D-Link DSL-2750E

Wireless N 300 ADSL2+ Modem Router

User Manual

D-Link
Building Networks for People

RECYCLABLE

2013/04/18

Ver. 1.00

Contents

1 Introduction

The DSL-2750E supports multiple line modes. With four 10/100 base-T Ethernet interfaces at the user end, the device provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users like net bars and office users. It provides high performance access to the Internet with a downstream rate of 24 Mbps and an upstream rate of 1 Mbps. It supports 3G WAN, 3G backup, Samba for USB storage and IPV6.

The device supports WLAN access, such as WLAN AP or WLAN device, to the Internet. It complies with specifications of IEEE 802.11, 802.11b/g/n, WEP, WPA, and WPA2 security.

1.1 Packing List

- 1 x DSL-2750E
- 1 x external splitter
- 1 x power adapter
- 1 x telephone cables (RJ-11)
- 1 x Ethernet cable (RJ-45)
- 1 x QIG
- 1 X CD

1.2 Safety Precautions

Take the following instructions to prevent the device from risks and damage caused by fire or electric power:

- Use the type of power marked in the volume label.
- Use the power adapter in the product package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines or plugs may cause electric shock or fire accidents. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device

are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.

- Do not put this device close to a heat source or under a high temperature occurs. Keep the device away from direct sunshine.
- Do not put this device close to an overdamp or watery place. Do not spill fluid on this device.
- Do not connect this device to a PC or electronic product unless instructed by our customer engineer or your broadband provider. Wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

1.3 LEDs and Interfaces

Note:

The figures in this document are for reference only.

Front Panel

Figure 1 Front panel

The following table describes the LEDs of the device.

LED	Color	Status	Description
Power	Green	Off	The power is off.
		On	The power is on and the initialization is normal.
	Red	On	The device is initiating.
		Blinks	The firmware is upgrading.
LAN 1/2/3/4	Green	Off	No LAN link.
		Blinks	Data is being transmitted through the LAN interface.
		On	The connection of LAN interface is normal.

LED	Color	Status	Description
WLAN	Green	Blinks	Data is transmitted through the WLAN interface.
		On	The connection of WLAN interface is normal.
		Off	The WLAN connection is not established.
WPS	Blue	Blinks	WPS negotiation is enabled, waiting for the clients.
		Off	WPS negotiation is not enabled on the device.
USB	Green	On	The connection of 3G or USB flash disk has been established.
		Blinking	Data is being transmitted.
		Off	The connection of 3G or USB flash disk is not established.
DSL	Green	Off	Initial self-test is failed.
		Blinks	The device is detecting itself.
		On	Initial self-test of the unit has passed and is ready.
Internet	Green	Off	The device is under the Bridge mode, DSL connection is not present, or the power is off.
		Blinks	Internet data is being transmitted in the routing mode.
		On	The IP is connected.
	Red	On	The device is attempted to become IP connected, but failed.

Rear Panel

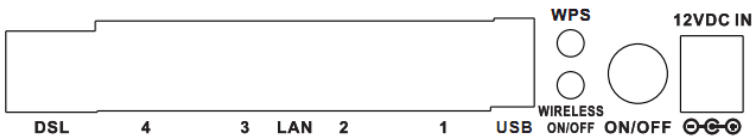


Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
DSL	RJ-11 interface that connects to the telephone set through the telephone cable.
LAN4/3/2/1	Ethernet RJ-45 interfaces that connect to the Ethernet interfaces of computers or Ethernet devices.
USB	USB port, for connecting the 3G network card or other USB storage devices.
WPS	Press the button for 1 second to enable WPS function.
WIRELESS ON/OFF	Press the button silently to enable WLAN function.
ON/OFF	Power on or off the device.
12V DC IN	Interface that connects to the power adapter. The power adapter output is: 12V DC 1A.
Reset (on the bottom case)	Reset to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for 1 second and then release.

1.4 System Requirements

- A 10 baseT/100BaseT Ethernet card is installed on your PC.
- A hub or switch (attached to several PCs through one of Ethernet interfaces on the device)
- Operating system: Windows Vista, Windows 7, Windows 98SE, Windows 2000, Windows ME or Windows XP
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or Firefox 1.5 or higher

1.5 Features

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- Leased line mode
- 1483B, 1483R, and MER access

- Multiple PVCs (eight at most) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Binding of ports with PVCs
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and NAPT
- Static route
- Firmware upgrade: Web, TFTP, FTP
- Reset to the factory defaults
- DNS relay
- Virtual server
- DMZ
- Two-level passwords and user names
- Web user interface
- Telnet CLI
- System status display
- PPP session PAP and CHAP
- IP filter
- IP QoS
- Remote access control
- Line connection status test
- Remote management (telnet and HTTP)
- Backup and restoration of configuration file
- Ethernet interface supports crossover detection, auto-correction and polarity correction
- UPnP
- IPV6
- 3G WAN and 3G Backup
- Samba for USB storage

2 Hardware Installation

2.1 DSL Uplink Connection

Step 1 Connect the **DSL** port of the device and the **Modem** port of the splitter with a telephone cable. Connect the phone to the **Phone** port of the splitter through a telephone cable. Connect the incoming line to the **Line** port of the splitter.

The splitter has three ports:

- Line: Connect to a wall phone port (RJ-11 jack).
- Modem: Connect to the DSL port of the device.
- Phone: Connect to a telephone set.

Step 2 Connect a **LAN** port of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).

Note:
Use twisted-pair cables to connect the device to a Hub or switch.

Step 3 Plug one end of the power adapter to the wall outlet and the other end to the **Power** port of the device.

Figure 3 displays the application diagram for the connection of the device, PC, splitter and telephone sets, when no telephone set is placed before the splitter.

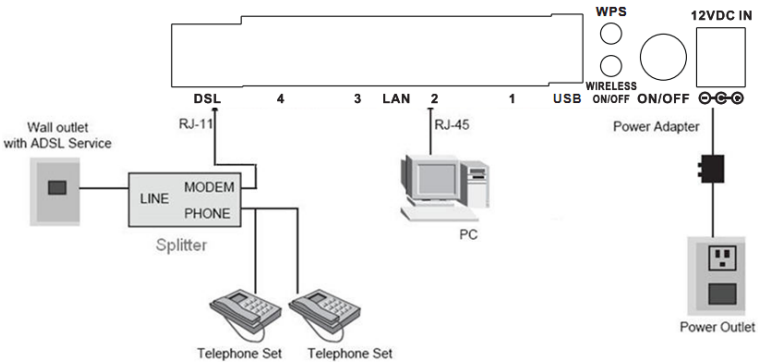


Figure 3 Connection diagram

3 Web Configuration

This chapter describes how to configure the device by using the Web-based configuration utility.

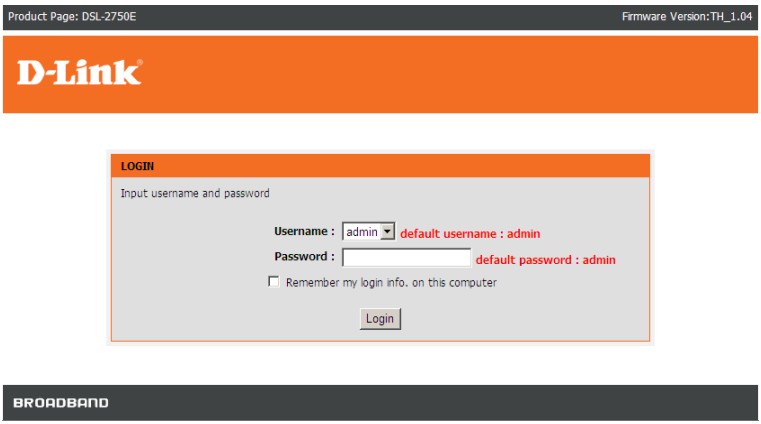
3.1 Accessing the Device

The following is the detailed description of accesing the device for the first time.

Step 1 Open the Internet Explorer (IE) browser and enter **http://192.168.1.1**.

Step 2 The **Login** page shown in the following figure appears. Enter the user name and password and click **Login**.

- The user name and password of the super user are **admin** and **admin**.



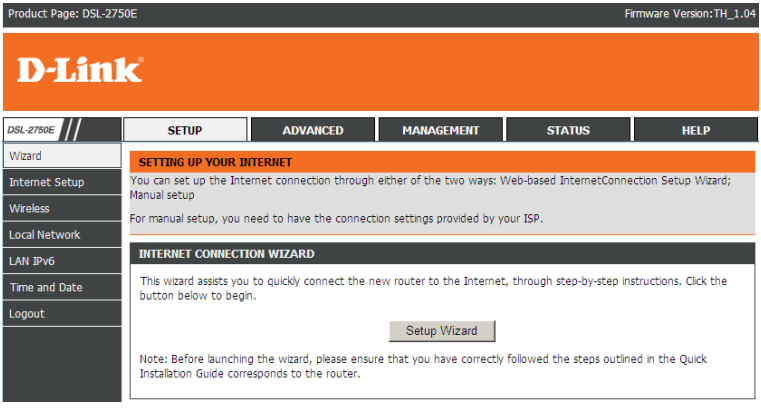
3.2 Setup

3.2.1 Wizard

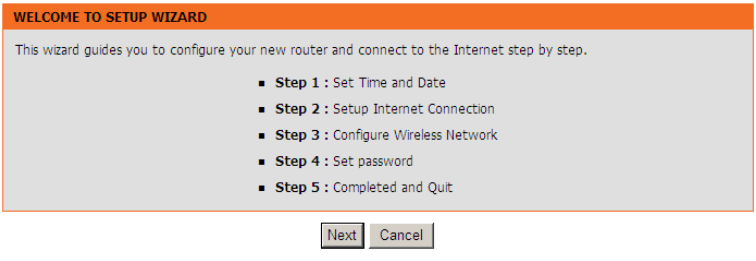
After login, the **Wizard** page under **Setup** tab appears.

Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe configuration parameters. When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Your physical WAN device can be

Ethernet, DSL, or both. Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or the protocol, such as PPPoA or PPPoE, that you use to communicate over the Internet.

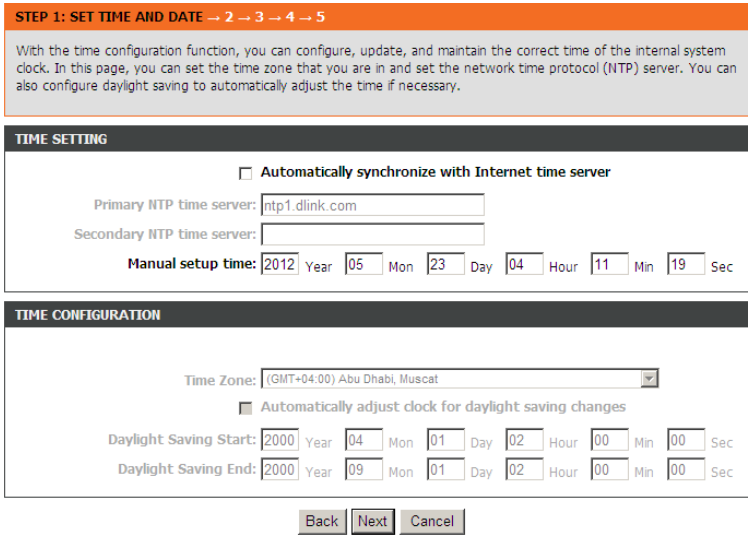


Click **Setup Wizard**. The page shown in the following figure appears.



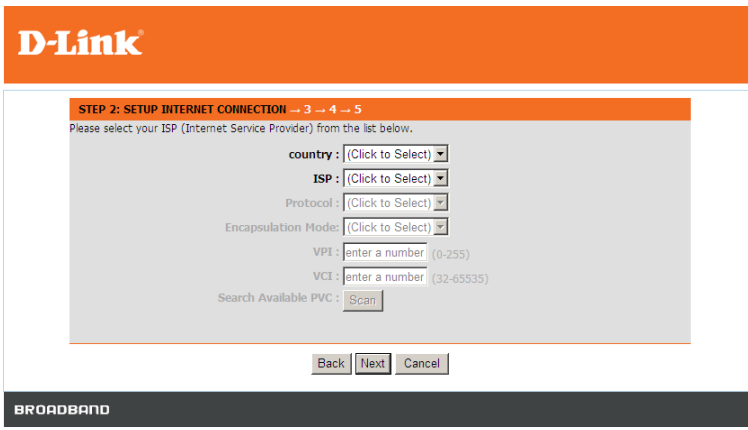
There are 5 steps to configure the device. Click **Next** to continue.

Step 1 Set the time and date.



Step 2 Configure the Internet connection.

Click **Next** after time and date setting and the following page appears. In this page, you can set the internet connection.



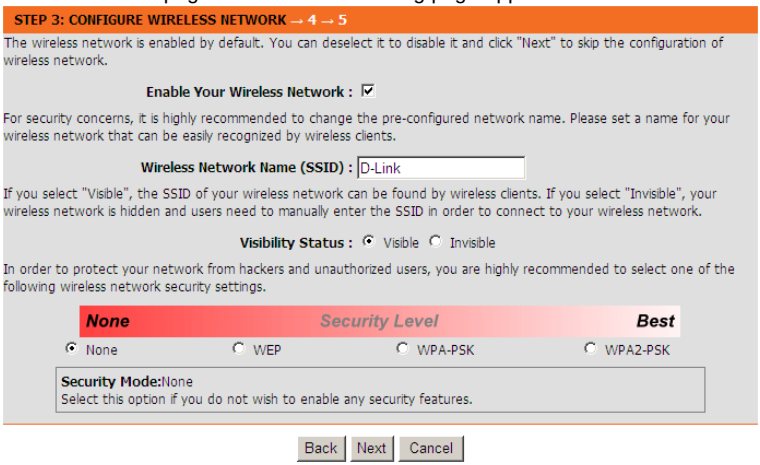
The following table describes the fields in this page.

Field	Description
Country	Select the country you located from the drop-down list.
ISP	Select the ISP you subscribed the internet service from.
Protocol	Select the protocol you subscribed from your ISP.
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select **LLC** or **VCMUX**.
PVC Settings	**VPI**: The virtual path between two points in an ATM network. Its valid value is from **0** to **255**. **VCI**: The virtual channel between two points in an ATM network, ranging from **32** to **65535** (0 to 31 is reserved for local management of ATM traffic).

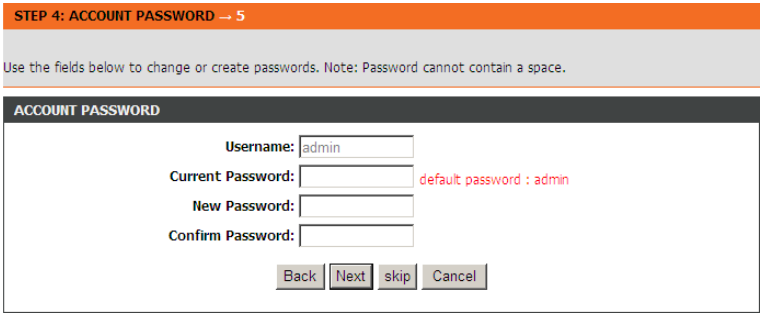
Note:

Different protocol requires entering different information. You can fill in the entries according to what your ISP provides you.

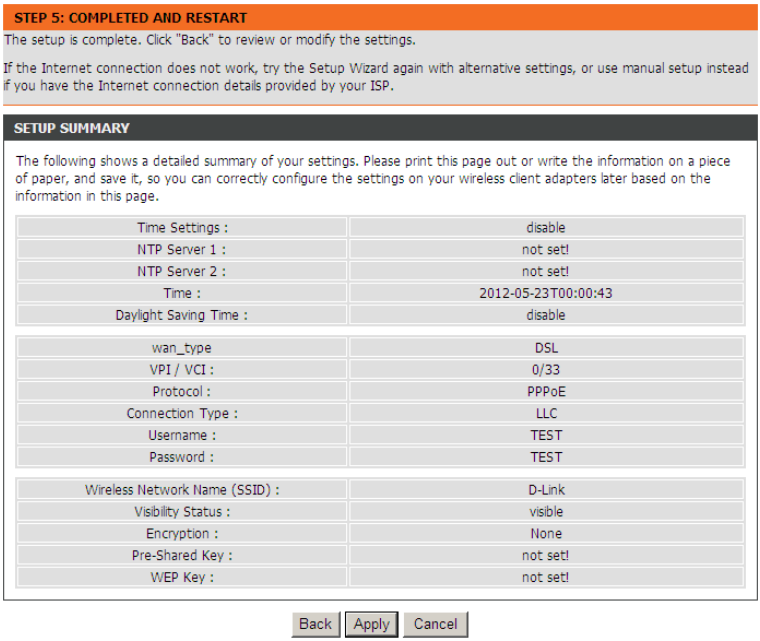
Click **Next**. The page shown in the following page appears.



Step 3 Configure the wireless network. Enter the information and click **Next** to go to the next step.



Step 4 Change or create the password of an account. Click **Next** to go to the next step.



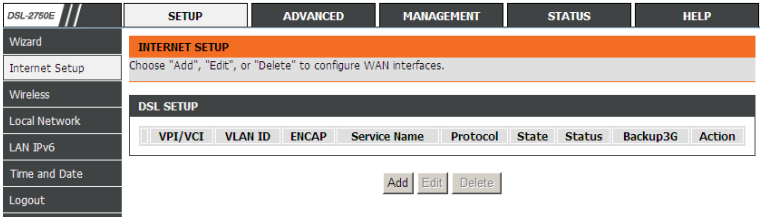
Step 5 Click **Apply** to save the settings.

Note:

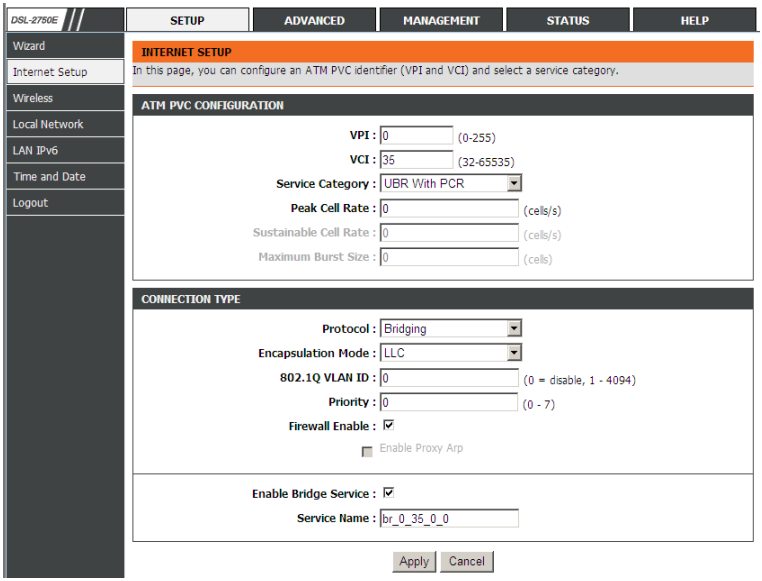
In each step of the Wizard page, you can click **Back** to review or modify the previous settings. Click **Cancel** to exit the wizard page.

3.2.2 Internet Setup

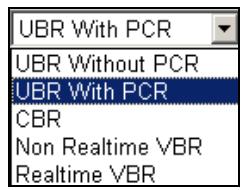
Choose **Setup** > **Internet Setup**. The page shown in the following figure appears. In this page, you can configure the WAN interface of the device.

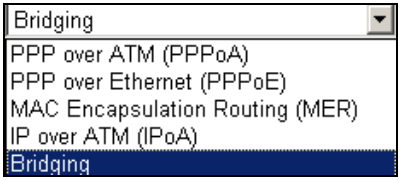


Click **Add** and the page shown in the following figure appears.



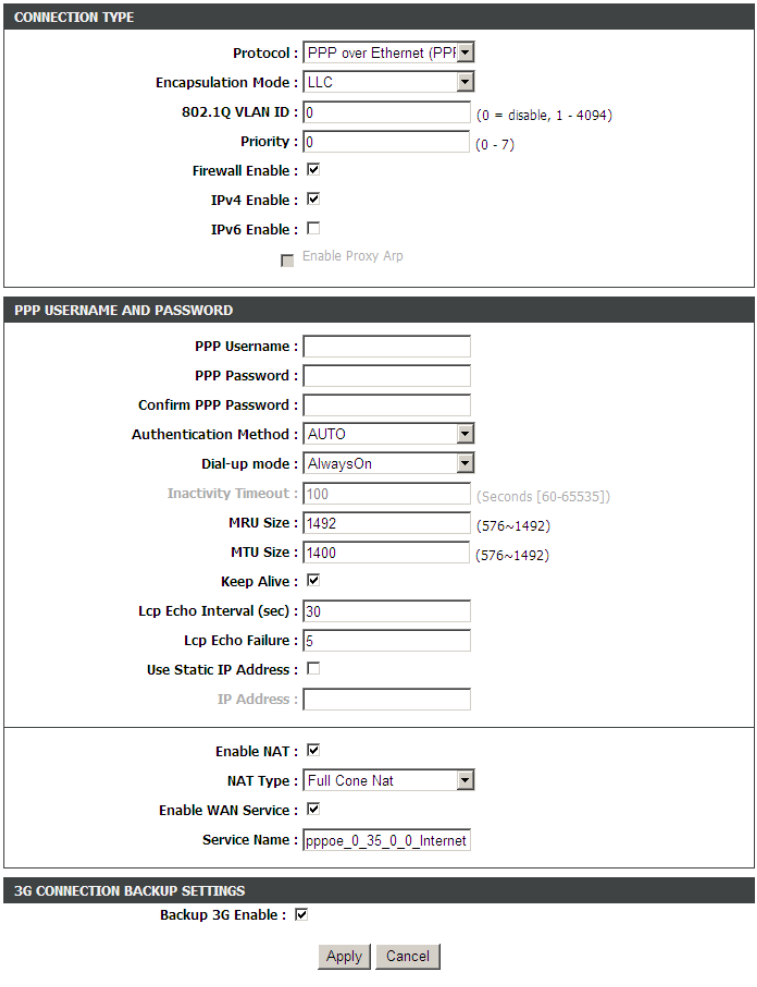
The following table describes the parameters in this page.

Field	Description
PVC Settings	**VPI**: The virtual path between two points in an ATM network. Its valid value is from **0** to **255**. **VCI**: The virtual channel between two points in an ATM network, ranging from **32** to **65535** (0 to 31 is reserved for local management of ATM traffic). The values of VPI and VCI are provided by your ISP.
Service Category	You can select from the drop-down list. 

Field	Description
Protocol	Selected the protocol you subscribed from your ISP. It displays the protocol type used for this WAN connection. 
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select **LLC** or **VCMUX**.
802.1Q VLAN ID	You can enable or disable this function. The value ranges from **1** to **4094**. Value **0** means to disable this function.

- **PPPoE** or **PPPoA**

If the protocol is selected to be **PPP over Ethernet (PPPoE)** or **PPP over ATM (PPPoA)**, the following page appears.



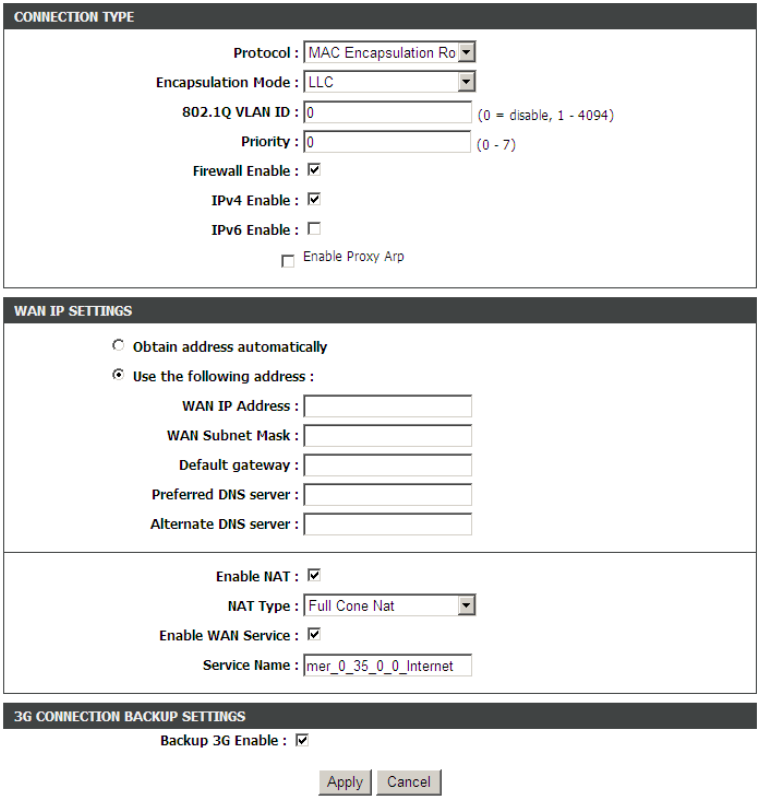
The following table describes the parameters of this page

Field	Description
PPP Username	The correct user name provided by your ISP.

Field	Description
PPP Password	The correct password provided by your ISP
Authentication Method	To authenticate whether the PPP username and password are correct. The value can be **AUTO**, **PAP**, **CHAP** or **MS-CHAP**. Usually, you can select AUTO.
Dial-up mode	● **AlwaysOn**: If you select it, the system automatically establishes a connection. If the network is disconnected because of external factors when you are using the Internet access service, the system tries connection every certain time (for example, 10 seconds) until the connection is established. If you pay for Internet access in the monthly fee mode, you are recommended to use this connection mode. ● **OnDemand**: If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the set time of **Idle Timeout**, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access. ● **Manual:** If you select it, you need to manually set dialup connection after startup.
MRU Size	You can keep it as default.
Use Static IP Address	If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
Enable NAT	NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

- **MAC Encapsulation Routing/IPoA**

Choose Protocol to be **MAC Encapsulation Routing** or **IP over ATM (IPoA)**, and the following page appears.



The following table describes the parameters of this page

Field	Description
WAN IP Address	Enter the WAN IP address provided by the ISP.
WAN Subnet	Enter the WAN subnet mask provided by the ISP. It

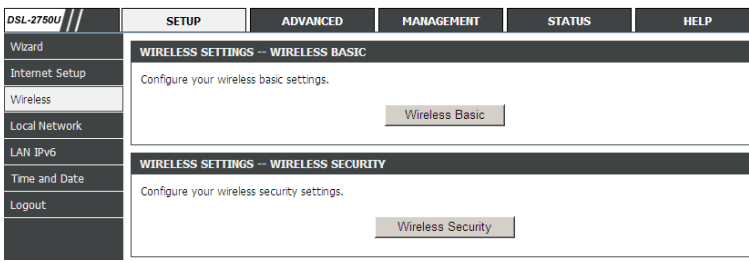
Field	Description
Mask	varies depending on the network type. It is usually 255.255.255.0
Default Gateway	Enter the IP address of the gateway provided by the ISP. It is the IP address used for connecting to the ISP.
Preferred DNS Server	Enter the IP address of the primary DNS server if necessary
Alternate DNS Server	If the ISP provides another DNS server, enter the IP address of that DNS server.

After setting, click **Apply** to make the settings take effect.

3.2.3 Wireless

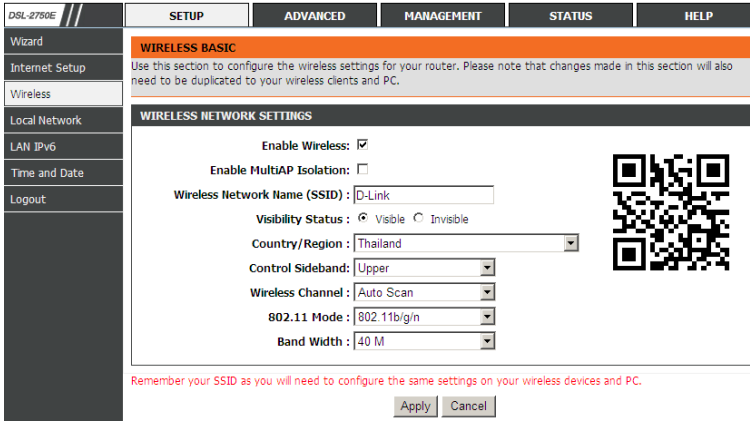
This section describes the wireless LAN and basic configuration. A wireless LAN can be as simple as two computers with wireless LAN cards communicating in a pear-to-pear network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to wired LAN.

Choose **Setup** > **Wireless**. The **Wireless** page shown in the following figure appears.



3.2.3.1 Wireless Basics

In the **Wireless** page, click **Wireless Basic**. The page shown in the following figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.



The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select this to turn Wi-Fi on.
Enable MultiAP Isolation	Select this to turn MultiAP isolation on.
Wireless Network Name (SSID)	The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.
Visibility Status	Select **Visible**, the SSID can be detected. Select **Invisible**, the SSID cannot be detected.
Country	Select the country you located from the drop-down list.
Control Sideband	Choose the channel selection mode as **Upper** or **Lower**.
Wireless Channel	Select the wireless channel from the pull-down menu. It is different for different country.
802.11 Mode	Select the appropriate 802.11 mode based on the

Field	Description
	wireless clients in your network. It is recommended to keep it as default.
Band Width	Select the appropriate band of **20M**, **40M** or **20M/40M** according to your subscribed broadband service.

There is a **2-Dimension Code** on the right of the page. This code can help your cellphone connect to the wireless network of DSL-**2750E** automatically by shooting the 2-Dimension code with the cellphone.

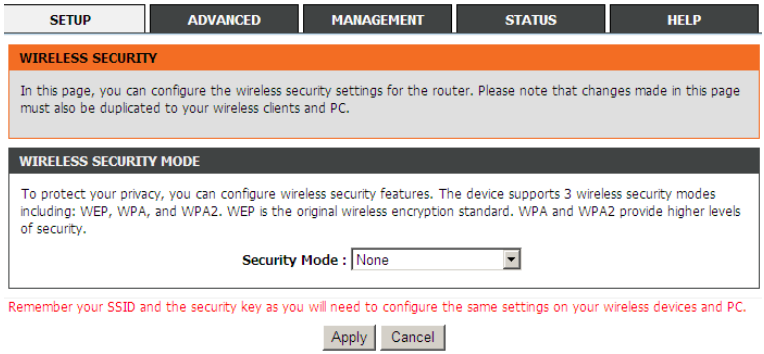
Note:

A cellphone can not connect to the wireless network unless a 2-Dimension code software is installed on your cellphone.

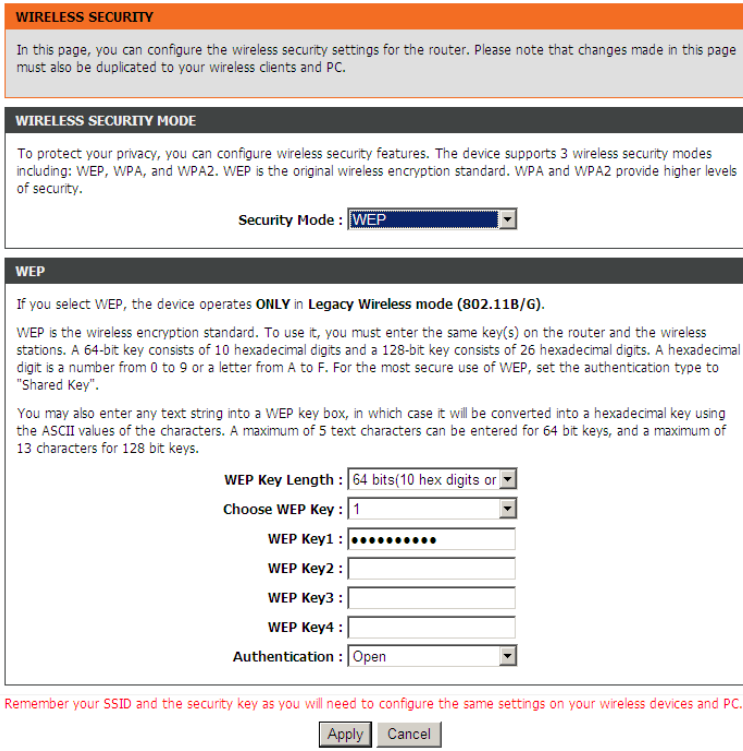
Click **Apply** to save the settings.

3.2.3.2 Wireless Security

In the **Wireless** page, click **Wireless Security**. The page shown in the following figure appears. Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and wired network.



If the Security Mode is set to be **WEP**, the following page appears.

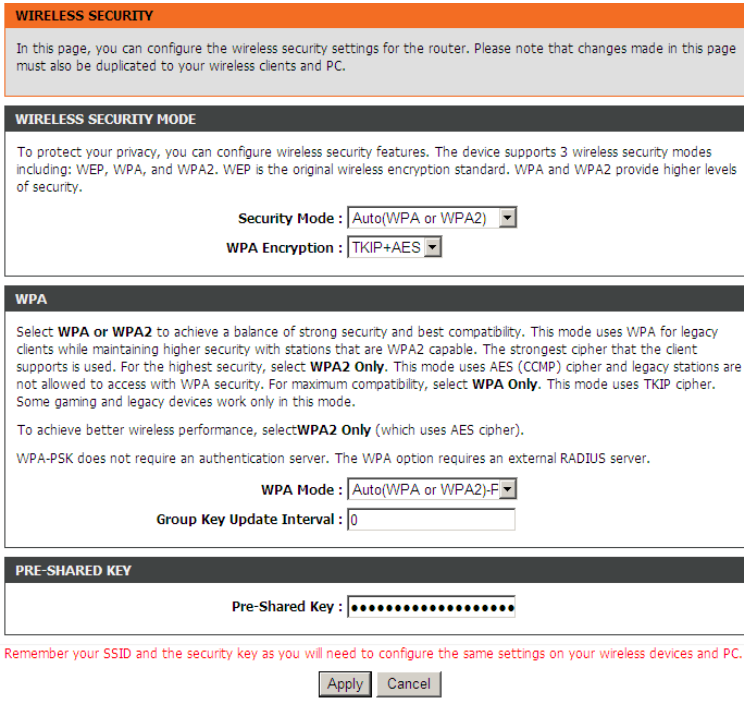


The following table describes the parameters of this page.

Field	Description
Security Mode	Configure the wireless encryption mode. You can choose **None**, **WEP**, **Auto (WPA or WPA2)**, **WPA 2 Only** or **WPA Only**. ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and

Field	Description
	WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. Key differences between WPA and WEP are user authentication and improved data encryption.
WEP Key Length	Choose the WEP key length. You can Choose **64-bit** or **128-bit**.
Choose WEP Key	Choose the index of WEP Key. You can choose **Key 1**, **2**, **3** or **4**.
WEP Key 1/2/3/4	The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission. The default key 1 is **1234567890**.
Authentication	There are 2 authentications in WEP encryption. **Open** and **Share key**. Both authentications support WEP encryption. But the message header is different in wireless broadcast.

If the Security Mode is set to be **Auto (WPA or WPA2)**, **WPA2 only**, or **WPA only**, the following page appears.



The above figure shows the when the Security Mode is set as **Auto (WPA or WPA2)**. The following table describes the parameters in this page.

Field	Description
WPA Encryption	You can select WPA encryption to be **AES** or **TKIP+AES**.
WPA Mode	● Select **Auto (WPA or WPA2)-PSK**, enter the pre-shared key in the **Pre-Shared Key** field. ● Select **Auto (WPA or WPA2)-Enterprise (RADIUS)**, enter the port, IP address, and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the modem.
Group Key	When WPA encryption is applied, messages sent are

Field	Description
Update Interval	encrypted with a password. For higher security, WPA password is updated periodically. This value is the update interval of the WPA password.

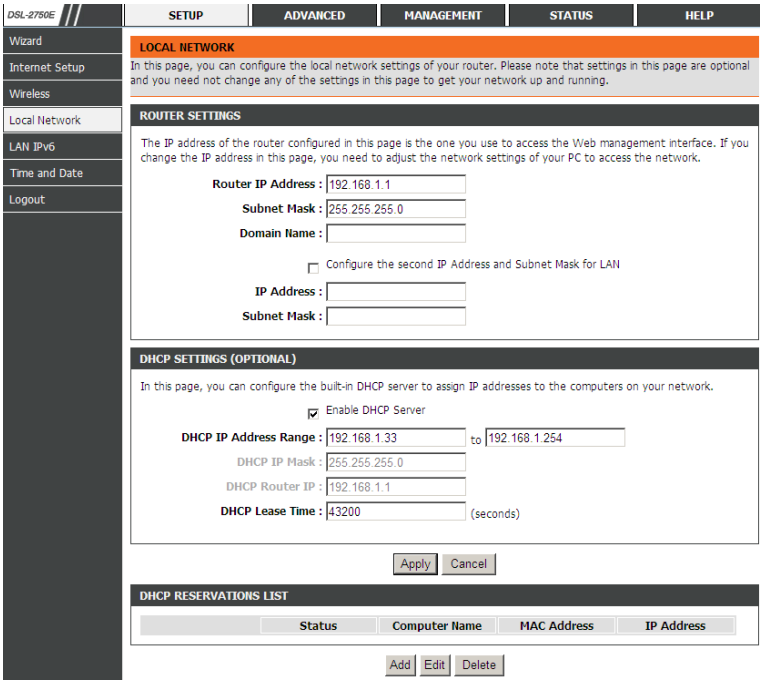
Click **Apply** to save the settings.

3.2.4 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP service to manage the IP settings for the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if you change the IP address of the device.

You can also enable the secondary LAN IP address. The two LAN IP addresses must be in different networks.

Choose **Setup** > **Local Network**. The **Local Network** page shown in the following figure appears.



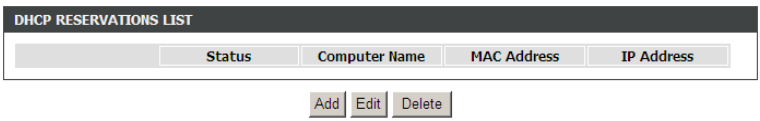
The following table describes the parameters in this page

Field	Description
Router IP Address	Enter the IP address of LAN interface. It is recommended to use an address from a block that is reserved for private use. This address block is **192.168.1.1**- **192.168.255.254**.
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from **255.255.0.0**-**255.255.255.254**.
Domin Name	Enter the domain name if you know. If you leave this blank, the domain name obtained by DHCP from the ISP is used. You must enter host name (system name) on each individual PC. The domain name can be assigned from the router through the DHCP

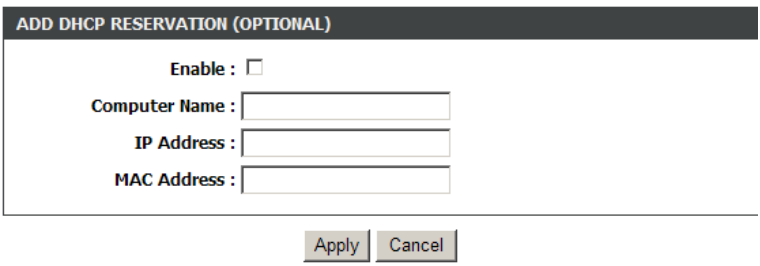
Field	Description
	server.
Configure the second IP Address and Subnet Mask for LAN	Select it to enable the secondary LAN IP address. The two LAN IP addresses must be in the different network.
Enable DHCP Server	Enable the router to assign IP addresses, IP default gateway and DNS Servers to the host in Windows95, Windows NT and other operation systems that support the DHCP client.
DHCP IP Address Range	It specifies the first IP address in the IP address pool. The router assigns IP address that base on the IP pool range to the host.
DHCP Lease Time	The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.

Click **Apply** to make the settings take effect.

The **DHCP RESERVATIONS LIST** shown in the following figure appears.



Click **Add** to add DHCP (optional). The page shown in the following figure appears.

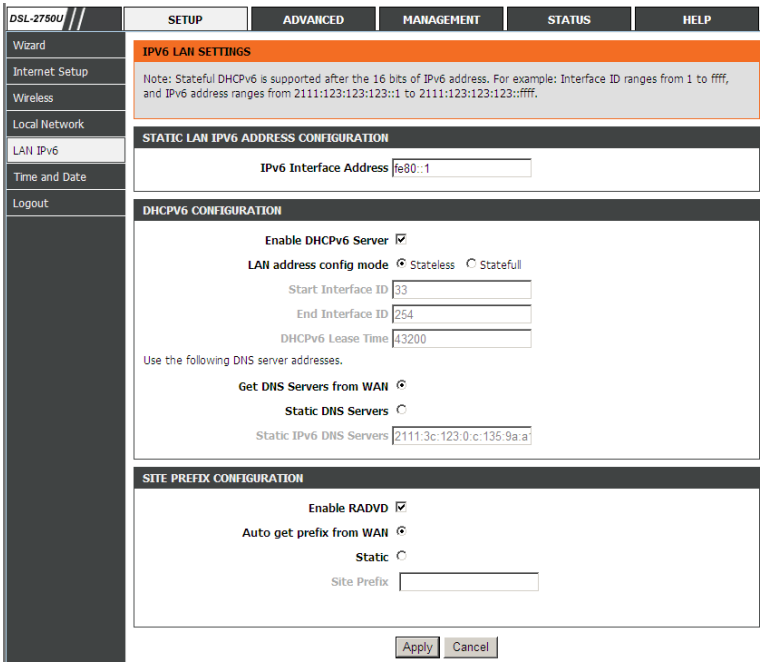


Select **Enable** to reserve the IP address for the designated PC with the configured MAC address. The **Computer Name** helps you to recognize the PC with the MAC address, for example, Father's Laptop. Click **Apply** to save the settings.

After the DHCP reservation is saved, the DHCP reservations list displays the configuration.

3.2.5 LAN IPv6

Choose **Setup** > **LAN IPv6**. The page shown in the following figure appears.This page allows you to config IPv6 LAN.



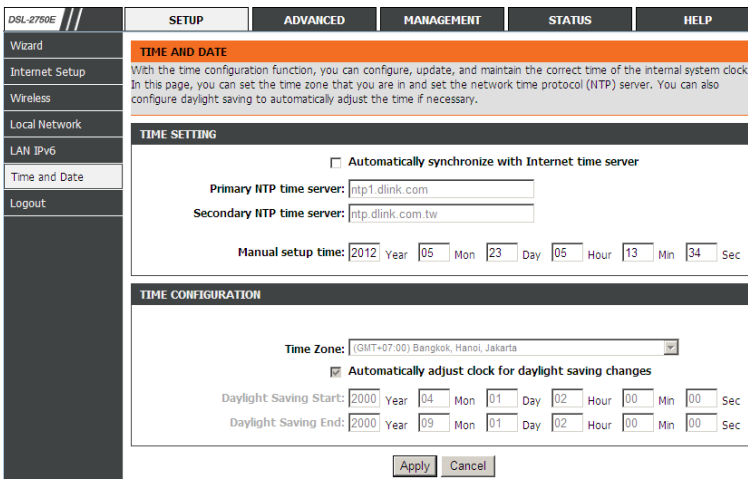
The following table describes the parameters of this page.

Field	Description
IPv6 Interface Address	The address through which PCs access the gateway. For example, 192.168.1.1.

Field	Description
Enable DHCPv6 Server	Choose to enable or disable DHCPv6 service.
LAN address config mode	Set the mode address obtaining mode of LAN PCs. You may choose **Stateless** or **Statefull**.
Start/End Interface ID	The address pool using DHCPv6 for address assignment under statefull mode.
DHCPv6 Lease Time	The address lease time using DHCPv6 for address assignment under statefull mode.
Enable RADVD	Choose to enable or disable router advertisement (RADVD) service.
Auto get prefix from WAN	Use the site prefix obtained at the WAN side as the prefix to issue.
Static	Manually add a site prefix.

3.2.6 Time and Date

Choose **Setup** > **Time and Date**. The page shown in the following figure appears.



In the **Time and Date** page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

Select **Automatically synchronize with Internet time servers**.

Enter the specific time server and select the time zone from the corresponding drop-down lists.

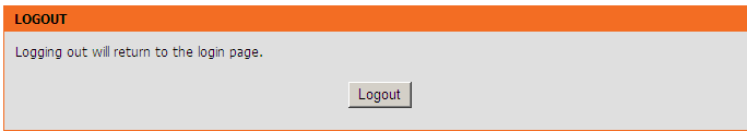
Select **Automatically adjust clock for daylight saving changes** if necessary.

Set the daylight as you want.

Click **Apply** to save the settings.

3.2.7 Logout

Choose **Setup** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



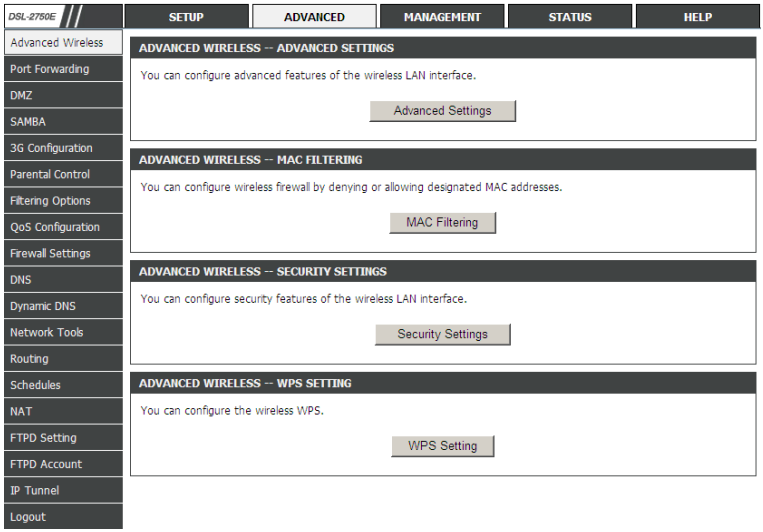
3.3 Advanced

This section includes advanced features for network management, security and administrative tools to manage the device. You can view status and other information used to examine performance and troubleshoot.

3.3.1 Advanced Wireless

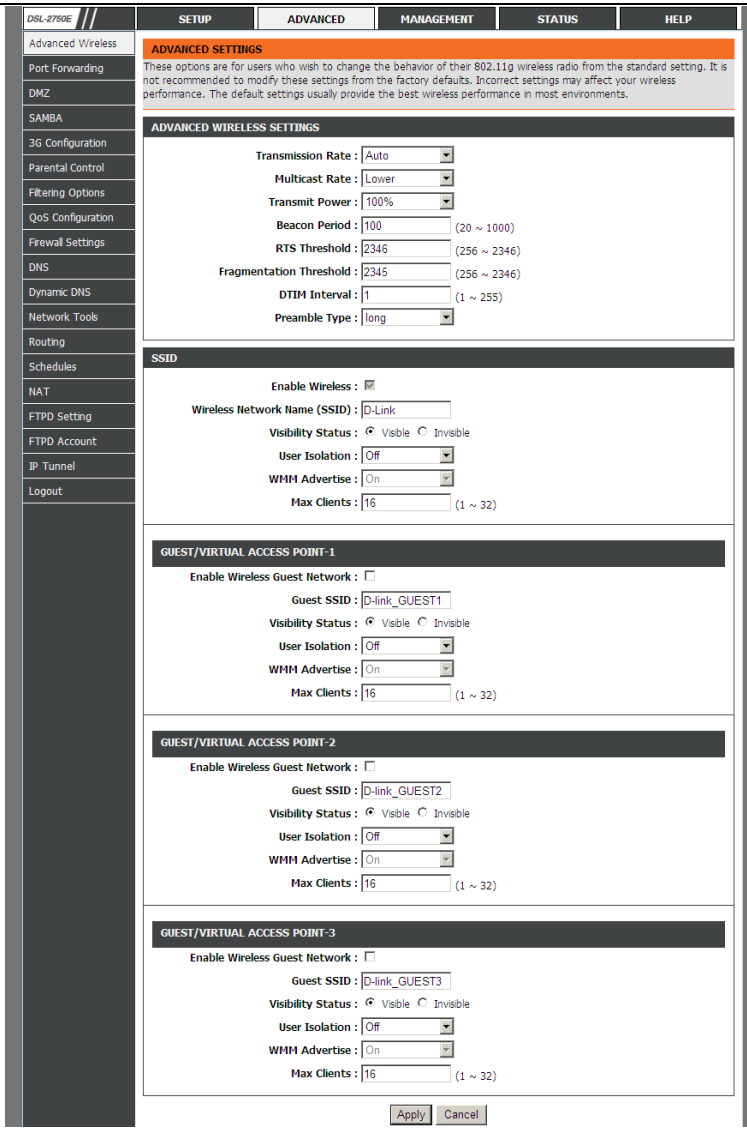
This function is used to modify the standard 802.11g wireless radio settings. It is suggested not to change the defaults, as incorrect settings may reduce the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

Choose **ADVANCED** > **Advanced Wireless**. The page shown in the following figure appears.



3.3.1.1 Advanced Settings

Select **Advance Settings.** The page shown in the following figure appears.


DSL-2750E
SETUP
ADVANCED
MANAGEMENT
STATUS
HELP
Advanced Wireless
Port Forwarding
DMZ
SAMBA
3G Configuration
Parental Control
Filtering Options
QoS Configuration
Firewall Settings
DNS
Dynamic DNS
Network Tools
Routing
Schedules
NAT
FTPD Setting
FTPD Account
IP Tunnel
Logout
ADVANCED SETTINGS
These options are for users who wish to change the behavior of their 802.11g wireless radio from the standard setting. It is not recommended to modify these settings from the factory defaults. Incorrect settings may affect your wireless performance. The default settings usually provide the best wireless performance in most environments.
ADVANCED WIRELESS SETTINGS
Transmission Rate : Auto
Multicast Rate : Lower
Transmit Power : 100%
Beacon Period : 100 (20 ~ 1000)
RTS Threshold : 2346 (256 ~ 2346)
Fragmentation Threshold : 2345 (256 ~ 2346)
DTIM Interval : 1 (1 ~ 255)
Preamble Type : long
SSID
Enable Wireless :
Wireless Network Name (SSID) : D-Link
Visibility Status : Visible Invisible
User Isolation : Off
WMM Advertise : On
Max Clients : 16 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-1
Enable Wireless Guest Network :
Guest SSID : D-link_GUEST1
Visibility Status : Visible Invisible
User Isolation : Off
WMM Advertise : On
Max Clients : 16 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-2
Enable Wireless Guest Network :
Guest SSID : D-link_GUEST2
Visibility Status : Visible Invisible
User Isolation : Off
WMM Advertise : On
Max Clients : 16 (1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-3
Enable Wireless Guest Network :
Guest SSID : D-link_GUEST3
Visibility Status : Visible Invisible
User Isolation : Off
WMM Advertise : On
Max Clients : 16 (1 ~ 32)
Apply
Cancel

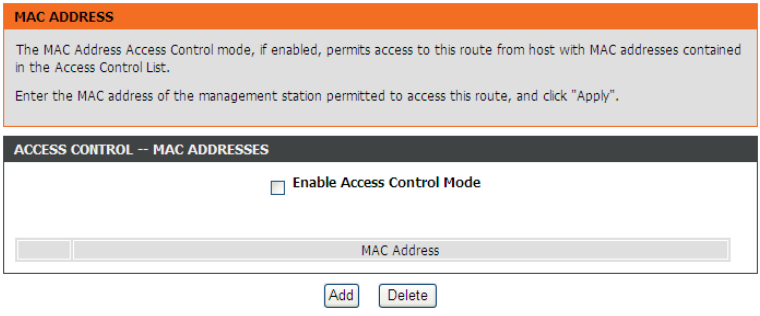
Wireless Network Name (SSID): The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Do not change these settings unless you know the effect of changes on the device.

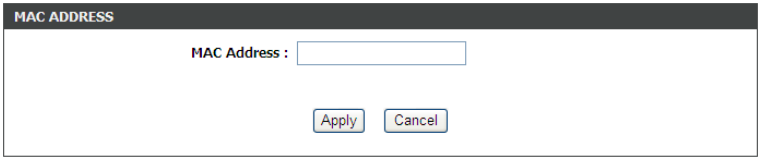
Click **Apply** to save the settings.

3.3.1.2 MAC Filtering

Select **MAC Filtering**. The page shown in the following figure appears.



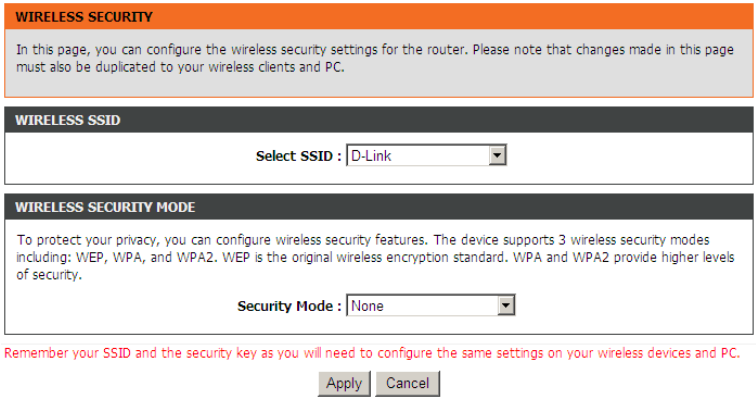
Choose **Enable Access Control Mode**, and then click **Add** to add a MAC Address as shown in the following figure.



Click **Apply** to finish.

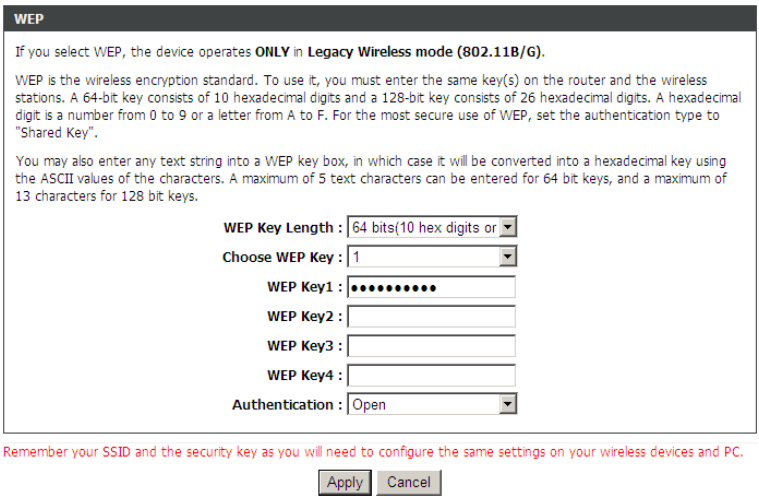
3.3.1.3 Security Settings

Select **Security Settings**. The page shown in the following figure appears.

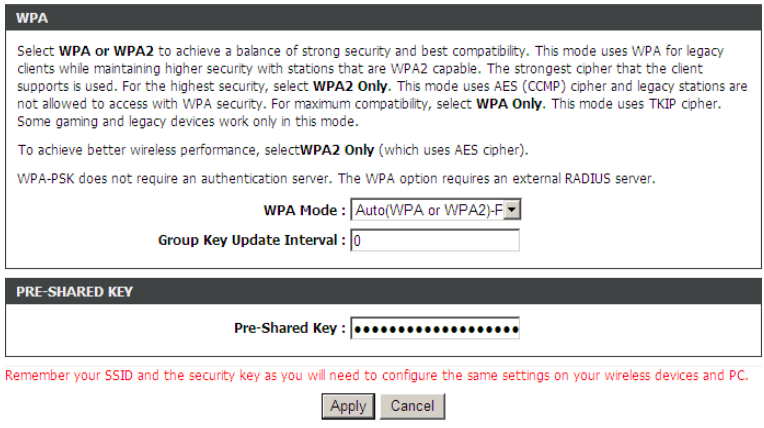


Select the SSID that you want to configure from the drop-down list. Select the encryption type from the **Security Mode** drop-down list.You can select **None**, **WEP**, **AUTO (WPA or WPA2)**, **WPA Only** or **WPA2 Only**.

If you select **WEP**, the page shown in the following figure appears.



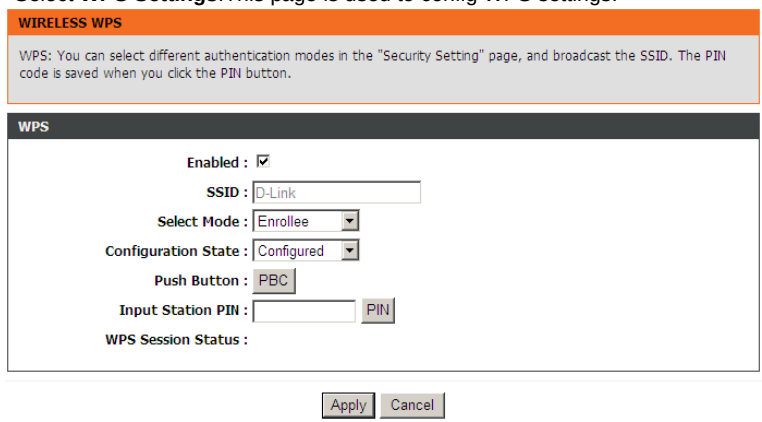
If you select **AUTO (WPA or WPA2)**, **WPA Only** or **WPA2 Only**, the page shown in the following figure appears.



Click **Apply** to save the settings. For detailed configuration, you may refer to 3.2.3.2 Wireless Security.

3.3.1.4 WPS Settings

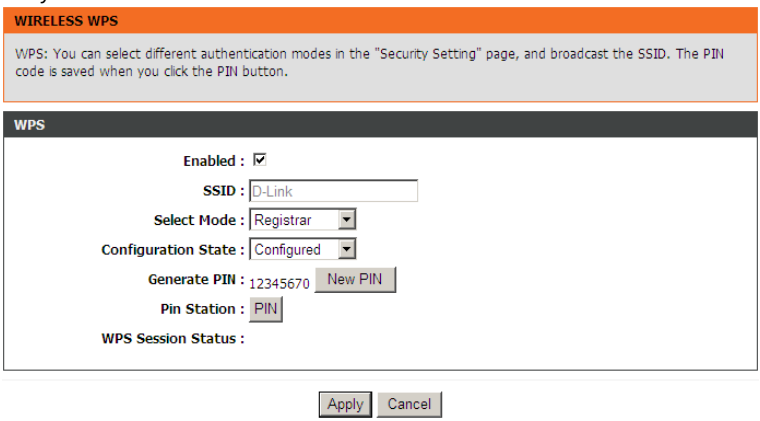
Select **WPS Settings**.This page is used to config WPS settings.



The following table describes the parameters of this page.

Field	Description
Enabled	To enable WPS function and be able to set the following settings.
SSID	The name of your wireless network.
Select Mode	Select the mode either **Registar** or **Enrollee**. When a router is in Registar mode, the client should be in Enrollee mode, and vice versa.
Configuration State	When **Configured** state is selected, wireless parameters (for example, the encryption password) are provided by the CPE in WPS negotiation. When **Unconfigured** state is selected, wireless parameters are provided by the connecting user end (for example, PC).
Push Button	Press the button, the CPE will connect the station automaticlly.
Input Station PIN	You need to enter a pin which the Enrollee generated. Press the button to connect the other with the pin.

When **Registrar** mode is chosen, the following page appears. In this condition, only PIN button can be used.



The following table describes the parameters of this page.

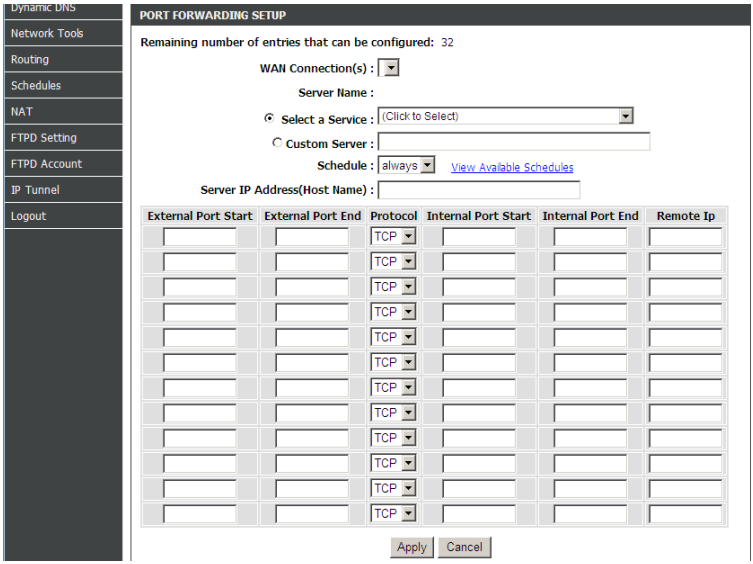
Field	Description
Generate PIN	Press the button to generate a pin used by the AP and the station.
PIN Station	Press the button to connect the station with the pin.
WPS Session Status	Display the session status.

3.3.2 Port Forwarding

This function is used to open ports in your device and re-direct data through those ports to a single PC on your network (WAN-to-LAN traffic). It allows remote users to access services on your LAN, such as FTP for file transfers or SMTP and POP3 for e-mail. The device accepts remote requests for these services at your global IP address. It uses the specified TCP or UDP protocol and port number, and redirects these requests to the server on your LAN with the LAN IP address you specify. Note that the specified private IP address must be within the available range of the subnet where the device is in.

Choose **ADVANCED** > **Port Forwarding**. The page shown in the following figure appears.

Click **Add** to add a virtual server.



Select a service for a preset application, or enter a name in the **Custom Server** field.

Enter an IP address in the **Server IP Address** field to appoint the corresponding PC to receive forwarded packets.

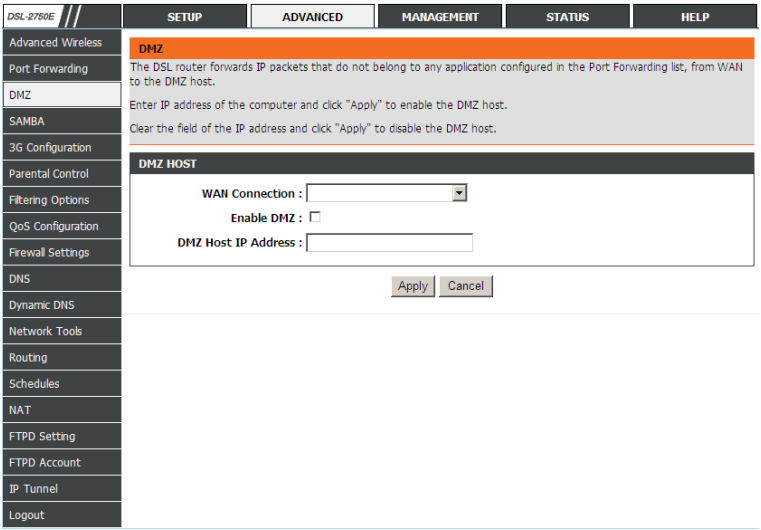
The **Ports** show the ports that you want to open on the device. The **TCP/UDP** means the protocol type of the opened ports.

Click **Apply** to save the settings.

3.3.3 DMZ

DMZ is the abbreviation of the Demilitarized Zone. Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

Choose **ADVANCED** > **DMZ**. The page shown in the following figure appears.

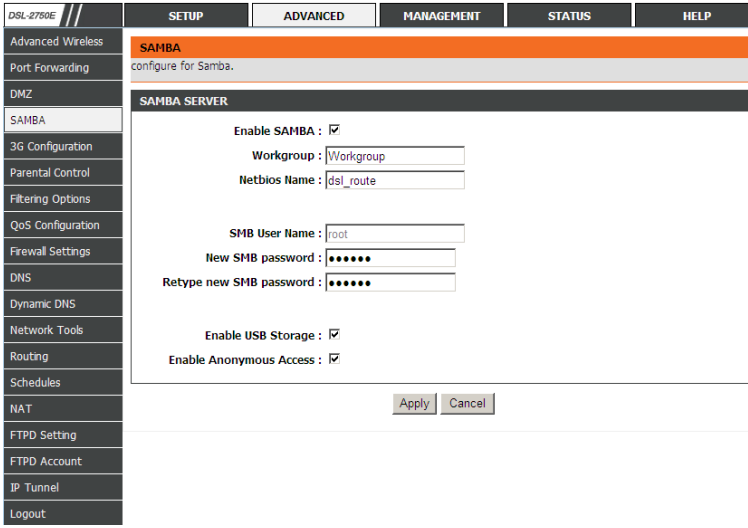


Click **Apply** to save the settings.

3.3.4 SAMBA

SAMBA enables the workstation in the network to share the USB flash disk connected to the 2750E.

Choose **ADVANCED** > **SAMBA**. The page shown in the following figure appears. In this page you can configure the SAMBA.



3.3.5 3G Configuration

Choose **ADVANCED** > **3G Configuration**. （Ensure your 3G card is connected the USB interface of 2750E）

Note:

It will take about 2 minutes for 2750E to connect the 3G network..

- **3G card without PIN protect**

Plug a 3G card without PIN protection, 2750E will detect the inserted 3G card and try to connect automatically.

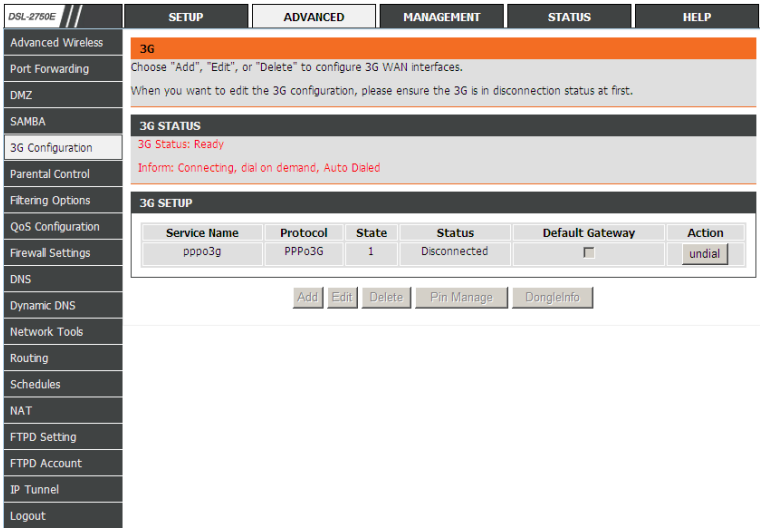
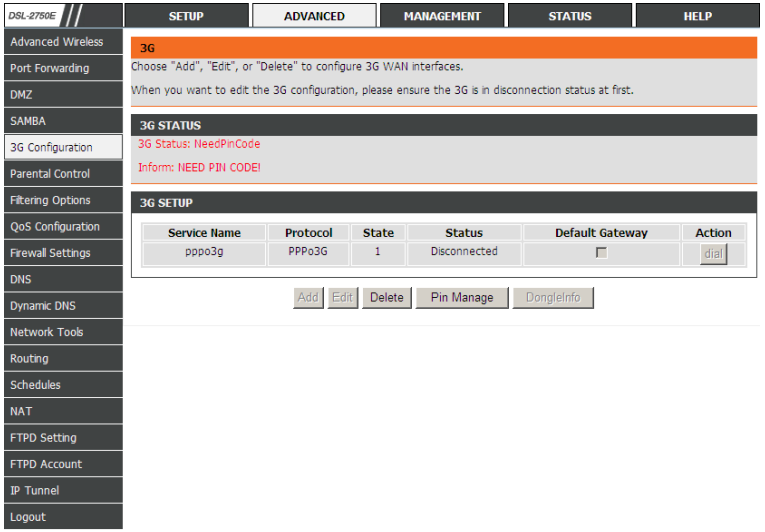


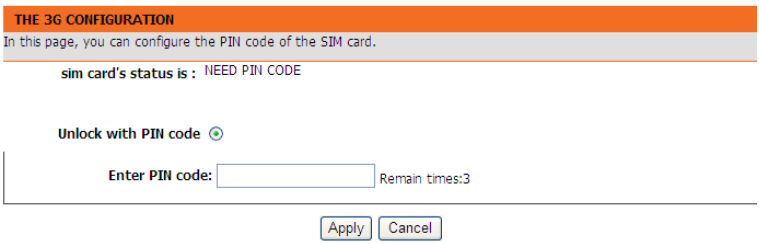
Figure 4 Main page

- **3G card with PIN protect**

If the inserted 3G card has PIN protect function, the page will be shown as the following figure appears. You'll be required to enter a PIN code which provided by your ISP before connecting to 3G network. Follow the instructions below to authenticate the pin code.

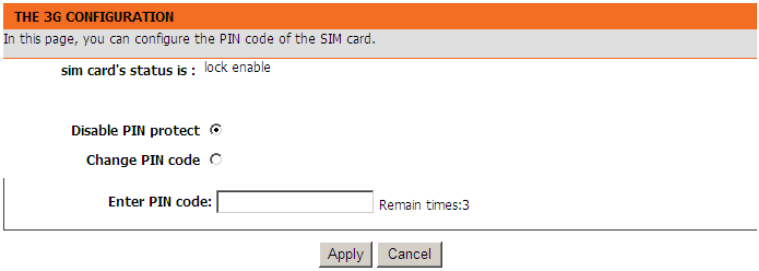


Step1 Click **Pin Manage**, the following page appears.



Step2 Enter the Pin provided by your ISP, then click **Apply**, the following page appears. This page indicates the pin authentication is complete.

Seconds later, the page will automatically skip to the following page.



In this page, you can choose to

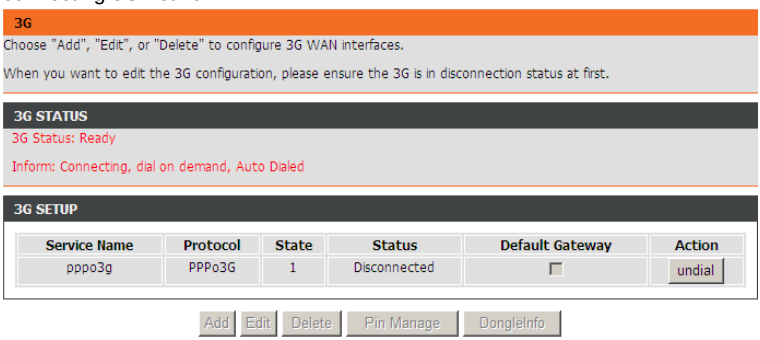
- keep the Pin protection of the 3G card
- Disable the Pin protection of the 3G card.
- Change the Pin code.

- Keep the PIN Protect

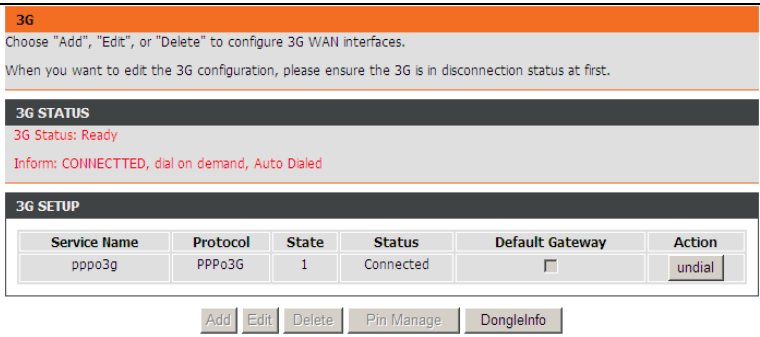
Check **Disable PIN protect**, then click **Apply**. The following page will appear.

This page indicates that the PIN protection remains effective.

Seconds later, the page will skip to the following page, the device continues to connecting 3G network.

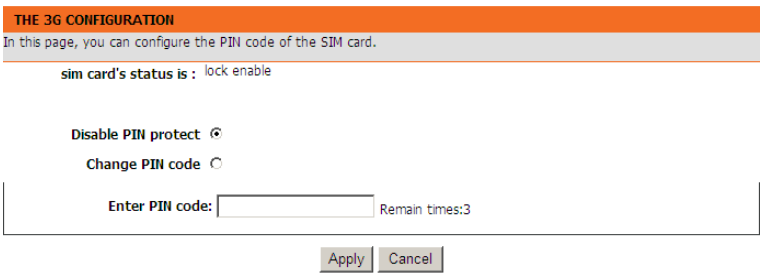


If the 3G connection is established, you can see the following page.



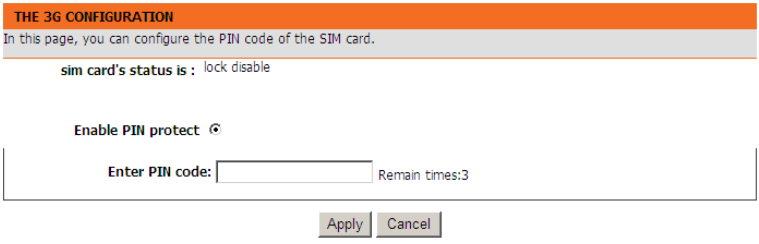
- Disable PIN Protect

Click **Pin Manage** in the main page, and the following page appears.

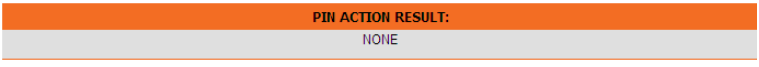


In this page, check **Disable PIN protect** and enter the pin code in **Enter PIN code** field, and then click **Apply**. The following page will appear.

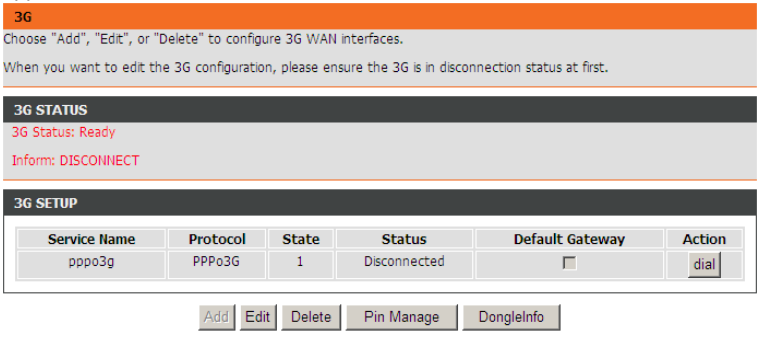
This page indicates that the PIN protect function is disabled. The page will skip to the following page seconds later.



In this page, click **Apply**, and the page appears as the following figure appears.



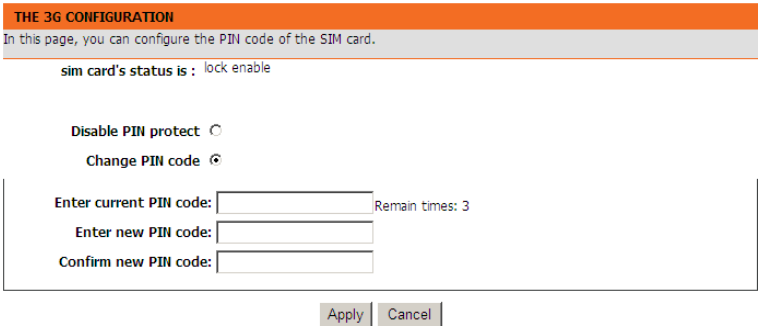
Seconds later, the page will go back to the main page shown as following figure appears.



Click **dial** to connect the 3G network.

- Change PIN Code

Check **Change PIN code**, and the following page appears.



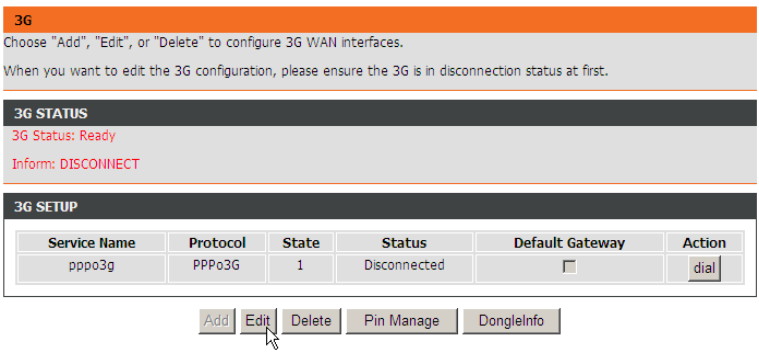
Enter the required PIN code and click **Apply**. If the operation is successful, the following page will appear.

Note:

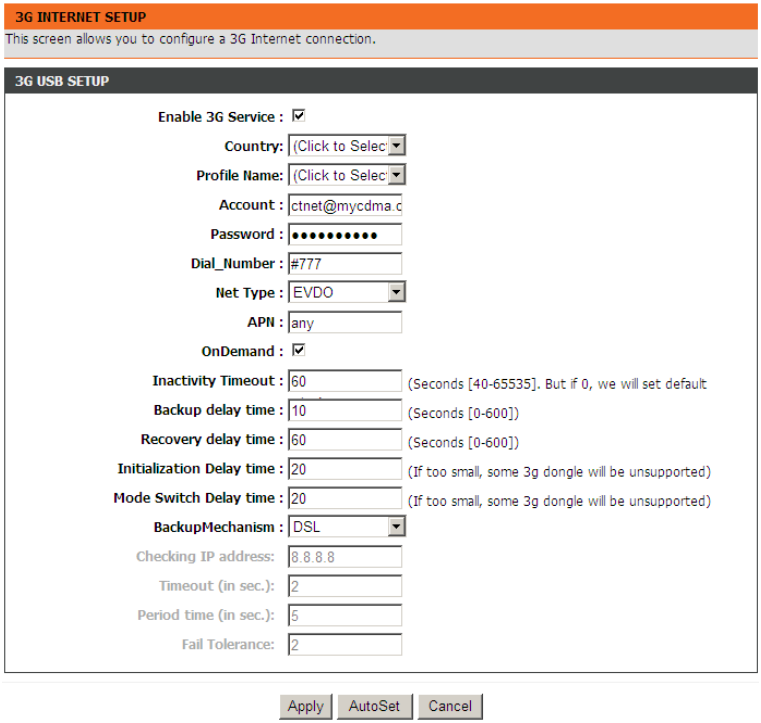
If you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.

- **Edit an Existing 3G Configuration**

If you want to edit an existing 3G configuration, click **Edit** in the main page of **3G configuration**.



Click **Edit**, and the following page appears.



The following table describes the parameters of this page.

Field	Description
Country	Choose the country you located in the dropdown list.
Profile Name	Choose the ISP you subscribed service from.
Dial_Number	The number to be dialed to connect to 3G network. It's recommended to keep it as default.
Net Type	Choose the 3G network access type.
Backup Delay	The response time for 3G connection dial-up after

Field	Description
Time	DSL or Ethernet uplink is disconnected.
Recovery Delay Time	The time interval to re-dial.
Initialize Delay Time	The time for 3G card to initialize.
Mode Switch Delay Time	The time for mode switch.

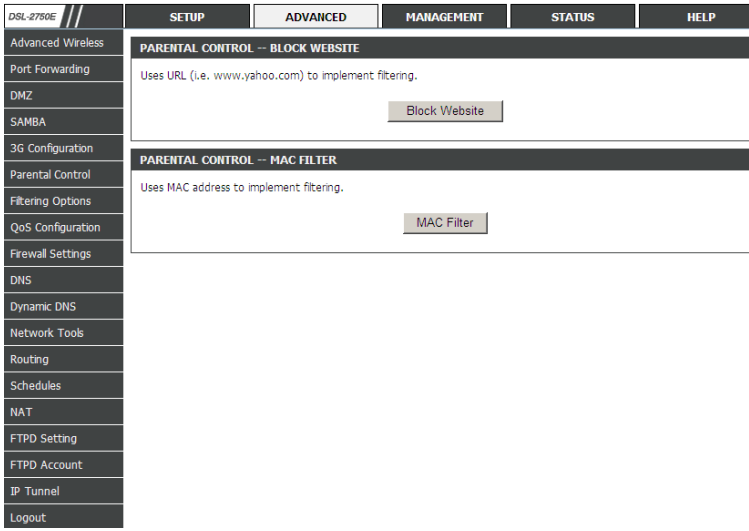
After setting, click **Apply** to make the settings take effect. Click **AutoSet** to keep the settings as default.

Note:

If you want to go back to the main page of 3G configuration, click **3G Configuration** listed in the menu of left pane.

3.3.6 Parental Control

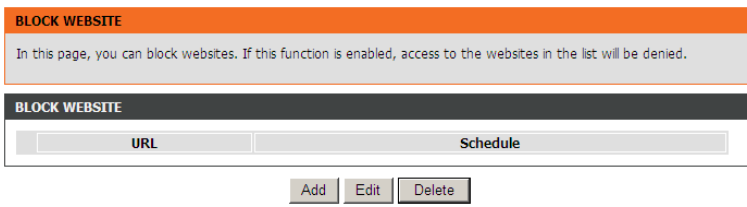
Choose **ADVANCED** > **Parental Control**. The **Parent Control** page shown in the following figure appears.



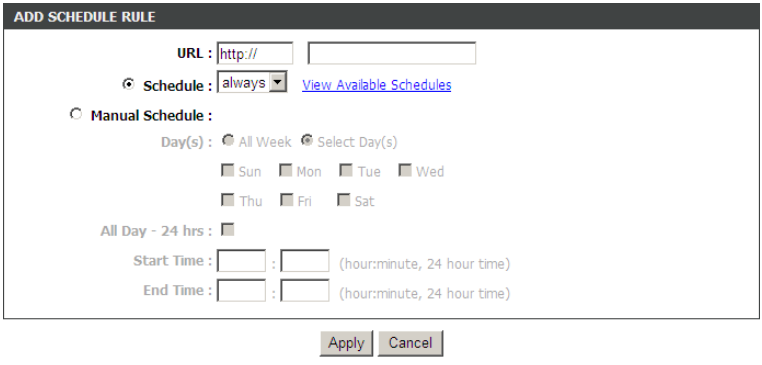
This page provides two useful tools for restricting the Internet access. **Block Websites** allows you to quickly create a list of all websites that you wish to stop users from accessing. **MAC Filter** allows you to control when clients or PCs connected to the device are allowed to access the Internet.

3.3.6.1 Block Website

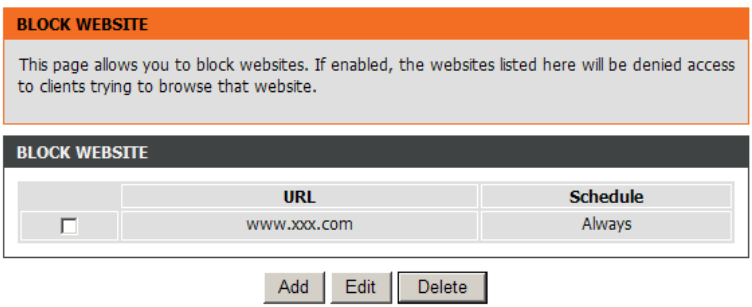
In the **Parent Control** page, click **Block Website**. The page shown in the following figure appears.



Click **Add**. The page shown in the following page appears.

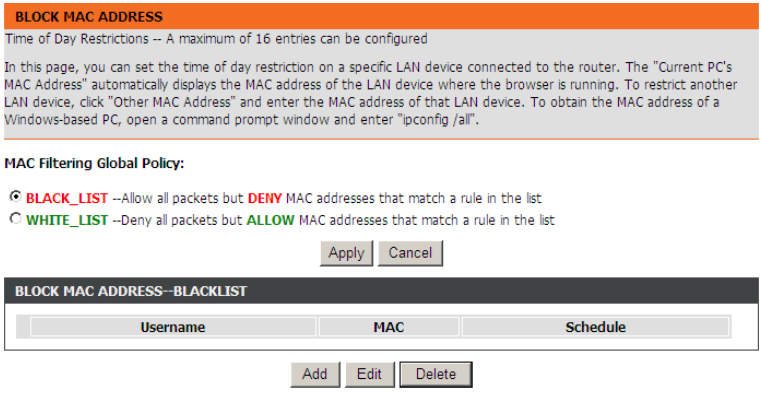


Enter the website in the **URL** field. Select the **Schedule** from the drop-down list, or select **Manual Schedule** and select the corresponding time and days.
Click **Apply** to add the website to the **BLOCK WEBSITE** table. The page shown in the following figure appears.

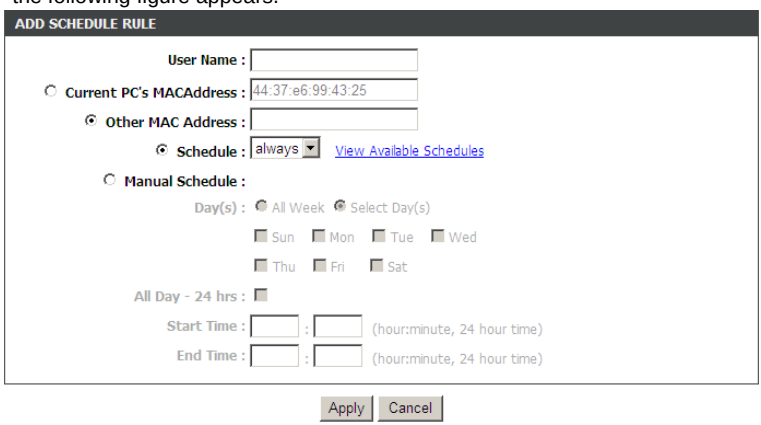


3.3.6.2 MAC Filter

In the **Parent Control** page, click **MAC Filter**. The page shown in the following figure appears.



Choose **BLACK_LIST** or **WHITE_LIST**, and then click **Add**. The page shown in the following figure appears.



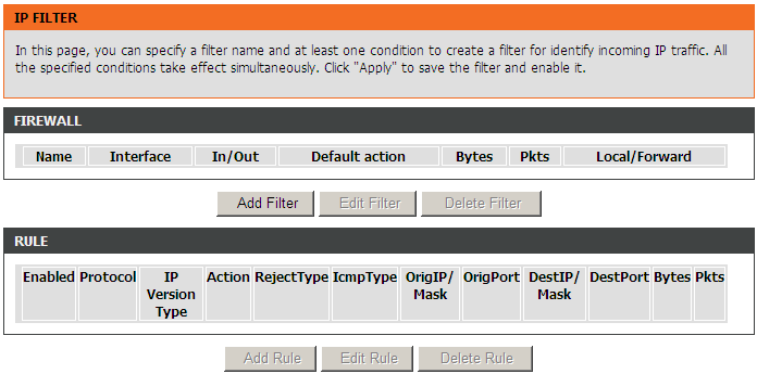
Enter the use name and MAC address and select the corresponding time and days. Click **Apply** to add the MAC address to the **BLOCK MAC ADDRESS Table**.

3.3.7 Filtering Options

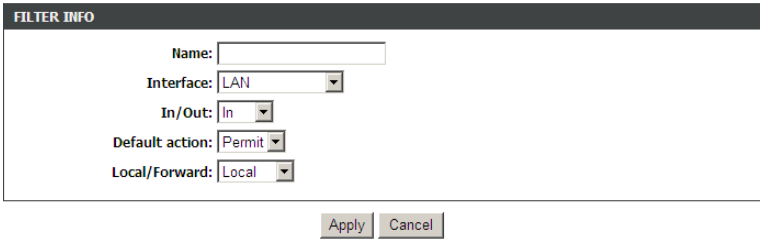
Choose **ADVANCED** > **Filtering Options**. The **Filtering Options** page shown in the following figure appears.

3.3.7.1 IP Filtering

Click **IP Filtering**. The page shown in the following figure appears. In this page, you may configure IP firewall function.



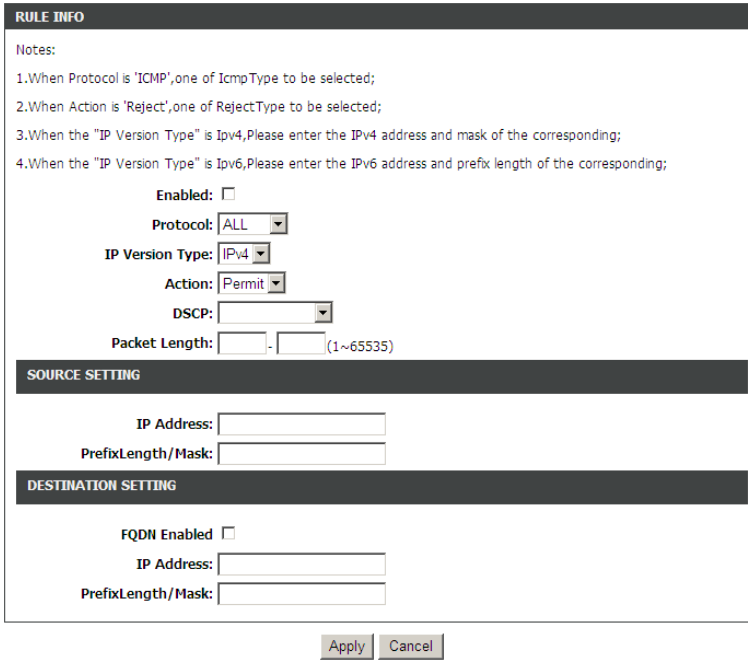
Click **Add Filter**. The page shown in the following figure appears.



Enter the **Filter Name** and specify at least one of the following criteria: Interface, In/Out, Default action and Local/Forward.
Click **Apply** to save the settings.

Note:
The settings are applicable only when the firewall is enabled.

Click **Add Rule**. The page shown in the following figure appears.

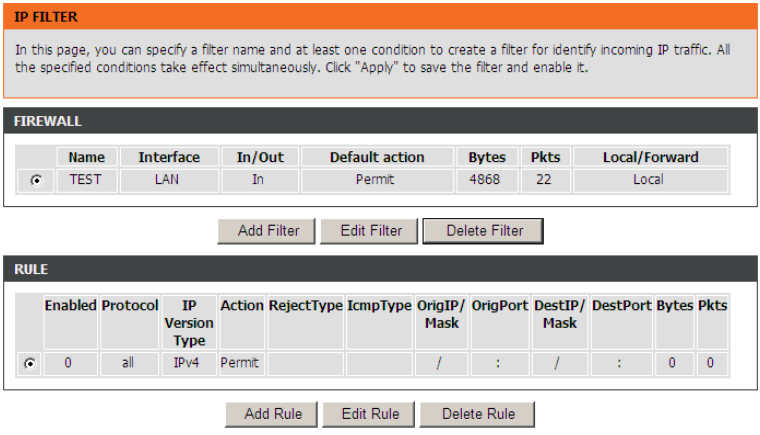


The following table describes the parameters of this page.

Field	Description
Enable	Tick in the box to enable a firewall rule.
Protocol	Choose a protocol corresponding to the rule. You may choose **TCP**, **UDP** or **ICMP**.
Action	The action when the rule is matched. **Permit** means allowing the message to pass, **Drop** means discarding messages without a reply, and **Reject** means discarding messages with a reply.
DSCP	Differentiated Services Code Point. It is used to mark the IP QoS.
IP Address	Original IP address
PrefixLength/Mask	Original address mask

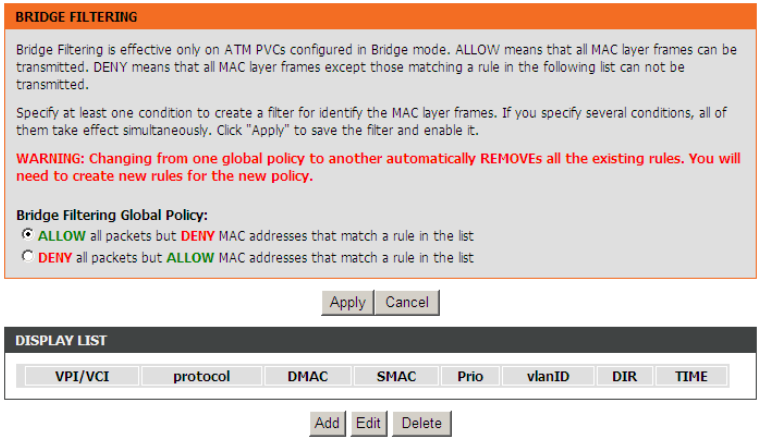
Field	Description
IP Address	Destination IP address
PrefixLength/Mask	Destination address mask

After setting the parameters, click **Apply**. The page shown in the following figure appears.

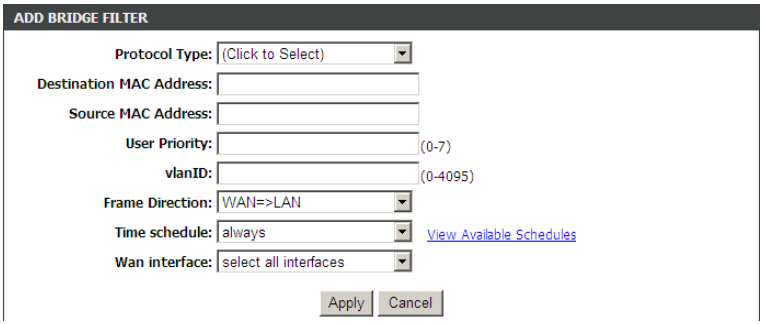


3.3.7.2 Bridge Filtering

In the **Filtering Options** page, click **Bridge Filtering**. The page shown in the following figure appears.This page is used to configure bridge parameters. In this page, you can change the settings or view some information of the bridge and its attached ports.



Click **Add** to add a bridge filter. The page shown in the following figure appears.



The following table describes the parameters of this page.

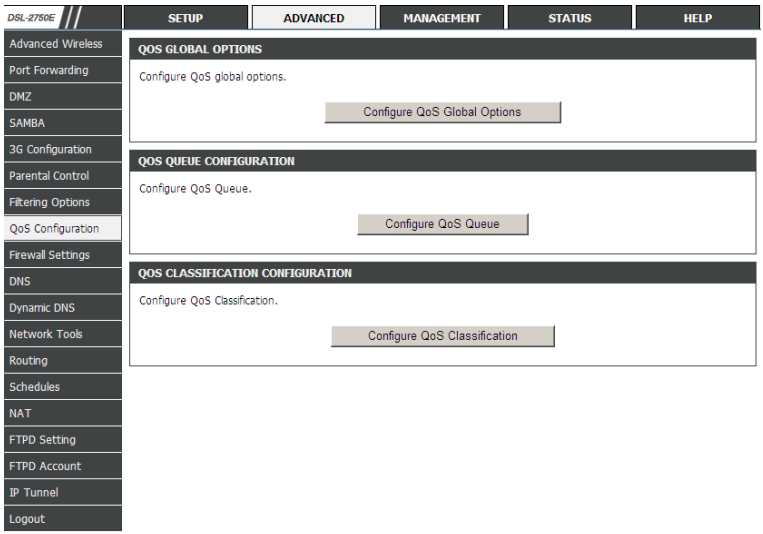
Field	Description
Protocol Type	Choose a third-layer protocol type for bridge filtering from the drop-down list. You may choose **PPPoE**, **IPv4**, **IPv6**, **AppleTalk**, **IPX**, or **NetBEUI**.
Destination MAC Address	The MAC address of sendee of the message.
Source MAC	The MAC address of sender of the message.

Field	Description
Address	
Frame Direction	Choose the sending direction as **WAN to LAN** or **LAN to WAN**.
Time schedule	Choose the filtering strategy as **always** or **never**.
Wan interface	Set an effective interface for the bridge filtering rule.

Click **Apply** to save the settings.

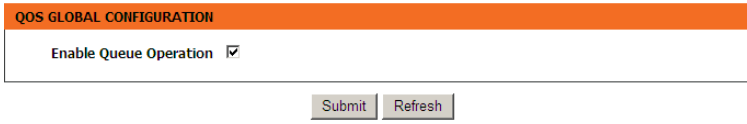
3.3.8 QoS Configuration

Choose **ADVANCED** > **QoS Configuration**. The **QoS Configuration** page shown in the following figure appears.



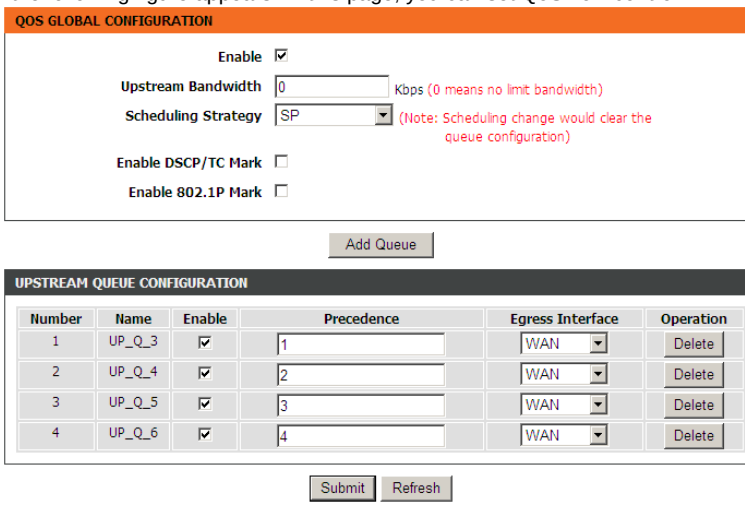
3.3.8.1 QoS Global Options

In the **QoS Configuration** page, click **Configure QoS Global Options**. The page shown in the following figure appears.You can tick in the checkbox and then click **Submit** to enable queuing operation.



3.3.8.2 QoS Queue Config

In the **QoS Configuration** page, click **QoS Queue Config**. The page shown in the following figure appears. In this page, you can set QoS flow control.



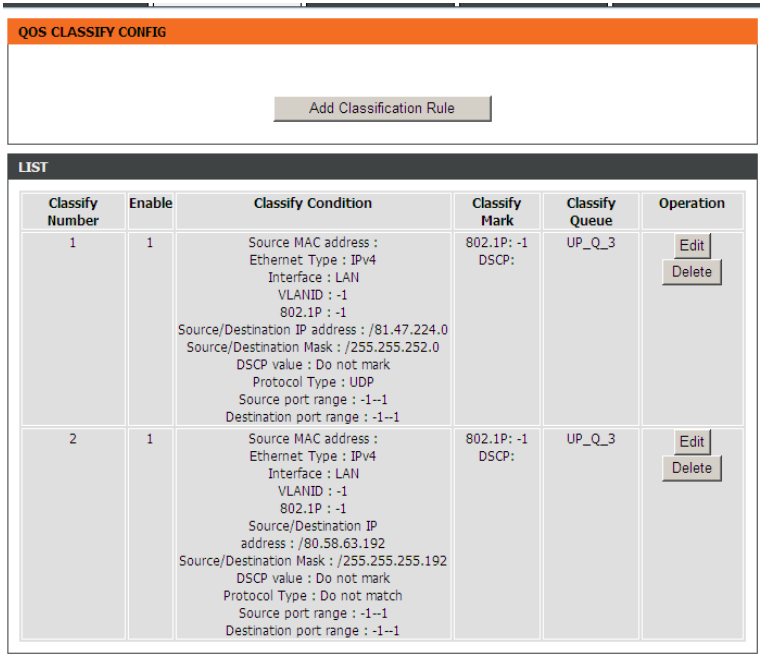
The following table describes the parameters of this page.

Field	Description
Enable	Tick in the box to enable queue.
Upstream Bandwidth	Total bandwith for upstream flow.
Scheduling Strategy	Scheduling algorithm of QoS queue.
Enable DSCP/TC Mark	You may tick in the box to permit DSCP/TC Mark.
Enable 802.1P Mark	You may tick in the box to permit 802.1P Mark.

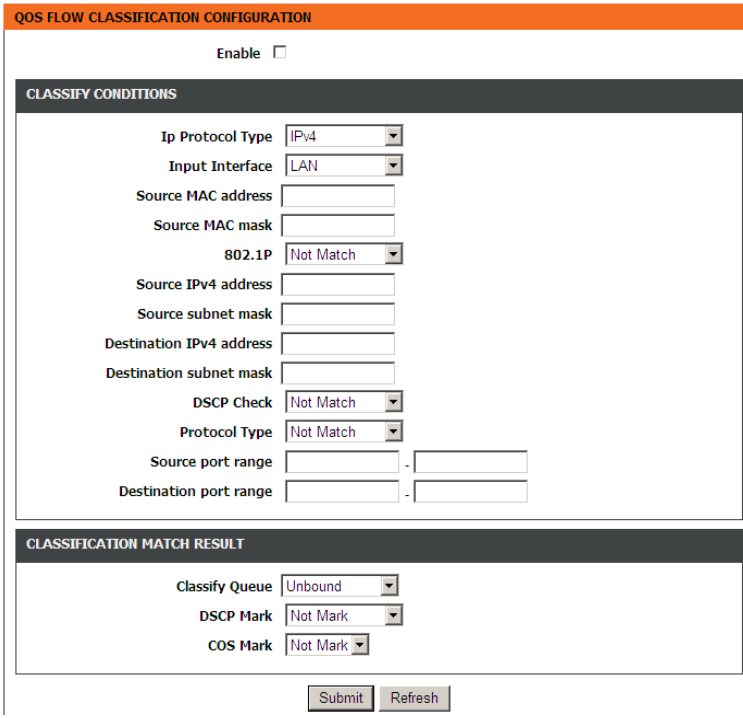
After modifying a queue, click **Submit** to enable the modification. Click **Refresh** to refresh the queue.

3.3.8.3 QoS Classification

In the **QoS Configuration** page, click **QoS Classification**. The page shown in the following figure appears.You can configure QoS queue rule.



Click **Add Classification Rule**. The page shown in the following figure appears.



The following table describes the parameters of this page.

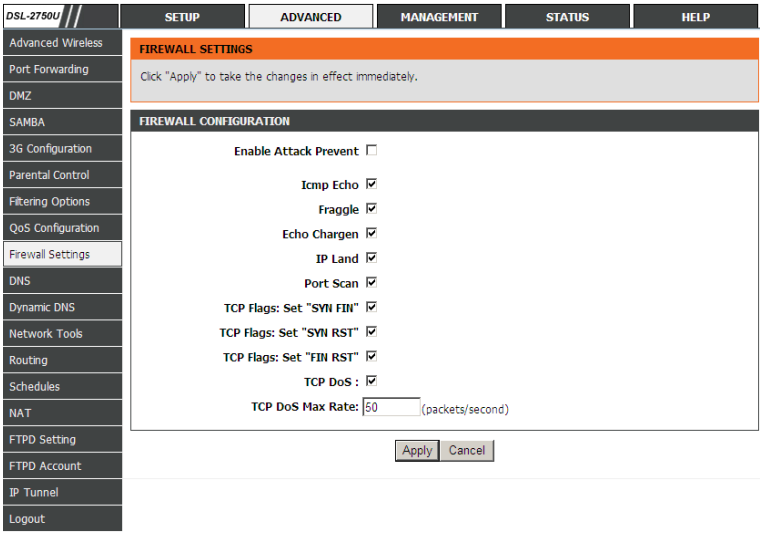
Field	Description
Enable	Tick in the box to enable this QoS rule.
Ip Protocol Type	Select the protocol type as **IPv4** or **IPv6**.
Input Interface	Based on the Classify Type, choose a WAN/LAN interface.
802.1P	Choose a matched 802.1P VLAN priority.
DSCP Check	Choose a matched DSCP type.
Protocol Type	Choose a protocol type matching with the QoS rule.
Classify Queue	Choose a QoS queue for the rule.
DSCP Mark	Set a DSCP Mark for this QoS rule.

Field	Description
COS Mark	Set a COS Mark for this QoS rule.

You may click **Edit** to modify the existing classification rule.

3.3.9 Firewall Settings

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.
Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.
Choose **ADVANCED** > **Firewall Settings**. The page shown in the following figure appears.



Click **Apply** to save the settings.

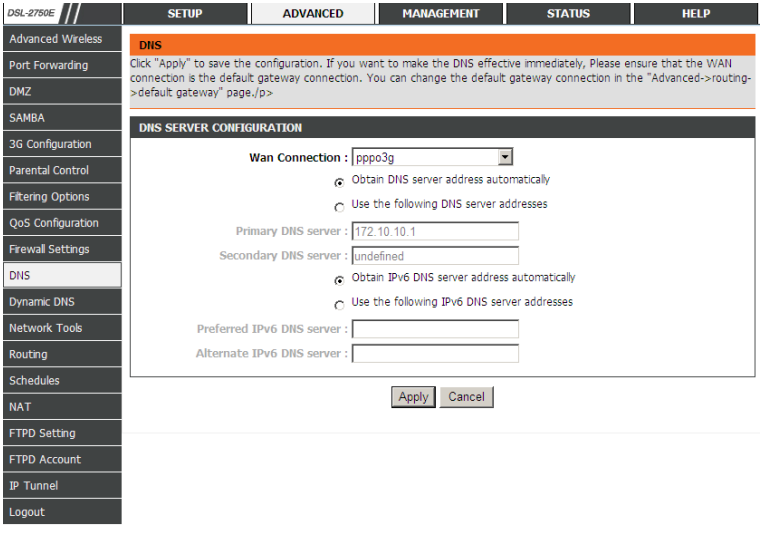
3.3.10 DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to

remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **ADVANCED** > **DNS**. The page shown in the folllowin g figure appears.



If you are using the device for DHCP service on the LAN or using DNS servers on the ISP network, select **Obtain DNS server address automatically**.

If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the preferred DNS server and the alternate DNS server.

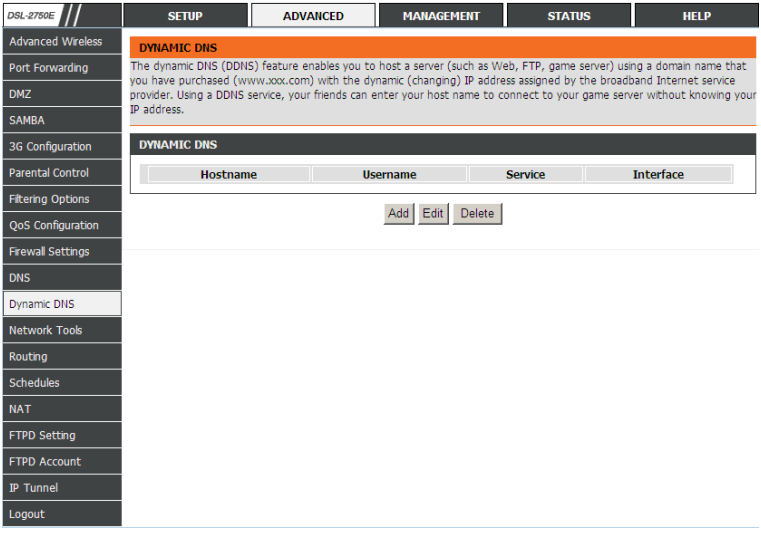
Click **Apply** to save the settings.

3.3.11 Dynamic DNS

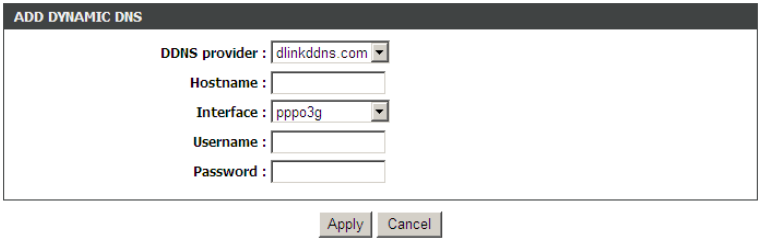
The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host

name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of hostname.dyndns.org and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers (DyndDNS.org or dlinkddns.com).

Choose **ADVANCED** > **Dynamic DNS**. The page shown in the following page appears.



Click **Add** to add dynamic DNS. The page shown in the following figure appears.



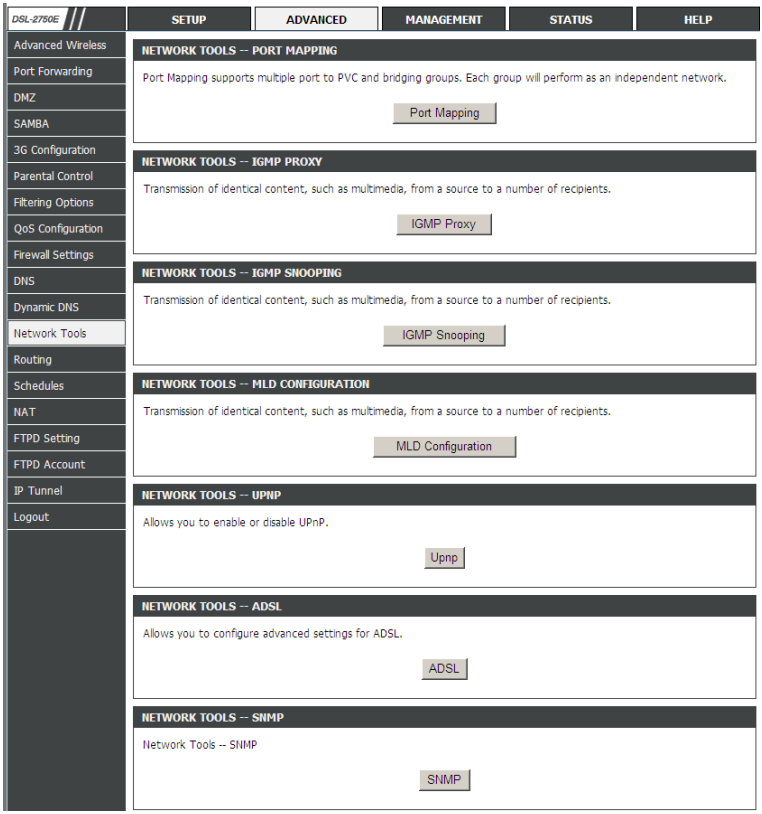
The following table describes the parameters of this page.

Field	Description
DDNS provider	Select one of the DDNS registration organizations from the down-list drop. Available servers include DynDns.org and dlinkddns.com.
Host Name	Enter the host name that you registered with your DDNS service provider.
Username	Enter the user name for your DDNS account.
Password	Enter the password for your DDNS account.

Click **Apply** to save the settings.

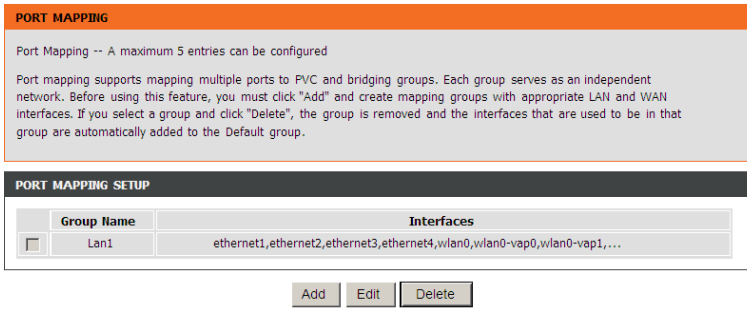
3.3.12 Network Tools

Choose **ADVANCED** > **Network Tools**. The page shown in the following figure appears.

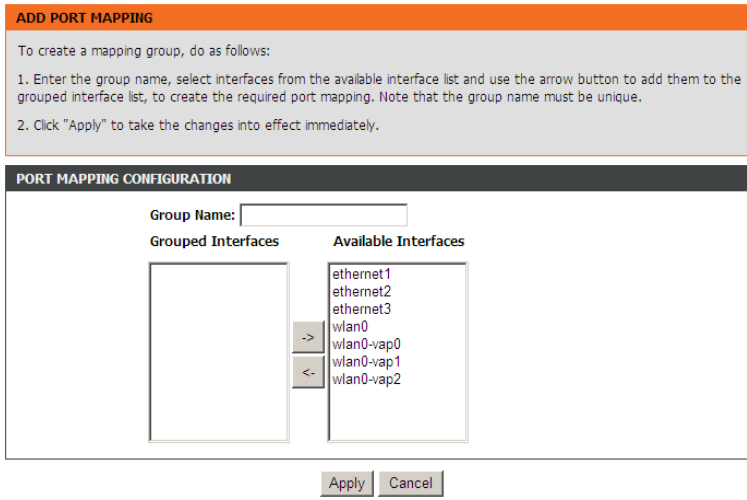


3.3.12.1 Port Mapping

Choose **ADVANCED** > **Network Tools** and click **Port Mapping**. The page shown in the following figure appears. In this page, you can bind the WAN interface and the LAN interface to the same group.



Click **Add** to add port mapping. The page shown in the following figure appears.



The procedure for creating a mapping group is as follows:

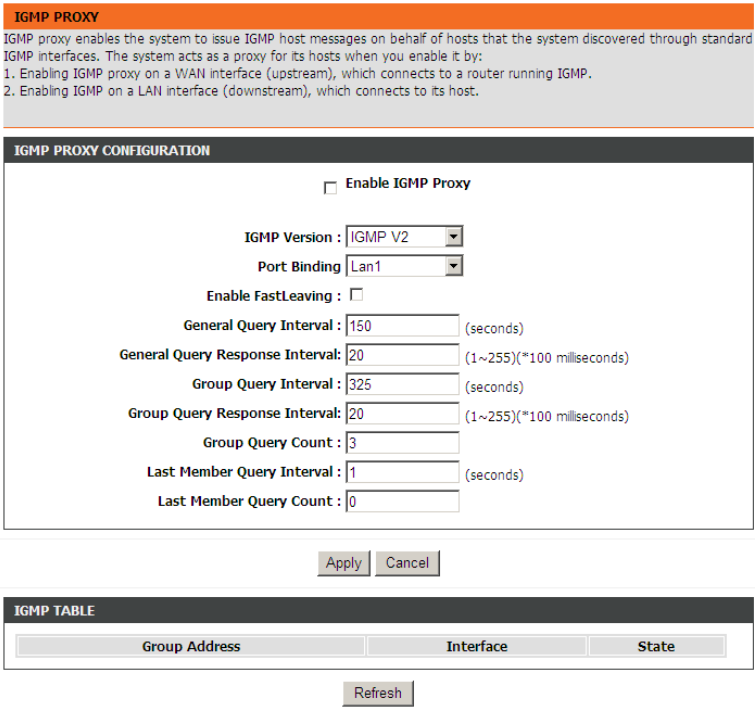
Step 1 Enter the group name.

Step 2 Select interfaces from the **Available Interface** list and click the **<-** arrow button to add them to the grouped interface list, in order to create the required mapping of the ports. The group name must be unique.

Step 3 Click **Apply** to save the settings.

3.3.12.2 IGMP Proxy

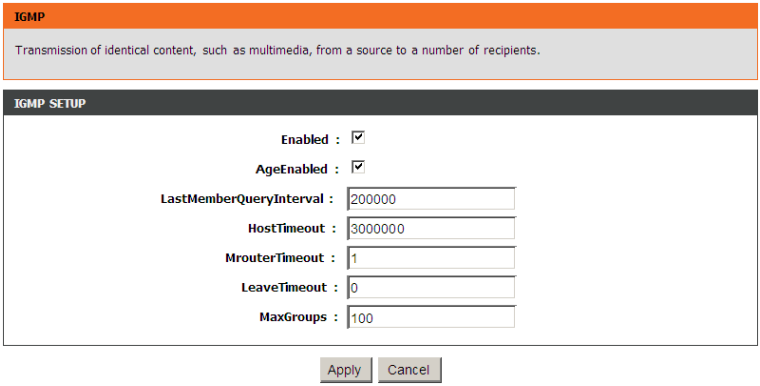
Choose **ADVANCED** > **Network Tools** and click **IGMP Proxy**. The page shown in the following figure appears.



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 after you enable it.

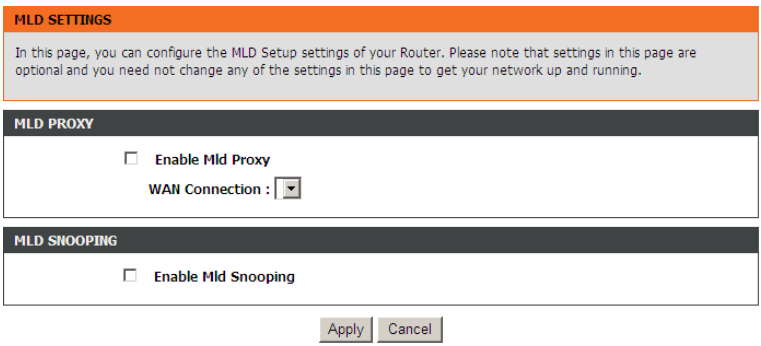
3.3.12.3 IGMP Snooping

When IGMP Snooping is enabled, the multicast data transmits through the specific LAN port which has received the request report.



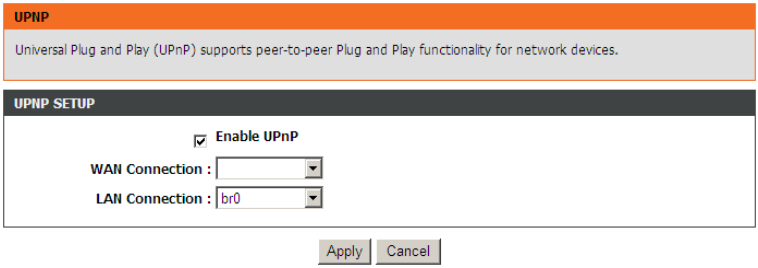
3.3.12.4 MLD Configuration

Choose **ADVANCED** > **Network Tools** and click **MLD Configuration**. The page shown in the following figure appears.



3.3.12.5 UPnP

Choose **ADVANCED** > **Network Tools** and click **UPnP**. The page shown in the following figure appears.



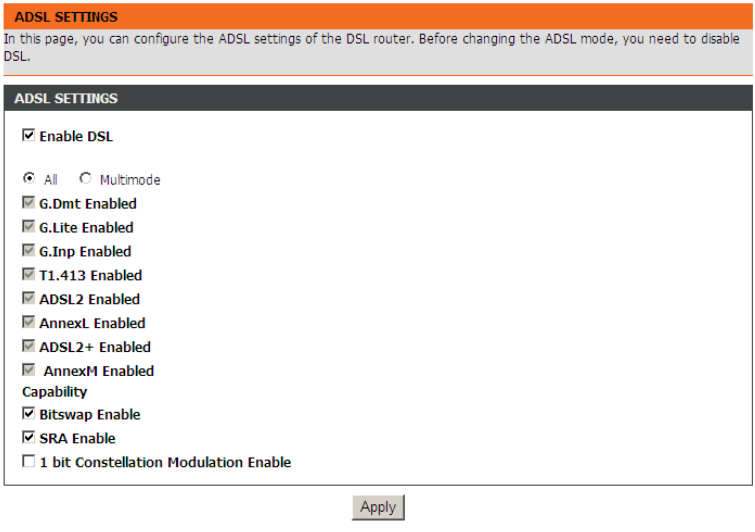
In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Click **Apply** to save the settings.

3.3.12.6 ADSL

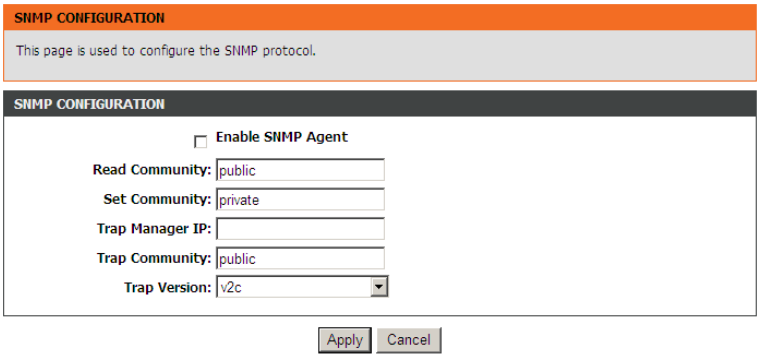
Choose **ADVANCED** > **Network Tools** and click **ADSL**. The page shown in the following figure appears.



In this page, you can select the DSL modulation. Normally, you can remain this factory default setting. The device negotiates the modulation mode with DSLAM. Click **Apply** to save the settings.

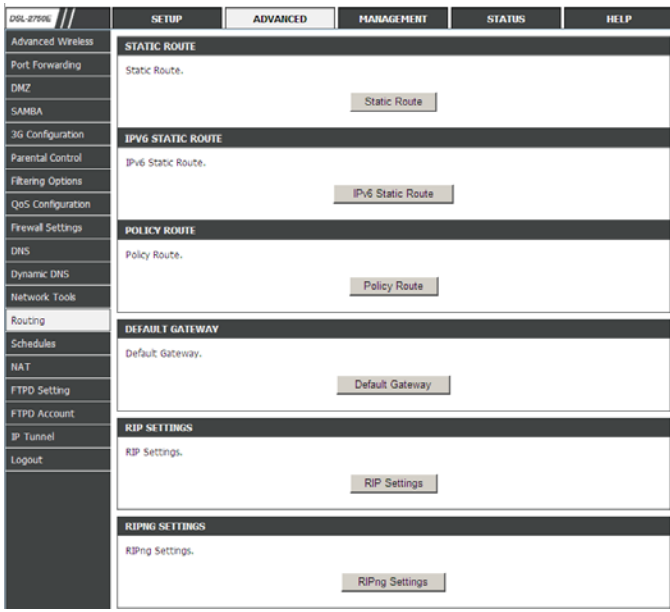
3.3.12.7 SNMP

Choose **ADVANCED** > **Network Tools** and click **SNMP**. The page shown in the following figure appears. In this page, you can set SNMP parameters.



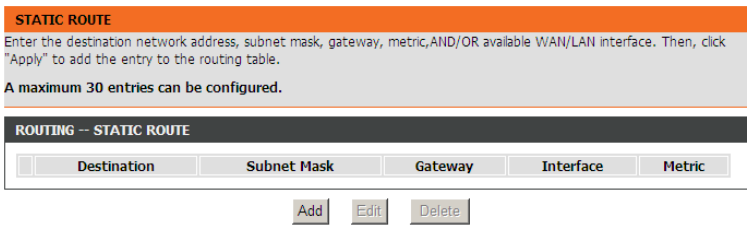
3.3.13 Routing

Choose **ADVANCED** > **Routing**. The page shown in the following page appears.

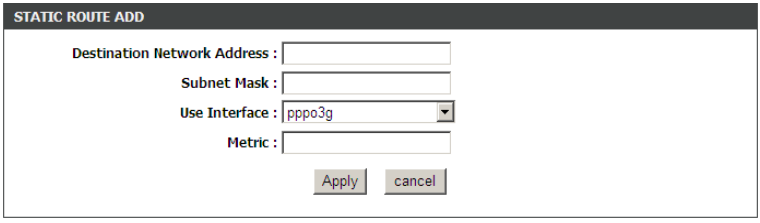


3.3.13.1 Static Route

Choose **ADVANCED** > **Routing** and click **Static Route**. The page shown in the following figure appears. This page is used to configure the routing information. In this page, you can add or delete IP routes.



Click **Add** to add a static route. The page shown in the following figure appears.



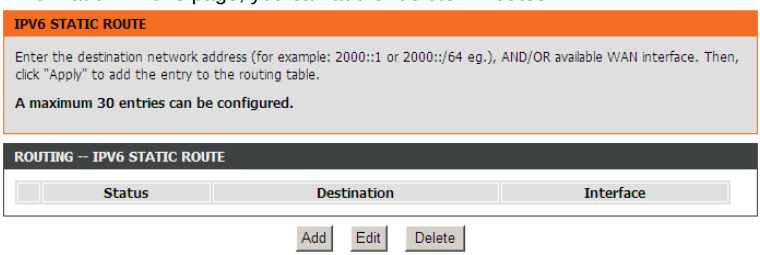
The following table describes the parameters of this page.

Field	Description
Destination Network Address	The destination IP address of the router.
Subnet Mask	The subnet mask of the destination IP
Use Interface	The interface name of the router output port.

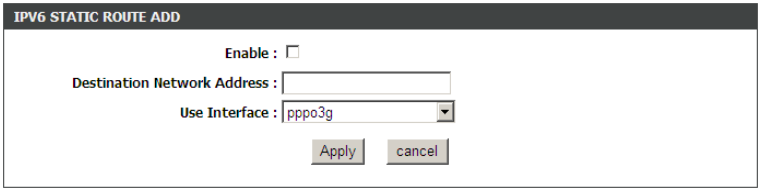
Click **Apply** to save the settings.

3.3.13.2 IPv6 Static Route

Choose **ADVANCED** > **Routing** and click **IPv6 Static Route**. The page shown in the following figure appears. This page is used to configure the routing information. In this page, you can add or delete IP routes.



Click **Add** to add a static route. The page shown in the following figure appears.



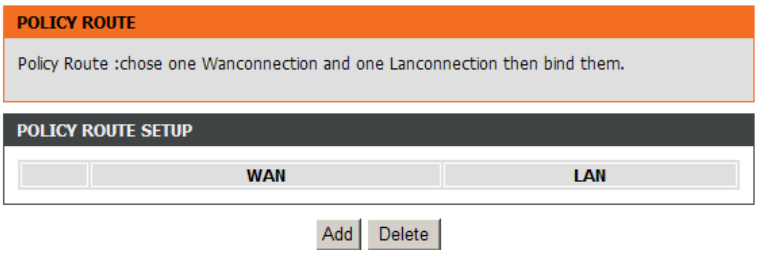
The following table describes the parameters of this page.

Field	Description
Destination Network Address	The destination IPv6 address of the router.
Use Interface	The interface name of the router output port.

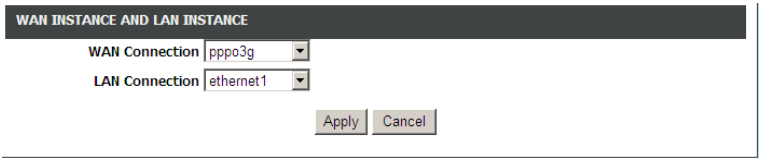
Click **Apply** to save the settings.

3.3.13.3 Policy Route

Choose **ADVANCED** > **Routing** and click **IPv6 Static Route**. The page shown in the following figure appears. The policy route binds one WAN connection and one LAN interface.

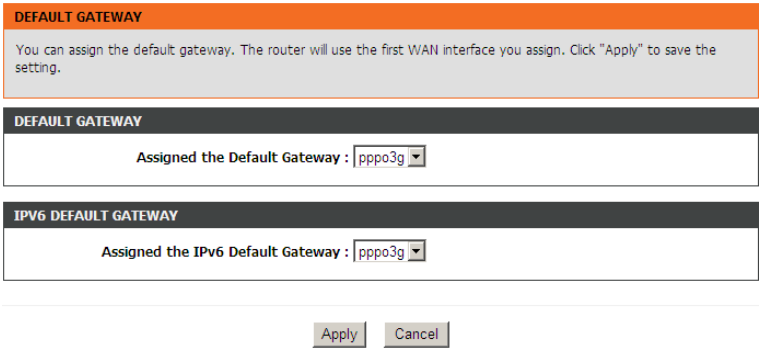


Click **add**, the page shown in the following figure appears.



3.3.13.4 Default Gateway

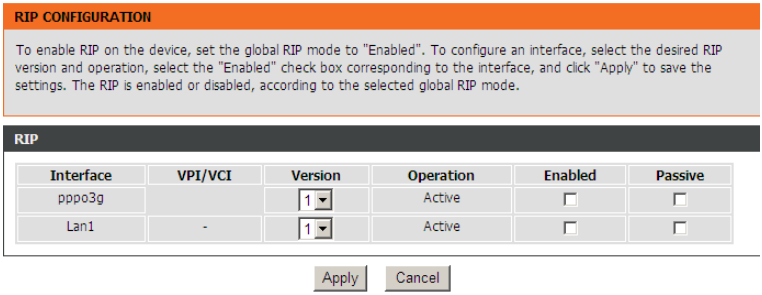
Choose **ADVANCED** > **Routing** and click **Default Gateway**. The page shown in the following figure appears. You may assign a default gateway for the router to use first.



Click **Apply** to save the settings.

3.3.13.5 RIP

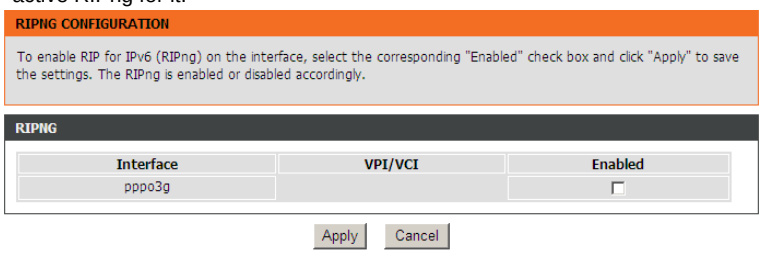
Choose **ADVANCED** > **Routing** and click **RIP Settings**. The page shown in the following figure appears. This page is used to select the interfaces on your device that use RIP and the version of the protocol used.



If you are using this device as a RIP-enabled device to communicate with others using the routing information protocol, enable RIP and click **Apply** to save the settings.

3.3.13.6 RIPng

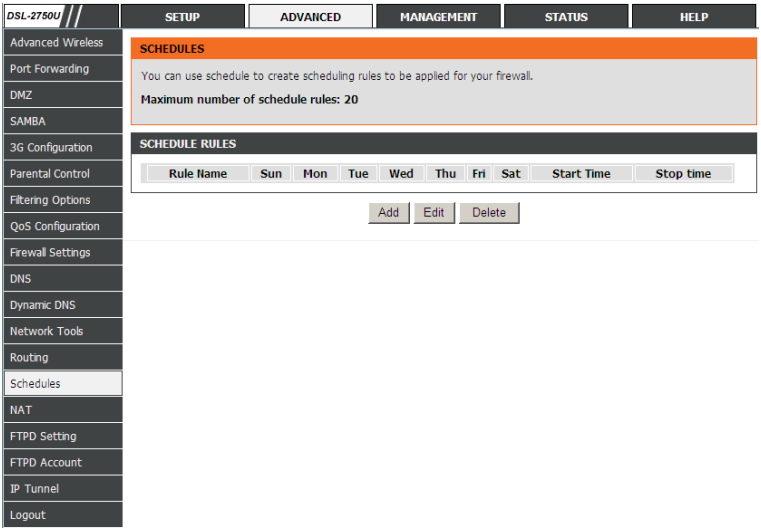
Choose **ADVANCED** > **Routing** and click **RIPng Settings**. The page shown in the following figure appears. In this page, you may choose an interface and active RIPng for it.



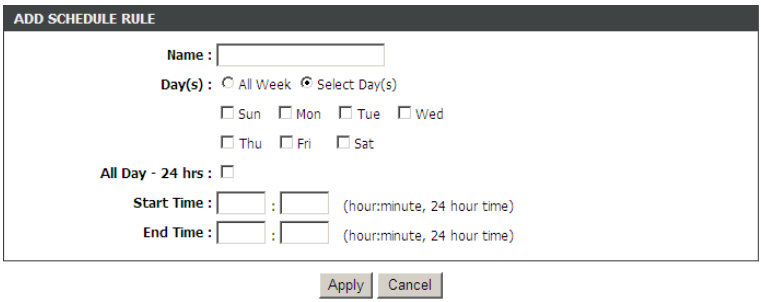
Click **Apply** to save the settings.

3.3.14 Schedules

Choose **ADVANCED** > **Schedules**. The page shown in the following figure appears.



Click **Add** to add schedule rule. The page shown in the following figure appears.

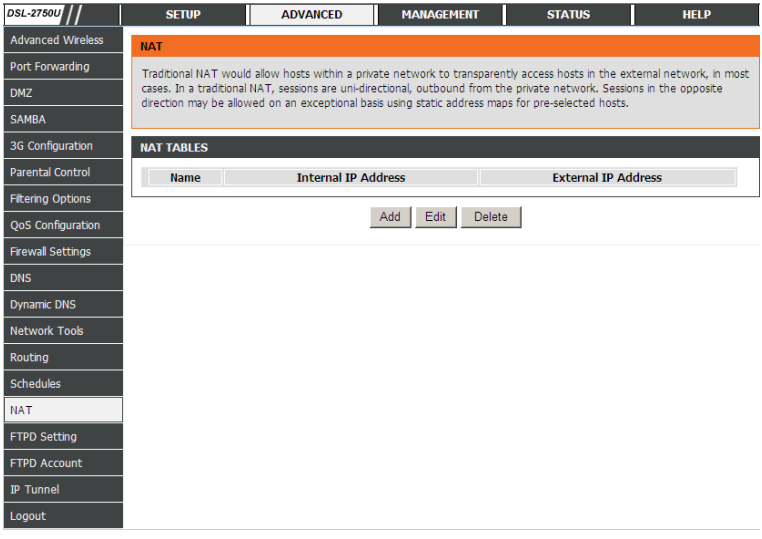


Click **Apply** to save the settings.

3.3.15 NAT

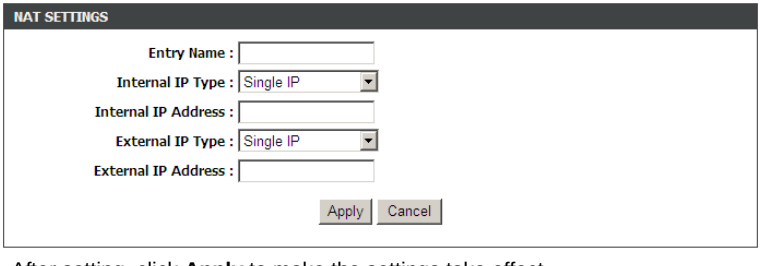
Choose **ADVANCED** > **NAT**. The page shown in the following figure appears. Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT,

sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts.



In this page, you are allowed to add, edit or remove a virtual server entry.

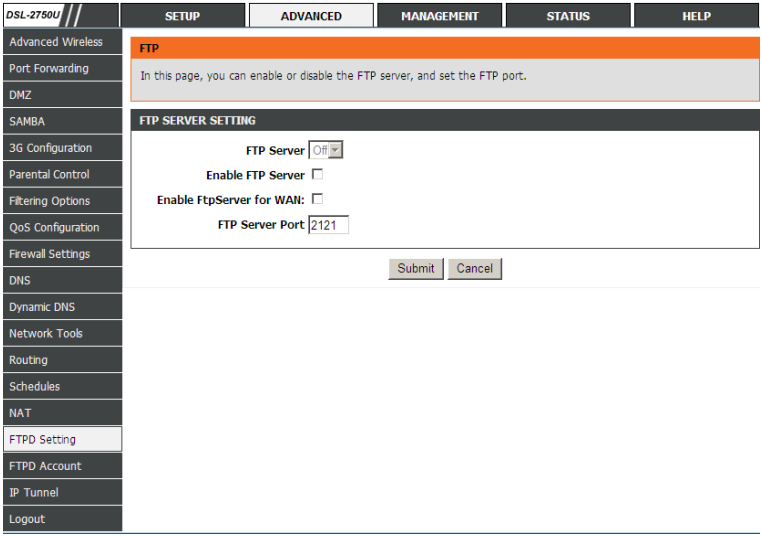
Click **Add** to add an NAT server. The page shown in the following figure appears.



After setting, click **Apply** to make the settings take effect.

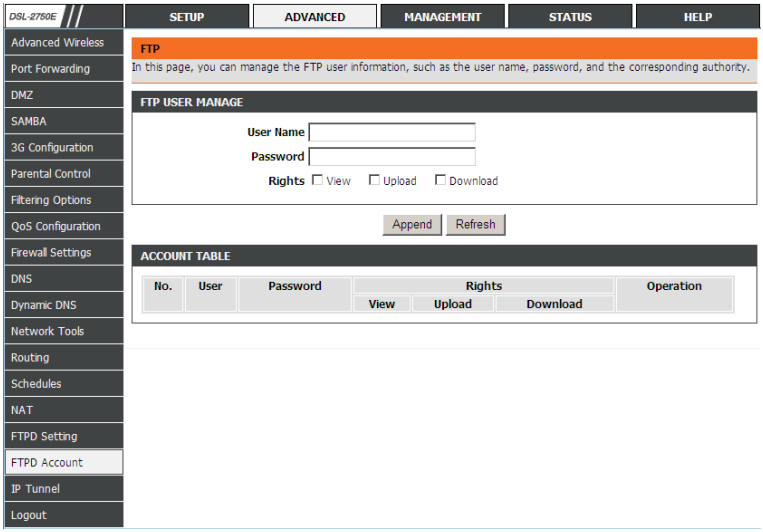
3.3.16 FTPD Setting

Choose **ADVANCED** > **FTPD Setting**. The page shown in the following figure appears. In this page, you can enable or disable the FTP server and set the FTP port.



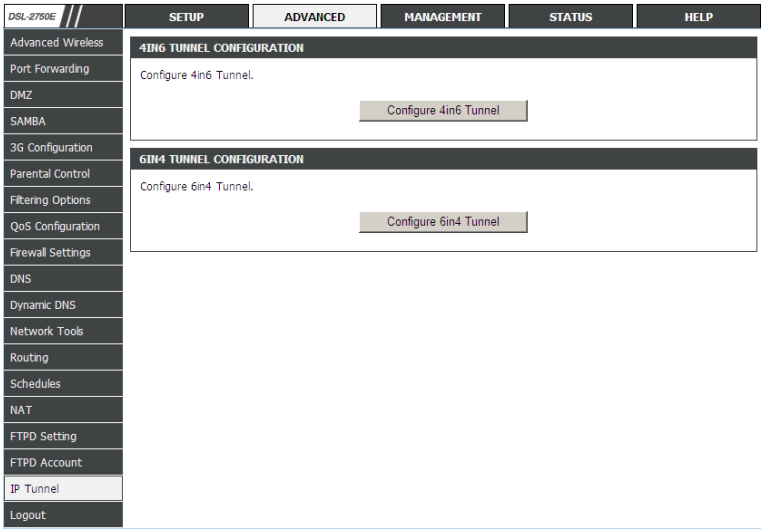
3.3.17 FTPD Account

Choose **ADVANCED** > **FTPD Account**. The page shown in the following figure appears. In this page, you can manage the FTP user information, such as the user name, password, and the corresponding authority.



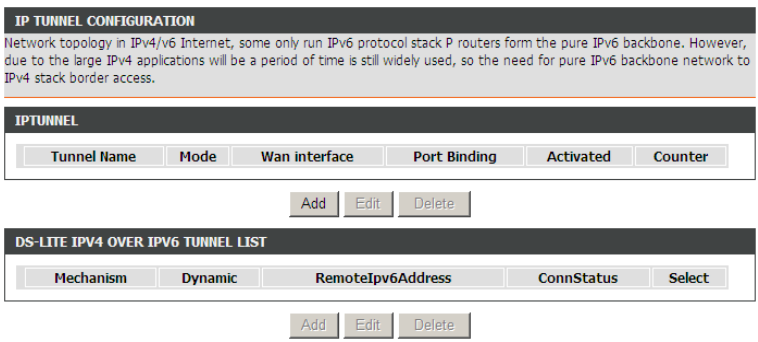
3.3.18 IP Tunnel

Choose **ADVANCED** > **IP Tunnel**. The page shown in the following figure appears.

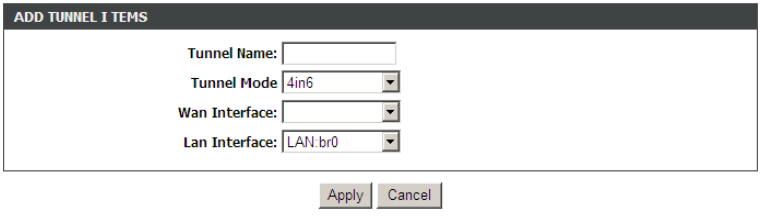


3.3.18.14in6 Tunnel

Choose **ADVANCED** > **IP Tunnel** and then click **4in6 Tunnel**. The page shown in the following figure appears. In this page, you can configure IPv4 penetration through IPv6 network. When only IPv6 access is provided by your ISP, you can access the Internet via IPv4 and IPv6.



Click **Add** below the table **IPTUNNEL** to add tunnel items. The page shown in the following figure appears.

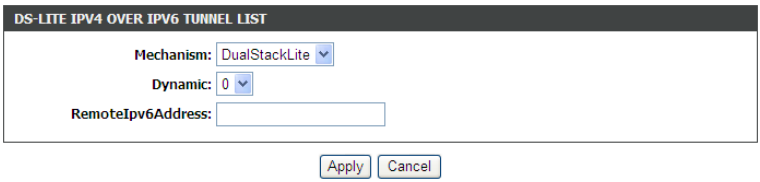


The following table describes the parameters of this page.

Field	Description
Tunnel Name	Set a tunnel name.
Tunnel Mode	Select the tunnel mode as 4 in6 or 6in4.
Wan Interface	Choose a WAN interface used for the tunnel.
Lan Interface	Choose a LAN interface used for the tunnel.

Click **Apply** to enable the settings.

Click **Add** below the table **DS-Lite IPv4 over IPv6 Tunnel List** to add a DS-Lite item，which is a 4in6 tunnel. The page shown in the following figure appears.



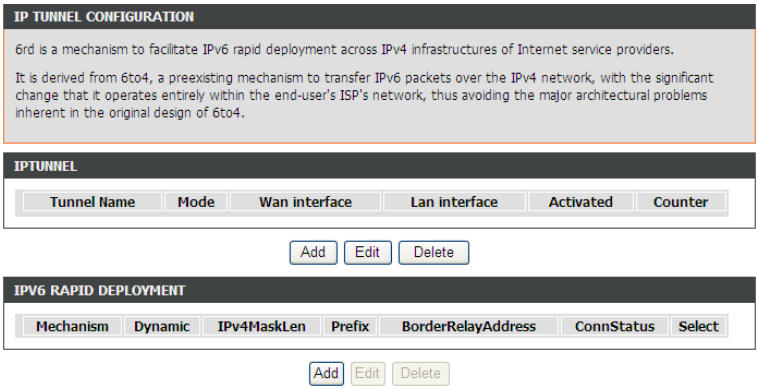
The following table describes the parameters of this page.

Field	Description
Mechanism	The tunnel type is DS-Lite, which is 4in6 tunnel.
Dynamic	Set the obtaining mode of remote IPv6 addresses. You can select **0** or **1**.
RemoteIPv6Address	Set the remote end IPv6 address of the tunnel.

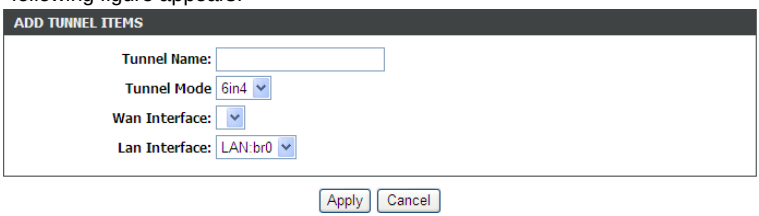
Click **Apply** to enable the settings.

3.3.18.26in4 Tunnel

Choose **ADVANCED** > **IP Tunnel** and then click **6in4 Tunnel**. The page shown in the following figure appears. In this page, you can configure IPv6 penetration through IPv4 network. When only IPv4 access is provided by your ISP, you can access the Internet via IPv4 and IPv6.



Click **Add** below the table **IPTUNNEL** to add tunnel items. The page shown in the following figure appears.



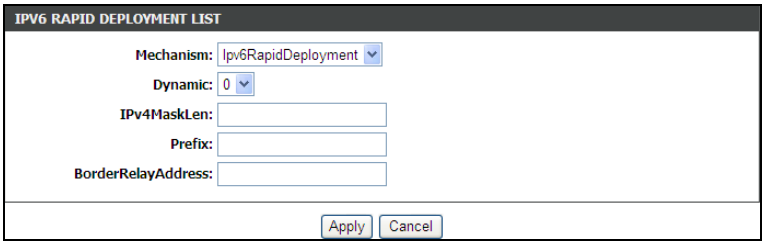
The following table describes the parameters of this page.

Field	Description
Tunnel Name	Set a tunnel name.
Tunnel Mode	Select the tunnel mode as 4 in6 or 6in4.

Wan Interface	Choose a WAN interface used for the tunnel.
Lan Interface	Choose a LAN interface used for the tunnel.

Click **Apply** to enable the settings.

Click **Add** below the table **IPv6 Rapid Deployment** to add a 6RD item, which is a 6in4 tunnel. The page shown in the following figure appears.



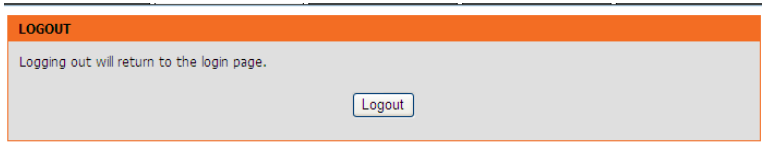
The following table describes the parameters of this page.

Field	Description
Mechanism	The tunnel type is 6RD, which is a 6in4 tunnel.
Dynamic	Set the obtaining mode of Border Relay Address. You may choose **0** or **1**.
IPv4MaskLen	Set the subnet mask digits of the IPv4 address of the local WAN interface.
Prefix	Set the IPv6 prefix of the 6RD tunnel.
BorderRelayAddress	Set the Border Relay IPv4 address at the remote end.

Click **Apply** to enable the settings.

3.3.19 Logout

Choose **ADVANCED** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.

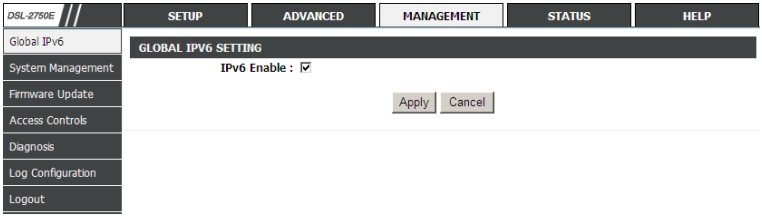


3.4 Management

In the main interface, click **Management** tab to enter the Management menu as shown in the following figure. The submenus are **Global IPv6**, **System Management**, **Firmware Update**, **Access Controls**, **Diagnosis**, **Log Configuration** and **Logout**.

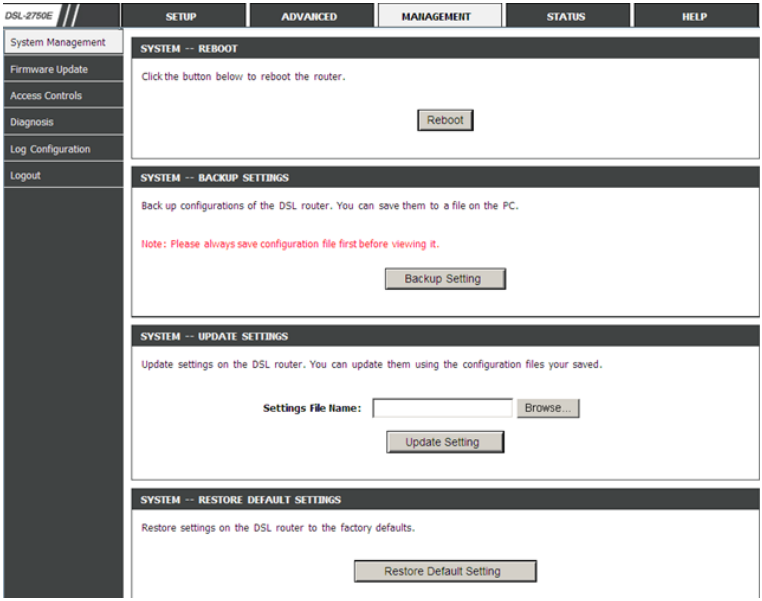
3.4.1 Global IPv6

Choose **MANAGEMENT** > **Global IPv6**. The page shown in the following figure appears. In this page you can enable or disable IPv6 function.



3.4.2 System Management

Choose **MANAGEMENT** > **System Management**. The page shown in the following figure appears.



In this page, you can reboot device, back up the current settings to a file, update settings from the file saved previously and restore the factory defaults.
The buttons in this page are described as follows.

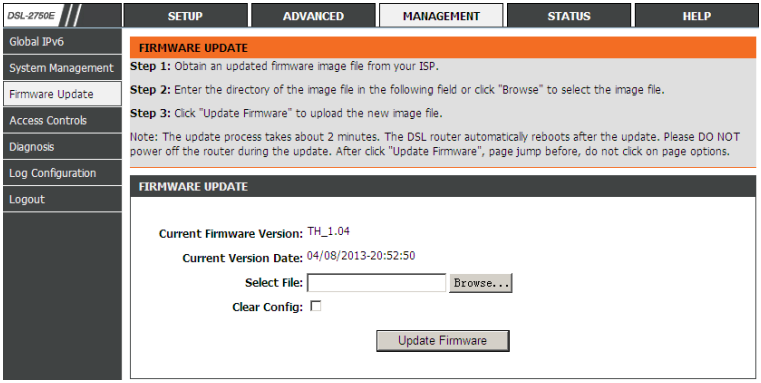
Field	Description
Reboot	Click this button to reboot the device.
Backup Setting	Click this button to save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.
Update setting	Click **Browse** to select the configuration file of device and then click **Update Settings** to begin updating the device configuration.
Restore Default Setting	Click this button to reset the device to default settings.

Note:

Do not turn off your device or press the Reset button while an operation in this page is in progress.

3.4.3 Firmware Update

Choose **MANAGEMENT** > **Firmware Update**. The page shown in the following figure appears. In this page, you can upgrade the firmware of the device.



To update the firmware, take the following steps.

Step 1 Click **Browse…**to find the file.

Step 2 Select **Click Config**.

Step 3 Click **Update Firmware** to copy the file.

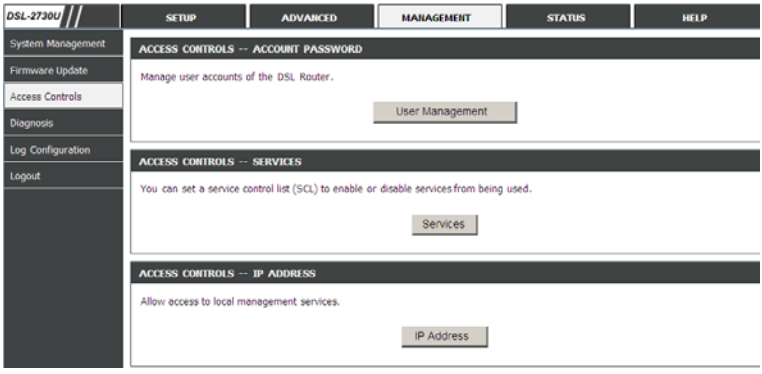
The device loads the file and reboots automatically.

Note:

Do not turn off your device or press the Reset button while an operation in this page is in progress.

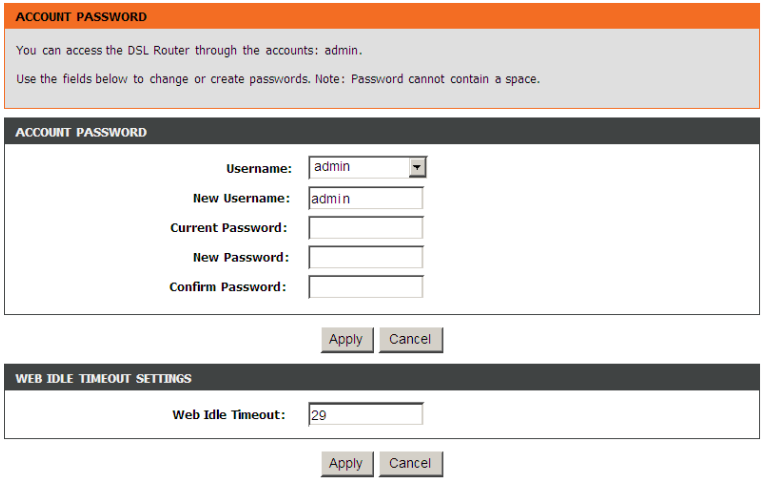
3.4.4 Access Controls

Choose **MANAGEMENT** > **Access Controls**. The **Access Controls** page shown in the following figure appears. The page contains **User Management**, **Services** and **IP Address**.



3.4.4.1 User Management

In the **Access Controls** page, click **User Management**. The page shown in the following figure appears. In this page, you can change the password of the user and set time for automatic logout.

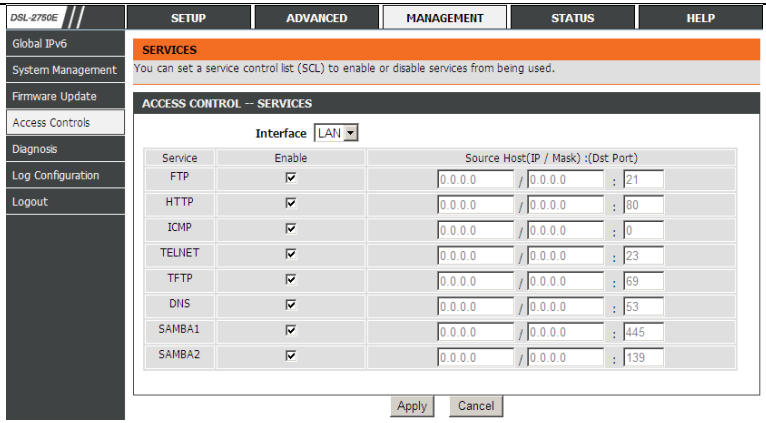


You should change the default password to secure your network. Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you need to reset the device to the factory default settings and all configuration settings of the device are lost.

Enter the current and new passwords and confirm the new password to change the password. Click **Apply** to apply the settings.

3.4.4.2 Services

In the **Access Controls** page, click **Services**. The page shown in the following figure appears.



In this page, you can enable or disable the services that are used by the remote host. For example, if telnet service is enabled and port is 23, the remote host can access the device by telnet through port 23. Normally, you need not change the settings.

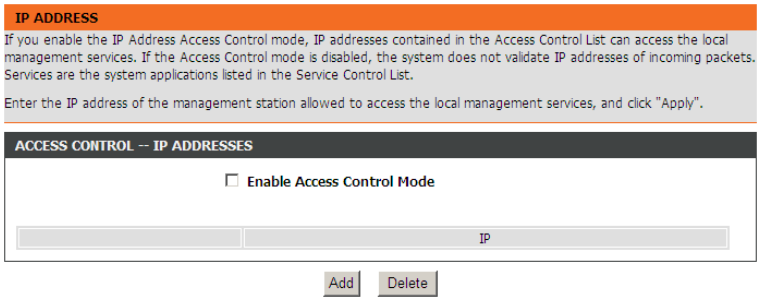
Select the management services that you want to enable or disable on the LAN or WAN interface. Click **Apply** to apply the settings.

Note:

If you disable HTTP service, you cannot access the configuration page of the device any more.

3.4.4.3 IP Address

In the **Access Controls** page, click **IP Address**. The page shown in the following figure appears.

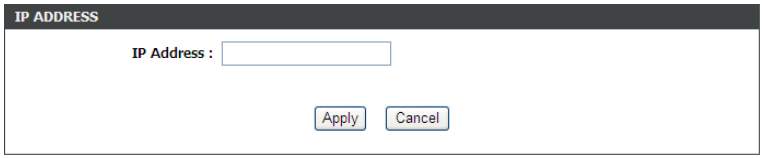


In this page, you can configure the IP address for access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device. Tick **Enable Access Control Mode** to enable ACL.

Note:

If you enable the ACL, ensure that IP address of the host is in the ACL list.

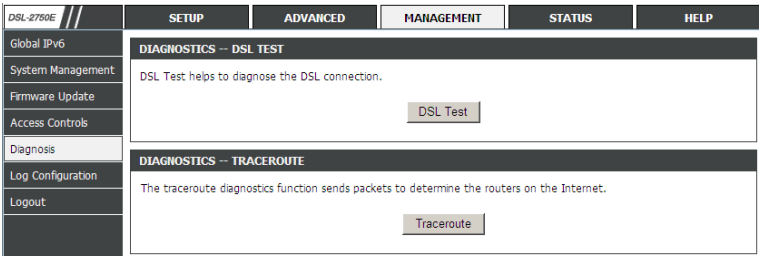
To add an IP address to the IP list, cick **Add**. The page shown in the following figure appears.



Click **Apply** to apply the settings.

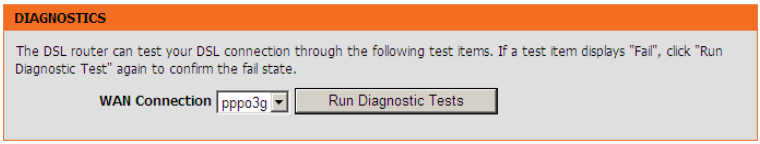
3.4.5 Diagnosis

Choose **MANAGEMENT**> **Diagnosis**. The **Diagnosis** page shown in the following figure appears. The page contains **DSL Test** and **Traceroute**.

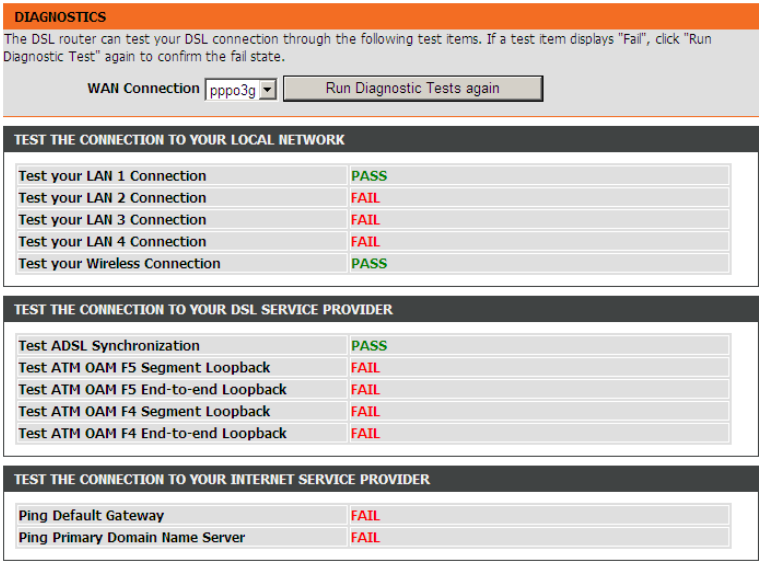


3.4.5.1 DSL Test

In the **Diagnosis** page, click **DSL Test**. The page shown in the following figure appears. In this page, you can test your DSL connection.

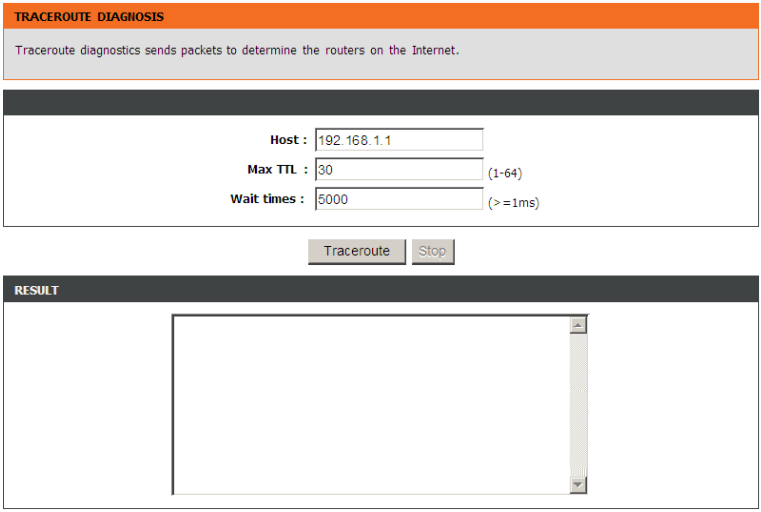


Click **Run Diagnostic Tests**. After testing, the following figure appears.

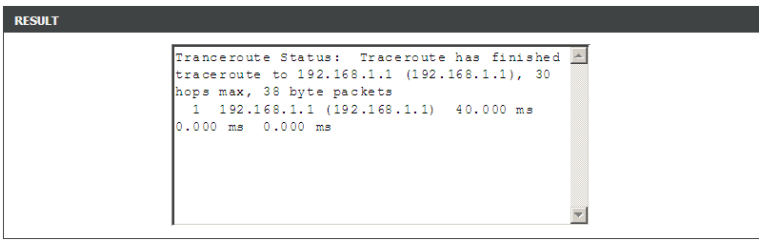


3.4.5.2 Traceroute

In the **Diagnosis** page, click **Traceroute**. The page shown in the following figure appears. In this page, you can determine the routers on the Internet by sending packets.

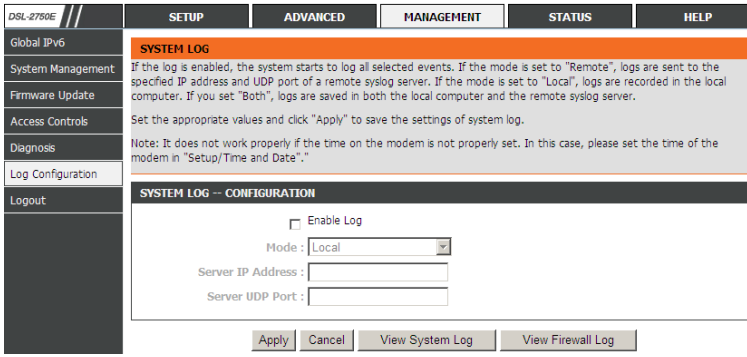


Click **Traceroute** to begin diagnosis. After finish, the page shown in the following figure appears.



3.4.6 Log Configuration

Choose **MANAGEMENT** > **Log Configuration**. The **System Log** page shown in the following figure appears.



This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. Available event severity levels are as follows: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. In this page, you can enable or disable the system log function.

To log the events, take the following steps.

Step 1 Select **Enable Log** check box.

Step 2 Select the display mode from the **Mode** drop-down list.

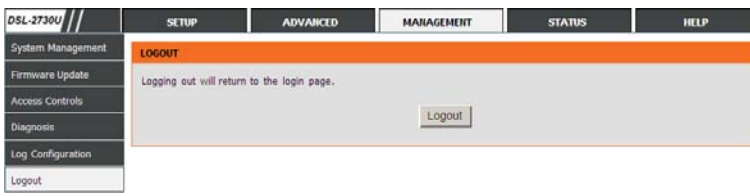
Step 3 Enter the **Server IP Address** and **Server UDP Port** if the **Mode** is set to **Both** or **Remote**.

Step 4 Click **Apply** to apply the settings.

Step 5 Click **View System Log** to view the detail information of system log.

3.4.7 Logout

Choose **MANAGEMENT** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.

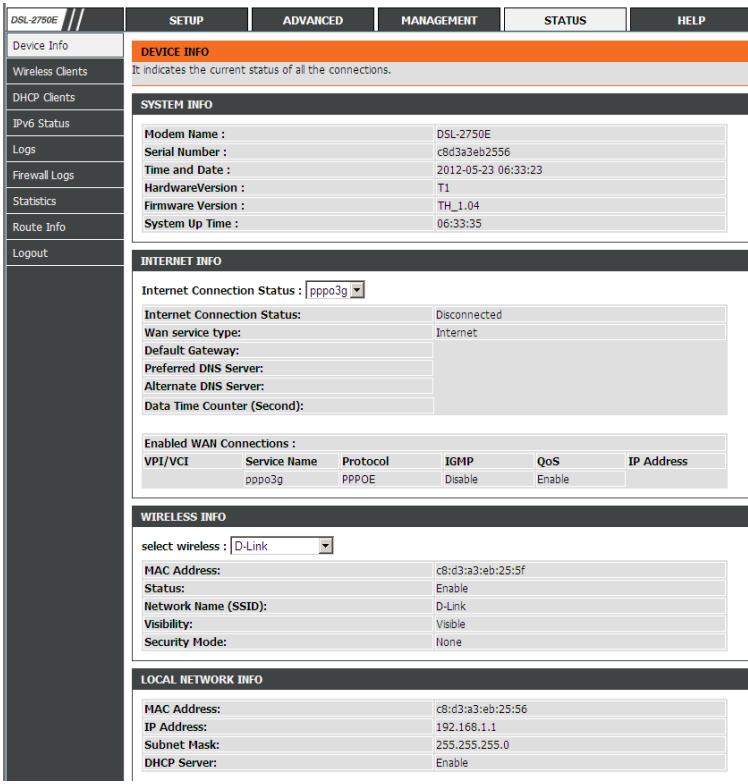


3.5 Status

In the main interface, click **Status** tab to enter the **Status** menu. The submenus are **Device Info**, **Wireless Clients**, **DHCP clients**, **Logs**, **Firewall logs**, **Statistics**, **Route Info** and **Logout**. You can view the system information and monitor performance.

3.5.1 Device Info

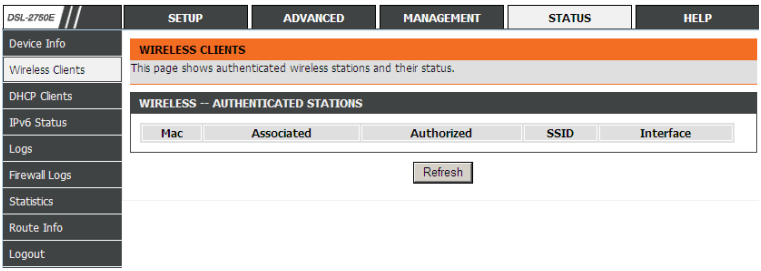
Choose **STATUS** > **Device Info**. The page shown in the following figure appears.



The page displays the summary of the device status. It includes the information of firmware version, upstream rate, downstream rate, uptime and Internet configuration (both wireless and Ethernet statuses).

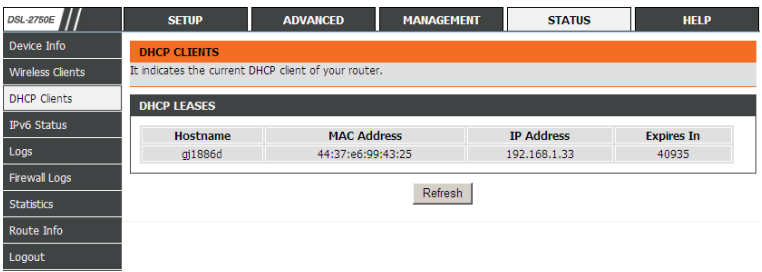
3.5.2 Wireless Clients

Choose **STATUS** > **Wireless Clients**. The page shown in the following page appears. The page displays authenticated wireless stations and their statuses.



3.5.3 DHCP Clients

Choose **STATUS** > **DHCP Clients**. The page shown in the following page appears. This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address and time expired(s).

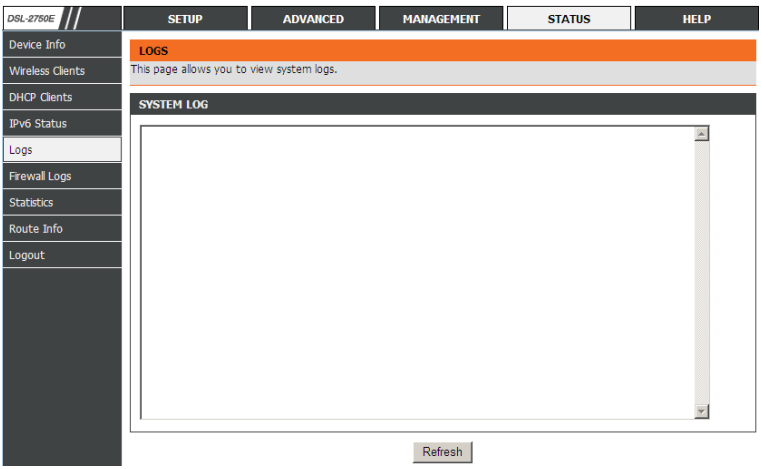


3.5.4 IPv6 Status

Choose **STATUS** > **IPv6 Status**. The page shown in the following page appears. This page displays the IPv6 Connection information.

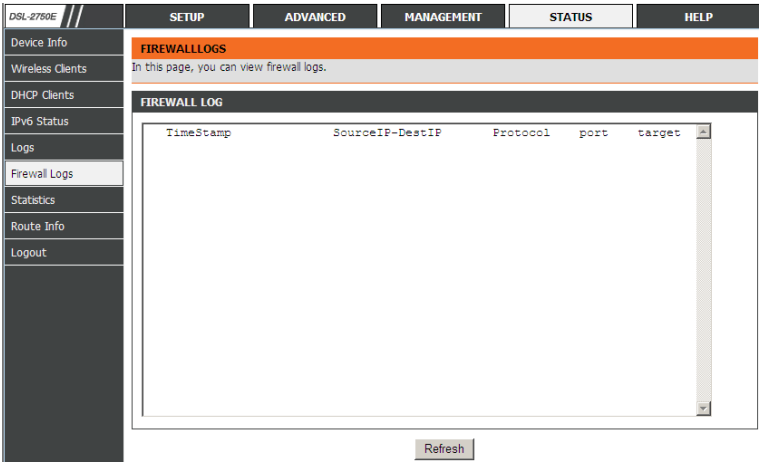
3.5.5 Logs

Choose **STATUS** > **Logs**. The page shown in the following figure appears. This page lists the system log. Click **Refresh** to refresh the system log shown in the table.



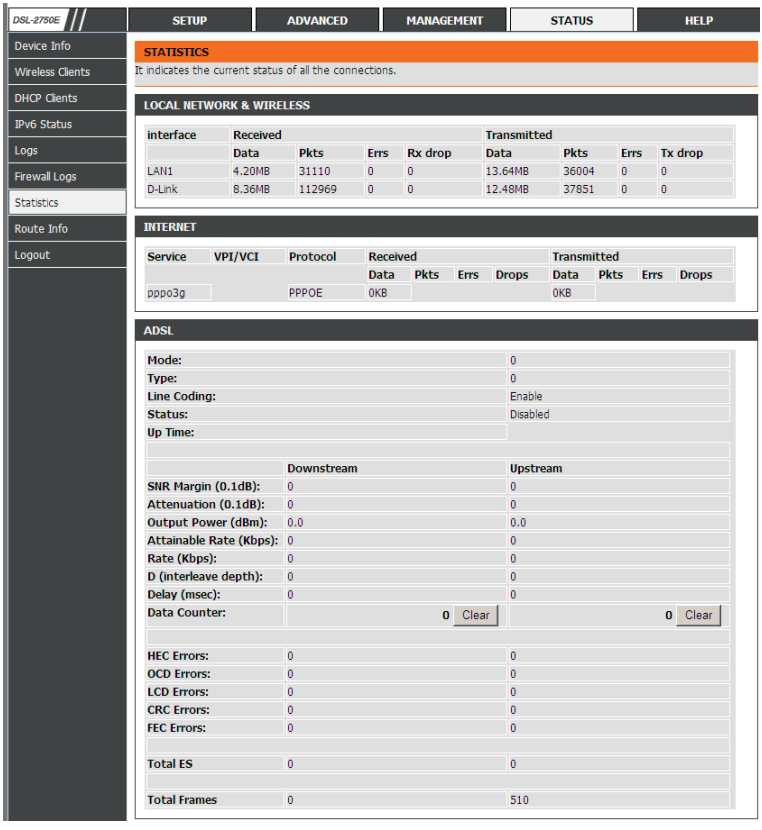
3.5.6 Firewall Logs

Choose **STATUS** > **Firewall Logs**. The page shown in the following figure appears. You can view firewall logs in this page. Click **Refresh** to refresh the system log shown in the table.



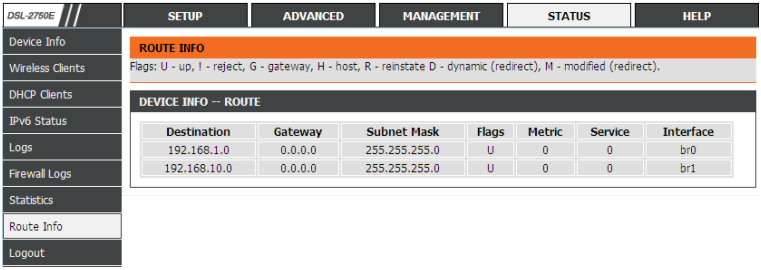
3.5.7 Statistics

Choose **STATUS** > **Statistics**. The page shown in the following figure appears. This page displays the statistics of the network and data transfer. This information helps technicians to identify if the device is functioning properly. The information does not affect the function of the device.



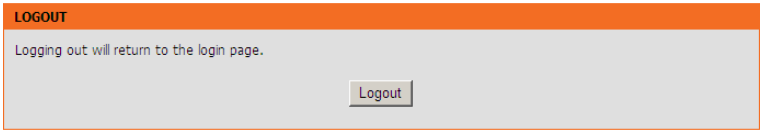
3.5.8 Route Info

Choose **STATUS** > **Route Info**. The page shown in the following figure appears. The table shows a list of destination routes commonly accessed by the network.



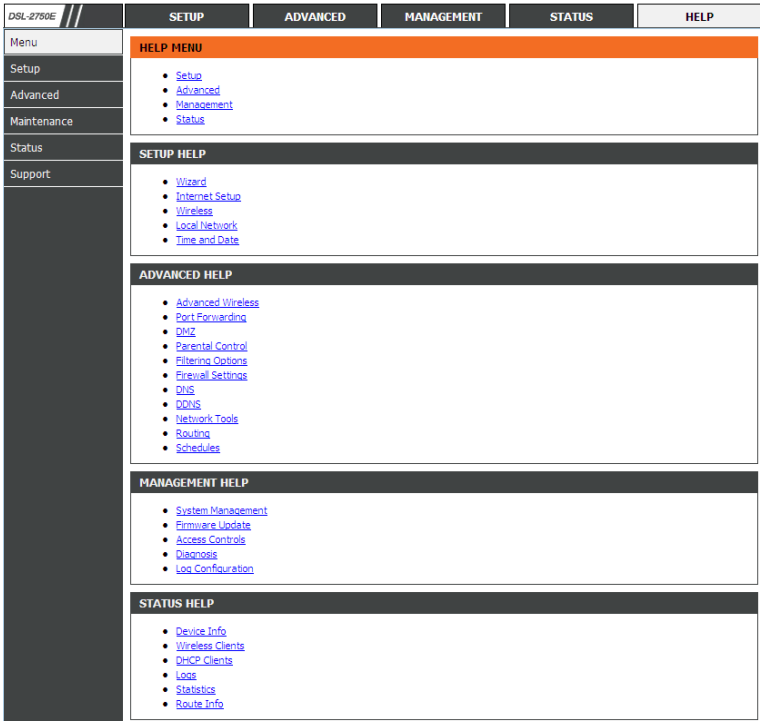
3.5.9 Logout

Choose **STATUS** > **Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



3.6 Help

In the main interface, click **Help** tab to enter the **Help** menu as shown in the following figure. This section provides detailed configuration information for the device. Click a wanted link to view corresponding information.


DSL-2750E
SETUP
ADVANCED
MANAGEMENT
STATUS
HELP
Menu
Setup
Advanced
Maintenance
Status
Support
HELP MENU
Setup
Advanced
Management
Status
SETUP HELP
Wizard
Internet Setup
Wireless
Local Network
Time and Date
ADVANCED HELP
Advanced Wireless
Port Forwarding
DMZ
Parental Control
Filtering Options
Firewall Settings
DNS
DDNS
Network Tools
Routing
Schedules
MANAGEMENT HELP
System Management
Firmware Update
Access Controls
Diagnosis
Log Configuration
STATUS HELP
Device Info
Wireless Clients
DHCP Clients
Logs
Statistics
Route Info