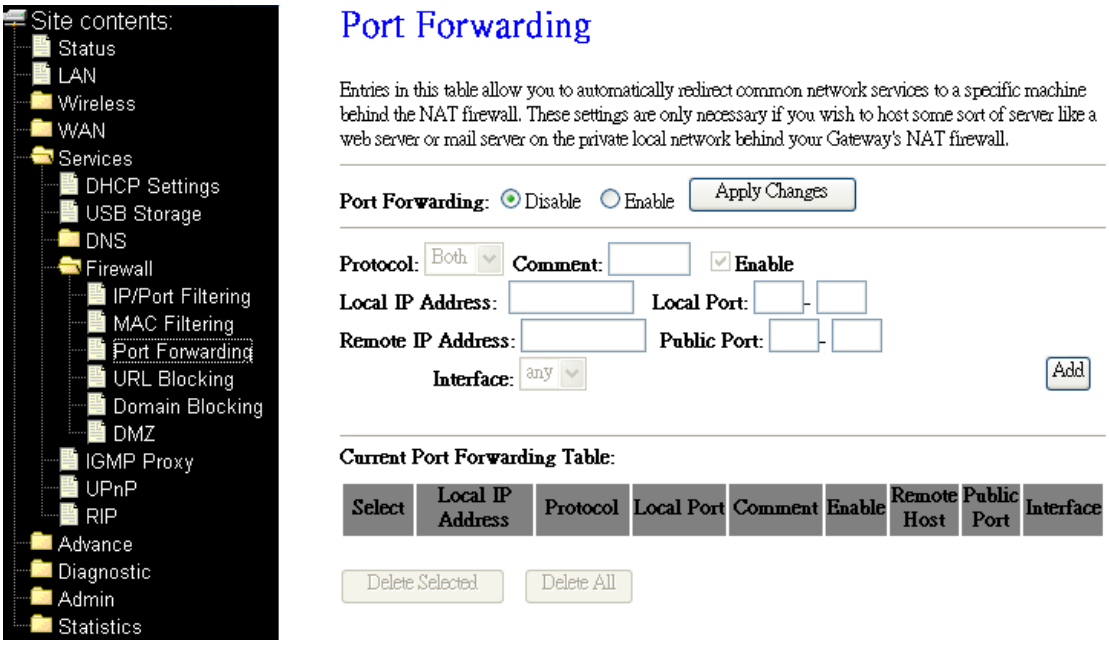
This page allows you to manage whether a LAN client is allowed to access the ADSL Router or not based on the MAC address of device. Entries in the below table are used to restrict certain types of data packets from your local network to Internet through the ADSL Router. Use of such filters can be helpful in securing or restricting your local network.



Field	Description
Outgoing Default Action	Select to deny or allow the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Action	Select to deny or allow the default action on the WAN to LAN bridging/forwarding path.
Rule Action	Select to deny or allow traffic when matching this rule.
Direction	Select the traffic bridging/forwarding direction.
Source MAC Address	Enter the source MAC address. It must be xxxxxxxxxxx format.
Destination MAC Address	Enter the destination MAC address. It must be xxxxxxxxxxx format.

4.5.4.3 Port Forwarding

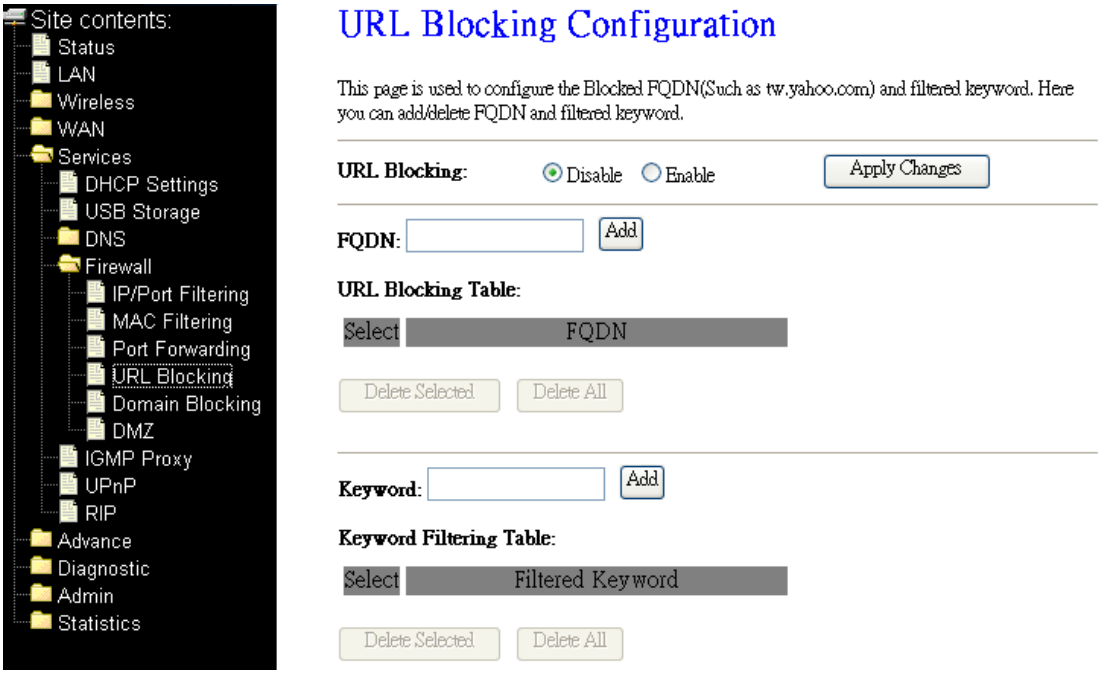
This page is used to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your ADSL Router's NAT firewall.



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

4.5.4.4 URL Blocking

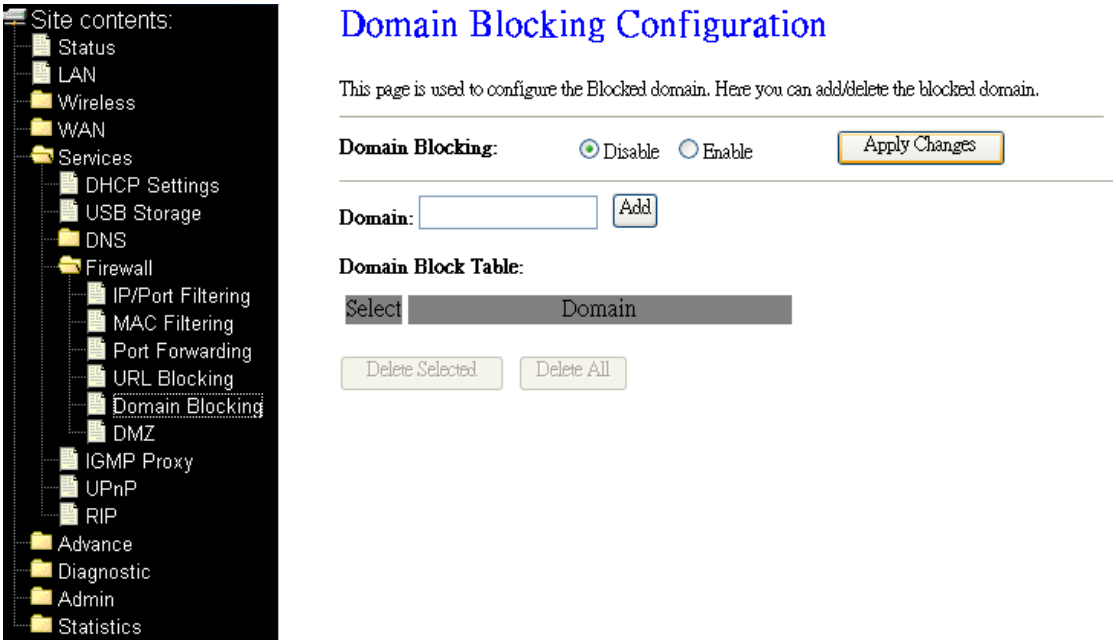
This page is used to configure the blocked FQDN (Fully Qualified Domain Name, such as http://www.yahoo.com) or filtered keywords. If you want to prevent computers in local network from accessing certain website (like pornography, violence, or anything you want to block), you can use this function to stop computers in local network from accessing the site you configured in this page.



Field	Description
URL Blocking Capability	Select the radio button to enable/disable URL blocking function.
FQDN	Enter the URL (host name or IP address of website, such as http://www.blocked-site.com or http://11.22.33.44) you want to block.
Keyword	Enter the keyword which is contained in URL (such as pornography, cartoon, stock or anything) you want to block.
Keyword Filtering Table	This table lists all the existing URL/Keywords in filtering table.

4.5.4.5 Domain Blocking

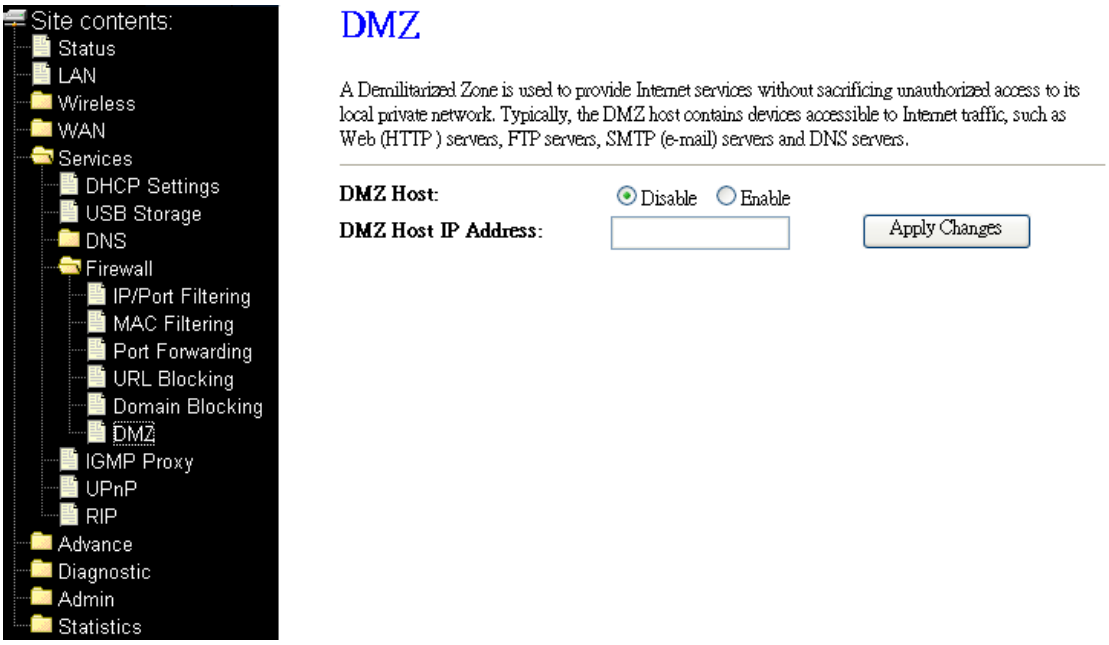
This page is used to configure the blocked domain. Here you can add or delete the blocked domain.



Field	Description
Domain Blocking Capability	Select the radio button to enable/disable domain blocking function.
Domain	Enter the domain you want to block.
Domain Block Table	This table lists all the existing domains in blocking table.

4.5.4.6 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.

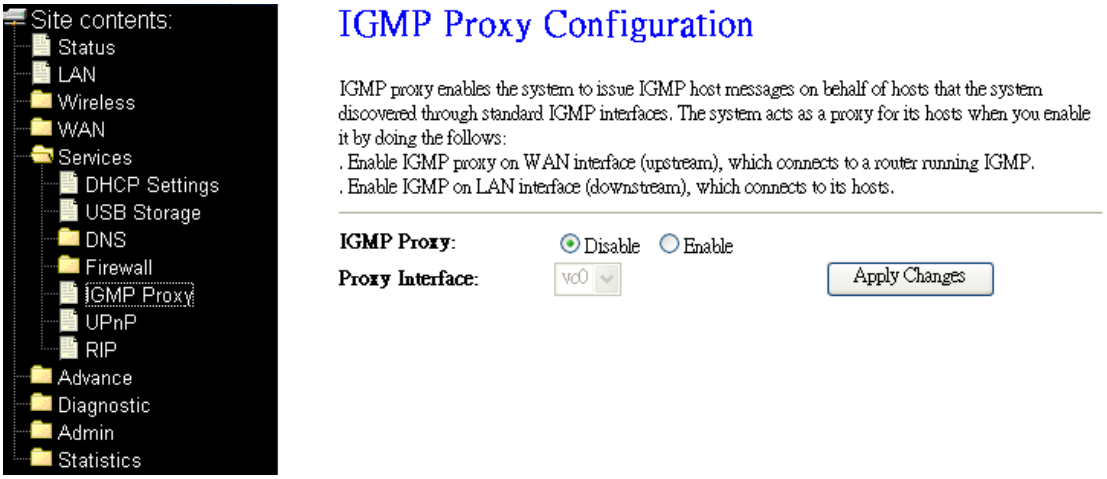


Field	Description
DMZ Host	Select the radio button to enable/disable DMZ.
DMZ Host IP Address	Enter the IP address of the DMZ host.

4.5.5 IGMP Proxy

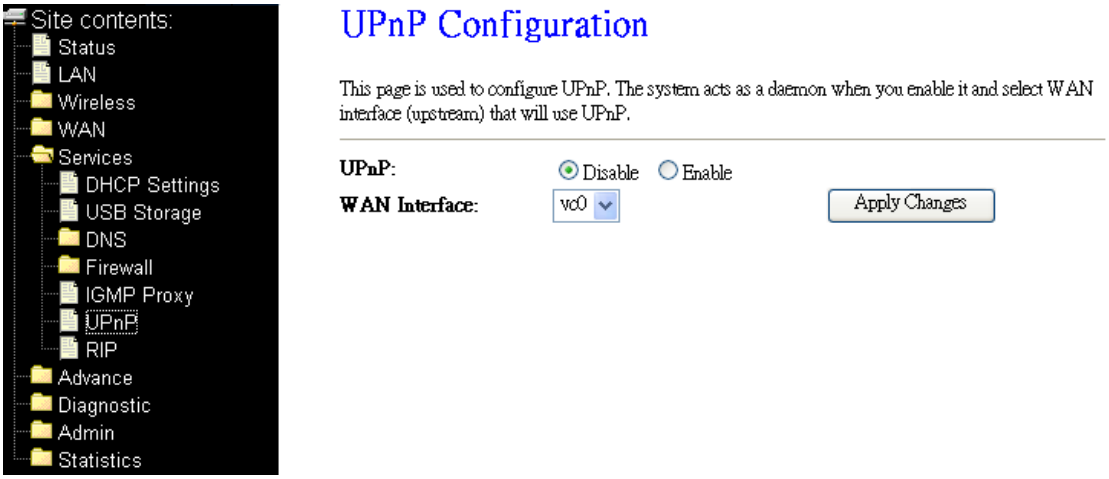
The page allows you to enable or disable the IGMP (Internet Group Management Protocol) proxy. IGMP is used to establish the multicast groups to forward the multicast packet to the member ports. It can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications.
IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:

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



4.5.6 UPnP

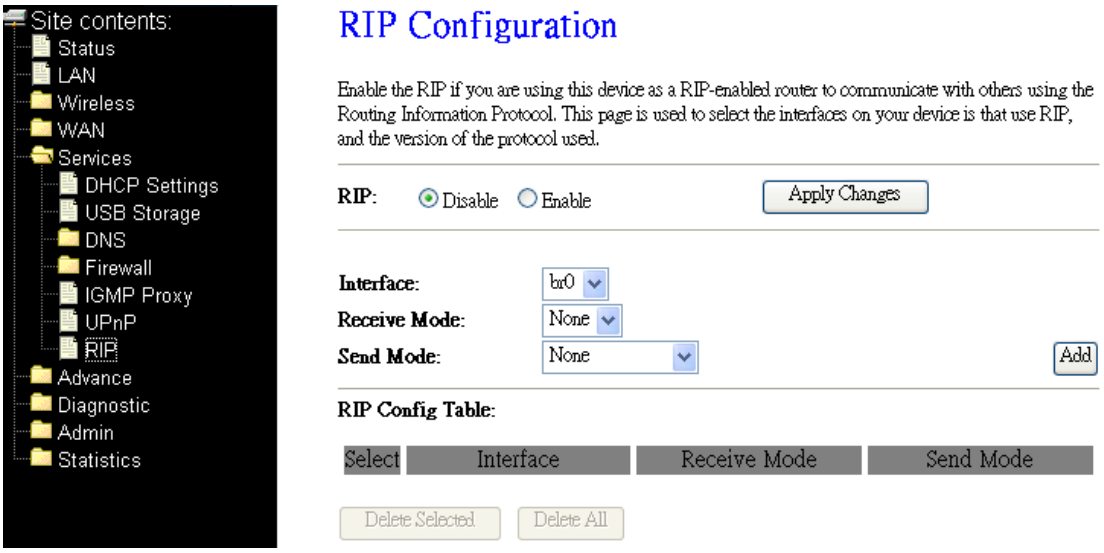
The Freeway DSL supports a control point for Universal Plug and Play (UPnP) version 1.0, and supports two key features: **NAT Traversal** and **Device Identification**. This feature requires one active WAN interface. In addition, the host should support this feature. In the presence of multiple WAN interfaces,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



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

4.5.7 RIP (Routing Information Protocol)

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 that uses RIP, and the version of the protocol used.

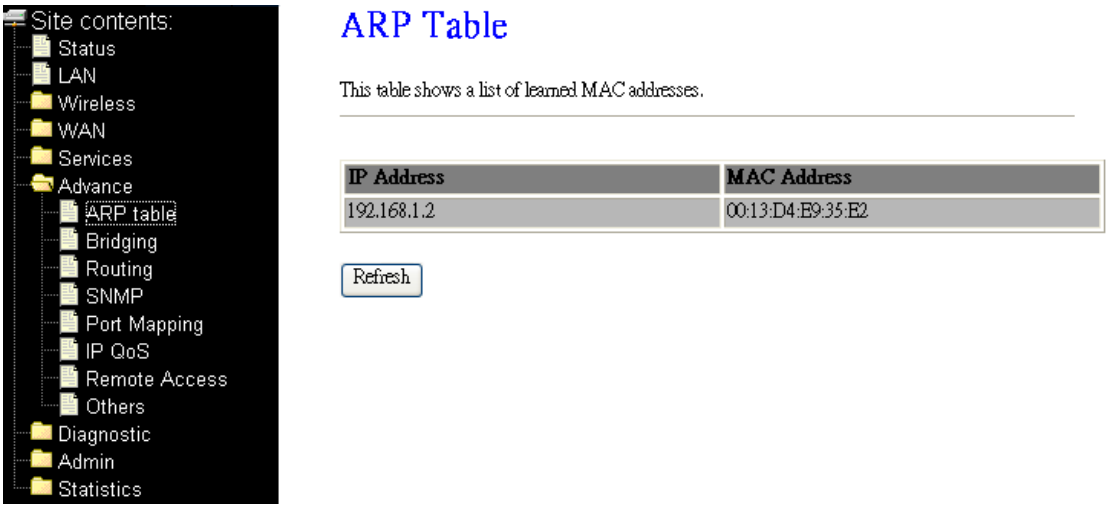


Field	Description
RIP	Select the radio button to enable/disable RIP.
Interface	Select an interface when using Freeway DSL as an RIP router to communicate with others.
Receive Mode	Select the RIP version from drop-down for receiving mode.
Send Mode	Select the RIP version from drop-down for sending mode.
RIP Config Table	This table lists all the information of RIP configuration.

4.6 Advanced

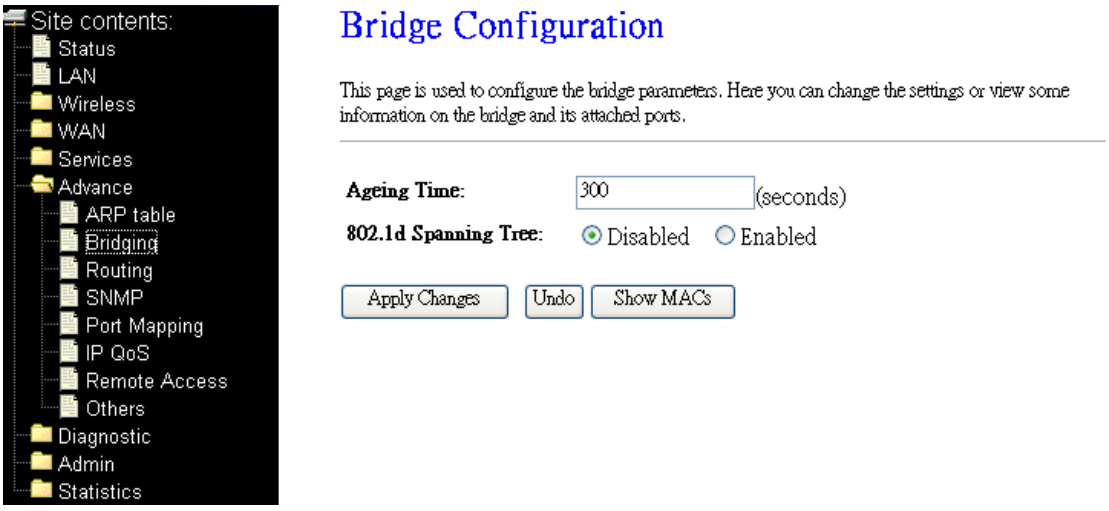
4.6.1 ARP (Address Resolution Protocol) Table

This table shows a list of learned MAC addresses (ARP table).



4.6.2 Bridging

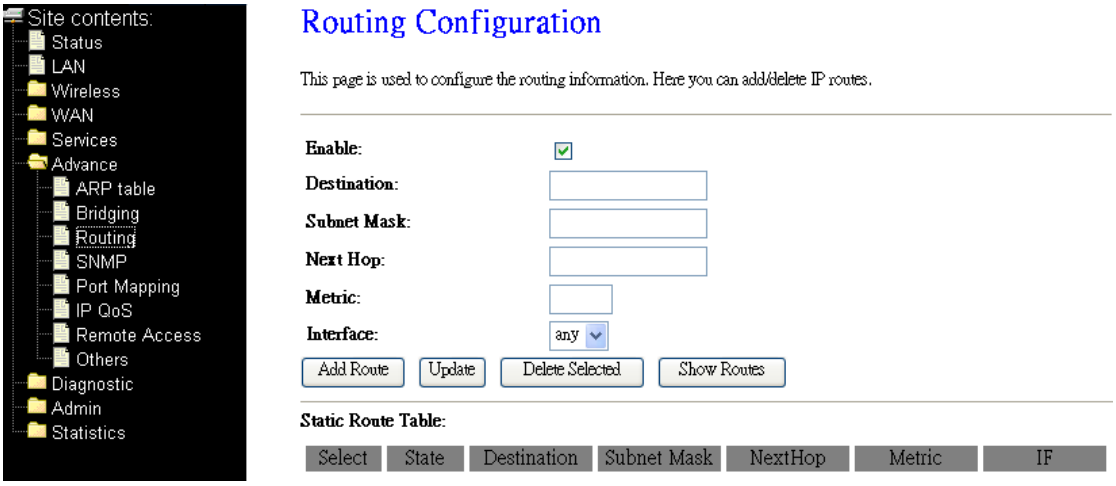
This page is used to configure the bridge parameters. A bridge is a device used to interconnect network segments and pass packets between those network segments. You can change the settings or view some information on the bridge and its attached ports.



Field	Description
Ageing Time	Configure the ageing time. The aging time is the number of seconds a MAC address will be kept in the forwarding database after having received a packet from this MAC address.
802.1d Spanning Tree	Select the radio button to enable/disable 802.1d spanning tree. If you are running multiple or redundant bridges, then you need to enable the Spanning Tree Protocol (STP) to handle multiple hops and avoid cyclic routes.

4.6.3 Routing

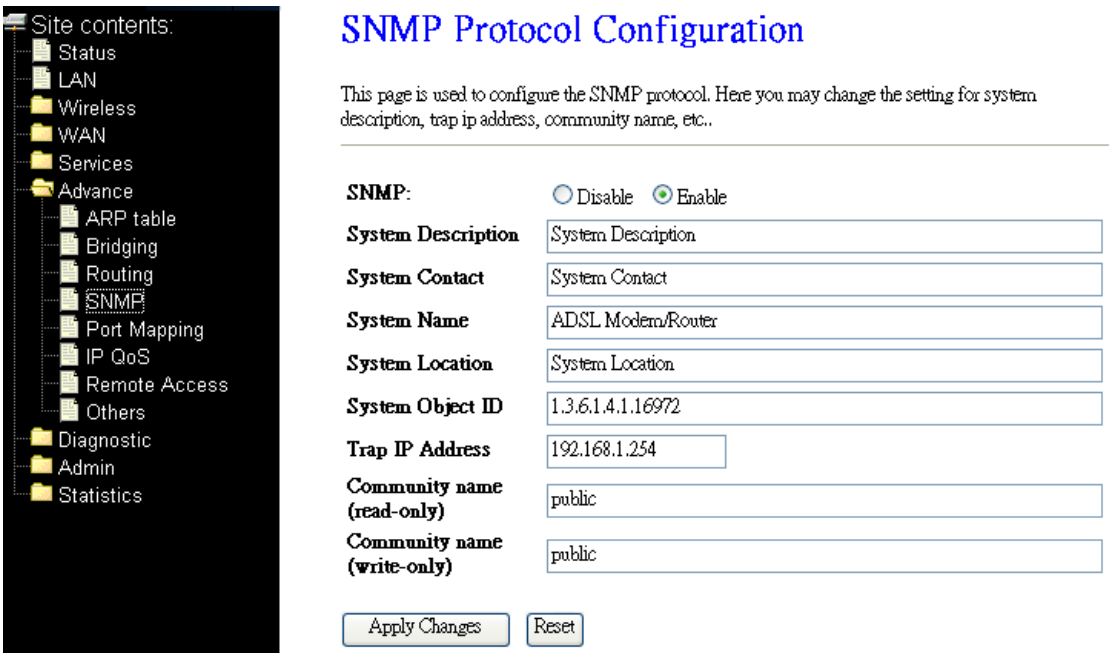
The Routing page enables you to define specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the Freeway DSL provide the most appropriate path for all your Internet traffic.
On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the Freeway DSL. 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 Freeway DSL 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.



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

4.6.4 SNMP (Simple Network Management Protocol)

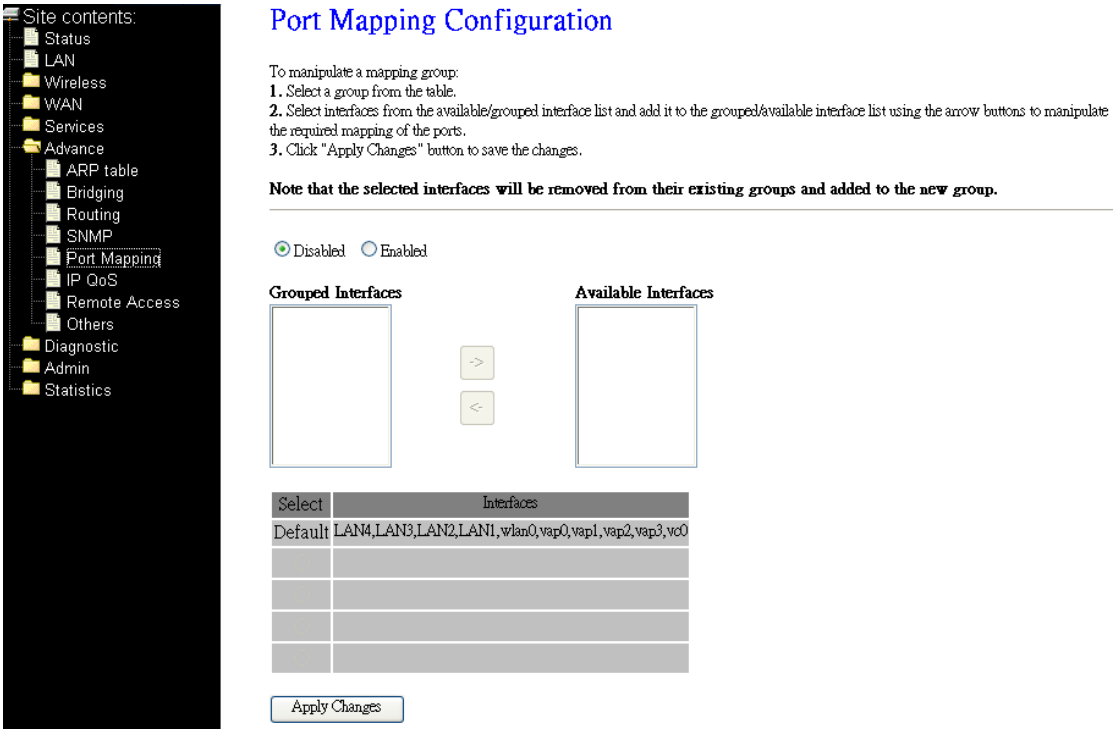
This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap IP address, community name, etc.



Field	Description
System Description	Specify a description for this system.
System Contact	Specify the system contact.
System Name	Specify the system name.
System Location	Specify the system location.
System Object ID	Specify the object ID.
Trap IP Address	Specifies the Trap host IP address.
Community Name (read-only)	Enter the read community string for authorizing read-only rights. The default string is public.
Community Name (write-only)	Enter the write community string for authorizing write-only rights. The default string is public.

4.6.5 Port Mapping

This page allows you to configure various port mapping groups which contains specific Internet connections and LAN ports. The data will be only transmitted and received among the interfaces in the group. To manipulate a mapping group:

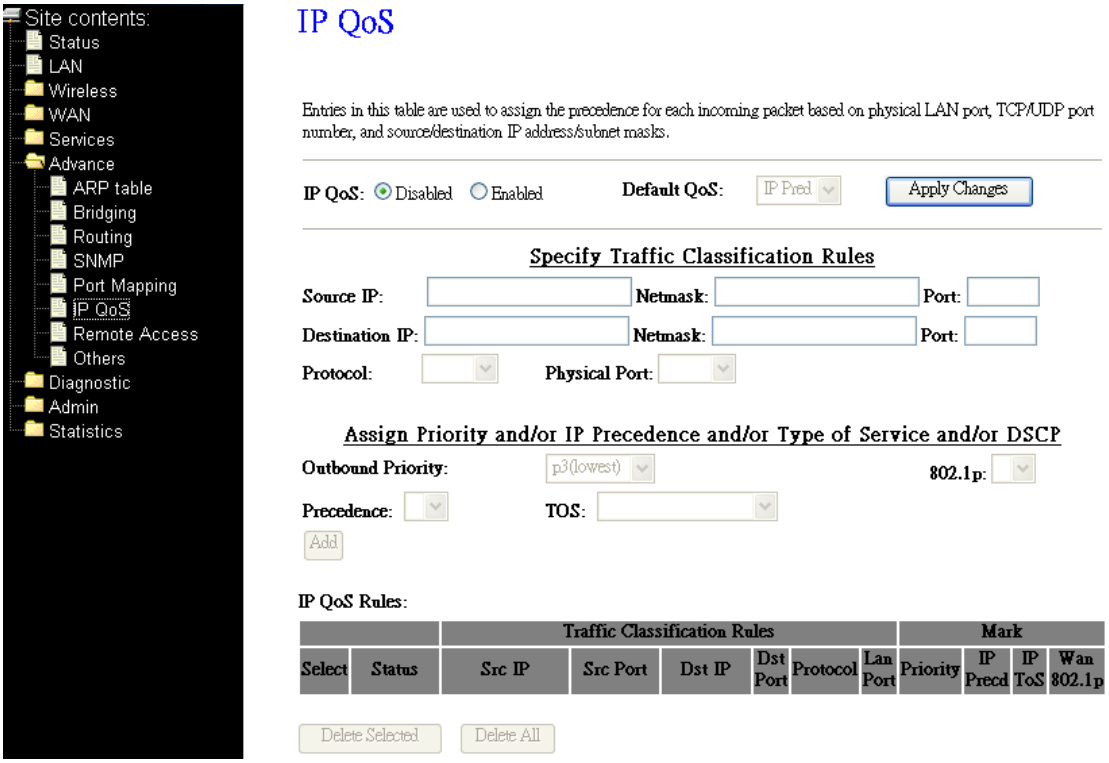


To configure port mapping, please follow the following instructions:

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. The selected interfaces will be removed from their existing groups and added to the new group.
3. Click "Apply Changes" button to save the changes.

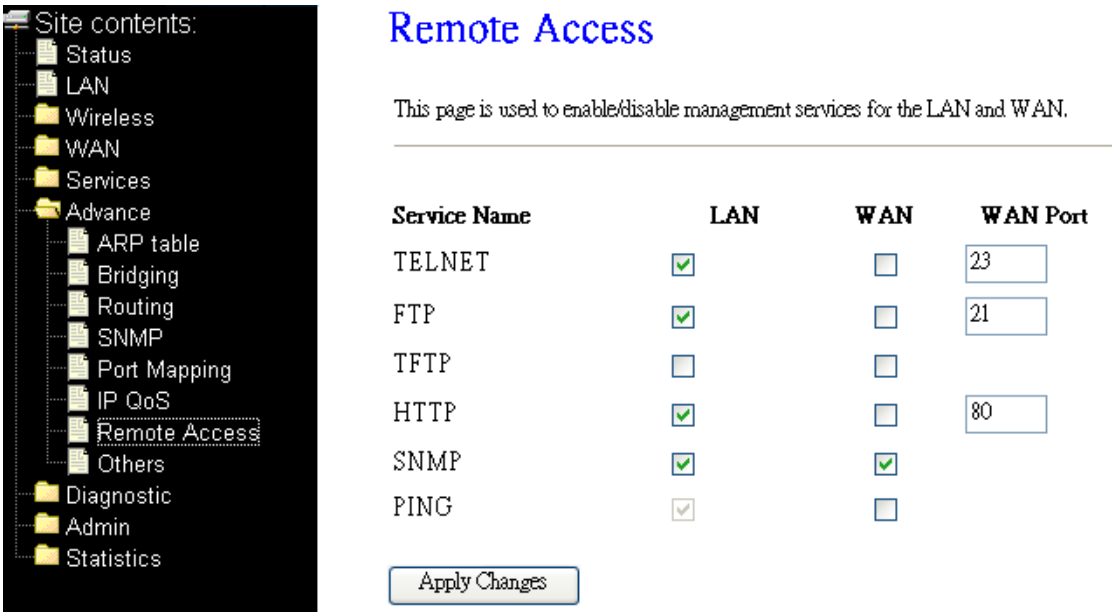
4.6.6 IP QoS (Quality of Service)

This page allows you to configure the data transmission priority based on layer three IP packets. Here you can assign the precedence to each incoming packet based on physical LAN port, TCP/UDP port number, and source/destination IP address/subnet masks.



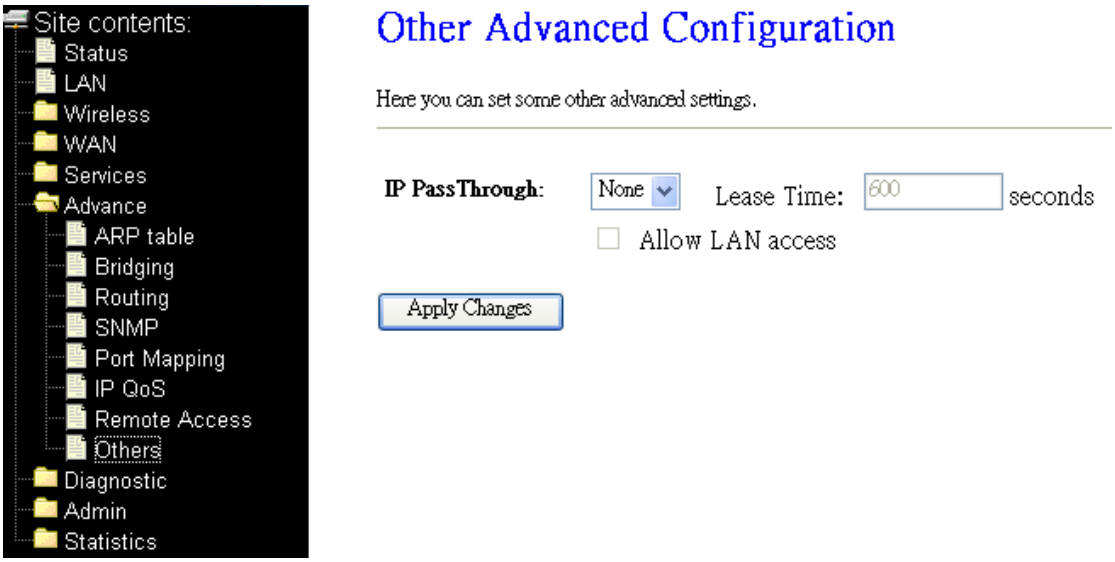
4.6.7 Remote Access

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



4.6.8 Others Advanced Configuration

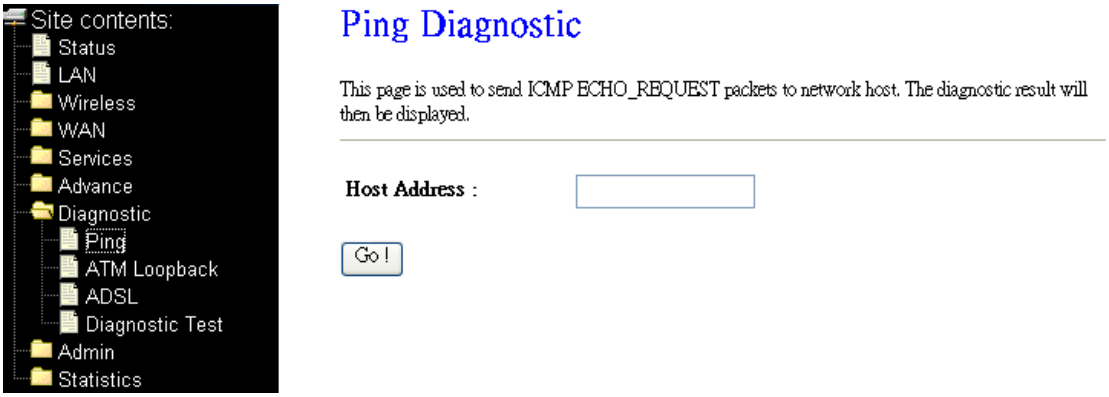
This page allows you to configure IP pass-through mode.



4.7 Diagnostic

4.7.1 Ping

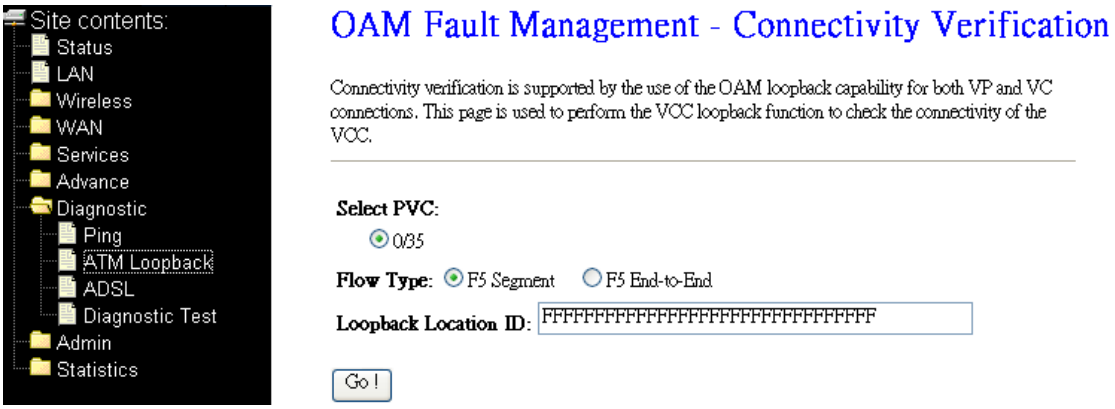
This page is used to send ICMP ECHO_REQUEST packets to network host. The diagnostic result will then be displayed.



Field	Description
Host Address	Enter the IP you want to PING and the press **Go!** Button to run ping diagnostic.

4.7.2 ATM Loopback

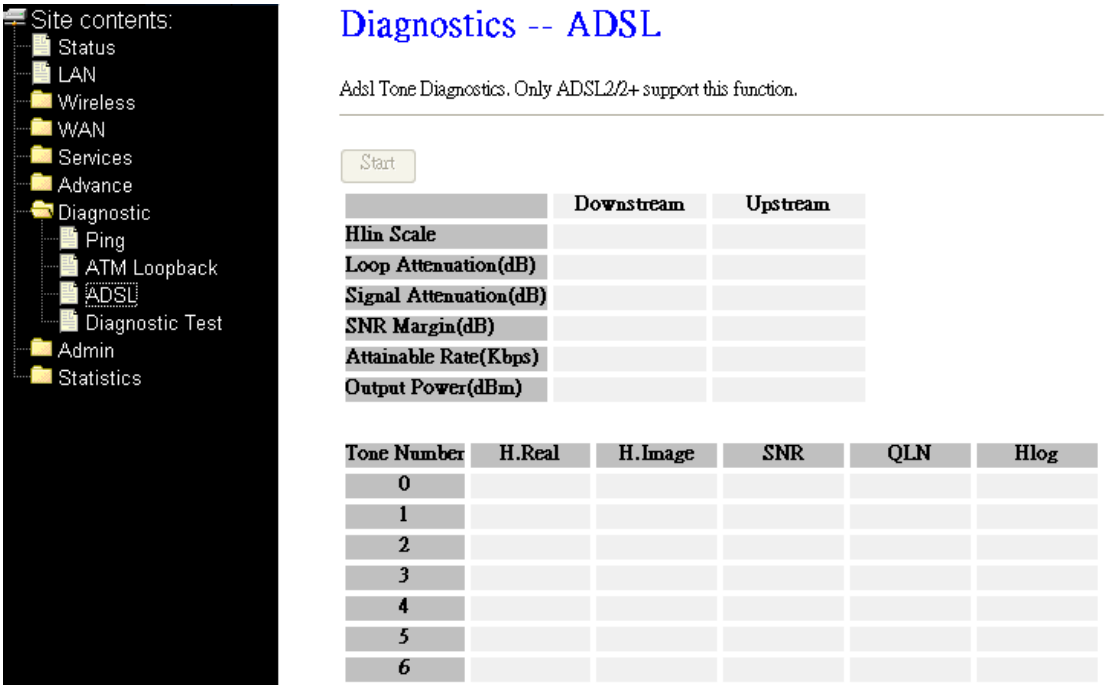
Connectivity verification is supported by the use of the OAM loopback capability for both VP ((Virtual Path) and VC (Virtual Channel) connections. This page is used to perform the VCC (Virtual Channel Connection) loopback function to check the connectivity of the VCC.



Field	Description
Select PVC	Select the PVC for connectivity verification.
Flow Type	Select the flow type to run loopback.
Loopback Location ID	Enter the location ID to run loopback.

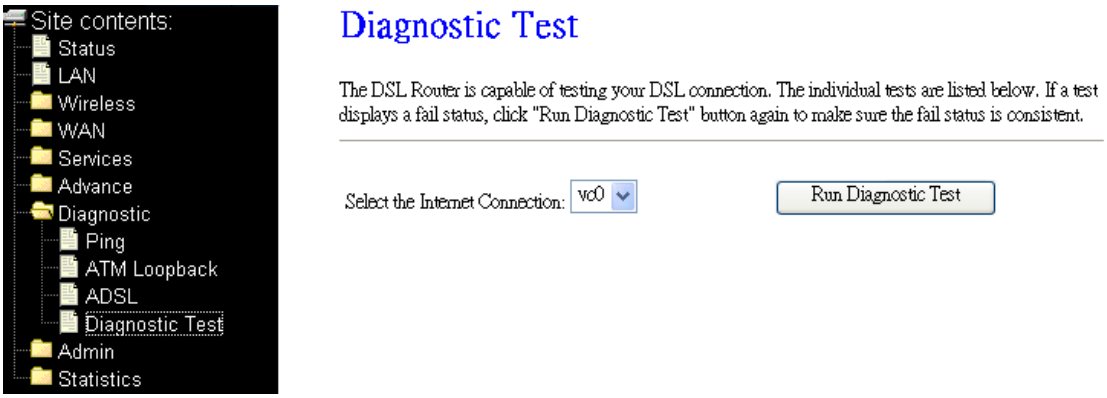
4.7.3 ADSL

This page shows the ADSL tone diagnostic information. 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.



4.7.4 Diagnostic Test

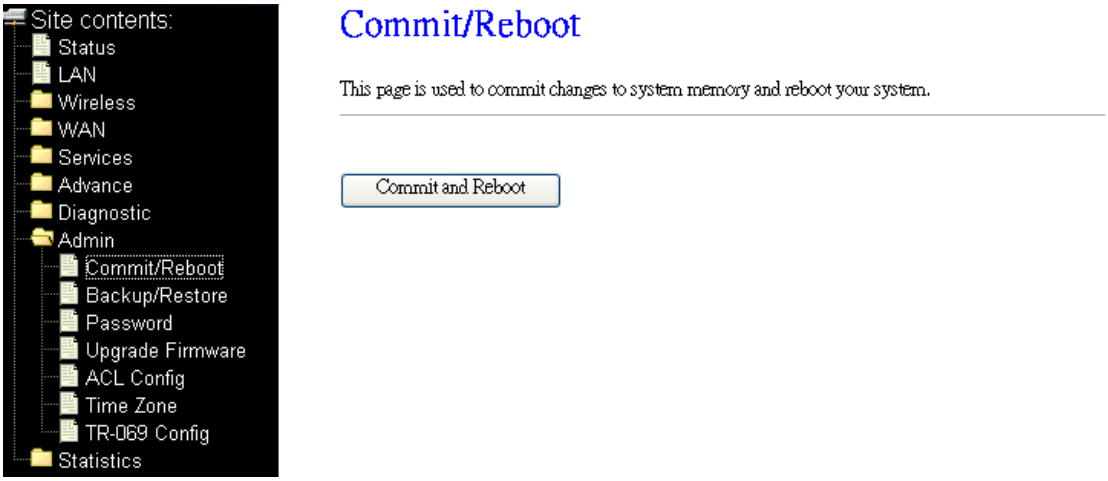
The Freeway DSL is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.



4.8 Admin

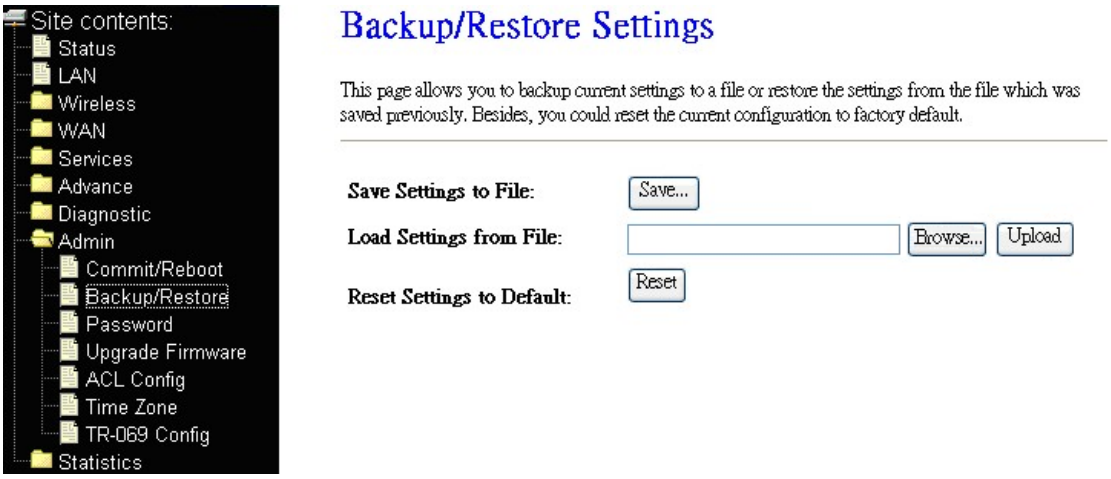
4.8.1 Commit/Reboot

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



4.8.2 Backup/Restore

This page allows you to backup current settings to a file, or restores the settings from a file which was saved previously. Besides, you could reset the current configuration to factory default. This is the same function as you press the Reset button on the rear panel for more than 8 seconds.



To save settings to a file, just click the **Save** button to save the file to a local drive.

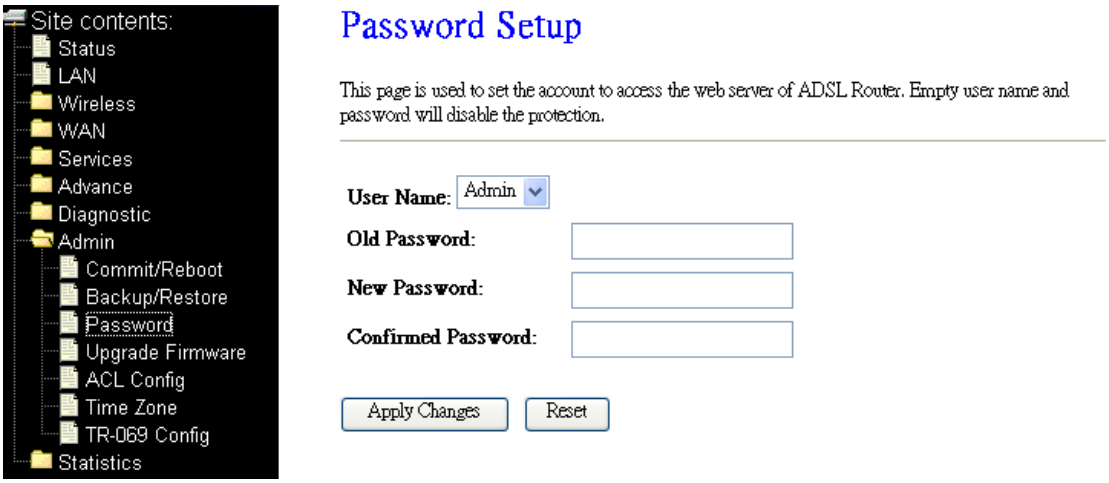
To load settings from a file, please follow the following instructions:
1. Click the **Browse** button to select the saved file.
2. Confirm your selection.
3. Click the **Upload** button to start restoring.

To reset all the current settings, just click **Reset** button to reset all settings to default value. This is the same as you push the **Reset** button on the rear panel of Freeway DSL.

IMPORTANT! Do NOT power off the Freeway DSL or press the Reset button while this procedure is in progress.

4.8.3 Password

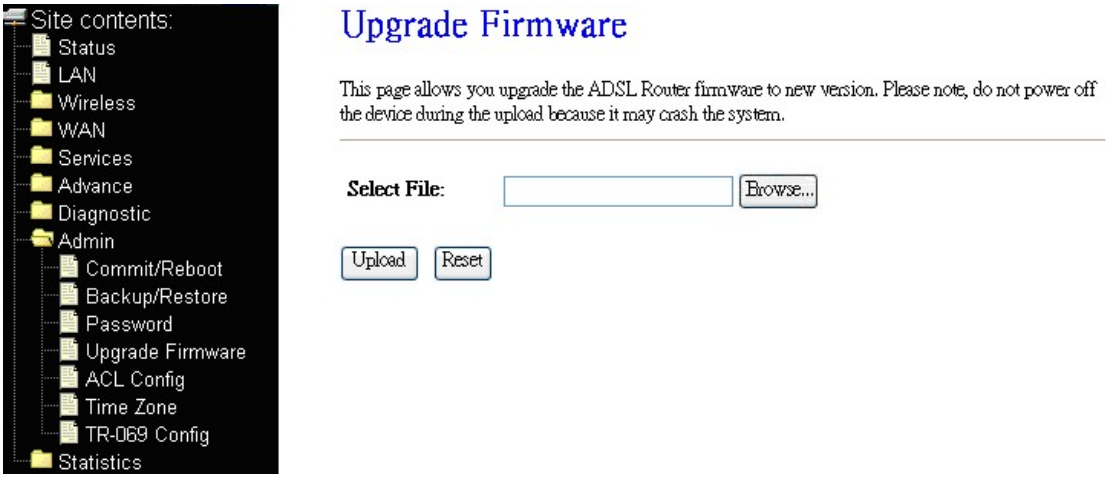
This page is used to set the account to access the web server of Freeway DSL. The first time you log into the system with default password and you may change it here. Empty user name and password will disable the protection.



Field	Description
User Name	Select the login user name.
Old Password	Enter the old password in this field.
New Password	Enter the new password in this field.
Confirmed Password	Enter the new password in this field to confirm the password.

4.8.4 Upgrade Firmware

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



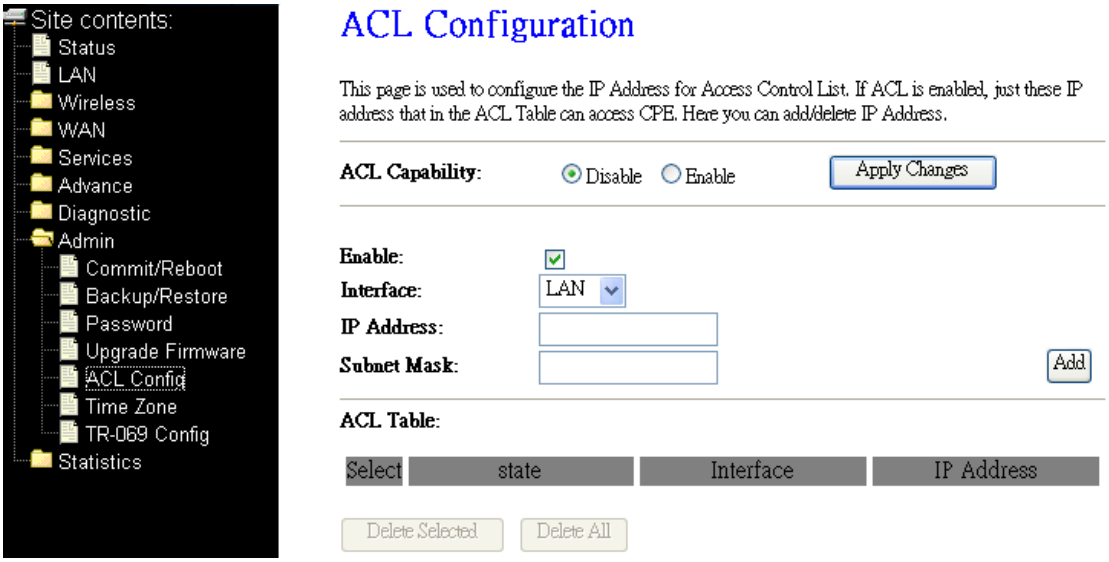
To upgrade firmware, please follow the following instructions:

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

IMPORTANT! Do NOT power off the Freeway DSL or press the Reset button while this procedure is in progress.

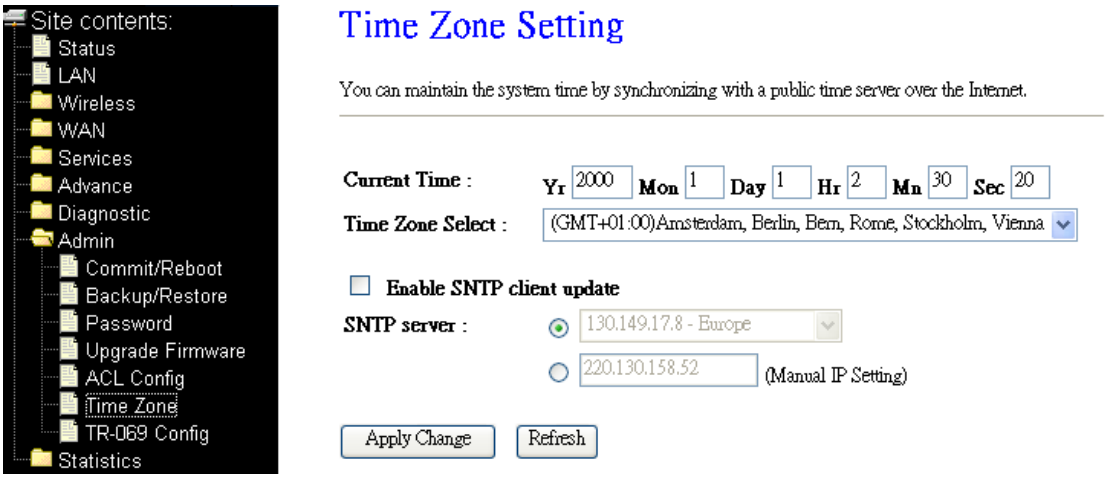
4.8.5 ACL Configuration

This page is used to configure the IP Address for ACL (Access Control List). If ACL is enabled, only the IP address that in the ACL Table can access Freeway DSL.



4.8.6 Time Zone

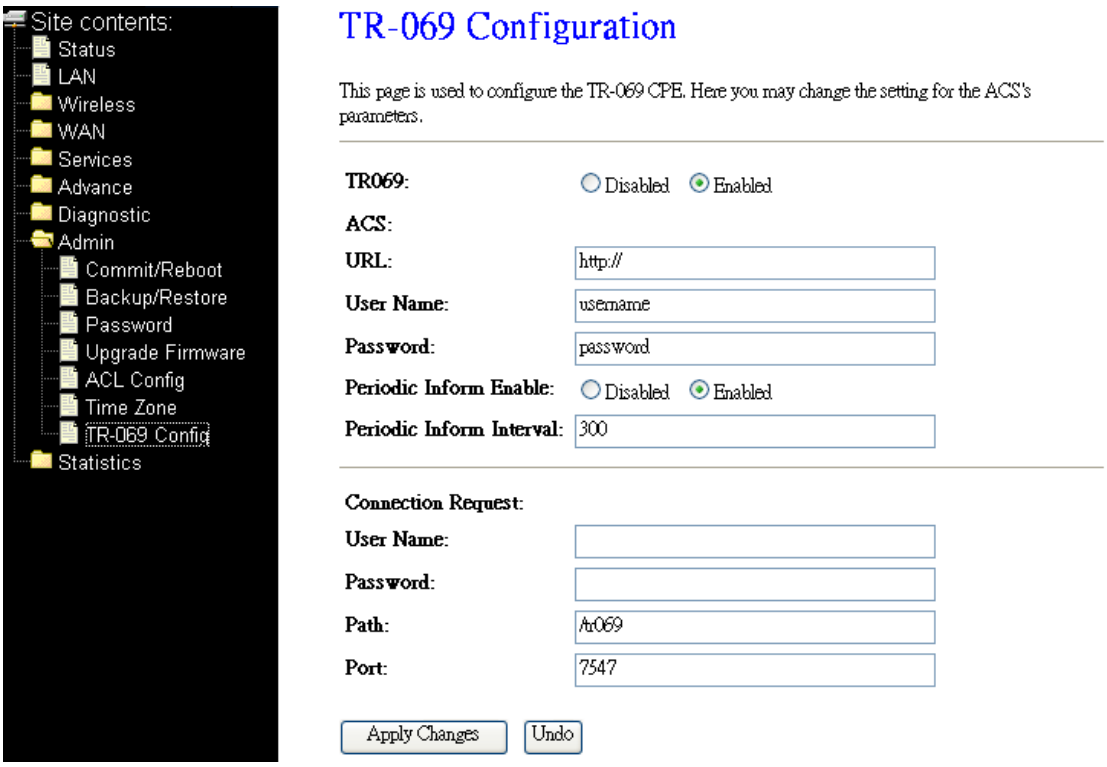
This page allows you to maintain the system time by synchronizing with a public time server over the Internet. Simple Network Timing Protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. The Freeway DSL supports SNTP client functionality in compliance with IETF RFC2030. This page allows you to manually configure the time and select Time Zone. Also, you can enable SNTP client update function and configure the SNTP server to let the Freeway DSL synchronize with the public SNTP servers.



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 Freeway DSL 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 setup it manually.

4.8.7 TR-069 Configuration

This page is used to configure the TR-069 (WAN Management Protocol) CPE (Customer Premises Equipment). Here you may change the setting for the ACS's parameters.

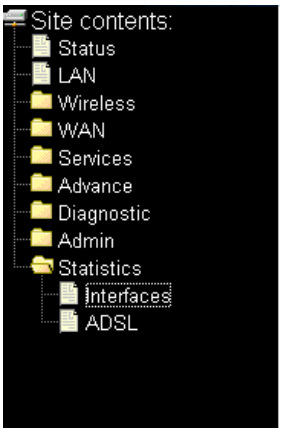


Field	Description
TR069	Enable or disable TR-069.
ACS URL	Enter the URL of the Auto Configuration Server (ACS) provided by the ISP.
ACS User Name	Enter the user name for the ACS to authenticate.
ACS Password	Enter the password for the ACS to authenticate.
Periodic Inform Enable	Enable or disable the Freeway DSL to connect to the ACS periodically.
Periodic Inform Interval	Enter the amount of time (in second) between a successful connection with an ACS server and a new attempt to connect to an ACS server. This field is enabled only when the Inform **Enabled** is selected.
Connection Request User Name	Enter the username used to authenticate an ACS making a connection request to the Freeway DSL.
Connection Request Password	Enter the password used to authenticate an ACS making a connection request to the Freeway DSL.
Connection Request path	Specify the path the ACS can use to reach the Freeway DSL.
Connection Request Port	Specify the port number the ACS can use to reach the Freeway DSL.

4.9 Statistics

4.9.1 Interfaces

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



Statistics -- Interfaces

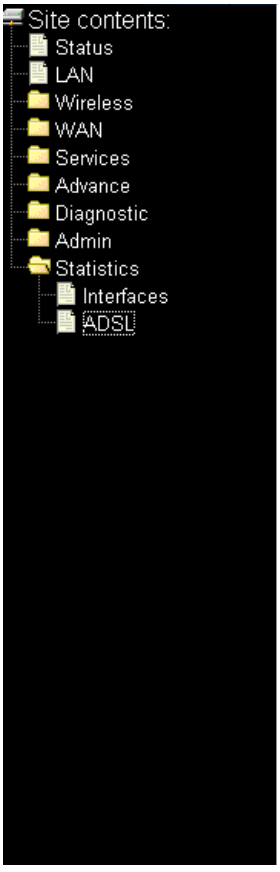
This page shows the packet statistics for transmission and reception regarding to network interface.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0	202	0	0	190	0	0
wlan0	1430	0	0	6540	0	0
0_35	0	0	0	0	202	0

Refresh

4.9.2 ADSL

This page shows the information of ADSL line status and statistics.



Statistics -- ADSL Line

Mode	
Latency	
Trellis Coding	Enable
Status	ACTIVATING.
Power Level	L0

	Downstream	Upstream
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power (dBm)	0.0	25.5
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

Appendix A. Troubleshooting

Below is a list of commonly asked questions. Before calling technical support, please look through these issues to see if they help solve your problem.

The Freeway DSL is not functional.

1. Check to see that the POWER LED is lit and than the network cables are installed correctly. Refer to the Quick Start Guide for more details.
2. Check to see that the LAN, DSL and Internet LEDs are lit.
3. Check the settings on your PC and Freeway DSL. Again, refer to the Quick Start Guide for more details.
4. From your PC, can you PING the Freeway DSL? Assuming that the Freeway DSL has DHCP enabled and your PC is on the same subnet as the Freeway DSL, you should be able to PING the Freeway DSL.
5. Can you PING the Internet? Your ISP should have provided the IP address of their server. If you can ping the Freeway DSL and your protocols are configured correctly, you should be able to ping the ISPs network. If you cannot PING the ISP's network, make sure your using the correct protocols with the correct VPI/VCI values.

I can't connect to the Freeway DSL.

1. Check to see that the POWER LED is lit and that the network cables are installed correctly.
2. Make sure that the PC and the Freeway DSL is on the same network segment. The Freeway DSL's default IP address is 192.168.1.1. If you are running a Windows based PC, you can open a DOS window and type IPCONFIG; make sure that the network adapter that is connected to the Freeway DSL is within the same subnet.
3. Also, your PC's Subnet Mask should match the Freeway DSL's subnet mask. The Freeway DSL has a default subnet mask of 255.255.255.0.
4. If this still does not work, press the Reset button for more than 8 seconds. This will place the Freeway DSL into its factory default state. Go through the above procedures again.

The DSL LED continues to blink but does not go solid.

1. Make sure you have DSL service. You should get some kind of information from your ISP which states that DSL service is installed. You can usually tell if the service is installed by listening to the ADSL phone line; you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.
2. This means that the DSL line is trying to train but for some reason it cannot establish a valid connection. The main cause of this is that you are too far away from the central office. Contact your DSL service provider for further assistance.
3. Verify that the DSL line is connected directly to the wall and to the line input on the Freeway DSL.

The Internet Link LED is always off.

1. Make sure you have DSL service. You should get some kind of information from your ISP which states that DSL service is installed. You can usually tell if the service is installed by listening to the phone line; you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.
2. Verify that the phone line is connected directly to the wall and to the line input on the Freeway DSL. If the Freeway DSL is connected to the wall outlet via a splitter, make sure you connect the Freeway DSL to the port labeled MODEM.

I cannot ping the Freeway DSL from the attached LAN.

1. Verify that the IP addresses are properly configured. In most cases, you enable the Freeway DSL's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Freeway DSL and any attached LAN devices.
2. Make sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP correctly.

I cannot connect using the web browser.

1. Be sure to have configured the Freeway DSL with a valid IP address, subnet mask and default gateway.
2. Check to see if you have a valid network connection to the Freeway DSL and the port you are using has not been disabled.
3. Check the network cabling between the attached PC and the Freeway DSL.

I forgot or lost the password.

1. Press the Reset button on the rear panel (holding it down for at least 8 seconds) to restore the factory defaults.

Appendix B. Specification

One ADSL port for WAN
One USB 2.0 host port for USB mass storage or printer
Four 10/100 Mbps Fast Ethernet ports for LAN
IEEE 802.11 b/g Wireless AP

ADSL Compliance
- Support Multi mode standard (ANSI T1.413 Issue 2, G.dmt, G.lite)
- ADSL2 G.dmt.bis (G.992.3)
- ADSL2 G.lite.bis (G.992.4)
- ADSL2+ (G.992.5)
- Reach Extended ADSL (RE ADSL)

ATM Protocols
- 8 PVC Support
- VC and LLC multiplexing
- OAM F4/F5 Loop Back

PPP Support
- PPP over ATM PVC (RFC 2364&RFC1577)
- PPP over Ethernet (RFC 2516)
- PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol)

Network Stack
- NAT: Static Port Mappings, NAT Policies, UPnP NAT Traversal
- Packet backbone: ICMP, ARP, RARP, UDP, TCP, Multicast, IPv4, DHCP Client / Relay / Server, DNS Proxy, DDNS, IGMP v1&v2, IGMP Proxy, IGMP Snooping
- Bridging: IEEE 802.1d Bridge
- Routing: Static route, RIP v1 / v2

Firewall / Security
- SPI: Stateful Packet Inspection Firewall
- DOS Protection
- Management Access Control for LAN/WAN
- IPSec / PPTP/L2TP Pass through
- Port Forwarding
- DMZ Host
- Filtering
  - Bi-direction IP Filter on LAN/WAN
  - IP/MAC/URL/Keyword Filtering
  - Domain Blocking

Quality of Service (QoS)
- Constant Bit Rate (CBR), Real-Time Variable Bit Rate (VBR-rt)
- Non-Real-Time Variable Bit Rate (VBR-nrt)

Management
- Remote / Local configuration & management
- Web / Telnet configuration & management
- Firmware upgrade through web management

Wireless Specification

- Standard: IEEE 802.11b/g for wireless LAN
- Frequency Band: 2.400 ~ 2.4835 GHz ISM Band
- Modulations
- 802.11g: OFDM (64QAM, 16QAM, QPSK, BPSK)
- 802.11b: CCK (11 Mbps, 5.5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
- Data Rate: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54Mbps
- Encryption
  - Hardware-based IEEE 802.11i encryption / decryption engine
  - Includes 64-bit/128-bit WEP, TKIP and AES
- Operating Range
  - Open space: 100m ~ 300m
  - Indoor: 35m ~ 100m