ADSL2+ 4-Port Switch Wired/Wireless Router FREEWAY DSL User's Manual

Revision 0.2
February 2008

FCCInformation

Federal Communication Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Table of Contents

1. Introduction

The FREEWAY DSL is an ADSL2+ router which integrates a 4-port Fast Ethernet Switch and Wireless AP (wirelsss model only). The 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 (wireless model only). The FREEWAY DSL is compatible with ADSL, ADSL2, and ADSL2+ lines for worldwide ADSL deployment. Not only supports versatile router features, the FREEWAY DSL supports robust QoS and IGMP features to ensure high quality triple play.

The FREEWAY DSL adopts easy to use web-GUI management interface. Its user friendly interface will amaze you with total difference experience. The 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 (wireless model only)
- Integrate ADSL router and wireless AP (Access Point) together (wireless model only)
- Enables sharing of broadband Internet connection
- Works with both PCs and Macintosh computers
- Connects four computers/devices through the LAN ports
- Connects 32 computer/devices wirelessly (wireless model only)
- Operates on 2.4 frequency band including all 802.11b/g mode (wireless model only)
- Security supports WPA/WPA2-PSK, & 64/128-bit WEP Encryption (wireless model only)
- 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)
- 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.

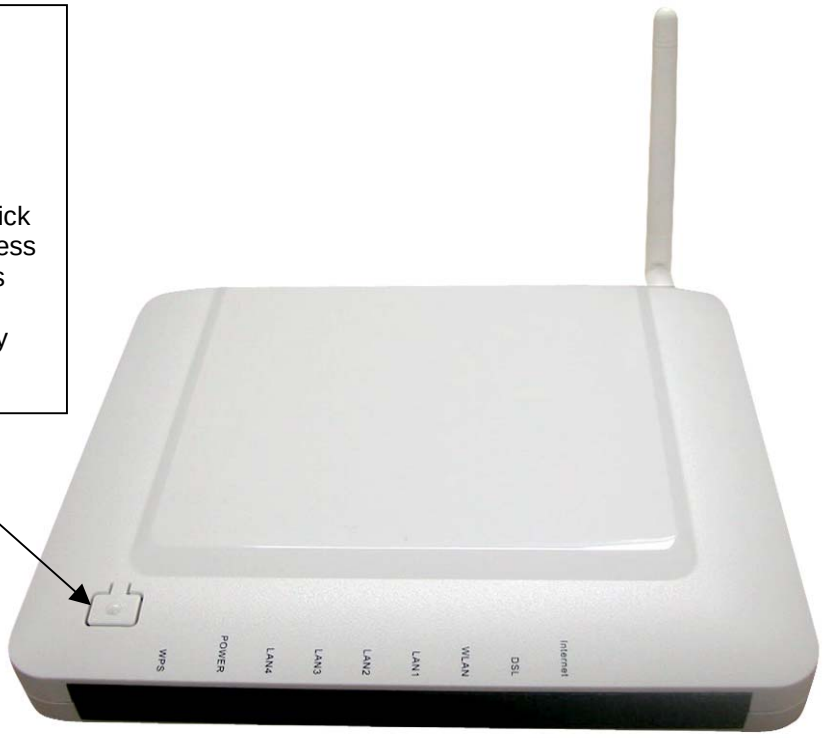
2. FREEWAY DSL Overview

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

2.1 LED Description

WPS Push Button (wireless model only)

Push the WPS 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.

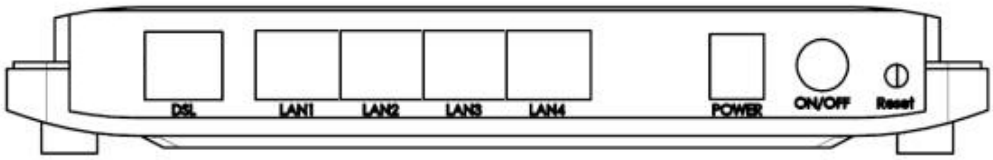


LED	Status	Description
Internet	**On**	The device is successfully connected to Internet.
	Fast Blinking	The device is sending/receiving data from Internet.
	Off	The WAN port is not connected to Internet.
DSL	**On**	The device is successfully linked with ADSL line (DSLAM).
	Fast Blinking	The device is trying to link with ADSL line (DSLAM).
	Off	The device is not linked with ADSL line (DSLAM).
WLAN (wireless model only)	**On**	The device is ready for wireless clients to connect.
	Fast Blinking	The data is sending/receiving via wireless.
	Off	The device is not ready for wireless clients to connect.
LAN1-4	**On**	The LAN port is connected to Ethernet device.
	Fast Blinking	The data is sending/receiving via this LAN port.
	Off	The LAN port is not connected to Ethernet device.
POWER	**On**	The device is power on.
	Off	The device is power off.
WPS (wireless model only)	**On**	A wireless client is joined the network successfully.
	Slow Blinking	The device is in wireless configuration process. (2 minutes maximum)
	Off	The device is not process any wireless configuration.

2.2 Ports and Buttons

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

Wireless Model Rear Panel



Wired Model Rear Panel

DSL: Connecter for accessing the Internet through ADSL line.

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

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 3 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.

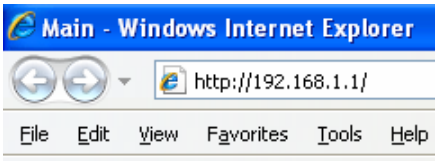
3. Setting up Your FREEWAY DSL

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.



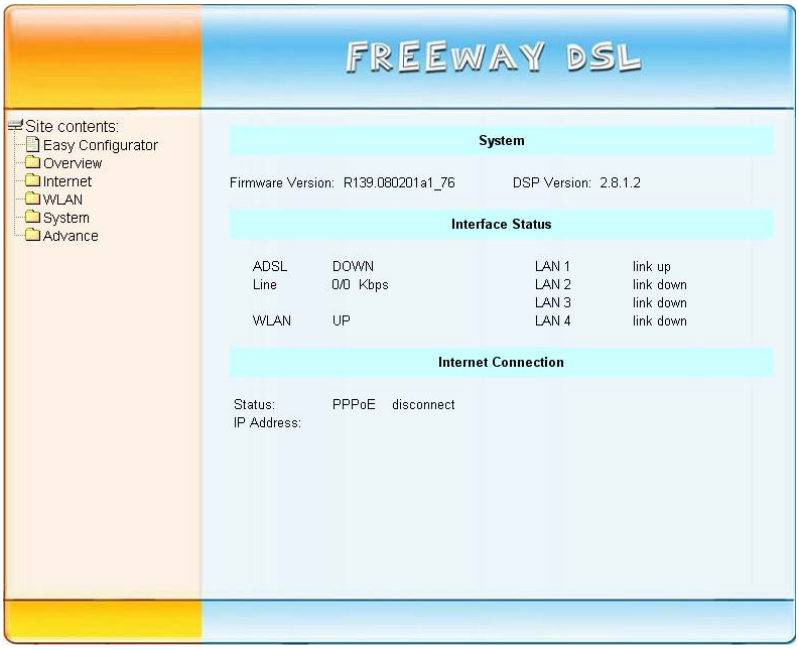
2. Enter user name as **Admin** and password as **Admin** (case sensitive).

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

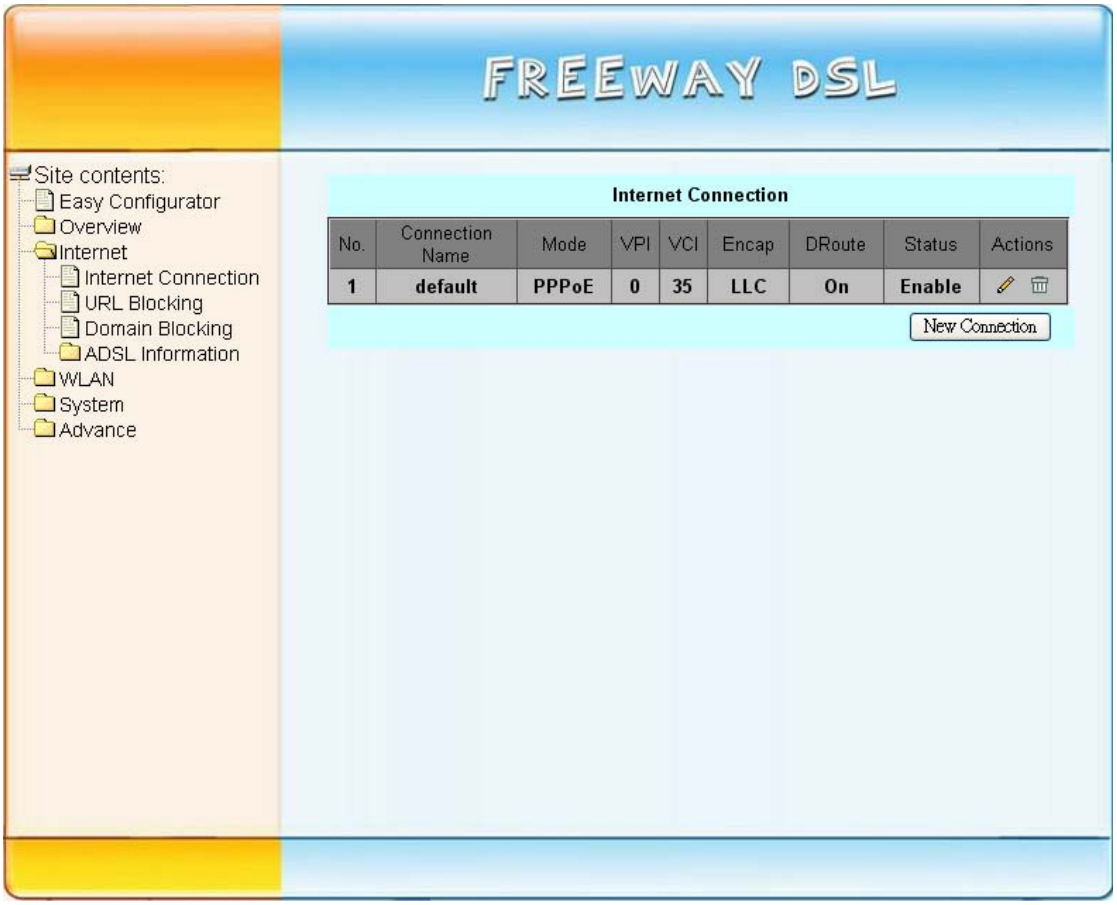
4.1 Overview

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

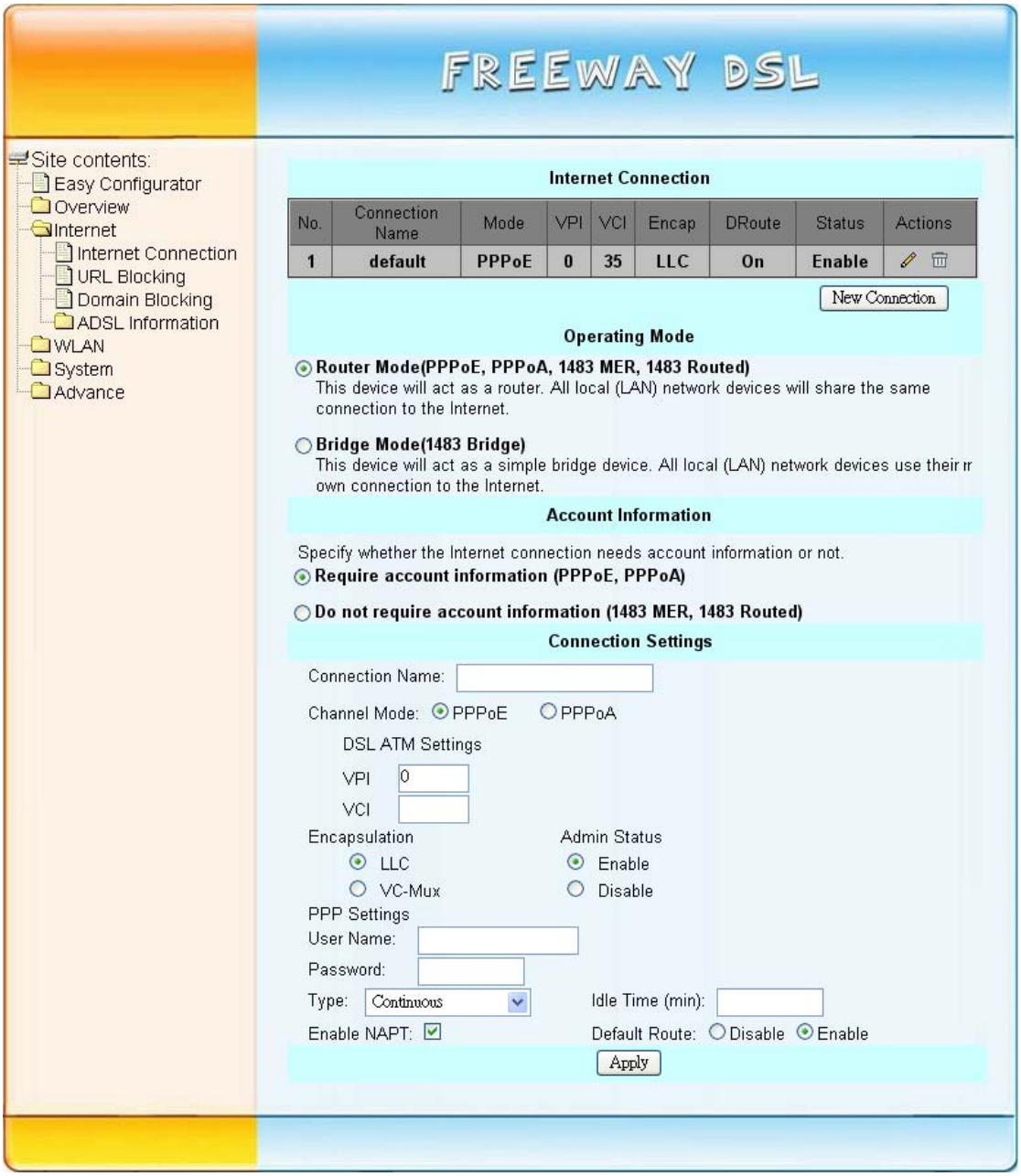
4.2 Internet

4.2.1 Internet Connection

The FREEWAY DSL supports multiple channel operation modes. The FREEWAY DSL is bridge mode enabled by factory default. There is a 1483-bridged mode PVC 0/35 in system.



You can click the **Edit** icon to edit the default configuration or click **New Connection** button to create a new connection.



Bridge Mode

1. Click **New Connection** button.
2. Select the connection Mode to **1483 Bridged**. Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM's setting.
3. Click **Apply** button to add this channel into Connection table.
4. Select **Save Settings/Reset** link from **System** menu at the left column of Web Application. Click **Save Settings/Reset** to save the settings permanently.
5. The new settings will take effect after reboot the system.

PPPoE / PPPoA Mode

1. Click **New Connection** button.
2. Select the connection Mode to **PPPoE** or **PPPoA**. Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM's setting.
3. Set User name and Password provided by the ISP.
4. Click **Apply** button to add this channel into Connection table.
5. Select **Save Settings/Reset** link from **System** menu at the left column of Web Application. Click **Save Settings/Reset** to save the settings permanently.
6. The new settings will take effect after reboot the system.

1483 MER (Mac Encapsulating Routing) Mode

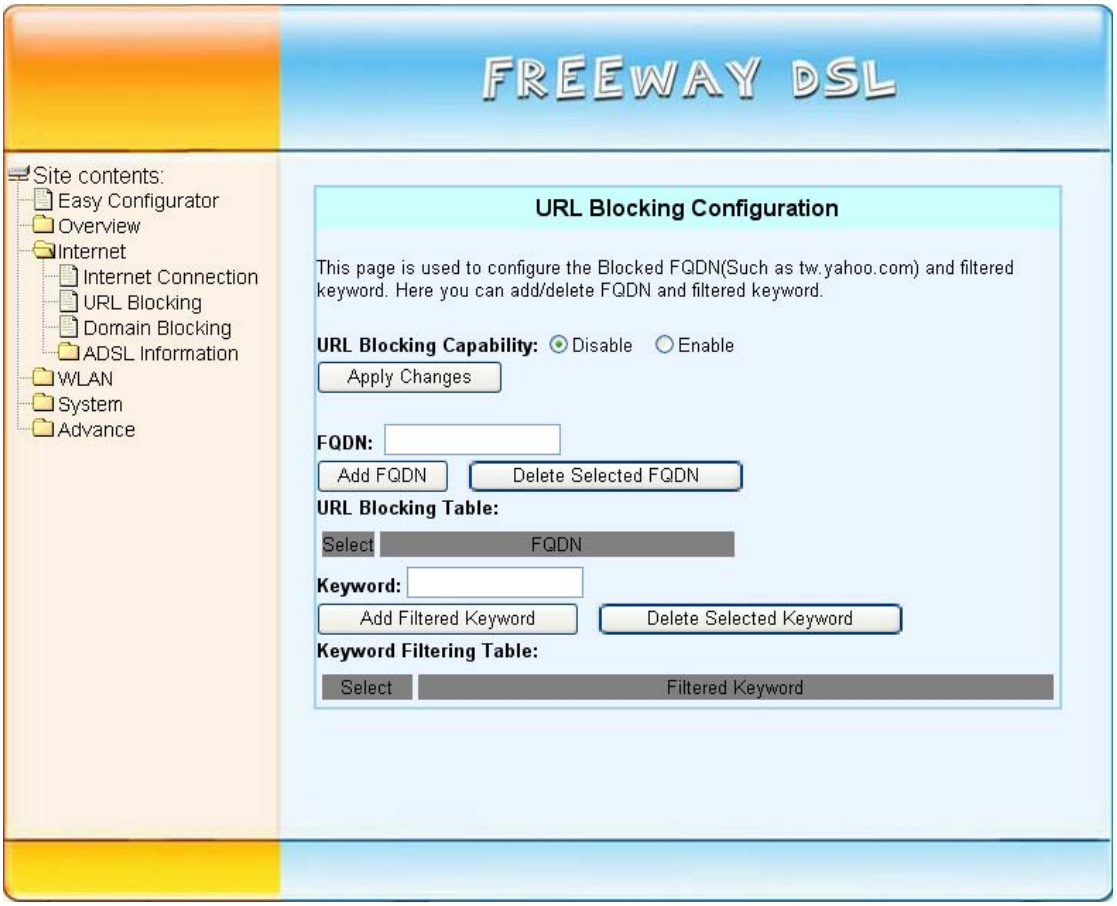
1. Click **New Connection** button.
2. Select the connection Mode to **1483 MER**. Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM's setting.
3. Set Local IP Address, Default Gateway and Subnet Mask (Fixed IP) provided by the ISP or select Dynamic IP (DHCP) to obtain them from the ISP.
4. Click **Apply** button to add this channel into Connection table.
5. Select **Save Settings/Reset** link from **System** menu at the left column of Web Application. Click **Save Settings/Reset** to save the settings permanently.
6. The new settings will take effect after reboot the system.

1483 Routed Mode

1. Click **New Connection** button.
2. Select the connection Mode to **1483 Routed**. Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM's setting.
3. Set Local IP Address, Default Gateway and Subnet Mask provided by the ISP.
4. Click **Apply** button to add this channel into Connection table.
5. Select **Save Settings/Reset** link from **System** menu at the left column of Web Application. Click **Save Settings/Reset** to save the settings permanently.
6. The new settings will take effect after reboot the system.

4.2.2 URL Blocking

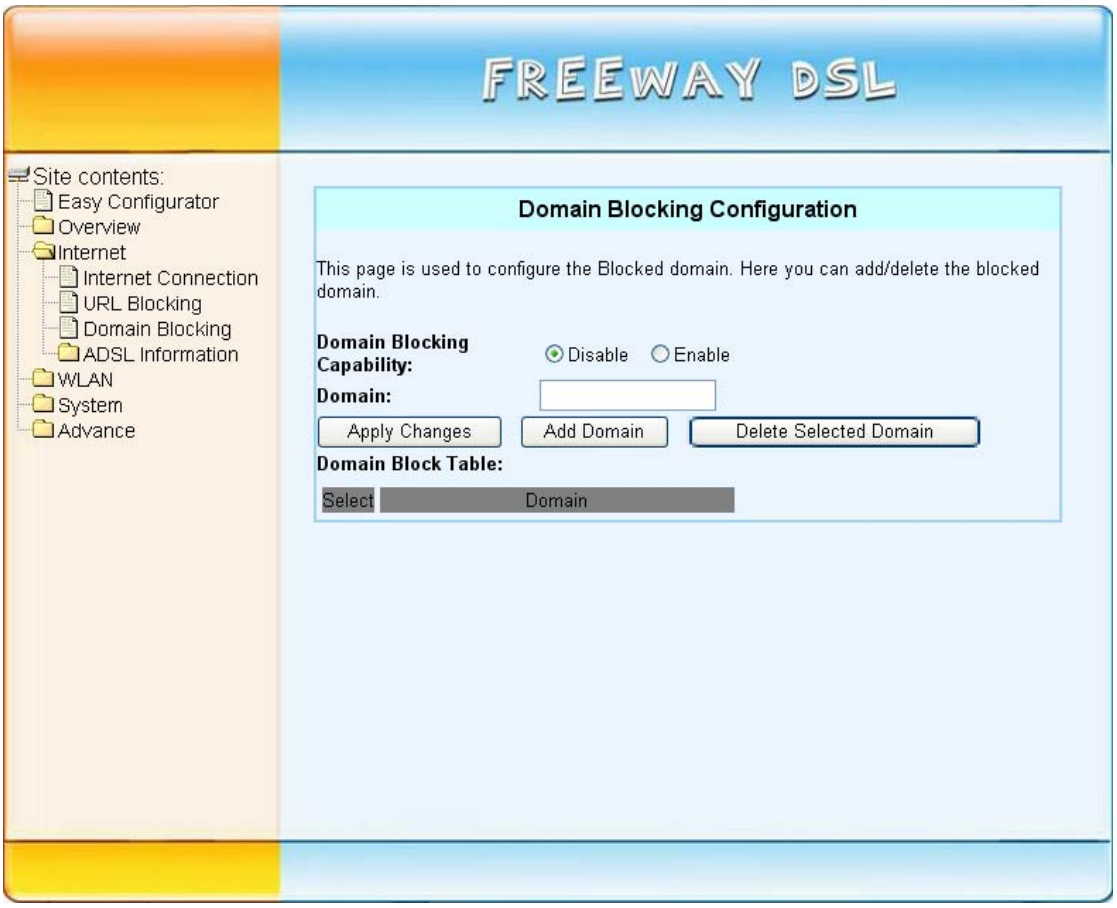
This page is used to configure the blocked FQDN (Fully Qualified Domain Name, such as http://www.yahoo.com) or filtered keywords. If you want to prevent computers in local network from accessing certain website (like pornography, violence, or anything you want to block), you can use this function to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

4.2.3 Domain Blocking

This page is used to configure the blocked Domains.

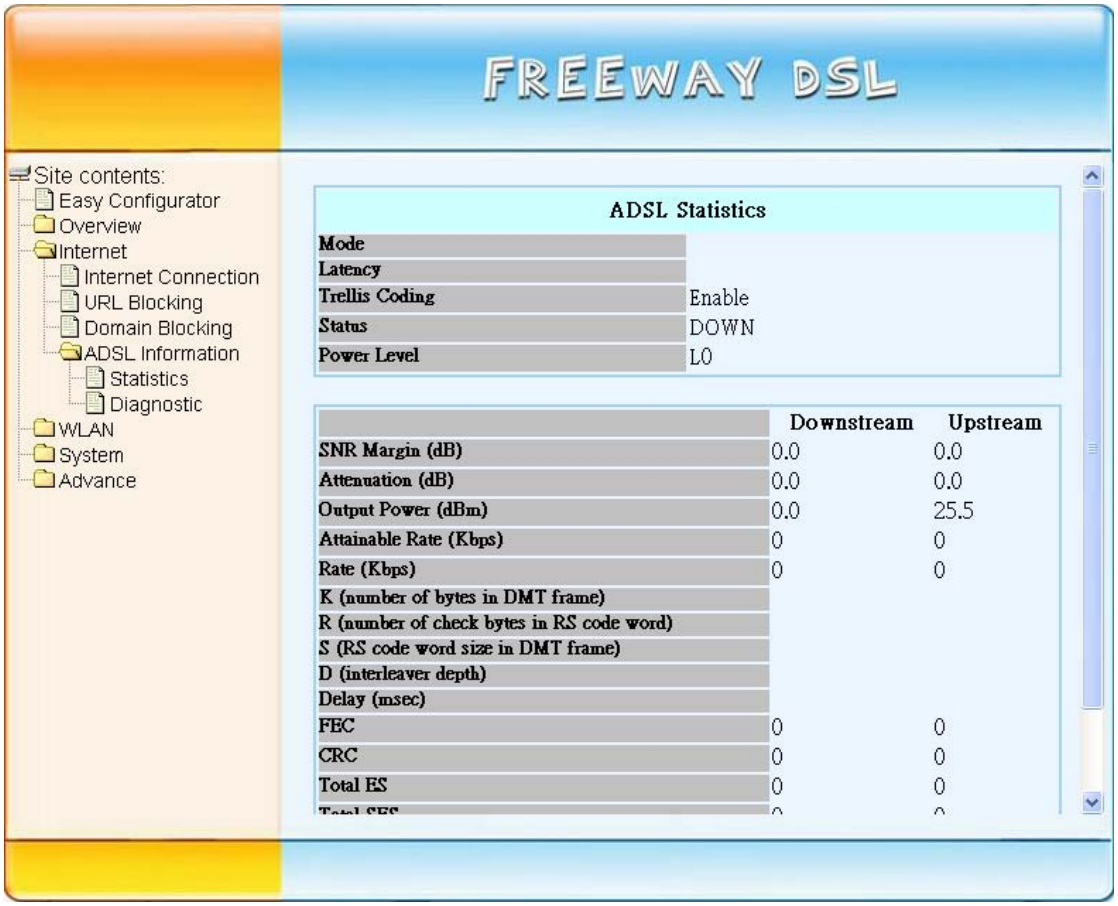


Field	Description
Domain Blocking Capability	Select the radio button to enable/disable domain blocking function.
Domain	Enter the domain you want to block.
Domain Block Table	This table lists all the existing domains in blocking table.

4.2.4 ADSL Information

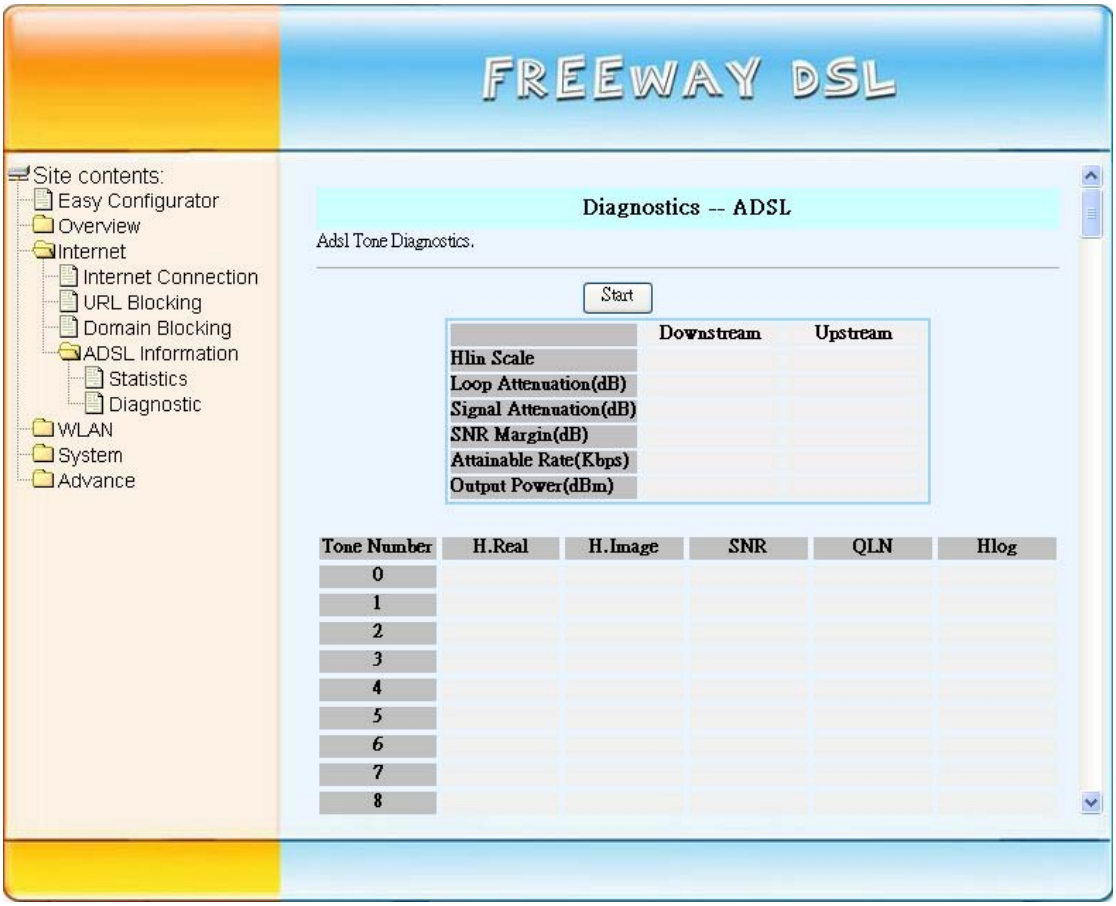
4.2.4.1 Statistics

This page shows the ADSL line statistics information.



4.2.4.2 Diagnostic

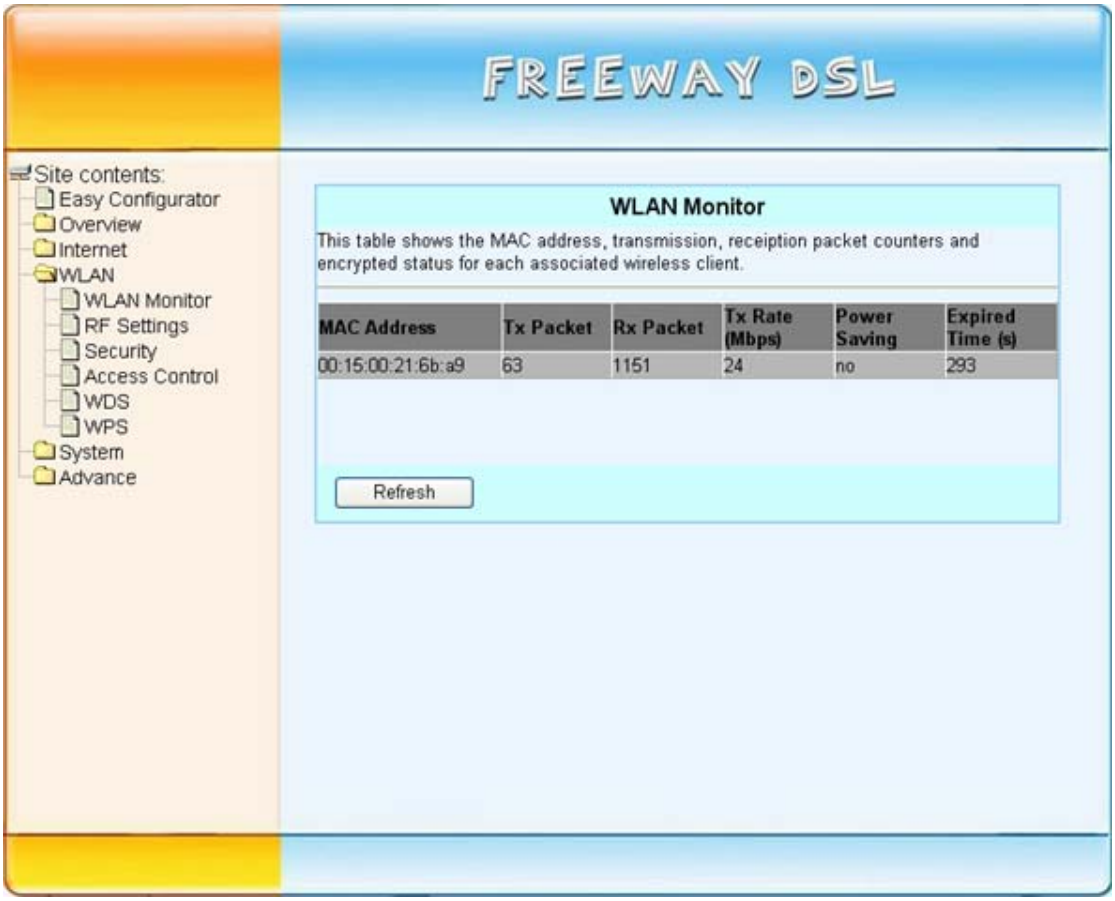
This page shows the ADSL tone diagnostic information. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.



4.3 WLAN (Wireless Model Only)

4.3.1 WLAN Monitor

This section provides the wireless network settings for your WLAN interface. The wireless interface enables the wireless AP function for FREEWAY DSL. To display updated information showing any new data since you opened this page, click **Refresh**.



4.3.2 RF Settings (Wireless Basic Settings)

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

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.

4.3.3 Wireless Advanced Settings

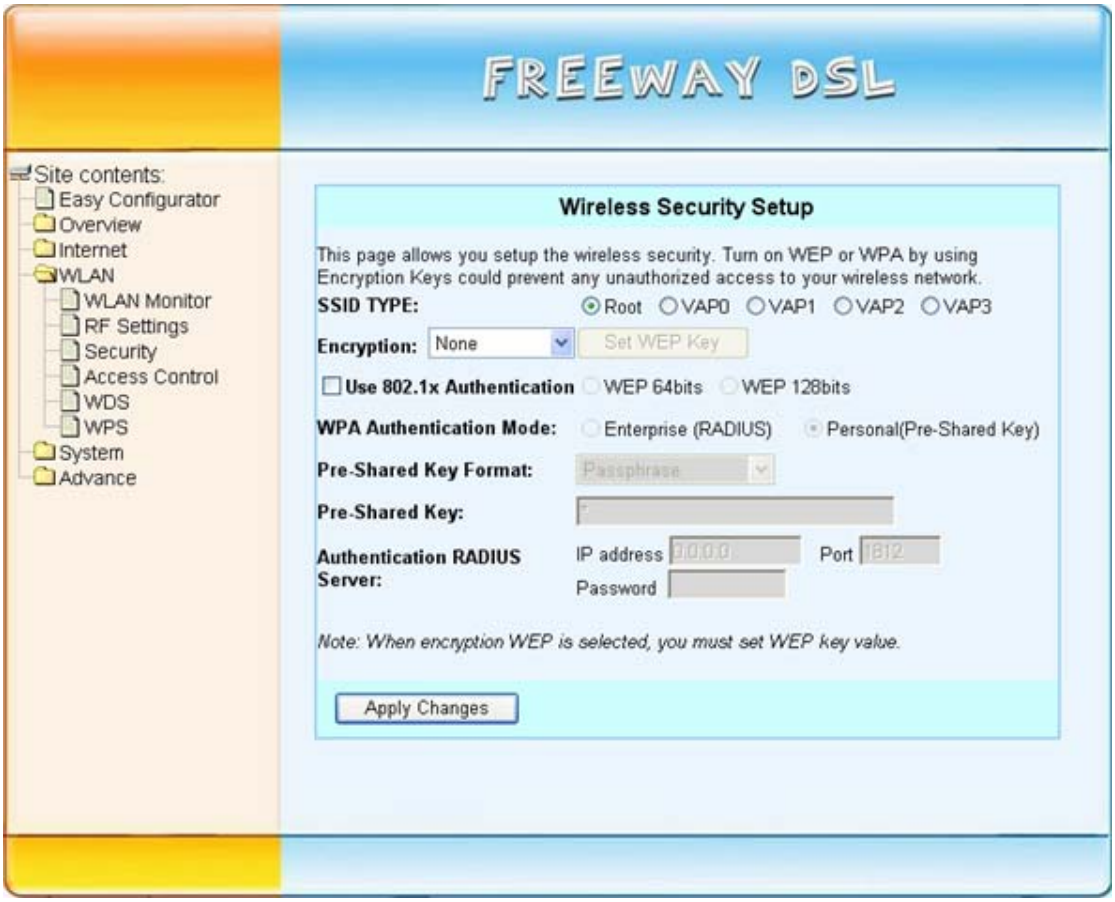
This page contains the wireless advanced settings. It is recommended that you remain this page as its default settings unless you have sufficient wireless knowledge.

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	When Relay Blocking is enabled, wireless clients will not be able to directly access other wireless clients.
Ethernet to Wireless Blocking	When enabled, traffic between Ethernet and wireless interfaces are not allowed.

4.3.4 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*.

4.3.5 Access Control

When Enable Access Control function, MAC address can be added into access control list and only those clients whose wireless MAC address are in the ACL (Access Control List) will be able to connect to your FREEWAY DSL (or AP).

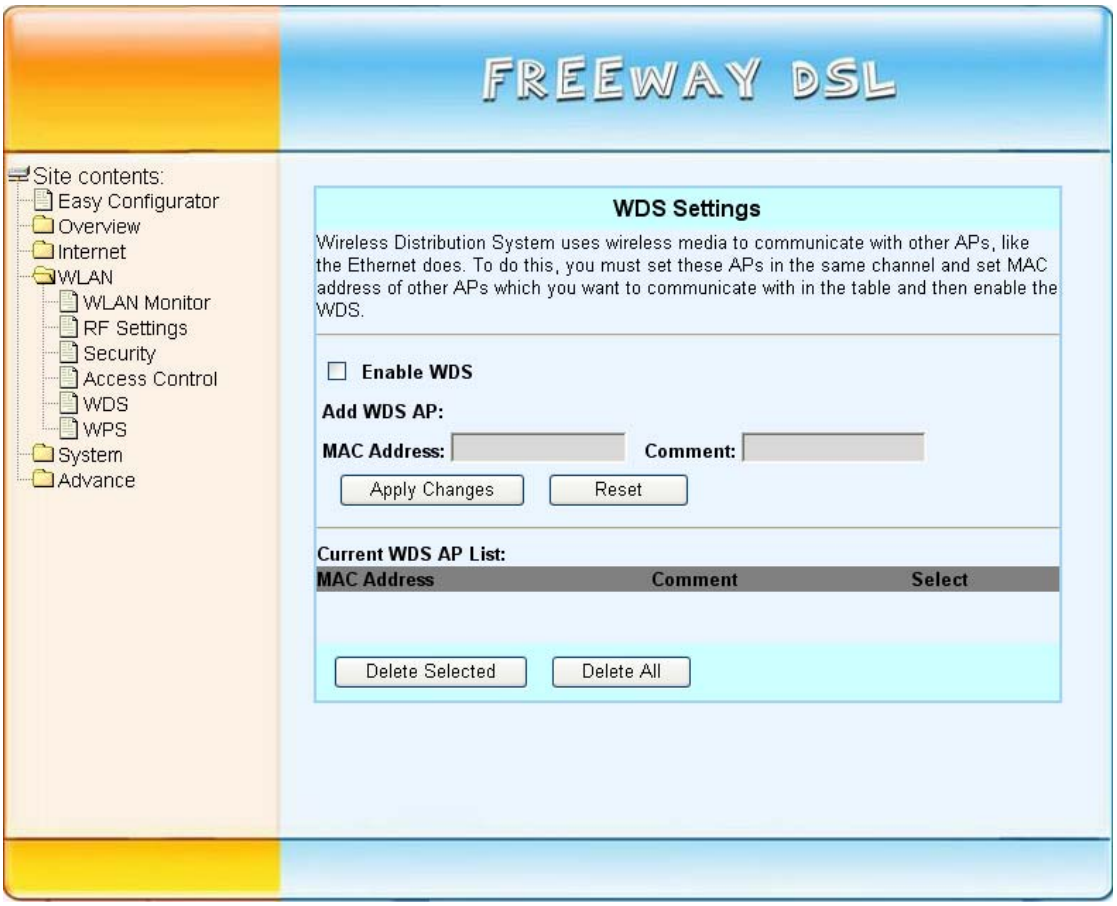
Field	Description
Wireless Access Control Mode	The Selections are: • **Disable:** Disable the wireless ACL function. • **Allow Listed:** When this option is selected, no wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to the FREEWAY DSL). • **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.

4.3.6 WDS

Wireless Distribution System (WDS) is a system that interconnects BSS (Basic Service Set) to build a premise wide network. The FREEWAY DSL supports the WDS protocol, which allows a point to point link to be established between two APs.

Note

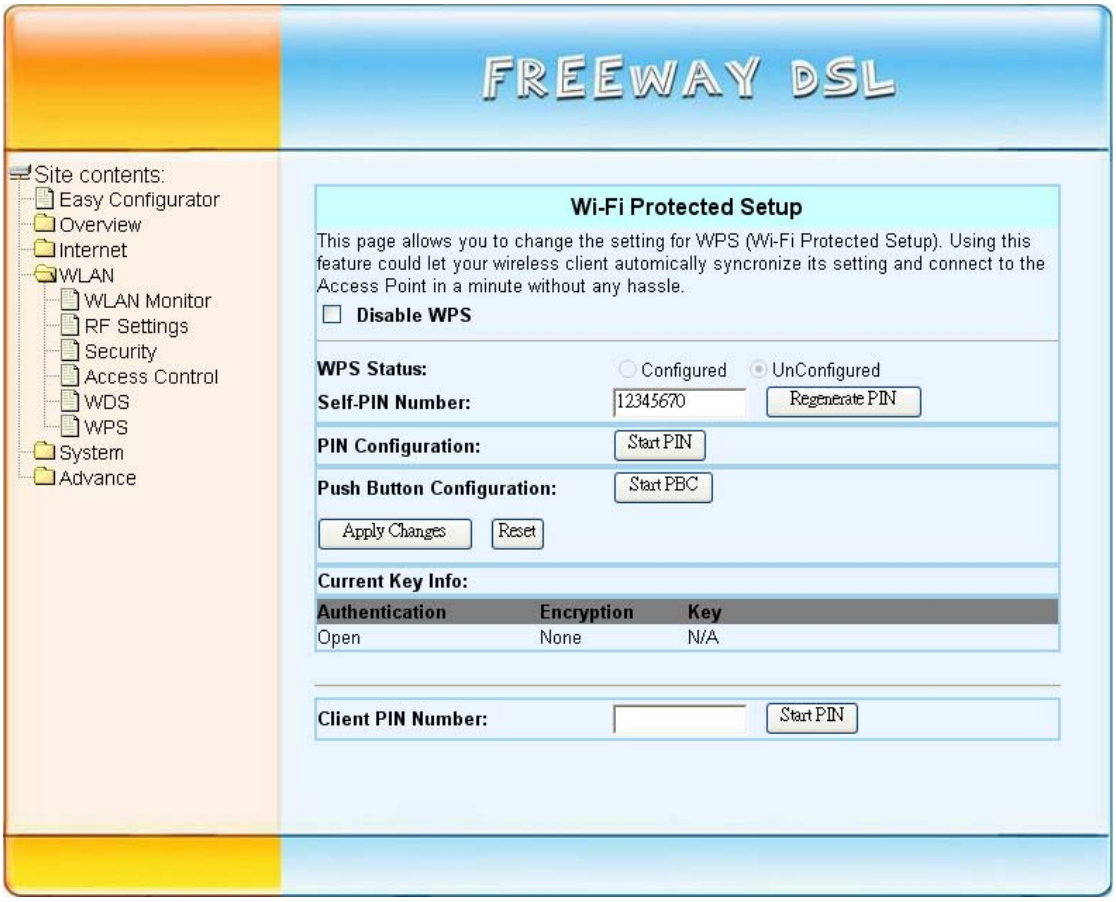
*Only if you select **AP+WDS** mode on the RF Settings page, this WDS page can be configured.*



Field	Description
Enable WDS	Check to enable the WDS function. Only if you select **AP+WDS** mode on the RF Settings page, this WDS page can be configured.
MAC Address	This is where you enter the MAC address of the peer AP's wireless interface that you are connecting to.
Comment	Enter the comment for this MAC address.
Current WDS AP List	It lists the peer MAC addresses of the WDS link. Any AP with its MAC address listed in this WDS AP list may have a WDS link to the device. You can select the entries at the Select column and apply to the following function buttons.

4.3.7 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.

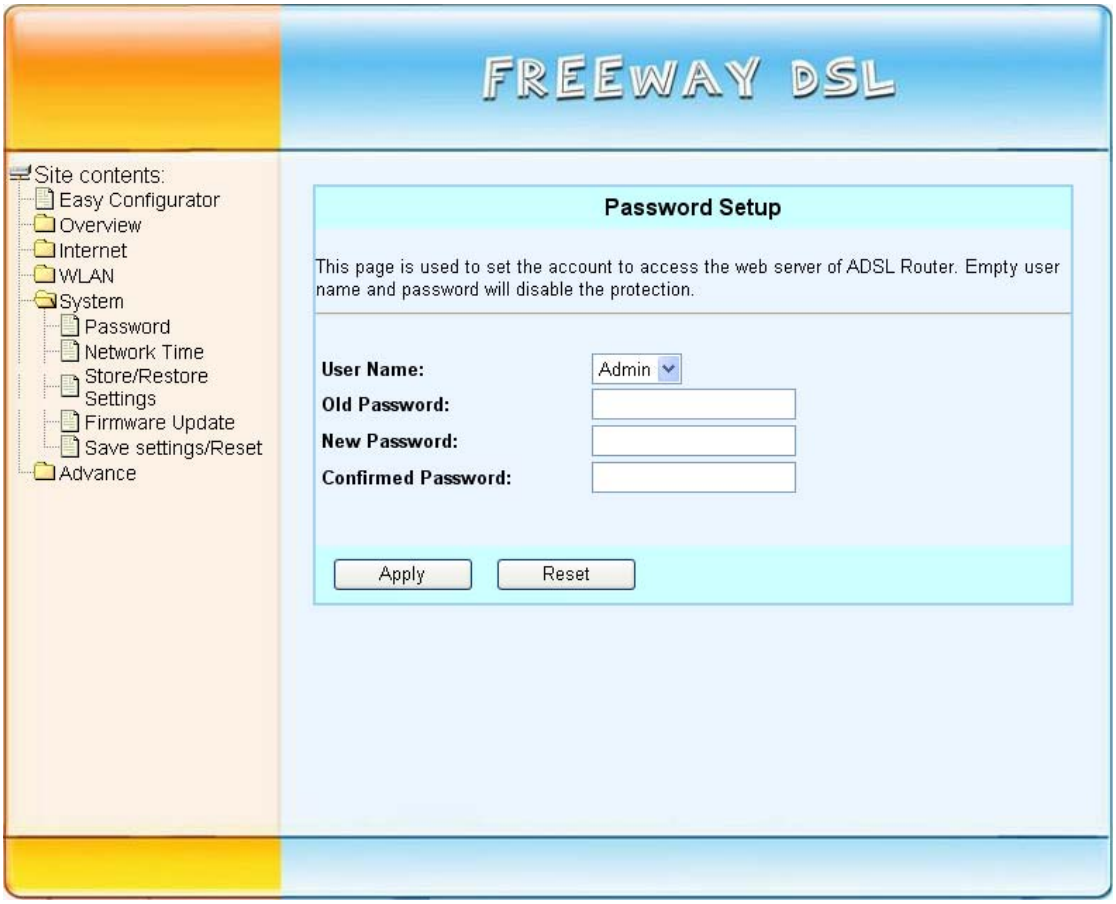


Field	Description
Disable WPS	Check this box to disable WPS function.
WPS Status	If the wireless security (encryption) function of the FREEWAY DSL is properly set, you will see "Configured" radio button in action mode, otherwise, "UnConfigured" is in action mode.
Self-PIN Number	The the PIN Number of 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.

4.4 System

4.4.1 Password

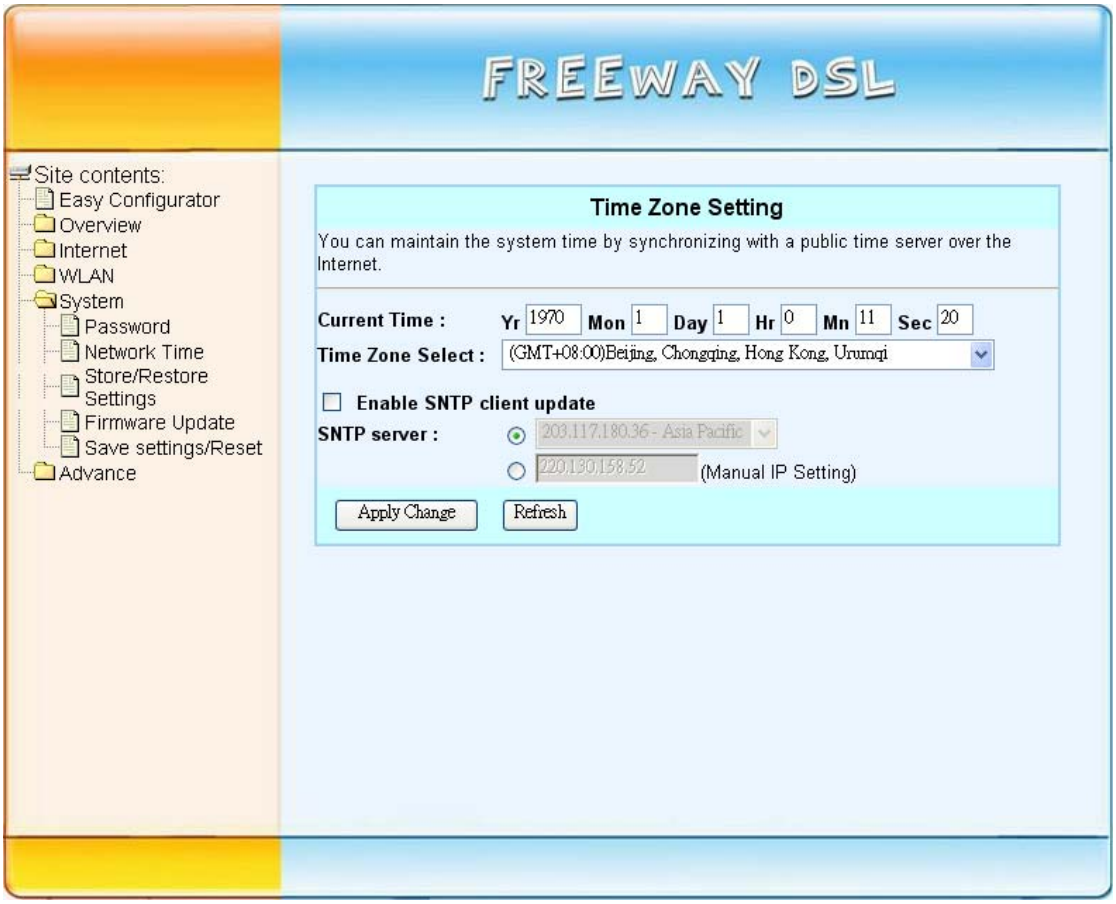
The first time you log into the system with default password. This page allows you to change the password for administrator.



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.

4.4.2 Network Time

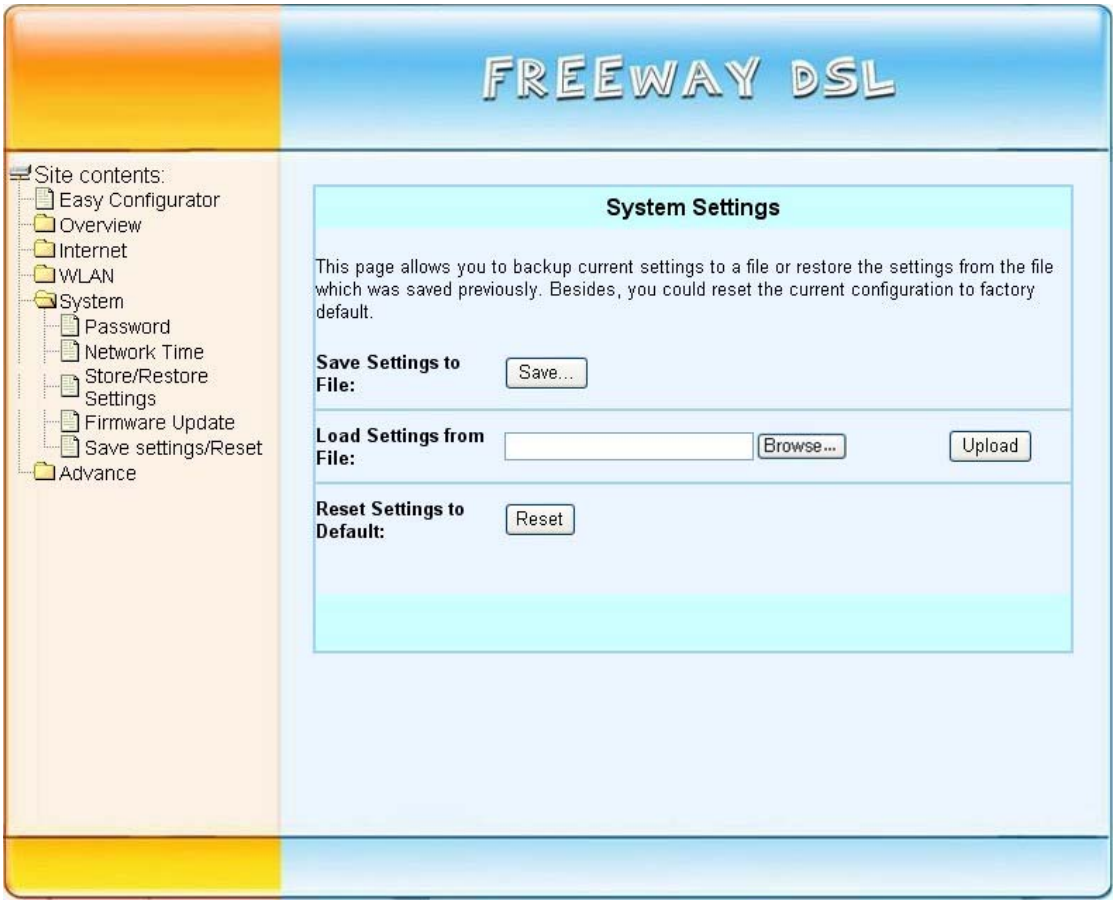
Simple Network Timing Protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. The FREEWAY DSL supports SNTP client functionality in compliance with IETF RFC2030. This page allows you to manually configure the time and select Time Zone. Also, you can enable SNTP client 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 set it manually.

4.4.3 Restore/Restore Settings

This page allows you to backup current settings to a file or restore the settings from a previously saved file. Also, you can reset the FREEWAY DSL to default settings.



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

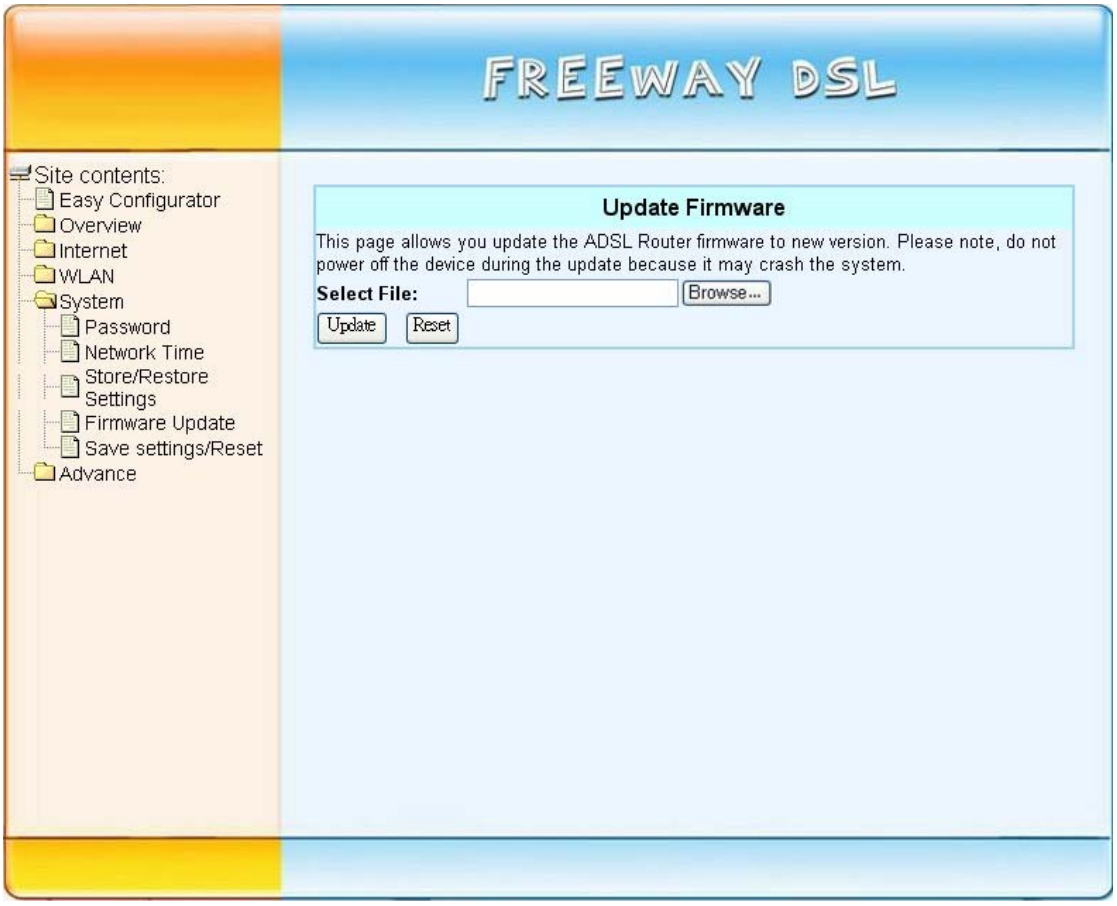
To load settings from a file, please follow the following instructions:
1. Click the **Browse** button to select the saved file.
2. Confirm your selection.
3. Click the **Upload** button to start restoring.

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.

4.4.4 Firmware Update

The system software used by this FREEWAY DSL is called "firmware". This page allows you to upgrade the firmware to newer version.



To upgrade firmware, please follow the following instructions:

4. Click the **Browse** button to select the firmware file.
5. Confirm your selection.
6. 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.

4.4.5 Save Settings/Reset

Whenever you use the Web Application to change system settings, the changes are initially placed in temporary storage. To save your changes for future use, you can use the Commit/Reboot function. This page allows you to save the changes permanently and reboot the system. Or you may lose the settings you made after power off or reboot.

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

4.5 Advanced

4.5.1 LAN

4.5.1.1 LAN

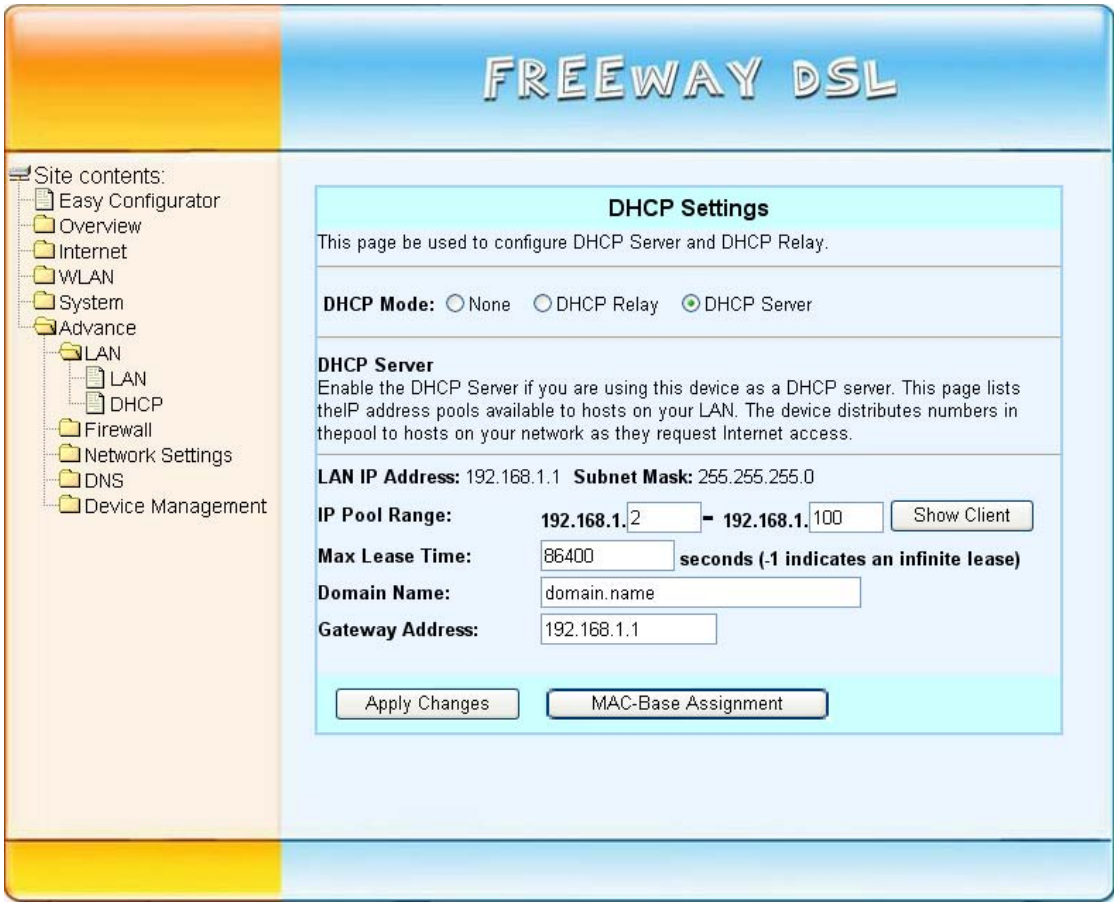
This page shows the current setting of LAN interface. You can set IP address and subnet mask for LAN interface in this page.

Field	Description
IP Address	Enter the IP address of FREEWAY DSL.
Subnet Mask	Enter the subnet mask for this network.

4.5.1.2 DHCP

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.

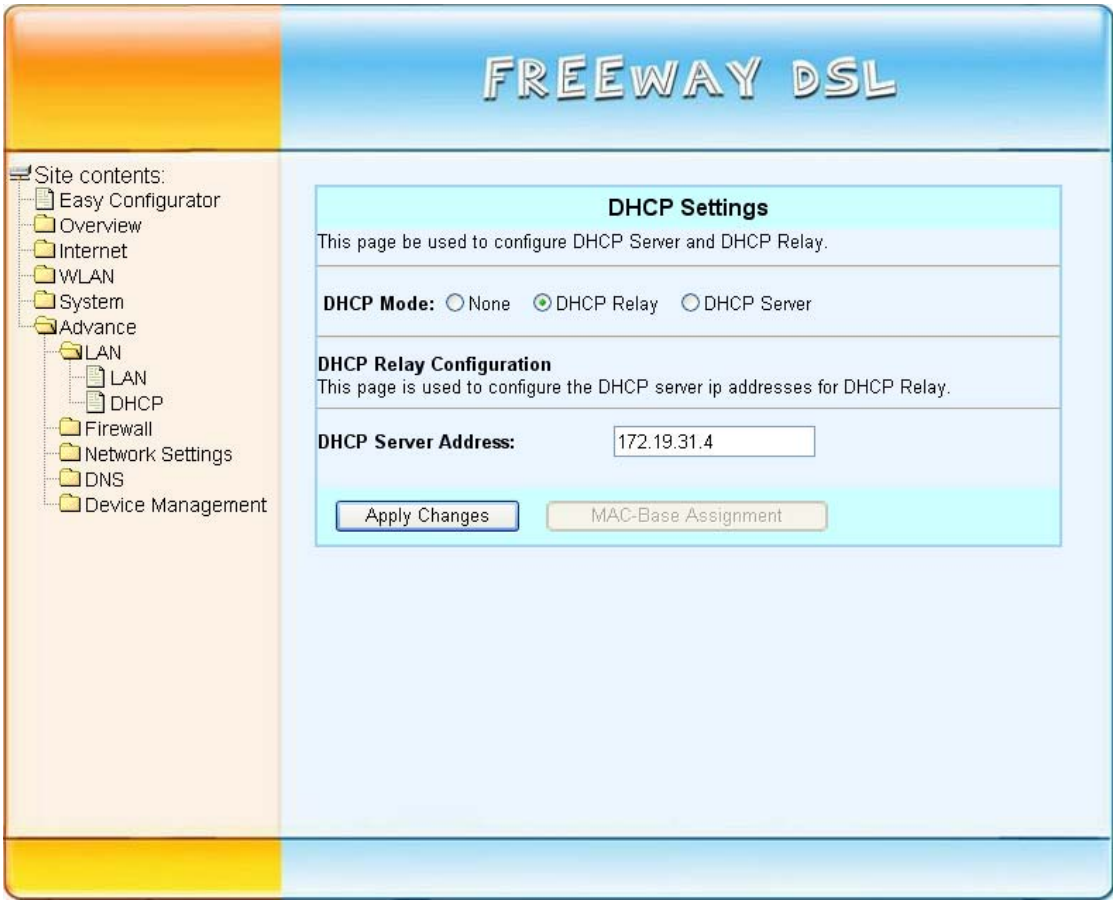
DHCP Server Configuration
By default, the FREEWAY DSL is configured as a DHCP server, with a predefined IP address pool from 192.168.1.2 to 192.168.1.100 (subnet mask 255.255.255.0).



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".

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.



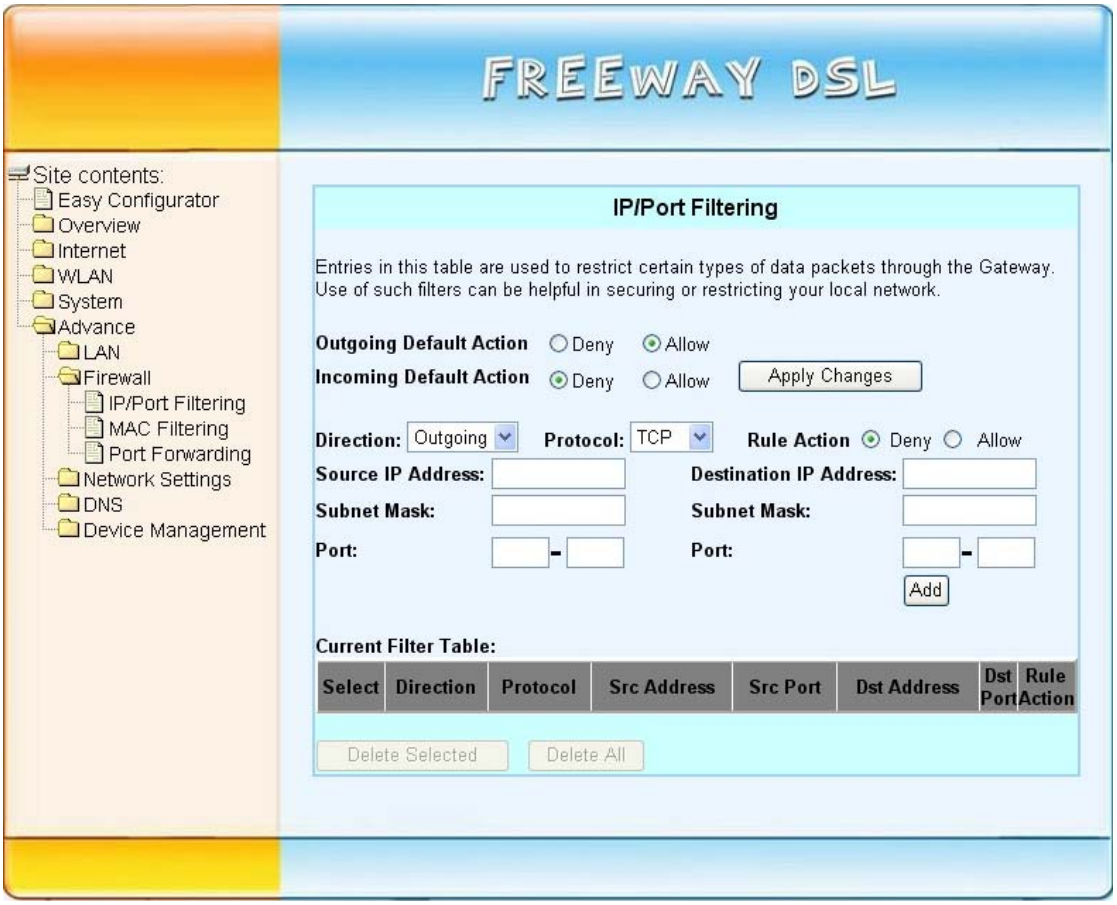
Field	Description
DHCP Server Address	Specify the IP address of your ISP's DHCP server. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

4.6 Firewall

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

4.6.1 IP/Port Filtering

This page allows you to deny/allow specific services or applications in the forwarding path.



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.

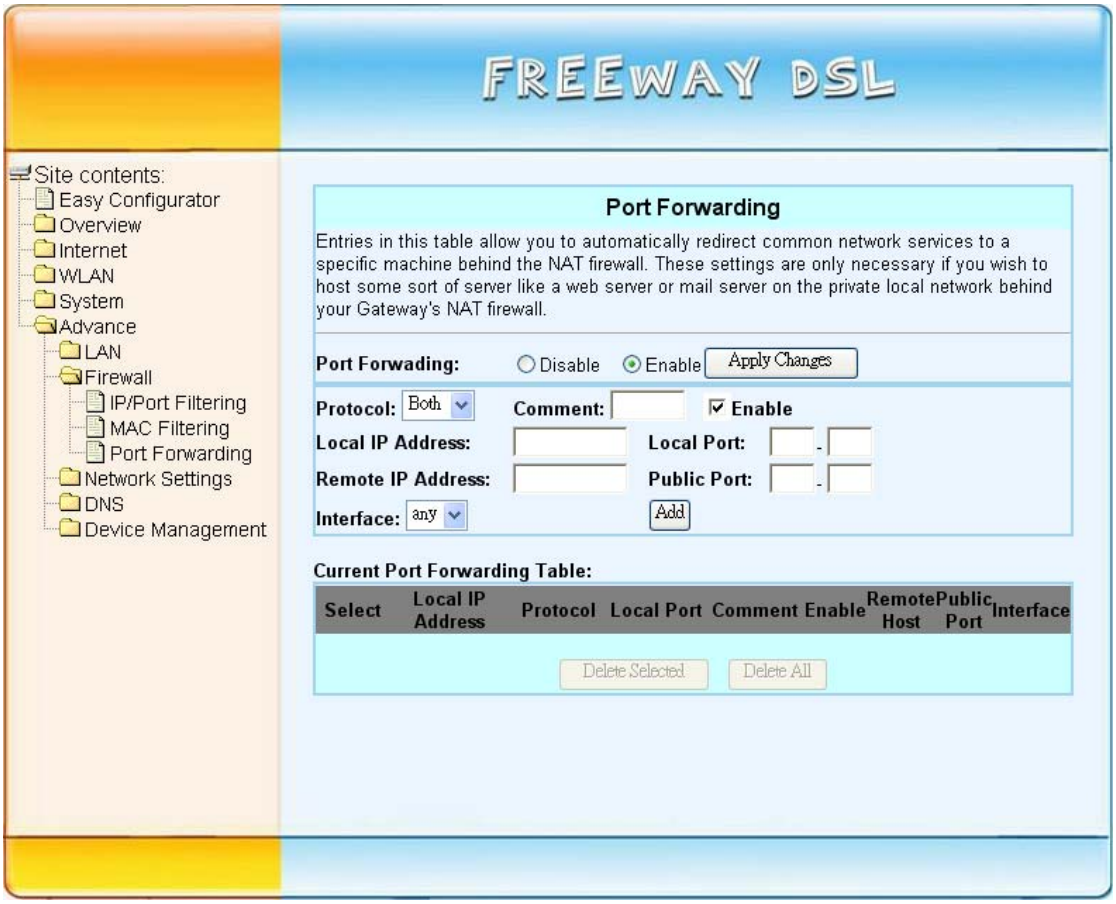
4.6.2 MAC Filtering

This page allows you to define rules to allow or deny frames through the FREEWAY DSL based on source MAC address, destination MAC address and traffic direction.

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.
Src MAC Address	Enter the source MAC address. It must be xxxxxxxxxxxx format.
Dst MAC Address	Enter the destination MAC address. It must be xxxxxxxxxxxx format.

4.6.3 Port Forwarding

This page allows you to configure port forwarding rules. Add a Port Forwarding entry will create a tunnel through your firewall so that the computers on the Internet can communicate to one of the computers on your LAN on a single port.



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.

4.7 Network Settings

4.7.1 Static Routing

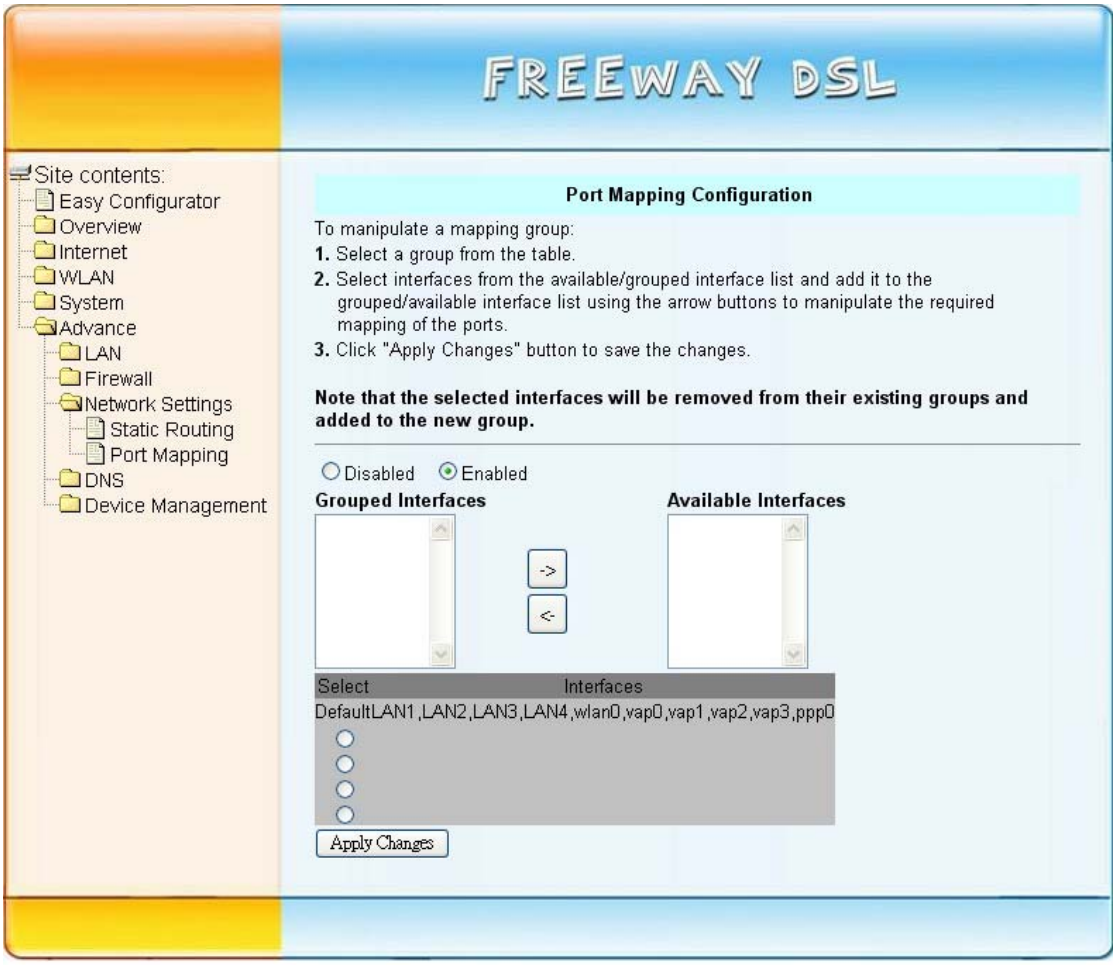
The Routing page enables you to define specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the FREEWAY DSL provide the most appropriate path for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

4.7.2 Port Mapping

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



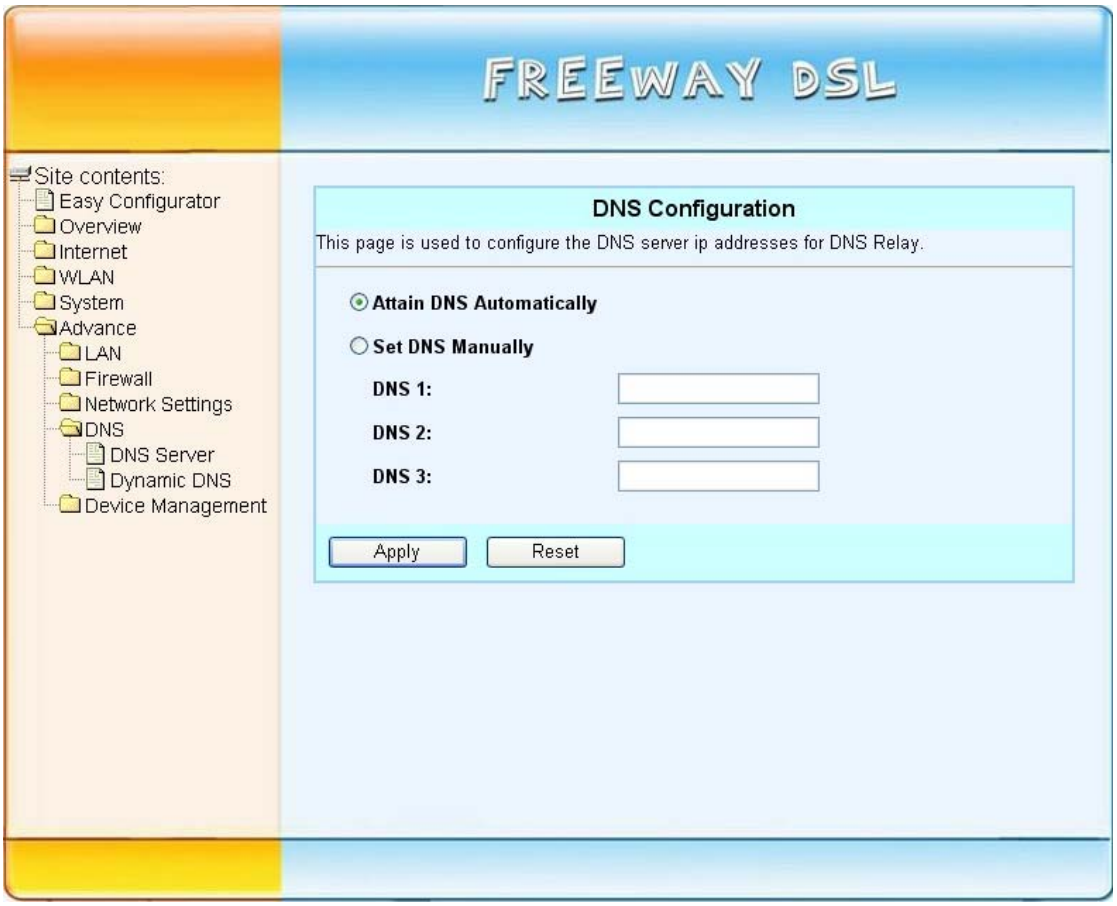
Field	Description
Enabled/Disabled	Radio buttons to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.
Grouped Interfaces	To manipulate a mapping group: 1. Select a group from the table. 2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports. 3. Click **Apply Changes** to save the changes.

4.8 DNS

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

4.8.1 DNS Server

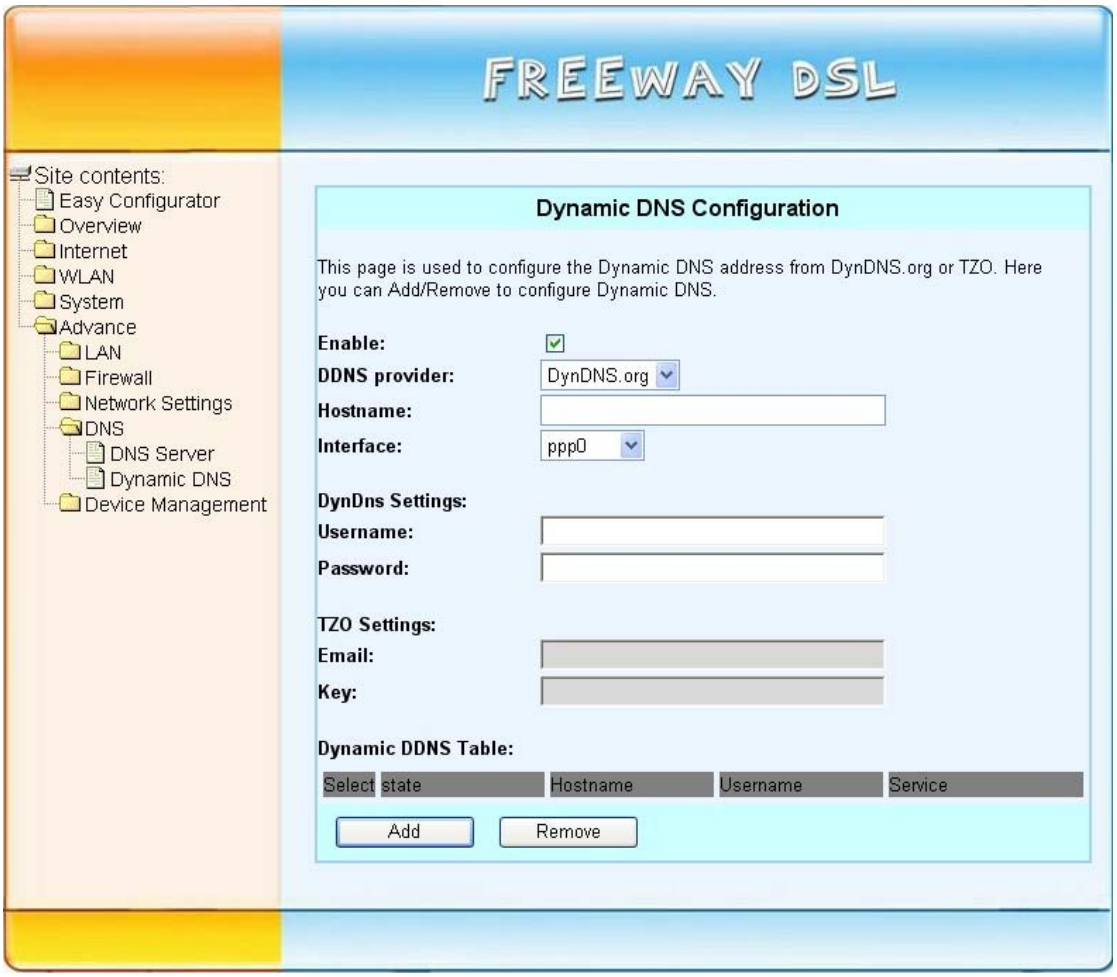
This page is used to select the way to obtain the IP addresses of the DNS servers.



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

4.8.2 DDNS (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 this item to enable this registration account for the DNS server.
DDNS Provider	There are two DDNS providers to be selected in order to register your device with: DynDNS and TZO. A charge may occur depends on the service you select.
Hostname	Enter the domain name to be registered with the DDNS server.
Interface	This field defaults to your device's WAN interface over which your device will be accessed.
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.

4.9 Device Management

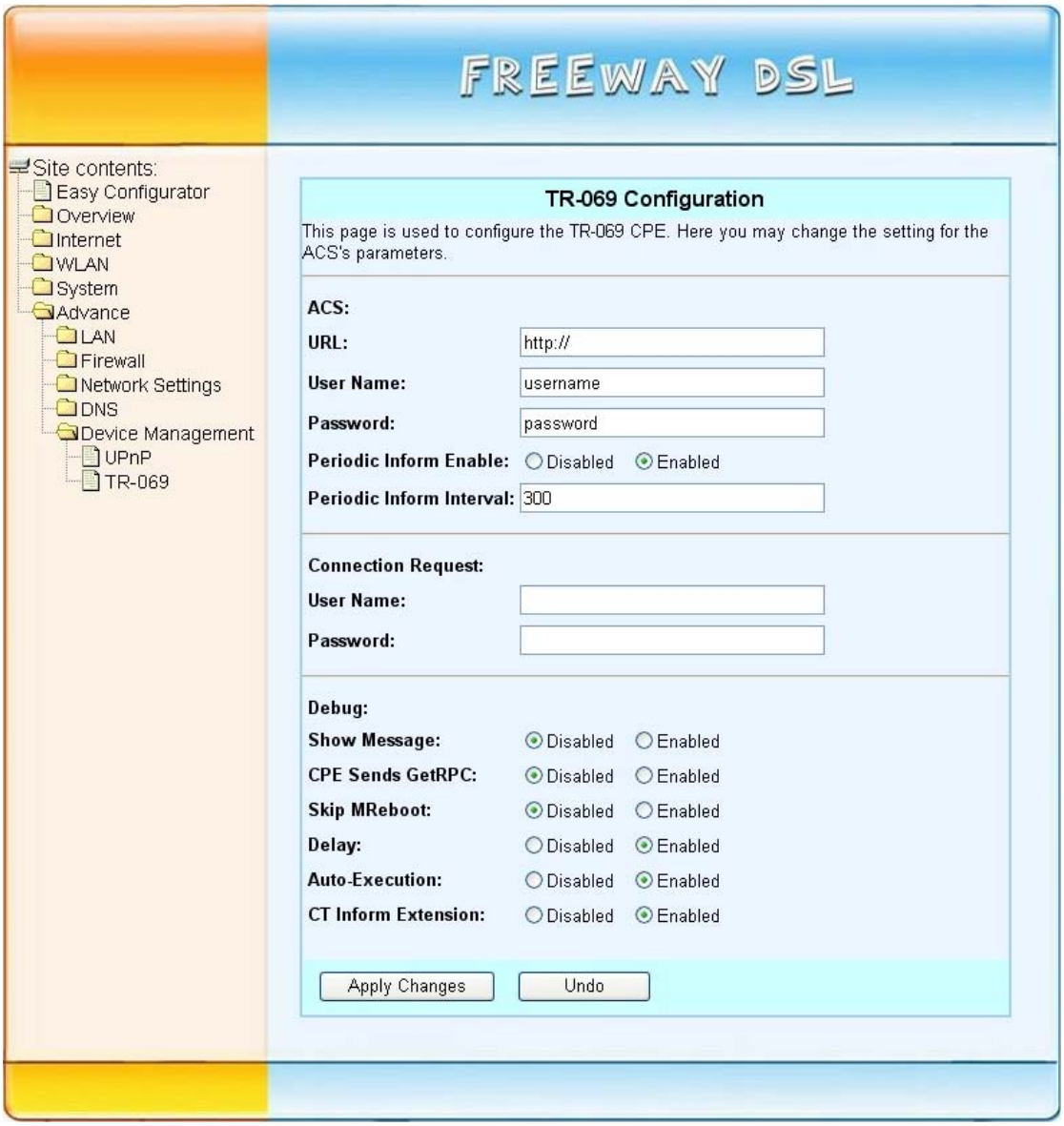
4.9.1 UPnP

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.

4.9.2 TR-069

The TR-069 (CPE WAN Management Protocol) function can secure remote host access to your FREEWAY DSL from LAN and WLAN interfaces for some services provided by it.



Field	Description
ACS URL	URL of the Auto Configuration Sserver (ACS) provided by the ISP.
User Name	Enter the user name for the ACS to authenticate.
Password	Enter the password for the ACS to authenticate.
Periodic Inform Enable	Enable/disables the FREEWAY DSL to connect to the ACS periodically.
Periodic Inform Interval	This field is enabled only when the Periodic Inform Enabled field is checked. It defines the amount of time (in seconds) between a successful connection with an ACS server and a new attempt to connect to an ACS server.
Connection Request Username	Enter the user name if the connection required authentication process.
Connection Request Password	Enter the password if the connection required authentication process.
Debug	Software debugging message. Specify/change the contents only when you are directed by a technical support representative.

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. 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 WAN 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 3 seconds) to restore the factory defaults.

Appendix B. Specification

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
- Adaptation Layers AAL5, AAL2 and AAL0 Support
- OAM F4/F5 Loop Back

PPP Support
- PPP over ATM PVC (RFC 2364&RFC1577)
- PPP over Ethernet (RFC 2516)
- PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) and MS-CHAP (Microsoft 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)
- Unspecified Bit Rate (VBR)

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

Wireless Specification (wireless model only)

- 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 54MbpsDSSS (Direct Sequence Spread Spectrum)
- 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