

D-Link **DSL-2750E**

Wireless N 300 ADSL2+ Modem Router

User Manual



D-Link[®]
Building Networks for People



RECYCLABLE

2013/05/29

Ver. 1.00

Contents

1	Introduction	1
1.1	Packing List	1
1.2	Safety Precautions	1
1.3	LEDs and Interfaces	2
1.4	System Requirements	4
1.5	Features	4
2	Hardware Installation	6
2.1	DSL Uplink Connection	6
3	Web Configuration	7
3.1	Accessing the Device	7
3.2	Setup	7
3.2.1	Wizard.....	7
3.2.2	Internet Setup	13
3.2.3	Wireless	19
3.2.4	Local Network	25
3.2.5	LAN IPv6.....	28
3.2.6	Time and Date	29
3.2.7	Logout.....	30
3.3	Advanced.....	30
3.3.1	Advanced Wireless	30
3.3.2	Port Forwarding	37
3.3.3	DMZ.....	39
3.3.4	SAMBA	40
3.3.5	3G Configuration.....	40
3.3.6	Parental Control.....	49
3.3.7	Filtering Options.....	52
3.3.8	QoS Configuration	58
3.3.9	Firewall Settings	62
3.3.10	DNS.....	62
3.3.11	Dynamic DNS.....	63
3.3.12	Network Tools.....	65
3.3.13	Routing	72
3.3.14	Schedules.....	76
3.3.15	NAT	77
3.3.16	FTPD Setting.....	79

3.3.17	FTPD Account	79
3.3.18	IP Tunnel	80
3.3.19	Logout	84
3.4	Management.....	85
3.4.1	Global IPv6	85
3.4.2	System Management.....	85
3.4.3	Firmware Update	87
3.4.4	Access Controls.....	88
3.4.5	Diagnosis	91
3.4.6	Log Configuration	94
3.4.7	Logout.....	95
3.5	Status	96
3.5.1	Device Info	96
3.5.2	Wireless Clients	97
3.5.3	DHCP Clients.....	97
3.5.4	IPv6 Status	97
3.5.5	Logs	98
3.5.6	Firewall Logs.....	99
3.5.7	Statistics	99
3.5.8	Route Info	100
3.5.9	Logout.....	101
3.6	Help	101

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.

It complies with specifications of IEEE 802.11, 802.11b/g/n, WEP, WPA, and WPA2 security. The WLAN of the device supports 2T2R.

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 label-marked power.
- Use the power adapter in the package.
- An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid overheating. The holes on the device are designed for heat dissipation to ensure running normally. Do not cover these heat dissipation holes.

- Do not put this device close to a heat source or high temperature place. Avoid the device direct exposing sunshine.
- Do not put this device close to over damp place. Do not spill any fluid on this device.
- Do not connect this device to PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any 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.
		Blinking	The firmware is upgrading.
LAN 1/2/3/4	Green	Off	No LAN link.
		Blinking	Data is being transmitted through the LAN interface.
		On	The connection of LAN interface is normal.

LED	Color	Status	Description
 WLAN	Green	Blinking	Data is transmitted through the WLAN interface.
		On	The connection of WLAN interface is normal.
		Off	The WLAN connection is not established.
 WPS	Green	Blinking	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.
		Blinking	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.
		Blinking	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

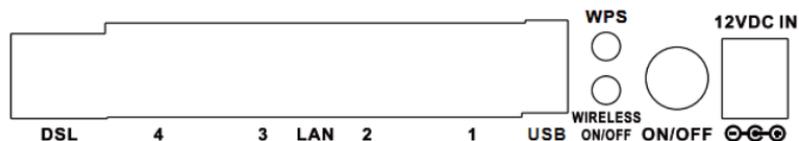


Figure 2 Rear panel

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 to enable WLAN function.
ON/OFF	Power on or off the device.
12V DC IN	Interface that connects to the power adapter.
Reset (on the bottom case)	Reset to the factory defaults. Keep the device powered on, push a paper clip into the hole, press and hold the button for 10 seconds, and then the system restores the default settings.

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

- 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 NAT
- 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.

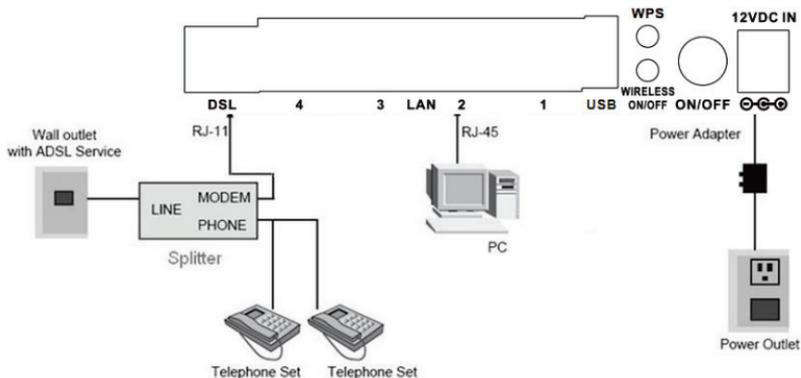


Figure 3 Connection diagram

3 Web Configuration

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

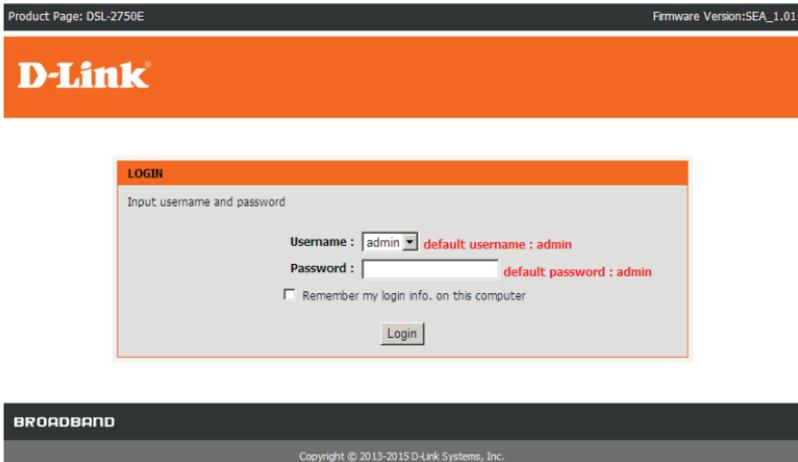
3.1 Accessing the Device

The following is the detailed description of accessing 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.

Product Page: DSL-2750E Firmware Version:SEA_1.01

D-Link

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	SETTING UP YOUR INTERNET				
Internet Setup	You can set up the Internet connection through either of the two ways: Web-based InternetConnection Setup Wizard; Manual setup				
Wireless	For manual setup, you need to have the connection settings provided by your ISP.				
Local Network	INTERNET CONNECTION WIZARD				
LAN IPv6	This wizard assists you to quickly connect the new router to the Internet, through step-by-step instructions. Click the button below to begin.				
Time and Date	<input type="button" value="Setup Wizard"/>				
Logout	Note: Before launching the wizard, please ensure that you have correctly followed the steps outlined in the Quick Installation Guide corresponds to the router.				

BROADBAND

Copyright © 2013-2015 D-Link Systems, Inc.

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

WELCOME TO SETUP WIZARD

This wizard guides you to configure your new router and connect to the Internet step by step.

- **Step 1** : Set Time and Date
- **Step 2** : Setup Internet Connection
- **Step 3** : Configure Wireless Network
- **Step 4** : Set password
- **Step 5** : Completed and Quit

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

Step 1 Set the time and date.

STEP 1: SET TIME AND DATE → 2 → 3 → 4 → 5

With the time configuration function, you can configure, update, and maintain the correct time of the internal system clock. In this page, you can set the time zone that you are in and set the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time if necessary.

TIME SETTING

Automatically synchronize with Internet time server

Primary NTP time server:

Secondary NTP time server:

Manual setup time: 2012 Year 05 Mon 23 Day 04 Hour 11 Min 19 Sec

TIME CONFIGURATION

Time Zone:

Automatically adjust clock for daylight saving changes

Daylight Saving Start: 2000 Year 04 Mon 01 Day 02 Hour 00 Min 00 Sec

Daylight Saving End: 2000 Year 09 Mon 01 Day 02 Hour 00 Min 00 Sec

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.

STEP 2: SETUP INTERNET CONNECTION → 3 → 4 → 5

Please select your ISP (Internet Service Provider) from the list below.

country:

ISP:

Protocol:

Encapsulation Mode:

VPI:

VCI:

Search Available PVC:

We set the parameters of this page based on PPPoE protocol as example.

1. Set the country to be **Singapore**.
2. Choose the ISP you subscribed the internet service from the dropdown list.
3. Set the protocol to be **PPPoE**.
4. Enter the **VPI** and **VCI** provided by your ISP.
5. Enter the **Username** and **Password** provided by your ISP.
6. Re-enter the password for confirmation.

STEP 2: SETUP INTERNET CONNECTION → 3 → 4 → 5

Please select your ISP (Internet Service Provider) from the list below.

country : Singapore

ISP : Pacific Internet(PPPoE)

Protocol : PPPoE

Encapsulation Mode: LLC

VPI : 0 (0-255)

VCI : 100 (32-65535)

Search Available PVC :

PPPOE PPPOA

Please enter the user name and password provided by your Internet service provider (ISP). Note that the information is case-sensitive. Click "Next" to continue.

Username :

Password :

Confirm Password :

Click **Next** to go to the next page.

Note:

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

STEP 3: CONFIGURE WIRELESS NETWORK → 4 → 5

The wireless network is enabled by default. You can deselect it to disable it and click "Next" to skip the configuration of wireless network.

Enable Your Wireless Network :

For security concerns, it is highly recommended to change the pre-configured network name. Please set a name for your wireless network that can be easily recognized by wireless clients.

Wireless Network Name (SSID) :

If you select "Visible", the SSID of your wireless network can be found by wireless clients. If you select "Invisible", your wireless network is hidden and users need to manually enter the SSID in order to connect to your wireless network.

Visibility Status : Visible Invisible

In order to protect your network from hackers and unauthorized users, you are highly recommended to select one of the following wireless network security settings.

<i>None</i>	<i>Security Level</i>		<i>Best</i>
<input checked="" type="radio"/> None	<input type="radio"/> WEP	<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK

Security Mode:None
Select this option if you do not wish to enable any security features.

Step 3 Configure the wireless network in this page.

1. Check **Enable Your Wireless Network**.
2. Set the **SSID** for your wireless network, you can also keep it as default.
3. Choose to display or hide your wireless network.
 - **Visible:** Your wireless network can be detected.
 - **Invisible:** Your wireless network cannot be detected. Wireless clients need to enter the SSID and password manually to join this wireless network.
4. Choose an encryption mode for the wireless network. It is recommended to choose **WPA2-PSK**.
5. Enter a new password in **WPA2 Pre-Shared Key**

STEP 3: CONFIGURE WIRELESS NETWORK → 4 → 5

The wireless network is enabled by default. You can deselect it to disable it and click "Next" to skip the configuration of wireless network.

Enable Your Wireless Network :

For security concerns, it is highly recommended to change the pre-configured network name. Please set a name for your wireless network that can be easily recognized by wireless clients.

Wireless Network Name (SSID) : D-Link

If you select "Visible", the SSID of your wireless network can be found by wireless clients. If you select "Invisible", your wireless network is hidden and users need to manually enter the SSID in order to connect to your wireless network.

Visibility Status : Visible Invisible

In order to protect your network from hackers and unauthorized users, you are highly recommended to select one of the following wireless network security settings.

None	Security Level		Best
<input type="radio"/> None	<input type="radio"/> WEP	<input type="radio"/> WPA-PSK	<input checked="" type="radio"/> WPA2-PSK

Security Mode: WPA2-PSK

Select this option if your wireless adapters support WPA2-PSK.

Please enter your wireless security key:

WPA2 Pre-Shared Key : ●●●●●●●●●●

(8-63 characters, such as a~z, A~Z, or 0~9, i.e. '%Fortress123&')

Note: Please enter the same key on your wireless clients to enable proper wireless connection.

Click **Next** to go to the next page.

STEP 4: ACCOUNT PASSWORD → 5

Use the fields below to change or create passwords. Note: Password cannot contain a space.

ACCOUNT PASSWORD

Username: admin

Current Password: default password : admin

New Password:

Confirm Password:

Step 4 In this page, you can change a new password. Click **Next** to go to the next step.

STEP 5: COMPLETED AND RESTART

The setup is complete. Click "Back" to review or modify the settings.

If the Internet connection does not work, try the Setup Wizard again with alternative settings, or use manual setup instead if you have the Internet connection details provided by your ISP.

SETUP SUMMARY

The following shows a detailed summary of your settings. Please print this page out or write the information on a piece of paper, and save it, so you can correctly configure the settings on your wireless client adapters later based on the information in this page.

Time Settings :	disable
NTP Server 1 :	not set!
NTP Server 2 :	not set!
Time :	2012-05-23T00:42:41
Daylight Saving Time :	disable
wan_type	DSL
VPI / VCI :	0/100
Protocol :	PPPoE
Connection Type :	LLC
Username :	test
Password :	test
Wireless Network Name (SSID) :	D-Link
Visibility Status :	visible
Encryption :	WPA2-PSK
Pre-Shared Key :	Pruebas pasarela basica
WEP Key :	not set!
New password:	not set!

Back Apply Cancel

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.

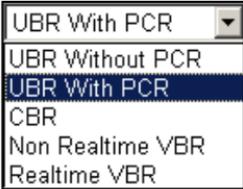
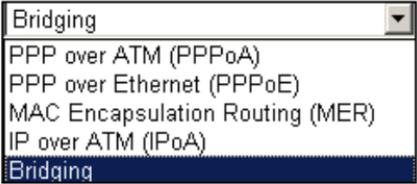
DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	INTERNET SETUP				
Internet Setup	Choose "Add", "Edit", or "Delete" to configure WAN interfaces.				
Wireless	DSL SETUP				
Local Network	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol State Status Backup3G Action
LAN IPv6					
Time and Date					
Logout	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

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

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	INTERNET SETUP				
Internet Setup	In this page, you can configure an ATM PVC identifier (VPI and VCI) and select a service category.				
Wireless	ATM PVC CONFIGURATION				
Local Network	VPI : <input type="text" value="0"/> (0-255) VCI : <input type="text" value="35"/> (32-65535) Service Category : <input type="text" value="UBR With PCR"/>				
LAN IPv6	Peak Cell Rate : <input type="text" value="0"/> (cells/s) Sustainable Cell Rate : <input type="text" value="0"/> (cells/s) Maximum Burst Size : <input type="text" value="0"/> (cells)				
Time and Date	CONNECTION TYPE				
Logout	Protocol : <input type="text" value="Bridging"/> Encapsulation Mode : <input type="text" value="LLC"/> 802.1Q VLAN ID : <input type="text" value="0"/> (0 = disable, 1 - 4094) Priority : <input type="text" value="0"/> (0 - 7) Firewall Enable : <input checked="" type="checkbox"/> <input type="checkbox"/> Enable Proxy Arp				
	Enable Bridge Service : <input checked="" type="checkbox"/> Service Name : <input type="text" value="br_0_35_0_0"/>				
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

The following table describes the parameters in this page.

Field	Description
PVC Settings	<p>VPI: The virtual path between two points in an ATM network. Its valid value is from 0 to 255.</p> <p>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).</p>

Field	Description
	The values of VPI and VCI are provided by your ISP.
Service Category	<p>You can select from the drop-down list.</p> 
Protocol	<p>Selected the protocol you subscribed from your ISP. It displays the protocol type used for this WAN connection.</p> 
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.

CONNECTION TYPE	
Protocol :	PPP over Ethernet (PPPoE) ▾
Encapsulation Mode :	LLC ▾
802.1Q VLAN ID :	0 (0 = disable, 1 - 4094)
Priority :	0 (0 - 7)
Firewall Enable :	<input checked="" type="checkbox"/>
IPv4 Enable :	<input checked="" type="checkbox"/>
IPv6 Enable :	<input type="checkbox"/>
	<input type="checkbox"/> Enable Proxy Arp
PPP USERNAME AND PASSWORD	
PPP Username :	<input type="text"/>
PPP Password :	<input type="password"/>
Confirm PPP Password :	<input type="password"/>
Authentication Method :	AUTO ▾
Dial-up mode :	AlwaysOn ▾
Inactivity Timeout :	100 (Seconds [60-65535])
MRU Size :	1492 (576~1492)
MTU Size :	1400 (576~1492)
Keep Alive :	<input checked="" type="checkbox"/>
Lcp Echo Interval (sec) :	30
Lcp Echo Failure :	5
Use Static IP Address :	<input type="checkbox"/>
IP Address :	<input type="text"/>
Enable NAT :	<input checked="" type="checkbox"/>
NAT Type :	Full Cone Nat ▾
Enable WAN Service :	<input checked="" type="checkbox"/>
Service Name :	pppoe_0_35_0_0_Internet
3G CONNECTION BACKUP SETTINGS	
Backup 3G Enable :	<input checked="" type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The following table describes the parameters of this page

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

Field	Description
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	<ul style="list-style-type: none"> ● 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.

CONNECTION TYPE	
Protocol :	MAC Encapsulation Ro
Encapsulation Mode :	LLC
802.1Q VLAN ID :	0 (0 = disable, 1 - 4094)
Priority :	0 (0 - 7)
Firewall Enable :	<input checked="" type="checkbox"/>
IPv4 Enable :	<input checked="" type="checkbox"/>
IPv6 Enable :	<input type="checkbox"/>
	<input type="checkbox"/> Enable Proxy Arp

WAN IP SETTINGS	
<input type="radio"/> Obtain address automatically	
<input checked="" type="radio"/> Use the following address :	
WAN IP Address :	<input type="text"/>
WAN Subnet Mask :	<input type="text"/>
Default gateway :	<input type="text"/>
Preferred DNS server :	<input type="text"/>
Alternate DNS server :	<input type="text"/>

Enable NAT :	<input checked="" type="checkbox"/>
NAT Type :	Full Cone Nat
Enable WAN Service :	<input checked="" type="checkbox"/>
Service Name :	mer_0_35_0_0_Internet

3G CONNECTION BACKUP SETTINGS	
Backup 3G Enable :	<input checked="" type="checkbox"/>

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 Mask	Enter the WAN subnet mask provided by the ISP. It varies depending on the network type. It is usually

Field	Description
	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 peer-to-peer 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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	WIRELESS SETTINGS -- WIRELESS BASIC				
Internet Setup	Configure your wireless basic settings.				
Wireless	<input type="button" value="Wireless Basic"/>				
Local Network	WIRELESS SETTINGS -- WIRELESS SECURITY				
LAN IPv6	Configure your wireless security settings.				
Time and Date	<input type="button" value="Wireless Security"/>				
Logout					

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	WIRELESS BASIC				
Internet Setup	Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.				
Wireless	WIRELESS NETWORK SETTINGS				
Local Network	<p>Enable Wireless: <input checked="" type="checkbox"/></p> <p>Enable MultiAP Isolation: <input type="checkbox"/></p> <p>Wireless Network Name (SSID): <input type="text" value="D-Link"/></p> <p>Visibility Status: <input checked="" type="radio"/> Visible <input type="radio"/> Invisible</p> <p>Country/Region: <input type="text" value="Singapore"/></p> <p>Control Sideband: <input type="text" value="Upper"/></p> <p>Wireless Channel: <input type="text" value="Auto Scan"/></p> <p>802.11 Mode: <input type="text" value="802.11b/g/n"/></p> <p>Band Width: <input type="text" value="20M/40M"/></p>				
LAN IPv6					
Time and Date					
Logout	<p>Remember your SSID as you will need to configure the same settings on your wireless devices and PC.</p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>				

The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select this to turn Wi-Fi on.
Enable MultiAP Isolation	Check MultiAP Isolation , the wireless APs that are connected to the 2750E cannot intercommunication.
Wireless Network Name (SSID)	Set the SSID for your wireless network. 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.
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 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 cell phone connect to the wireless network of **DSL-2750E** automatically by shooting the 2-Dimension code with the cell phone.

Note:

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

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.

SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
WIRELESS SECURITY				
In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.				
WIRELESS SECURITY MODE				
To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.				
Security Mode : <input type="text" value="None"/>				

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

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

WIRELESS SECURITY

In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode :

WEP

If you select WEP, the device operates **ONLY** in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it, you must enter the same key(s) on the router and the wireless stations. A 64-bit key consists of 10 hexadecimal digits and a 128-bit key consists of 26 hexadecimal digits. A hexadecimal digit is a number from 0 to 9 or a letter from A to F. For the most secure use of WEP, set the authentication type to "Shared Key".

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length :

Choose WEP Key :

WEP Key1 :

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

The following table describes the parameters of this page.

Field	Description
Security Mode	<p>Configure the wireless encryption mode. You can choose None, WEP, Auto (WPA or WPA2), WPA 2 Only or WPA Only.</p> <ul style="list-style-type: none"> ● 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.

WIRELESS SECURITY

In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode :
 WPA Encryption :

WPA

Select **WPA** or **WPA2** to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select **WPA2 Only** (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :
 Group Key Update Interval :

PRE-SHARED KEY

Pre-Shared Key :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

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	<ul style="list-style-type: none"> 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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP								
Wizard	LOCAL NETWORK												
Internet Setup	In this page, you can configure the local network settings of your router. Please note that settings in this page are optional and you need not change any of the settings in this page to get your network up and running.												
Wireless	ROUTER SETTINGS												
Local Network	The IP address of the router configured in this page is the one you use to access the Web management interface. If you change the IP address in this page, you need to adjust the network settings of your PC to access the network.												
LAN IPv6	Router IP Address : <input type="text" value="192.168.1.1"/> Subnet Mask : <input type="text" value="255.255.255.0"/> Domain Name : <input type="text"/> <input type="checkbox"/> Configure the second IP Address and Subnet Mask for LAN IP Address : <input type="text"/> Subnet Mask : <input type="text"/>												
Time and Date	DHCP SETTINGS (OPTIONAL)												
Logout	In this page, you can configure the built-in DHCP server to assign IP addresses to the computers on your network.												
	<input checked="" type="checkbox"/> Enable DHCP Server DHCP IP Address Range : <input type="text" value="192.168.1.33"/> to <input type="text" value="192.168.1.254"/> DHCP IP Mask : <input type="text" value="255.255.255.0"/> DHCP Router IP : <input type="text" value="192.168.1.1"/> DHCP Lease Time : <input type="text" value="43200"/> (seconds)												
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>												
	DHCP RESERVATIONS LIST												
	<table border="1"> <thead> <tr> <th>Status</th> <th>Computer Name</th> <th>MAC Address</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>					Status	Computer Name	MAC Address	IP Address				
Status	Computer Name	MAC Address	IP Address										
	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>												

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 .
Domain 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.

DHCP RESERVATIONS LIST			
Status	Computer Name	MAC Address	IP Address

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

ADD DHCP RESERVATION (OPTIONAL)	
Enable :	<input type="checkbox"/>
Computer Name :	<input type="text"/>
IP Address :	<input type="text"/>
MAC Address :	<input type="text"/>

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	IPv6 LAN SETTINGS				
Internet Setup	Note: Stateful DHCPv6 is supported after the 16 bits of IPv6 address. For example: Interface ID ranges from 1 to ffff, and IPv6 address ranges from 2111:123:123::1 to 2111:123:123::ffff.				
Wireless					
Local Network	STATIC LAN IPV6 ADDRESS CONFIGURATION				
LAN IPv6	IPv6 Interface Address <input type="text" value="fe80::1"/>				
Time and Date	DHCPV6 CONFIGURATION				
Logout	Enable DHCPv6 Server <input type="checkbox"/> LAN address config mode <input checked="" type="radio"/> Stateless <input type="radio"/> Statefull Start Interface ID <input type="text" value="33"/> End Interface ID <input type="text" value="254"/> DHCPv6 Lease Time <input type="text" value="43200"/> Use the following DNS server addresses. Get DNS Servers from WAN <input checked="" type="radio"/> Static DNS Servers <input type="radio"/> Static IPv6 DNS Servers <input type="text" value="2111:3c:123:0:c:135:9a:a"/>				
	SITE PREFIX CONFIGURATION				
	Enable RADVD <input type="checkbox"/> Auto get prefix from WAN <input checked="" type="radio"/> Static <input type="radio"/> Site Prefix <input type="text"/>				
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	TIME AND DATE				
Internet Setup	With the time configuration function, you can configure, update, and maintain the correct time of the internal system clock. In this page, you can set the time zone that you are in and set the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time if necessary.				
Wireless	TIME SETTING				
Local Network	<input type="checkbox"/> Automatically synchronize with Internet time server Primary NTP time server: <input type="text" value="ntp1.dlink.com"/> Secondary NTP time server: <input type="text" value="ntp.dlink.com.tw"/> Manual setup time: 2012 Year 05 Mon 23 Day 05 Hour 13 Min 34 Sec				
LAN IPv6	TIME CONFIGURATION				
Time and Date	Time Zone: <input type="text" value="(GMT+07:00) Bangkok, Hanoi, Jakarta"/> <input checked="" type="checkbox"/> Automatically adjust clock for daylight saving changes Daylight Saving Start: 2000 Year 04 Mon 01 Day 02 Hour 00 Min 00 Sec Daylight Saving End: 2000 Year 09 Mon 01 Day 02 Hour 00 Min 00 Sec				
Logout	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

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.

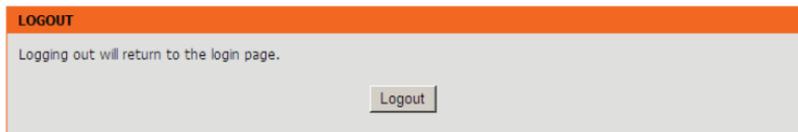
Select **Automatically adjust clock for daylight saving changes** if necessary.

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	ADVANCED WIRELESS -- ADVANCED SETTINGS				
Port Forwarding	You can configure advanced features of the wireless LAN interface.				
DMZ	Advanced Settings				
SAMBA					
3G Configuration	ADVANCED WIRELESS -- MAC FILTERING				
Parental Control	You can configure wireless firewall by denying or allowing designated MAC addresses.				
Filtering Options	MAC Filtering				
QoS Configuration					
Firewall Settings	ADVANCED WIRELESS -- SECURITY SETTINGS				
DNS	You can configure security features of the wireless LAN interface.				
Dynamic DNS	Security Settings				
Network Tools					
Routing	ADVANCED WIRELESS -- WPS SETTING				
Schedules	You can configure the wireless WPS.				
NAT	WPS Setting				
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

3.3.1.1 Advanced Settings

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

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	ADVANCED SETTINGS				
Port Forwarding	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.				
DMZ	ADVANCED WIRELESS SETTINGS				
SAMBA	Transmission Rate : <input type="text" value="Auto"/> Multicast Rate : <input type="text" value="Lower"/> Transmit Power : <input type="text" value="100%"/> Beacon Period : <input type="text" value="100"/> (20 ~ 1000) RTS Threshold : <input type="text" value="2346"/> (256 ~ 2346) Fragmentation Threshold : <input type="text" value="2345"/> (256 ~ 2346) DTIM Interval : <input type="text" value="1"/> (1 ~ 255) Preamble Type : <input type="text" value="long"/>				
3G Configuration	SSID				
Parental Control	Enable Wireless : <input checked="" type="checkbox"/> Wireless Network Name (SSID) : <input type="text" value="D-Link"/> Visibility Status : <input checked="" type="radio"/> Visible <input type="radio"/> Invisible User Isolation : <input type="text" value="Off"/> WMM Advertise : <input type="text" value="On"/> Max Clients : <input type="text" value="16"/> (1 ~ 32)				
Filtering Options	GUEST/VIRTUAL ACCESS POINT-1				
QoS Configuration	Enable Wireless Guest Network : <input type="checkbox"/> Guest SSID : <input type="text" value="D-link_GUEST1"/> Visibility Status : <input checked="" type="radio"/> Visible <input type="radio"/> Invisible User Isolation : <input type="text" value="Off"/> WMM Advertise : <input type="text" value="On"/> Max Clients : <input type="text" value="16"/> (1 ~ 32)				
Firewall Settings	GUEST/VIRTUAL ACCESS POINT-2				
DNS	Enable Wireless Guest Network : <input type="checkbox"/> Guest SSID : <input type="text" value="D-link_GUEST2"/> Visibility Status : <input checked="" type="radio"/> Visible <input type="radio"/> Invisible User Isolation : <input type="text" value="Off"/> WMM Advertise : <input type="text" value="On"/> Max Clients : <input type="text" value="16"/> (1 ~ 32)				
Dynamic DNS	GUEST/VIRTUAL ACCESS POINT-3				
Network Tools	Enable Wireless Guest Network : <input type="checkbox"/> Guest SSID : <input type="text" value="D-link_GUEST3"/> Visibility Status : <input checked="" type="radio"/> Visible <input type="radio"/> Invisible User Isolation : <input type="text" value="Off"/> WMM Advertise : <input type="text" value="On"/> Max Clients : <input type="text" value="16"/> (1 ~ 32)				
Routing	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				
Schedules					
NAT					
FTP Setting					
FTP Account					
IP Tunnel					
Logout					

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.

The router supports multiple SSID. The settings in this page 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.

The screenshot shows a configuration page with an orange header titled "MAC ADDRESS". Below the header, there is a grey box containing the text: "The MAC Address Access Control mode, if enabled, permits access to this route from host with MAC addresses contained in the Access Control List. Enter the MAC address of the management station permitted to access this route, and click 'Apply'". Below this is a dark grey section titled "ACCESS CONTROL - MAC ADDRESSES". It features a checkbox labeled "Enable Access Control Mode" which is currently unchecked. Below the checkbox is a text input field labeled "MAC Address". At the bottom of this section are two buttons: "Add" and "Delete".

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

The screenshot shows a dialog box with a dark grey header titled "MAC ADDRESS". Inside the dialog, there is a label "MAC Address:" followed by a text input field. At the bottom of the dialog are two buttons: "Apply" and "Cancel".

Click **Apply** to finish.

3.3.1.3 Security Settings

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

WIRELESS SECURITY

In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.

WIRELESS SSID

Select SSID :

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

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.

WEP

If you select WEP, the device operates **ONLY** in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it, you must enter the same key(s) on the router and the wireless stations. A 64-bit key consists of 10 hexadecimal digits and a 128-bit key consists of 26 hexadecimal digits. A hexadecimal digit is a number from 0 to 9 or a letter from A to F. For the most secure use of WEP, set the authentication type to "Shared Key".

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length :

Choose WEP Key :

WEP Key1 :

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

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

WPA

Select **WPA** or **WPA2** to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select **WPA2 Only** (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval :

PRE-SHARED KEY

Pre-Shared Key :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

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.

WIRELESS WPS

WPS: You can select different authentication modes in the "Security Setting" page, and broadcast the SSID. The PIN code is saved when you click the PIN button.

WPS

Enabled :

SSID :

Select Mode :

Configuration State :

Push Button :

Input Station PIN :

WPS Session Status :

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 Registrar or Enrollee . When a router is in Registrar 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 automatically.
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.

WIRELESS WPS

WPS: You can select different authentication modes in the "Security Setting" page, and broadcast the SSID. The PIN code is saved when you click the PIN button.

WPS

Enabled :

SSID :

Select Mode :

Configuration State :

Generate PIN :

Pin Station :

WPS Session Status :

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.

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 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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	DMZ				
Port Forwarding	The DSL router forwards IP packets that do not belong to any application configured in the Port Forwarding list, from WAN to the DMZ host.				
DMZ	Enter IP address of the computer and click "Apply" to enable the DMZ host.				
SAMBA	Clear the field of the IP address and click "Apply" to disable the DMZ host.				
3G Configuration	DMZ HOST				
Parental Control	WAN Connection : <input type="text"/>				
Filtering Options	Enable DMZ : <input type="checkbox"/>				
QoS Configuration	DMZ Host IP Address : <input type="text"/>				
Firewall Settings	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	SAMBA				
Port Forwarding	configure for Samba.				
DMZ	SAMBA SERVER				
SAMBA	Enable SAMBA : <input checked="" type="checkbox"/> Workgroup : <input type="text" value="Workgroup"/> Netbios Name : <input type="text" value="dsl_route"/> SMB User Name : <input type="text" value="root"/> New SMB password : <input type="password" value="*****"/> Retype new SMB password : <input type="password" value="*****"/> Enable USB Storage : <input checked="" type="checkbox"/> Enable Anonymous Access : <input checked="" type="checkbox"/>				
3G Configuration	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				
Parental Control					
Filtering Options					
QoS Configuration					
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

3.3.5 3G Configuration

Choose **ADVANCED** > **3G Configuration** and the page shown in the following figure appears. (Ensure your 3G card is connected the USB interface of 2750E)

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP												
Advanced Wireless	3G																
Port Forwarding	Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.																
DMZ	When you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.																
SAMBA	3G STATUS																
3G Configuration	3G Status: NoDongle																
Parental Control	Inform: NO USB CARD																
Filtering Options	3G SETUP																
QoS Configuration	<table border="1"> <thead> <tr> <th>Service Name</th> <th>Protocol</th> <th>State</th> <th>Status</th> <th>Default Gateway</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="6" style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Pin Manage"/> <input type="button" value="DongleInfo"/> </td> </tr> </tbody> </table>					Service Name	Protocol	State	Status	Default Gateway	Action	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Pin Manage"/> <input type="button" value="DongleInfo"/>					
Service Name	Protocol	State	Status	Default Gateway	Action												
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Pin Manage"/> <input type="button" value="DongleInfo"/>																	
Firewall Settings																	
DNS																	

If there is no 3G WAN interface listed in 3G SETUP table, click **Add** in this page, and the following page appears.

3G USB SETUP

Enable 3G Service :
Country: [(Click to Select)]
Profile Name: [(Click to Select)]
Account :
Password :
Dial_Number : *99#
Net Type: Auto
APN : internet
OnDemand :
Inactivity Timeout : 0 (Seconds [40-65535]. But if 0, we will set default)
Backup delay time : 60 (Seconds [0-600])
Recovery delay time : 60 (Seconds [0-600])
Initialization Delay time : 20 (If too small, some 3g dongle will be unsupported)
Mode Switch Delay time : 20 (If too small, some 3g dongle will be unsupported)
BackupMechanism : DSL
Checking IP address: 8.8.8.8
Timeout (in sec.): 1
Period time (in sec.): 1
Fail Tolerance: 1

[Apply] [AutoSet] [Cancel]

Select the country and profile name, set the account and password for your 3G network, then click **Apply**. A 3G WAN interface is added.

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.

DSL-2750E //	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP												
Advanced Wireless	3G																
Port Forwarding	Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.																
DMZ	When you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.																
SAMBA	3G STATUS																
3G Configuration	3G Status: Ready																
Parental Control	Inform: Connecting, dial on demand, Auto Dailed																
Filtering Options	3G SETUP																
QoS Configuration	<table border="1"> <thead> <tr> <th>Service Name</th> <th>Protocol</th> <th>State</th> <th>Status</th> <th>Default Gateway</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>pppo3g</td> <td>PPPo3G</td> <td>1</td> <td>Disconnected</td> <td><input type="checkbox"/></td> <td>undial</td> </tr> </tbody> </table>					Service Name	Protocol	State	Status	Default Gateway	Action	pppo3g	PPPo3G	1	Disconnected	<input type="checkbox"/>	undial
Service Name	Protocol	State	Status	Default Gateway	Action												
pppo3g	PPPo3G	1	Disconnected	<input type="checkbox"/>	undial												
Firewall Settings	<div style="text-align: center;"> Add Edit Delete Pin Manage DongleInfo </div>																
DNS																	
Dynamic DNS																	
Network Tools																	
Routing																	
Schedules																	
NAT																	
FTPD Setting																	
FTPD Account																	
IP Tunnel																	
Logout																	

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.

DSL-2750E //	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP												
Advanced Wireless	3G																
Port Forwarding	Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.																
DMZ	When you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.																
SAMBA	3G STATUS																
3G Configuration	3G Status: NeedPinCode																
Parental Control	Inform: NEED PIN CODE!																
Filtering Options	3G SETUP																
QoS Configuration	<table border="1"> <thead> <tr> <th>Service Name</th> <th>Protocol</th> <th>State</th> <th>Status</th> <th>Default Gateway</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>ppp3g</td> <td>PPPo3G</td> <td>1</td> <td>Disconnected</td> <td><input type="checkbox"/></td> <td><input type="button" value="dial"/></td> </tr> </tbody> </table>					Service Name	Protocol	State	Status	Default Gateway	Action	ppp3g	PPPo3G	1	Disconnected	<input type="checkbox"/>	<input type="button" value="dial"/>
Service Name	Protocol	State	Status	Default Gateway	Action												
ppp3g	PPPo3G	1	Disconnected	<input type="checkbox"/>	<input type="button" value="dial"/>												
Firewall Settings	<div style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Pin Manage"/> <input type="button" value="DongleInfo"/> </div>																
DNS																	
Dynamic DNS																	
Network Tools																	
Routing																	
Schedules																	
NAT																	
FTPD Setting																	
FTPD Account																	
IP Tunnel																	
Logout																	

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

THE 3G CONFIGURATION

In this page, you can configure the PIN code of the SIM card.

sim card's status is : NEED PIN CODE

Unlock with PIN code

Enter PIN code: Remain times:3

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

PIN ACTION RESULT:

Action is OK!

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

THE 3G CONFIGURATION

In this page, you can configure the PIN code of the SIM card.

sim card's status is : lock enable

Disable PIN protect

Change PIN code

Enter PIN code: Remain times:3

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.

PIN ACTION RESULT:

NONE

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.

3G

Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

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

3G STATUS

3G Status: Ready

Inform: Connecting, dial on demand, Auto Dialed

3G SETUP

Service Name	Protocol	State	Status	Default Gateway	Action
pppo3g	PPPo3G	1	Disconnected	<input type="checkbox"/>	<input type="button" value="undial"/>

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

3G

Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

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

3G STATUS

3G Status: Ready

Inform: CONNECTED, dial on demand, Auto Dialed

3G SETUP

Service Name	Protocol	State	Status	Default Gateway	Action
pppo3g	PPPo3G	1	Connected	<input type="checkbox"/>	<input type="button" value="undial"/>

- **Disable PIN Protect**

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

THE 3G CONFIGURATION

In this page, you can configure the PIN code of the SIM card.

sim card's status is : lock enable

Disable PIN protect

Change PIN code

Enter PIN code: Remain times:3

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.

PIN ACTION RESULT:

Action is OK!

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

THE 3G CONFIGURATION

In this page, you can configure the PIN code of the SIM card.

sim card's status is : lock disable

Enable PIN protect 

Enter PIN code: Remain times:3

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

PIN ACTION RESULT:

NONE

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

3G

Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

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

3G STATUS

3G Status: Ready

Inform: DISCONNECT

3G SETUP

Service Name	Protocol	State	Status	Default Gateway	Action
ppp03g	PPPo3G	1	Disconnected	<input type="checkbox"/>	<input type="button" value="dial"/>

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

- Change PIN Code

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

THE 3G CONFIGURATION

In this page, you can configure the PIN code of the SIM card.

sim card's status is : lock enable

Disable PIN protect

Change PIN code

Enter current PIN code: Remain times: 3

Enter new PIN code:

Confirm new PIN code:

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

PIN ACTION RESULT:

Action is OK!

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**.

3G

Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

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

3G STATUS

3G Status: Ready

Inform: DISCONNECT

3G SETUP

Service Name	Protocol	State	Status	Default Gateway	Action
ppp3g	PPPo3G	1	Disconnected	<input type="checkbox"/>	<input type="button" value="dial"/>

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

3G INTERNET SETUP

This screen allows you to configure a 3G Internet connection.

3G USB SETUP

Enable 3G Service :

Country:

Profile Name:

Account :

Password :

Dial_Number :

Net Type :

APN :

OnDemand :

Inactivity Timeout : (Seconds [40-65535]. But if 0, we will set default)

Backup delay time : (Seconds [0-600])

Recovery delay time : (Seconds [0-600])

Initialization Delay time : (If too small, some 3g dongle will be unsupported)

Mode Switch Delay time : (If too small, some 3g dongle will be unsupported)

BackupMechanism :

Checking IP address:

Timeout (in sec.):

Period time (in sec.):

Fail Tolerance:

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.

Field	Description
Backup Delay Time	The response time for 3G connection dial-up after 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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	PARENTAL CONTROL -- BLOCK WEBSITE				
Port Forwarding	Uses URL (i.e. www.yahoo.com) to implement filtering.				
DMZ	Block Website				
SAMBA	PARENTAL CONTROL -- MAC FILTER				
3G Configuration	Uses MAC address to implement filtering.				
Parental Control	MAC Filter				
Filtering Options					
QoS Configuration					
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

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.

BLOCK WEBSITE

In this page, you can block websites. If this function is enabled, access to the websites in the list will be denied.

URL	Schedule
-----	----------

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

ADD SCHEDULE RULE

URL :

Schedule : [View Available Schedules](#)

Manual Schedule :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed
 Thu Fri Sat

All Day - 24 hrs :

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

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.

BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

<input type="checkbox"/>	URL	Schedule
<input type="checkbox"/>	www.xxx.com	Always

Add

Edit

Delete

3.3.6.2 MAC Filter

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

BLOCK MAC ADDRESS

Time of Day Restrictions -- A maximum of 16 entries can be configured

In this page, you can set the time of day restriction on a specific LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click "Other MAC Address" and enter the MAC address of that LAN device. To obtain the MAC address of a Windows-based PC, open a command prompt window and enter "ipconfig /all".

MAC Filtering Global Policy:

- BLACK_LIST** --Allow all packets but **DENY** MAC addresses that match a rule in the list
- WHITE_LIST** --Deny all packets but **ALLOW** MAC addresses that match a rule in the list

Apply

Cancel

BLOCK MAC ADDRESS--BLACKLIST

Username	MAC	Schedule

Add

Edit

Delete

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

ADD SCHEDULE RULE

User Name :

Current PC's MACAddress :

Other MAC Address :

Schedule : [View Available Schedules](#)

Manual Schedule :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed

Thu Fri Sat

All Day - 24 hrs :

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	FILTERING OPTIONS -- IP FILTERING				
Port Forwarding	Uses IP address to implement filtering.				
DMZ	IP Filtering				
SAMBA	FILTERING OPTIONS -- BRIDGE FILTERING				
3G Configuration	Uses MAC address to implement filtering. Useful only in bridge mode.				
Parental Control	Bridge Filtering				
Filtering Options					
QoS Configuration					
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

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.

IP FILTER

In this page, you can specify a filter name and at least one condition to create a filter for identify incoming IP traffic. All the specified conditions take effect simultaneously. Click "Apply" to save the filter and enable it.

FIREWALL

Name	Interface	In/Out	Default action	Bytes	Pkts	Local/Forward
Add Filter Edit Filter Delete Filter						

RULE

Enabled Protocol	IP Version Type	Action	RejectType	IcmpType	OrigIP/ Mask	OrigPort	DestIP/ Mask	DestPort	Bytes	Pkts
Add Rule Edit Rule Delete Rule										

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

FILTER INFO

Name:	<input type="text"/>
Interface:	LAN
In/Out:	In
Default action:	Permit
Local/Forward:	Local

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.

RULE INFO	
Notes:	
1. When Protocol is 'ICMP', one of IcmpType to be selected;	
2. When Action is 'Reject', one of RejectType to be selected;	
3. When the "IP Version Type" is Ipv4, Please enter the IPv4 address and mask of the corresponding;	
4. When the "IP Version Type" is Ipv6, Please enter the IPv6 address and prefix length of the corresponding;	
Enabled: <input type="checkbox"/>	
Protocol: ALL	
IP Version Type: IPv4	
Action: Permit	
DSCP:	
Packet Length: . (1~65535)	
SOURCE SETTING	
IP Address:	
PrefixLength/Mask:	
DESTINATION SETTING	
FQDN Enabled <input type="checkbox"/>	
IP Address:	
PrefixLength/Mask:	

Apply Cancel

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
IP Address	Destination IP address

Field	Description
PrefixLength/Mask	Destination address mask

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

IP FILTER

In this page, you can specify a filter name and at least one condition to create a filter for identify incoming IP traffic. All the specified conditions take effect simultaneously. Click "Apply" to save the filter and enable it.

FIREWALL

	Name	Interface	In/Out	Default action	Bytes	Pkts	Local/Forward
☺	TEST	LAN	In	Permit	4868	22	Local

RULE

	Enabled	Protocol	IP Version Type	Action	RejectType	IcmpType	OrigIP/ Mask	OrigPort	DestIP/ Mask	DestPort	Bytes	Pkts
☺	0	all	IPv4	Permit			/	:	/	:	0	0

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.

BRIDGE FILTERING

Bridge Filtering is effective only on ATM PVCs configured in Bridge mode. ALLOW means that all MAC layer frames can be transmitted. DENY means that all MAC layer frames except those matching a rule in the following list can not be transmitted.

Specify at least one condition to create a filter for identify the MAC layer frames. If you specify several conditions, all of them take effect simultaneously. Click "Apply" to save the filter and enable it.

WARNING: Changing from one global policy to another automatically REMOVES all the existing rules. You will need to create new rules for the new policy.

Bridge Filtering Global Policy:

- ALLOW** all packets but **DENY** MAC addresses that match a rule in the list
 DENY all packets but **ALLOW** MAC addresses that match a rule in the list

Apply Cancel

DISPLAY LIST

VPI/VCI protocol DMAC SMAC Prio vlanID DIR TIME

Add Edit Delete

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

ADD BRIDGE FILTER

Protocol Type: (Click to Select) ▼
 Destination MAC Address:
 Source MAC Address:
 User Priority: (0-7)
 vlanID: (0-4095)
 Frame Direction: WAN=>LAN ▼
 Time schedule: always ▼ [View Available Schedules](#)
 Wan interface: select all interfaces ▼

Apply Cancel

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.

The screenshot shows the QoS Configuration page with a sidebar on the left and a main content area on the right. The sidebar contains a list of menu items: DSL-2750E, SETUP, ADVANCED, MANAGEMENT, STATUS, HELP, Advanced Wireless, Port Forwarding, DMZ, SAMBA, 3G Configuration, Parental Control, Filtering Options, QoS Configuration (highlighted), Firewall Settings, DNS, Dynamic DNS, Network Tools, Routing, Schedules, NAT, FTPD Setting, FTPD Account, IP Tunnel, and Logout. The main content area is titled 'QoS Configuration' and is divided into three sections:

- QoS GLOBAL OPTIONS**: Configure QoS global options. A button labeled 'Configure QoS Global Options' is visible.
- QoS QUEUE CONFIGURATION**: Configure QoS Queue. A button labeled 'Configure QoS Queue' is visible.
- QoS CLASSIFICATION CONFIGURATION**: Configure QoS Classification. A button labeled 'Configure QoS Classification' is visible.

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.

QOS GLOBAL CONFIGURATION

Enable Queue Operation

Submit

Refresh

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.

QOS GLOBAL CONFIGURATION

Enable Upstream Bandwidth Kbps (0 means no limit bandwidth)Scheduling Strategy (Note: Scheduling change would clear the queue configuration)Enable DSCP/TC Mark Enable 802.1P Mark

Add Queue

UPSTREAM QUEUE CONFIGURATION

Number	Name	Enable	Precedence	Egress Interface	Operation
1	UP_Q_3	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	WAN <input type="text" value="v"/>	Delete
2	UP_Q_4	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	WAN <input type="text" value="v"/>	Delete
3	UP_Q_5	<input checked="" type="checkbox"/>	<input type="text" value="3"/>	WAN <input type="text" value="v"/>	Delete
4	UP_Q_6	<input checked="" type="checkbox"/>	<input type="text" value="4"/>	WAN <input type="text" value="v"/>	Delete

Submit

Refresh

The following table describes the parameters of this page.

Field	Description
Enable	Tick in the box to enable queue.
Upstream Bandwidth	Total bandwidth 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.

QOS CLASSIFY CONFIG

LIST

Classify Number	Enable	Classify Condition	Classify Mark	Classify Queue	Operation
1	1	Source MAC address : Ethernet Type : IPv4 Interface : LAN VLANID : -1 802.1P : -1 Source/Destination IP address : /81.47.224.0 Source/Destination Mask : /255.255.252.0 DSCP value : Do not mark Protocol Type : UDP Source port range : -1--1 Destination port range : -1--1	802.1P: -1 DSCP:	UP_Q_3	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
2	1	Source MAC address : Ethernet Type : IPv4 Interface : LAN VLANID : -1 802.1P : -1 Source/Destination IP address : /80.58.63.192 Source/Destination Mask : /255.255.255.192 DSCP value : Do not mark Protocol Type : Do not match Source port range : -1--1 Destination port range : -1--1	802.1P: -1 DSCP:	UP_Q_3	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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

QOS FLOW CLASSIFICATION CONFIGURATION

Enable

CLASSIFY CONDITIONS

Ip Protocol Type

Input Interface

Source MAC address

Source MAC mask

802.1P

Source IPv4 address

Source subnet mask

Destination IPv4 address

Destination subnet mask

DSCP Check

Protocol Type

Source port range -

Destination port range -

CLASSIFICATION MATCH RESULT

Classify Queue

DSCP Mark

COS Mark

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	FIREWALL SETTINGS				
Port Forwarding	Click "Apply" to take the changes in effect immediately.				
DMZ	FIREWALL CONFIGURATION				
SAMBA	Enable Attack Prevent <input type="checkbox"/>				
3G Configuration	Icmp Echo <input checked="" type="checkbox"/>				
Parental Control	Fraggle <input checked="" type="checkbox"/>				
Filtering Options	Echo Chargen <input checked="" type="checkbox"/>				
QoS Configuration	IP Land <input checked="" type="checkbox"/>				
Firewall Settings	Port Scan <input checked="" type="checkbox"/>				
DNS	TCP Flags: Set "SYN FIN" <input checked="" type="checkbox"/>				
Dynamic DNS	TCP Flags: Set "SYN RST" <input checked="" type="checkbox"/>				
Network Tools	TCP Flags: Set "FIN RST" <input checked="" type="checkbox"/>				
Routing	TCP DoS : <input checked="" type="checkbox"/>				
Schedules	TCP DoS Max Rate: <input type="text" value="50"/> (packets/second)				
NAT	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

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 following figure appears.

The screenshot shows the 'DNS SERVER CONFIGURATION' page in the DSL-2750E web interface. The left sidebar contains a menu with items like 'Advanced Wireless', 'Port Forwarding', 'DMZ', 'SMB', '3G Configuration', 'Parental Control', 'Filtering Options', 'QoS Configuration', 'Firewall Settings', 'DNS', 'Dynamic DNS', 'Network Tools', 'Routing', 'Schedules', 'NAT', 'FTPD Setting', 'FTPD Account', 'IP Tunnel', and 'Logout'. The main content area has a title bar 'DNS' and a sub-header 'DNS SERVER CONFIGURATION'. The configuration includes a 'Wan Connection' dropdown set to 'pppo3g', two radio buttons for 'Obtain DNS server address automatically' (selected) and 'Use the following DNS server addresses', and two radio buttons for 'Obtain IPv6 DNS server address automatically' (selected) and 'Use the following IPv6 DNS server addresses'. The 'Use the following DNS server addresses' section shows 'Primary DNS server' as '172.10.10.1' and 'Secondary DNS server' as 'undefined'. The 'Use the following IPv6 DNS server addresses' section shows 'Preferred IPv6 DNS server' and 'Alternate IPv6 DNS server' as empty text boxes. 'Apply' and 'Cancel' buttons are at the bottom.

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP								
Advanced Wireless	DYNAMIC DNS												
Port Forwarding	The dynamic DNS (DDNS) feature enables you to host a server (such as Web, FTP, game server) using a domain name that you have purchased (www.xxx.com) with the dynamic (changing) IP address assigned by the broadband Internet service provider. Using a DDNS service, your friends can enter your host name to connect to your game server without knowing your IP address.												
DMZ													
SAMBA													
3G Configuration	DYNAMIC DNS												
Parental Control	<table border="1"><thead><tr><th>Hostname</th><th>Username</th><th>Service</th><th>Interface</th></tr></thead><tbody><tr><td colspan="4" style="text-align: center;"><input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/></td></tr></tbody></table>					Hostname	Username	Service	Interface	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			
Hostname	Username	Service	Interface										
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>													
Filtering Options													
QoS Configuration													
Firewall Settings													
DNS													
Dynamic DNS													
Network Tools													
Routing													
Schedules													
NAT													
FTPD Setting													
FTPD Account													
IP Tunnel													
Logout													

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

ADD DYNAMIC DNS	
DDNS provider :	<input type="text" value="dlinkddns.com"/>
Hostname :	<input type="text"/>
Interface :	<input type="text" value="pppo3g"/>
Username :	<input type="text"/>
Password :	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	NETWORK TOOLS -- PORT MAPPING				
Port Forwarding	Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.				
DMZ	Port Mapping				
SAMBA					
3G Configuration	NETWORK TOOLS -- IGMP PROXY				
Parental Control	Transmission of identical content, such as multimedia, from a source to a number of recipients.				
Filtering Options	IGMP Proxy				
QoS Configuration					
Firewall Settings	NETWORK TOOLS -- IGMP SNOOPING				
DNS	Transmission of identical content, such as multimedia, from a source to a number of recipients.				
Dynamic DNS	IGMP Snooping				
Network Tools					
Routing	NETWORK TOOLS -- MLD CONFIGURATION				
Schedules	Transmission of identical content, such as multimedia, from a source to a number of recipients.				
NAT	MLD Configuration				
FTPD Setting					
FTPD Account	NETWORK TOOLS -- UPnP				
IP Tunnel	Allows you to enable or disable UPnP.				
Logout	Upnp				
	NETWORK TOOLS -- ADSL				
	Allows you to configure advanced settings for ADSL.				
	ADSL				
	NETWORK TOOLS -- SNMP				
	Network Tools -- SNMP				
	SNMP				

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.

PORT MAPPING

Port Mapping -- A maximum 5 entries can be configured

Port mapping supports mapping multiple ports to PVC and bridging groups. Each group serves as an independent network. Before using this feature, you must click "Add" and create mapping groups with appropriate LAN and WAN interfaces. If you select a group and click "Delete", the group is removed and the interfaces that are used to be in that group are automatically added to the Default group.

PORT MAPPING SETUP

Group Name	Interfaces
<input type="checkbox"/> Lan1	ethernet1,ethernet2,ethernet3,ethernet4,wlan0,wlan0-vap0,wlan0-vap1,...

Add

Edit

Delete

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

ADD PORT MAPPING

To create a mapping group, do as follows:

1. Enter the group name, select interfaces from the available interface list and use the arrow button to add them to the grouped interface list, to create the required port mapping. Note that the group name must be unique.
2. Click "Apply" to take the changes into effect immediately.

PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces	Available Interfaces
	ethernet1 ethernet2 ethernet3 wlan0 wlan0-vap0 wlan0-vap1 wlan0-vap2

Apply

Cancel

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

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by:

1. Enabling IGMP proxy on a WAN interface (upstream), which connects to a router running IGMP.
2. Enabling IGMP on a LAN interface (downstream), which connects to its host.

IGMP PROXY CONFIGURATION

Enable IGMP Proxy

IGMP Version :

Port Binding

Enable FastLeaving :

General Query Interval : (seconds)

General Query Response Interval : (1~255>(*100 milliseconds))

Group Query Interval : (seconds)

Group Query Response Interval : (1~255>(*100 milliseconds))

Group Query Count :

Last Member Query Interval : (seconds)

Last Member Query Count :

IGMP TABLE

Group Address	Interface	State

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.

IGMP

Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP SETUP

Enabled :

AgeEnabled :

LastMemberQueryInterval :

HostTimeout :

MrouterTimeout :

LeaveTimeout :

MaxGroups :

3.3.12.4 MLD Configuration

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

MLD SETTINGS

In this page, you can configure the MLD Setup settings of your Router. Please note that settings in this page are optional and you need not change any of the settings in this page to get your network up and running.

MLD PROXY

Enable Mld Proxy

WAN Connection :

MLD SNOOPING

Enable Mld Snooping

3.3.12.5 UPnP

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

UPnP
Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

UPnP SETUP
 Enable UPnP
WAN Connection :
LAN Connection :

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.

ADSL SETTINGS

In this page, you can configure the ADSL settings of the DSL router. Before changing the ADSL mode, you need to disable DSL.

ADSL SETTINGS

- Enable DSL
- All Multimode
- G.Dmt Enabled
- G.Lite Enabled
- G.Inp Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled
- Capability
- Bitswap Enable
- SRA Enable
- 1 bit Constellation Modulation Enable

Apply

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.

SNMP CONFIGURATION

This page is used to configure the SNMP protocol.

SNMP CONFIGURATION

- Enable SNMP Agent
- Read Community:
- Set Community:
- Trap Manager IP:
- Trap Community:
- Trap Version:

Apply

Cancel

3.3.13 Routing

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

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	STATIC ROUTE				
Port Forwarding	Static Route.				
DMZ	Static Route				
SAMBA	IPv6 STATIC ROUTE				
3G Configuration	IPv6 Static Route.				
Parental Control	IPv6 Static Route				
Filtering Options	POLICY ROUTE				
QoS Configuration	Policy Route.				
Firewall Settings	Policy Route				
DNS	DEFAULT GATEWAY				
Dynamic DNS	Default Gateway.				
Network Tools	Default Gateway				
Routing	RIP SETTINGS				
Schedules	RIP Settings.				
NAT	RIP Settings				
FTPD Setting	RIPNG SETTINGS				
FTPD Account	RIPng Settings.				
IP Tunnel	RIPng Settings				
Logout					

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.

STATIC ROUTE					
Enter the destination network address, subnet mask, gateway, metric, AND/OR available WAN/LAN interface. Then, click "Apply" to add the entry to the routing table.					
A maximum 30 entries can be configured.					
ROUTING -- STATIC ROUTE					
Destination	Subnet Mask	Gateway	Interface	Metric	
					Add Edit Delete

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

STATIC ROUTE ADD

Destination Network Address :

Subnet Mask :

Use Interface :

Metric :

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.

IPv6 STATIC ROUTE

Enter the destination network address (for example: 2000::1 or 2000::/64 eg.), AND/OR available WAN interface. Then, click "Apply" to add the entry to the routing table.

A maximum 30 entries can be configured.

ROUTING -- IPv6 STATIC ROUTE

Status	Destination	Interface

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

IPv6 STATIC ROUTE ADD	
Enable :	<input type="checkbox"/>
Destination Network Address :	<input type="text"/>
Use Interface :	ppp03g <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="cancel"/>	

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.

POLICY ROUTE		
Policy Route :chose one Wanconnection and one Lanconnection then bind them.		
POLICY ROUTE SETUP		
<input type="text"/>	<input type="text" value="WAN"/>	<input type="text" value="LAN"/>

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

WAN INSTANCE AND LAN INSTANCE	
WAN Connection	ppp03g <input type="button" value="v"/>
LAN Connection	ethernet1 <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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.

DEFAULT GATEWAY

You can assign the default gateway. The router will use the first WAN interface you assign. Click "Apply" to save the setting.

DEFAULT GATEWAY

Assigned the Default Gateway :

IPv6 DEFAULT GATEWAY

Assigned the IPv6 Default Gateway :

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.

RIP CONFIGURATION

To enable RIP on the device, set the global RIP mode to "Enabled". To configure an interface, select the desired RIP version and operation, select the "Enabled" check box corresponding to the interface, and click "Apply" to save the settings. The RIP is enabled or disabled, according to the selected global RIP mode.

RIP

Interface	VPI/VCI	Version	Operation	Enabled	Passive
ppp3g		1	Active	<input type="checkbox"/>	<input type="checkbox"/>
Lan1	-	1	Active	<input type="checkbox"/>	<input type="checkbox"/>

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.

RIPNG CONFIGURATION

To enable RIP for IPv6 (RIPng) on the interface, select the corresponding "Enabled" check box and click "Apply" to save the settings. The RIPng is enabled or disabled accordingly.

RIPNG

Interface	VPI/VCI	Enabled
ppp03g		<input type="checkbox"/>

Click **Apply** to save the settings.

3.3.14 Schedules

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

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																				
Advanced Wireless	SCHEDULES																								
Port Forwarding	You can use schedule to create scheduling rules to be applied for your firewall.																								
DMZ	Maximum number of schedule rules: 20																								
SAMBA	SCHEDULE RULES																								
3G Configuration	<table border="1"> <thead> <tr> <th>Rule Name</th> <th>Sun</th> <th>Mon</th> <th>Tue</th> <th>Wed</th> <th>Thu</th> <th>Fri</th> <th>Sat</th> <th>Start Time</th> <th>Stop time</th> </tr> </thead> <tbody> <tr> <td colspan="10" style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </td> </tr> </tbody> </table>					Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop time	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>									
Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop time																
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>																									
Parental Control																									
Filtering Options																									
QoS Configuration																									
Firewall Settings																									
DNS																									
Dynamic DNS																									
Network Tools																									
Routing																									
Schedules																									
NAT																									
FTPD Setting																									
FTPD Account																									
IP Tunnel																									
Logout																									

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

ADD SCHEDULE RULE

Name :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed
 Thu Fri Sat

All Day - 24 hrs :

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP						
Advanced Wireless	NAT										
Port Forwarding	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.										
DMZ											
SAMBA	NAT TABLES										
3G Configuration	<table border="1"> <thead> <tr> <th>Name</th> <th>Internal IP Address</th> <th>External IP Address</th> </tr> </thead> <tbody> <tr> <td colspan="3" style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </td> </tr> </tbody> </table>					Name	Internal IP Address	External IP Address	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		
Name	Internal IP Address	External IP Address									
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>											
Parental Control											
Filtering Options											
QoS Configuration											
Firewall Settings											
DNS											
Dynamic DNS											
Network Tools											
Routing											
Schedules											
NAT											
FTPD Setting											
FTPD Account											
IP Tunnel											
Logout											

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

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

NAT SETTINGS	
Entry Name :	<input type="text"/>
Internal IP Type :	<input type="text" value="Single IP"/>
Internal IP Address :	<input type="text"/>
External IP Type :	<input type="text" value="Single IP"/>
External IP Address :	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	FTP				
Port Forwarding	In this page, you can enable or disable the FTP server, and set the FTP port.				
DMZ	FTP SERVER SETTING				
SAMBA	FTP Server <input type="text" value="Off"/>				
3G Configuration	Enable FTP Server <input type="checkbox"/>				
Parental Control	Enable FtpServer for WAN: <input type="checkbox"/>				
Filtering Options	FTP Server Port <input type="text" value="2121"/>				
QoS Configuration	<input type="button" value="Submit"/> <input type="button" value="Cancel"/>				
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

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.

DSL-2750E //	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																	
Advanced Wireless	FTP																					
Port Forwarding	In this page, you can manage the FTP user information, such as the user name, password, and the corresponding authority.																					
DMZ	FTP USER MANAGE																					
SAMBA	User Name <input type="text"/> Password <input type="password"/> Rights <input type="checkbox"/> View <input type="checkbox"/> Upload <input type="checkbox"/> Download																					
3G Configuration	<input type="button" value="Append"/> <input type="button" value="Refresh"/>																					
Parental Control	ACCOUNT TABLE																					
Filtering Options	<table border="1"> <thead> <tr> <th rowspan="2">No.</th> <th rowspan="2">User</th> <th rowspan="2">Password</th> <th colspan="3">Rights</th> <th rowspan="2">Operation</th> </tr> <tr> <th>View</th> <th>Upload</th> <th>Download</th> </tr> </thead> <tbody> <tr> <td colspan="7"> </td> </tr> </tbody> </table>					No.	User	Password	Rights			Operation	View	Upload	Download							
No.	User	Password	Rights						Operation													
			View	Upload	Download																	
QoS Configuration																						
Firewall Settings																						
DNS																						
Dynamic DNS																						
Network Tools																						
Routing																						
Schedules																						
NAT																						
FTPD Setting																						
FTP Account																						
IP Tunnel																						
Logout																						

3.3.18 IP Tunnel

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

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	4IN6 TUNNEL CONFIGURATION				
Port Forwarding	Configure 4in6 Tunnel.				
DMZ	<input type="button" value="Configure 4in6 Tunnel"/>				
SAMBA	6IN4 TUNNEL CONFIGURATION				
3G Configuration	Configure 6in4 Tunnel.				
Parental Control	<input type="button" value="Configure 6in4 Tunnel"/>				
Filtering Options					
QoS Configuration					
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

3.3.18.1 4in6 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.

IP TUNNEL CONFIGURATION

Network topology in IPv4/v6 Internet, some only run IPv6 protocol stack P routers form the pure IPv6 backbone. However, due to the large IPv4 applications will be a period of time is still widely used, so the need for pure IPv6 backbone network to IPv4 stack border access.

IPTUNNEL

Tunnel Name	Mode	Wan interface	Port Binding	Activated	Counter
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					

DS-LITE IPV4 OVER IPV6 TUNNEL LIST

Mechanism	Dynamic	RemoteIPv6Address	ConnStatus	Select
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

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

ADD TUNNEL ITEMS

Tunnel Name:

Tunnel Mode:

Wan Interface:

Lan Interface:

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 apply and save 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.

DS-LITE IPV4 OVER IPV6 TUNNEL LIST

Mechanism:

Dynamic:

RemoteIpv6Address:

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.

3.3.18.2 6in4 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.

IP TUNNEL CONFIGURATION

6rd is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of Internet service providers.

It is derived from 6to4, a preexisting mechanism to transfer IPv6 packets over the IPv4 network, with the significant change that it operates entirely within the end-user's ISP's network, thus avoiding the major architectural problems inherent in the original design of 6to4.

IPTUNNEL

Tunnel Name	Mode	Wan interface	Lan interface	Activated	Counter
<div style="display: flex; justify-content: center; gap: 10px;"> Add Edit Delete </div>					

IPv6 RAPID DEPLOYMENT

Mechanism	Dynamic	IPv4MaskLen	Prefix	BorderRelayAddress	ConnStatus	Select
<div style="display: flex; justify-content: center; gap: 10px;"> Add Edit Delete </div>						

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

ADD TUNNEL ITEMS

Tunnel Name:

Tunnel Mode: 6in4

Wan Interface:

Lan Interface: LAN:br0

Apply Cancel

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 make the settings take effect.

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.

IPv6 RAPID DEPLOYMENT LIST

Mechanism:

Dynamic:

IPv4MaskLen:

Prefix:

BorderRelayAddress:

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.

LOGOUT

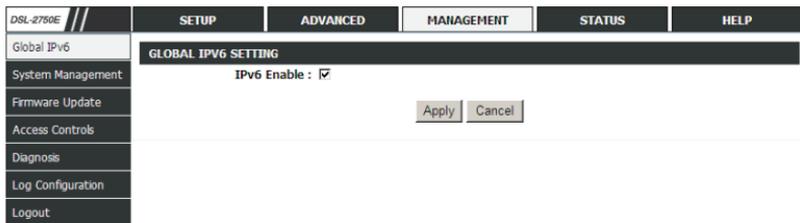
Logging out will return to the login page.

3.4 Management

In the main interface, click **Management** tab to enter the **Management** menu.

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
System Management	SYSTEM -- REBOOT				
Firmware Update	Click the button below to reboot the router.				
Access Controls	<input type="button" value="Reboot"/>				
Diagnosis	SYSTEM -- BACKUP SETTINGS				
Log Configuration	Back up configurations of the DSL router. You can save them to a file on the PC.				
Logout	<i>Note: Please always save configuration file first before viewing it.</i>				
	<input type="button" value="Backup Setting"/>				
	SYSTEM -- UPDATE SETTINGS				
	Update settings on the DSL router. You can update them using the configuration files your saved.				
	Settings file Name: <input type="text"/> <input type="button" value="Browse..."/>				
	<input type="button" value="Update Setting"/>				
	SYSTEM -- RESTORE DEFAULT SETTINGS				
	Restore settings on the DSL router to the factory defaults.				
	<input type="button" value="Restore Default Setting"/>				

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Global IPv6	FIRMWARE UPDATE				
System Management	Step 1: Obtain an updated firmware image file from your ISP.				
Firmware Update	Step 2: Enter the directory of the image file in the following field or click "Browse" to select the image file.				
Access Controls	Step 3: Click "Update Firmware" to upload the new image file.				
Diagnose	Note: The update process takes about 2 minutes. The DSL router automatically reboots after the update. Please DO NOT power off the router during the update. After click "Update Firmware", page jump before, do not click on page options.				
Log Configuration	FIRMWARE UPDATE				
Logout	Current Firmware Version: SEA_1.01 Current Version Date: 04/12/2013-18:36:48 Select File: <input type="text"/> <input type="button" value="Browse..."/> Clear Config: <input type="checkbox"/> <input type="button" value="Update Firmware"/>				

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.

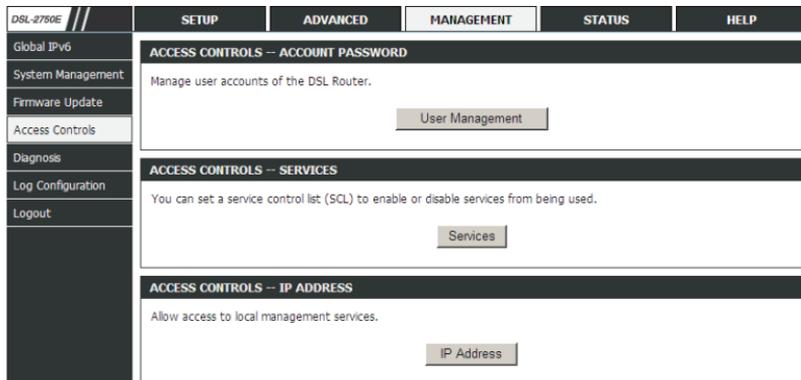
The device loads the file and reboots automatically.

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.

ACCOUNT PASSWORD

You can access the DSL Router through the accounts: admin.

Use the fields below to change or create passwords. Note: Password cannot contain a space.

ACCOUNT PASSWORD

Username:

New Username:

Current Password:

New Password:

Confirm Password:

WEB IDLE TIMEOUT SETTINGS

Web Idle Timeout:

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																																													
Global IPv6	SERVICES																																																	
System Management	You can set a service control list (SCL) to enable or disable services from being used.																																																	
Firmware Update	ACCESS CONTROL -- SERVICES																																																	
Access Controls	Interface <input type="text" value="LAN"/>																																																	
Diagnosis	<table border="1"> <thead> <tr> <th>Service</th> <th>Enable</th> <th colspan="3">Source Host(IP / Mask) : (Dst Port)</th> </tr> </thead> <tbody> <tr> <td>FTP</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="text" value="/ 0.0.0.0"/></td> <td><input type="text" value=": 21"/></td> </tr> <tr> <td>HTTP</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="text" value="/ 0.0.0.0"/></td> <td><input type="text" value=": 80"/></td> </tr> <tr> <td>ICMP</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="text" value="/ 0.0.0.0"/></td> <td><input type="text" value=": 0"/></td> </tr> <tr> <td>TELNET</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="text" value="/ 0.0.0.0"/></td> <td><input type="text" value=": 23"/></td> </tr> <tr> <td>TFTP</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="text" value="/ 0.0.0.0"/></td> <td><input type="text" value=": 69"/></td> </tr> <tr> <td>DNS</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="text" value="/ 0.0.0.0"/></td> <td><input type="text" value=": 53"/></td> </tr> <tr> <td>SAMBA1</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="text" value="/ 0.0.0.0"/></td> <td><input type="text" value=": 445"/></td> </tr> <tr> <td>SAMBA2</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0.0.0.0"/></td> <td><input type="text" value="/ 0.0.0.0"/></td> <td><input type="text" value=": 139"/></td> </tr> </tbody> </table>					Service	Enable	Source Host(IP / Mask) : (Dst Port)			FTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 21"/>	HTTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 80"/>	ICMP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 0"/>	TELNET	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 23"/>	TFTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 69"/>	DNS	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 53"/>	SAMBA1	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 445"/>	SAMBA2	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 139"/>
Service	Enable	Source Host(IP / Mask) : (Dst Port)																																																
FTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 21"/>																																														
HTTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 80"/>																																														
ICMP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 0"/>																																														
TELNET	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 23"/>																																														
TFTP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 69"/>																																														
DNS	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 53"/>																																														
SAMBA1	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 445"/>																																														
SAMBA2	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="/ 0.0.0.0"/>	<input type="text" value=": 139"/>																																														
Log Configuration	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>																																																	
Logout																																																		

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.

IP ADDRESS

If you enable the IP Address Access Control mode, IP addresses contained in the Access Control List can access the local management services. If the Access Control mode is disabled, the system does not validate IP addresses of incoming packets. Services are the system applications listed in the Service Control List.

Enter the IP address of the management station allowed to access the local management services, and click "Apply".

ACCESS CONTROL – IP ADDRESSES

Enable Access Control Mode

IP

Add

Delete

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, click **Add**. The page shown in the following figure appears.

IP ADDRESS

IP Address :

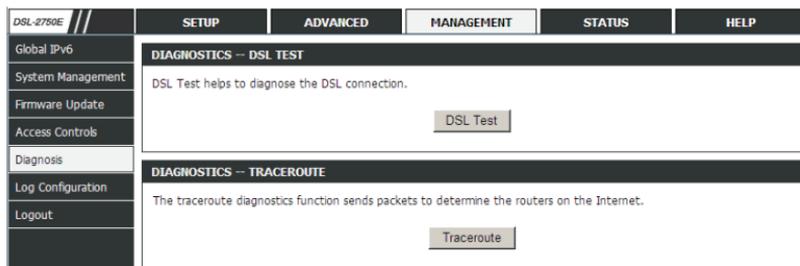
Apply

Cancel

Click **Apply** to apply the settings.

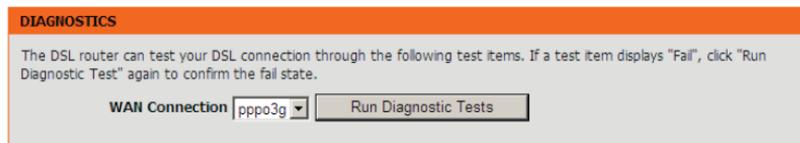
3.4.5 Diagnosis

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.

DIAGNOSTICS

The DSL router can test your DSL connection through the following test items. If a test item displays "Fail", click "Run Diagnostic Test" again to confirm the fail state.

WAN Connection

TEST THE CONNECTION TO YOUR LOCAL NETWORK

Test your LAN 1 Connection	PASS
Test your LAN 2 Connection	FAIL
Test your LAN 3 Connection	FAIL
Test your LAN 4 Connection	FAIL
Test your Wireless Connection	PASS

TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER

Test ADSL Synchronization	PASS
Test ATM OAM F5 Segment Loopback	FAIL
Test ATM OAM F5 End-to-end Loopback	FAIL
Test ATM OAM F4 Segment Loopback	FAIL
Test ATM OAM F4 End-to-end Loopback	FAIL

TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER

Ping Default Gateway	FAIL
Ping Primary Domain Name Server	FAIL

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.

TRACEROUTE DIAGNOSIS

Traceroute diagnostics sends packets to determine the routers on the Internet.

Host :	<input type="text" value="192.168.1.1"/>	
Max TTL :	<input type="text" value="30"/>	(1-64)
Wait times :	<input type="text" value="5000"/>	(>=1ms)

RESULT

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

RESULT

```
Traceroute Status: Traceroute has finished
traceroute to 192.168.1.1 (192.168.1.1), 30
hops max, 38 byte packets
 1  192.168.1.1 (192.168.1.1)  40.000 ms
0.000 ms  0.000 ms
```

3.4.6 Log Configuration

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

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Global IPv6	SYSTEM LOG				
System Management	If the log is enabled, the system starts to log all selected events. If the mode is set to "Remote", logs are sent to the specified IP address and UDP port of a remote syslog server. If the mode is set to "Local", logs are recorded in the local computer. If you set "Both", logs are saved in both the local computer and the remote syslog server.				
Firmware Update	Set the appropriate values and click "Apply" to save the settings of system log.				
Access Controls	Note: It does not work properly if the time on the modem is not properly set. In this case, please set the time of the modem in "Setup/Time and Date".				
Diagnosis					
Log Configuration					
Logout	SYSTEM LOG -- CONFIGURATION				
	<input type="checkbox"/> Enable Log Mode : Local Server IP Address : <input type="text"/> Server UDP Port : <input type="text"/>				
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="View System Log"/> <input type="button" value="View Firewall Log"/>				

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.

DSL-2730U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
System Management	LOGOUT				
Firmware Update	Logging out will return to the login page.				
Access Controls	<input type="button" value="Logout"/>				
Diagnosis					
Log Configuration					
Logout					

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Device Info	DEVICE INFO				
Wireless Clients	It indicates the current status of all the connections.				
DHCP Clients	SYSTEM INFO				
IPv6 Status	Modem Name : DSL-2750E				
Logs	Serial Number : c8d3a3eb2560				
Firewall Logs	Time and Date : 2012-05-23 06:11:54				
Statistics	Hardware Version : T1				
Route Info	Firmware Version : SEA_1.01				
Logout	System Up Time : 06:12:07				
	INTERNET INFO				
	Internet Connection Status : <input type="button" value="v"/>				
	Internet Connection Status:				
	Wan service type:				
	Default Gateway:				
	Preferred DNS Server:				
	Alternate DNS Server:				
	Downstream Line Rate (Kbps): 0				
	Upstream Line Rate (Kbps): 0				
	Data Time Counter (Second):				
	Enabled WAN Connections :				
	VPI/VCI	Service Name	Protocol	IGMP	QoS IP Address
	WIRELESS INFO				
	select wireless : <input type="button" value="v"/> D-Link				
	MAC Address: c8:d3:a3:eb:25:69				
	Status: Enable				
	Network Name (SSID): D-Link				
	Visibility: Visible				
	Security Mode: None				
	LOCAL NETWORK INFO				
	MAC Address: c8:d3:a3:eb:25:60				
	IP Address: 192.168.1.1				
	Subnet Mask: 255.255.255.0				
	DHCP Server: Disable				

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Device Info	WIRELESS CLIENTS				
Wireless Clients	This page shows authenticated wireless stations and their status.				
DHCP Clients	WIRELESS -- AUTHENTICATED STATIONS				
IPv6 Status	Mac	Associated	Authorized	SSID	Interface
Logs	<input type="button" value="Refresh"/>				
Firewall Logs					
Statistics					
Route Info					
Logout					

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).

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Device Info	DHCP CLIENTS				
Wireless Clients	It indicates the current DHCP client of your router.				
DHCP Clients	DHCP LEASES				
IPv6 Status	Hostname	MAC Address	IP Address	Expires In	
Logs	gl1886d	44:37:e6:99:43:25	192.168.1.33	40935	
Firewall Logs	<input type="button" value="Refresh"/>				
Statistics					
Route Info					
Logout					

3.5.4 IPv6 Status

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

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																								
Device Info	IPv6 STATUS																												
Wireless Clients	In this section you can see the information for the IPv6 Connection.																												
DHCP Clients	IPv6 CONNECTION																												
IPv6 Status	<table border="1"> <tr> <td>Wan Connection :</td> <td><input type="text"/></td> <td><input type="button" value="v"/></td> </tr> <tr> <td>Connection Type :</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>IPv6 Address/Prefix Len :</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>Gateway :</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>Pri Dns :</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>Sec Dns :</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>Prefix Info :</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>Status :</td> <td><input type="text"/></td> <td></td> </tr> </table>				Wan Connection :	<input type="text"/>	<input type="button" value="v"/>	Connection Type :	<input type="text"/>		IPv6 Address/Prefix Len :	<input type="text"/>		Gateway :	<input type="text"/>		Pri Dns :	<input type="text"/>		Sec Dns :	<input type="text"/>		Prefix Info :	<input type="text"/>		Status :	<input type="text"/>		
Wan Connection :	<input type="text"/>	<input type="button" value="v"/>																											
Connection Type :	<input type="text"/>																												
IPv6 Address/Prefix Len :	<input type="text"/>																												
Gateway :	<input type="text"/>																												
Pri Dns :	<input type="text"/>																												
Sec Dns :	<input type="text"/>																												
Prefix Info :	<input type="text"/>																												
Status :	<input type="text"/>																												
Logs	<input type="button" value="Refresh"/>																												
Firewall Logs																													
Statistics																													
Route Info																													
Logout																													

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP		
Device Info	LOGS						
Wireless Clients	This page allows you to view system logs.						
DHCP Clients	SYSTEM LOG						
IPv6 Status	<table border="1"> <tr> <td style="height: 200px;"></td> <td><input type="button" value="v"/></td> </tr> </table>					<input type="button" value="v"/>	
	<input type="button" value="v"/>						
Logs	<input type="button" value="Refresh"/>						
Firewall Logs							
Statistics							
Route Info							
Logout							

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.

The screenshot shows the DSL-2750E web interface. At the top, there are tabs for SETUP, ADVANCED, MANAGEMENT, STATUS, and HELP. The STATUS tab is selected. On the left, a navigation menu lists various options: Device Info, Wireless Clients, DHCP Clients, IPv6 Status, Logs, Firewall Logs (selected), Statistics, Route Info, and Logout. The main content area is titled 'FIREWALLLOGS' and contains the text 'In this page, you can view firewall logs.' Below this is a section titled 'FIREWALL LOG' which contains a table with the following headers: TimeStamp, SourceIP-DestIP, Protocol, port, and target. The table is currently empty. At the bottom of the page, there is a 'Refresh' button.

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																																																																																																									
Device Info	STATISTICS																																																																																																													
Wireless Clients	It indicates the current status of all the connections.																																																																																																													
DHCP Clients	LOCAL NETWORK & WIRELESS																																																																																																													
IPv6 Status	<table border="1"> <thead> <tr> <th rowspan="2">interface</th> <th colspan="4">Received</th> <th colspan="4">Transmitted</th> </tr> <tr> <th>Data</th> <th>Pkts</th> <th>Errs</th> <th>Rx drop</th> <th>Data</th> <th>Pkts</th> <th>Errs</th> <th>Tx drop</th> </tr> </thead> <tbody> <tr> <td>LAN2</td> <td>2.75MB</td> <td>13816</td> <td>0</td> <td>0</td> <td>5.31MB</td> <td>13085</td> <td>0</td> <td>0</td> </tr> <tr> <td>D-Link</td> <td>36.78MB</td> <td>247652</td> <td>0</td> <td>0</td> <td>14.48MB</td> <td>41610</td> <td>0</td> <td>0</td> </tr> </tbody> </table>					interface	Received				Transmitted				Data	Pkts	Errs	Rx drop	Data	Pkts	Errs	Tx drop	LAN2	2.75MB	13816	0	0	5.31MB	13085	0	0	D-Link	36.78MB	247652	0	0	14.48MB	41610	0	0																																																																						
interface	Received				Transmitted																																																																																																									
	Data	Pkts	Errs	Rx drop	Data	Pkts	Errs	Tx drop																																																																																																						
LAN2	2.75MB	13816	0	0	5.31MB	13085	0	0																																																																																																						
D-Link	36.78MB	247652	0	0	14.48MB	41610	0	0																																																																																																						
Logs	INTERNET																																																																																																													
Firewall Logs	<table border="1"> <thead> <tr> <th rowspan="2">Service</th> <th rowspan="2">VPI/VCI</th> <th rowspan="2">Protocol</th> <th colspan="4">Received</th> <th colspan="4">Transmitted</th> </tr> <tr> <th>Data</th> <th>Pkts</th> <th>Errs</th> <th>Drops</th> <th>Data</th> <th>Pkts</th> <th>Errs</th> <th>Drops</th> </tr> </thead> <tbody> <tr> <td colspan="11"> </td> </tr> </tbody> </table>					Service	VPI/VCI	Protocol	Received				Transmitted				Data	Pkts	Errs	Drops	Data	Pkts	Errs	Drops																																																																																						
Service	VPI/VCI	Protocol	Received						Transmitted																																																																																																					
			Data	Pkts	Errs	Drops	Data	Pkts	Errs	Drops																																																																																																				
Statistics	ADSL																																																																																																													
Route Info	<table border="1"> <tbody> <tr> <td>Mode:</td> <td colspan="4">0</td> </tr> <tr> <td>Type:</td> <td colspan="4">0</td> </tr> <tr> <td>Line Coding:</td> <td colspan="4">Enable</td> </tr> <tr> <td>Status:</td> <td colspan="4">Disabled</td> </tr> <tr> <td>Up Time:</td> <td colspan="4"> </td> </tr> <tr> <td> </td> <td colspan="2">Downstream</td> <td colspan="2">Upstream</td> </tr> <tr> <td>SNR Margin (0.1dB):</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Attenuation (0.1dB):</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Output Power (dBm):</td> <td>0.0</td> <td>0.0</td> <td>0.0</td> <td>0.0</td> </tr> <tr> <td>Attainable Rate (Kbps):</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Rate (Kbps):</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>D (interleave depth):</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Delay (msec):</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Data Counter:</td> <td>0</td> <td>Clear</td> <td>0</td> <td>Clear</td> </tr> <tr> <td>HEC Errors:</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>OCD Errors:</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>LCD Errors:</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>CRC Errors:</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>FEC Errors:</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Total ES</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Total Frames</td> <td>0</td> <td>510</td> <td>0</td> <td>0</td> </tr> </tbody> </table>					Mode:	0				Type:	0				Line Coding:	Enable				Status:	Disabled				Up Time:						Downstream		Upstream		SNR Margin (0.1dB):	0	0	0	0	Attenuation (0.1dB):	0	0	0	0	Output Power (dBm):	0.0	0.0	0.0	0.0	Attainable Rate (Kbps):	0	0	0	0	Rate (Kbps):	0	0	0	0	D (interleave depth):	0	0	0	0	Delay (msec):	0	0	0	0	Data Counter:	0	Clear	0	Clear	HEC Errors:	0	0	0	0	OCD Errors:	0	0	0	0	LCD Errors:	0	0	0	0	CRC Errors:	0	0	0	0	FEC Errors:	0	0	0	0	Total ES	0	0	0	0	Total Frames	0	510	0	0
Mode:	0																																																																																																													
Type:	0																																																																																																													
Line Coding:	Enable																																																																																																													
Status:	Disabled																																																																																																													
Up Time:																																																																																																														
	Downstream		Upstream																																																																																																											
SNR Margin (0.1dB):	0	0	0	0																																																																																																										
Attenuation (0.1dB):	0	0	0	0																																																																																																										
Output Power (dBm):	0.0	0.0	0.0	0.0																																																																																																										
Attainable Rate (Kbps):	0	0	0	0																																																																																																										
Rate (Kbps):	0	0	0	0																																																																																																										
D (interleave depth):	0	0	0	0																																																																																																										
Delay (msec):	0	0	0	0																																																																																																										
Data Counter:	0	Clear	0	Clear																																																																																																										
HEC Errors:	0	0	0	0																																																																																																										
OCD Errors:	0	0	0	0																																																																																																										
LCD Errors:	0	0	0	0																																																																																																										
CRC Errors:	0	0	0	0																																																																																																										
FEC Errors:	0	0	0	0																																																																																																										
Total ES	0	0	0	0																																																																																																										
Total Frames	0	510	0	0																																																																																																										
Logout																																																																																																														

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.

DSL-2750E	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																					
Device Info	ROUTE INFO																									
Wireless Clients	Flags: U - up, I - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).																									
DHCP Clients	DEVICE INFO -- ROUTE																									
IPv6 Status	<table border="1"> <thead> <tr> <th>Destination</th> <th>Gateway</th> <th>Subnet Mask</th> <th>Flags</th> <th>Metric</th> <th>Service</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td>192.168.1.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td>0</td> <td>br0</td> </tr> <tr> <td>192.168.10.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td>0</td> <td>br1</td> </tr> </tbody> </table>					Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br0	192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	br1
Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface																				
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br0																				
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	br1																				
Logs																										
Firewall Logs																										
Statistics																										
Route Info																										
Logout																										

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.

LOGOUT
Logging out will return to the login page.
<input type="button" value="Logout"/>

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	HELP MENU				
Setup	<ul style="list-style-type: none">• Setup• Advanced• Management• Status				
Advanced					
Maintenance					
Status	SETUP HELP				
Support	<ul style="list-style-type: none">• Wizard• Internet Setup• Wireless• Local Network• Time and Date				
	ADVANCED HELP				
	<ul style="list-style-type: none">• Advanced Wireless• Port Forwarding• DMZ• Parental Control• Filtering Options• Firewall Settings• DNS• DDNS• Network Tools• Routing• Schedules				
	MANAGEMENT HELP				
	<ul style="list-style-type: none">• System Management• Firmware Update• Access Controls• Diagnosis• Log Configuration				
	STATUS HELP				
	<ul style="list-style-type: none">• Device Info• Wireless Clients• DHCP Clients• Logs• Statistics• Route Info				