

D-Link DSL-2750U

Wireless N ADSL2+ Modem Router



D-Link®
Building Networks for People



RECYCLABLE

2013/03/21

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	5
2	Hardware Installation	6
2.1	DSL Uplink Connection	6
2.2	Ethernet Uplink Connection	7
3	Web Configuration	8
3.1	Accessing the Device	8
3.2	Setup	9
3.2.1	Wizard	9
3.2.2	Internet Setup	16
3.2.3	Wireless	24
3.2.4	Local Network	31
3.2.5	LAN IPv6	34
3.2.6	Time and Date	35
3.2.7	Logout	36
3.3	Advanced	36
3.3.1	Advanced Wireless	36
3.3.2	Port Forwarding	43
3.3.3	DMZ	44
3.3.4	3G Configuration	45
3.3.5	Parental Control	53
3.3.6	Filtering Options	56
3.3.7	QoS Configuration	61
3.3.8	Firewall Settings	64
3.3.9	DNS	65
3.3.10	Dynamic DNS	66
3.3.11	Network Tools	68
3.3.12	Routing	75
3.3.13	Schedules	80
3.3.14	NAT	81

3.3.15	FTPD Setting	82
3.3.16	FTPD Account	82
3.3.17	IP Tunnel	83
3.3.18	Logout	87
3.4	Management.....	87
3.4.1	Global IPv6	88
3.4.2	System Management.....	88
3.4.3	Firmware Update	90
3.4.4	Access Controls.....	91
3.4.5	Diagnosis	94
3.4.6	Log Configuration	96
3.4.7	Logout.....	97
3.5	Status.....	98
3.5.1	Device Info	98
3.5.2	Wireless Clients	99
3.5.3	DHCP Clients	99
3.5.4	IPv6 Status.....	99
3.5.5	Logs	100
3.5.6	Firewall Logs.....	101
3.5.7	Statistics.....	101
3.5.8	Route Info	102
3.5.9	Logout.....	103
3.6	Help	103

1 Introduction

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

The device supports WLAN access, such as WLAN AP or WLAN device, to the Internet. It complies with specifications of IEEE 802.11, 802.11b/g/n, WEP, WPA, and WPA2 security. The WLAN of the device supports 2T2R.

1.1 Packing List

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

1.2 Safety Precautions

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

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

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

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

1.3 LEDs and Interfaces

Note:

The figures in this document are for reference only.

Front Panel



Figure 1 Front panel

The following table describes the LEDs of the device.

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

LED	Color	Status	Description
 WLAN	Green	Blinks	Data is transmitted through the WLAN interface.
		On	The connection of WLAN interface is normal.
		Off	The WLAN connection is not established.
 WPS	Blue	Blinks	WPS negotiation is enabled, waiting for the clients.
		Off	WPS negotiation is not enabled on the device.
 USB	Green	On	The connection of 3G or USB flash disk has been established.
		Blinking	Data is being transmitted.
		Off	The connection of 3G or USB flash disk is not established.
 DSL	Green	Off	Initial self-test is failed.
		Blinks	The device is detecting itself.
		On	Initial self-test of the unit has passed and is ready.
 Internet	Green	Off	The device is under the Bridge mode, DSL connection is not present, or the power is off.
		Blinks	Internet data is being transmitted in the routing mode.
		On	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.
LAN/WAN	This Ethernet RJ-45 interface has two functions. ● Worked as a WAN interface that connects to the WAN for Ethernet uplink ● Worked as a LAN interface that connects to the Ethernet interfaces of computers or Ethernet devices.
LAN3/2/1	Ethernet RJ-45 interfaces that connect to the Ethernet interfaces of computers or Ethernet devices.
USB	USB port, for connecting the 3G network card or other USB storage devices.
WPS	Press the button for 1 second to enable WPS function.
WIRELESS ON/OFF	Press the button silently to enable WLAN function.
ON/OFF	Power on or off the device.
12V DCIN	Interface that connects to the power adapter. The power adapter output is: 12 V DC 1A.
Reset (on the bottom case)	Reset to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for 1 second and then release.

1.4 System Requirements

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

1.5 Features

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- Leased line mode
- 1483B, 1483R, and MER access
- Multiple PVCs (eight at most) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Binding of ports with PVCs
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and 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.

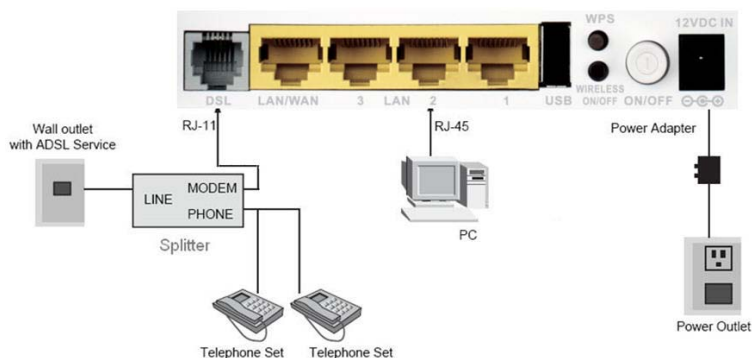


Figure 3 Connection diagram

2.2 Ethernet Uplink Connection

- Step 1** Connect the LAN interface of the wireless router to your PC with RJ45 Ethernet cable.
- Step 2** Connect the WAN interface of the wireless router to the uplink network device with RJ45 Ethernet cable.
- Step 3** Connect the power adapter to the power socket of the wireless router.
- Figure 4 displays the Ethernet uplink connection.

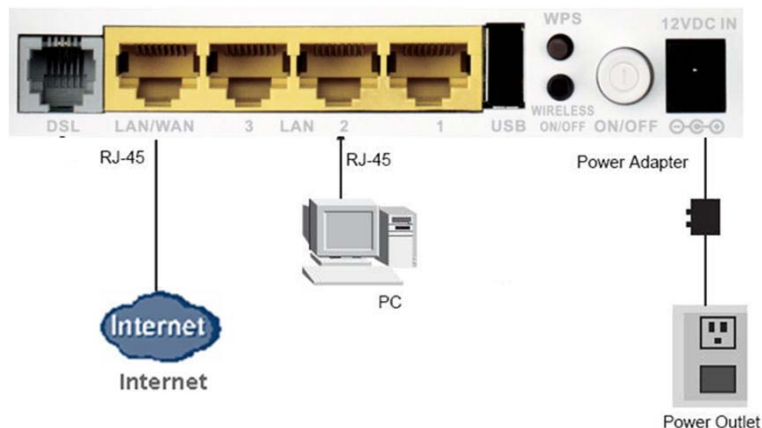


Figure 4 Connection diagram in the mode of Ethernet uplink connection

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

Product Page: DSL-2750U Firmware Version: ME_1.06

D-Link

LOGIN

Input username and password

Username :

Password :

☐ Remember my login info. on this computer

Login

BROADBAND

If you log in as the super user successfully, the page shown in the following figure appears.



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

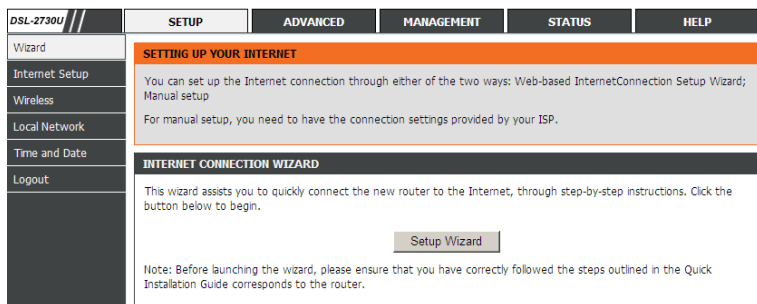
3.2 Setup

In the main interface, click **Setup** tab to enter the **Setup** menu as shown in the following figure. The submenus are **Wizard**, **Internet Setup**, **Wireless**, **Local Network**, **LAN IPv6**, **Time and Date** and **Logout**.

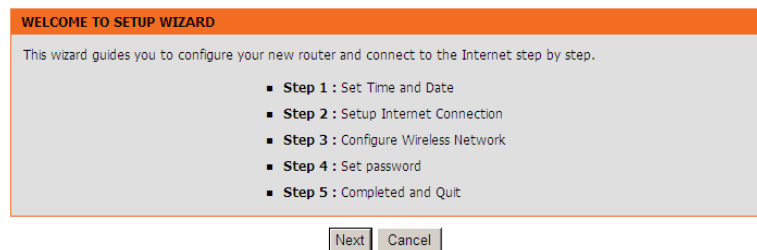
3.2.1 Wizard

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.

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



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



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

Step 1 Set the time and date.

STEP 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.

There are two WAN access types: **Ethernet Uplink** and **DSL Uplink**. Choose one according to your needs.

If the internet service you subscribed is **PPPoE** or **PPPoA**, you can choose the **Protocol** to be **PPPoE** or **PPPoA**. Set the VPI and VCI. Enter the user name and password provided by your ISP.

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

If you want to change WAN access type, you can click on "Ethernet" or "DSL".

note : If you select the WAN access type is "Ethernet", Please send line to LAN1 port!

When search available PVC, according to different condition, need the time is different!

WAN Access Type : ☐ Ethernet ☒ DSL

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

Protocol : PPPoE

Encapsulation Mode: LLC

VPI : 0 (0-255)

VCI : 35 (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 :

If the internet service you subscribed is **Dynamic IP**, you can choose **Protocol** to be **Dynamic IP**. The page shown in the following figure appears.

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

If you want to change WAN access type, you can click on "Ethernet" or "DSL".

note : If you select the WAN access type is "Ethernet", Please send line to LAN1 port!

When search available PVC, according to different condition, need the time is different!

WAN Access Type : ☐ Ethernet ☒ DSL

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

Protocol : Dynamic IP

Encapsulation Mode: LLC

VPI : 0 (0-255)

VCI : 35 (32-65535)

Search Available PVC : Scan

Back Next Cancel

If the Protocol is **Bridge**, the page shown in the following figure appears.

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

If you want to change WAN access type, you can click on "Ethernet" or "DSL".

note : If you select the WAN access type is "Ethernet", Please send line to LAN1 port!

When search available PVC, according to different condition, need the time is different!

WAN Access Type : ☐ Ethernet ☒ DSL

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

Protocol : Bridge

Encapsulation Mode: LLC

VPI : 0 (0-255)

VCI : 35 (32-65535)

Search Available PVC : Scan

Back Next Cancel

If the Protocol is **Static IP**, the page shown in the following figure appears.

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

If you want to change WAN access type, you can click on "Ethernet" or "DSL".

note : If you select the WAN access type is "Ethernet", Please send line to LAN1 port!

When search available PVC, according to different condition, need the time is different!

WAN Access Type : ☐ Ethernet ☒ DSL

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

Protocol :

Encapsulation Mode:

VPI : (0-255)

VCI : (32-65535)

Search Available PVC :

STATIC IP

You have selected Static IP Internet connection. Please enter the appropriate information as provided by your ISP.

To guarantee the performance of the auto PVC scan feature, please enter the information of VPI/VCI numbers if your ISP has provided it.

Click Next to continue.

IP Address :

Subnet Mask :

Default Gateway :

Primary DNS Server :

Enter the **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS Server** provided by your ISP.

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

Note:

If you select the WAN access type to be **Ethernet**, Please connected the LAN/WAN port of the 2750U to WAN uplink port of the modem through Ethernet cable. When search available PVC, according to different condition, need the time is different!

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.

None	Security Level		Best
☒ None	☐ WEP	☐ WPA-PSK	☐ WPA2-PSK

Security Mode: None

Select this option if you do not wish to enable any security features.

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

STEP 4: ACCOUNT PASSWORD → 5

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

ACCOUNT PASSWORD

Username:

Current Password:

New Password:

Confirm Password:

Step 4 Change or create the password of an account. 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 :	2012-05-23T04:30:46
Daylight Saving Time :	disable
wan_type	DSL
VPI / VCI :	0/35
Protocol :	PPPoE
Connection Type :	VCMUX
Username :	test
Password :	test
Wireless Network Name (SSID) :	D-Link
Visibility Status :	visible
Encryption :	None
Pre-Shared Key :	not set!
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

- **WAN Access Type: DSL**

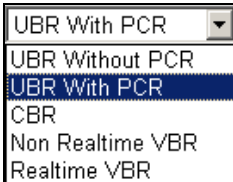
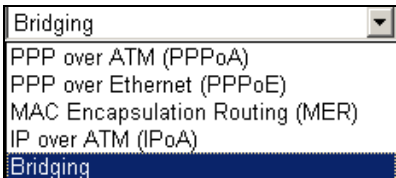
Choose **Setup > Internet Setup**. The page shown in the following figure appears. Choose **WAN Access Type** to be **DSL**. In this page, you can configure the WAN interface of the device.

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP									
Wizard	INTERNET SETUP													
Internet Setup	Choose "Add", "Edit", or "Delete" to configure WAN interfaces.													
Wireless	If you want to change WAN access type, you can click on "Ethernet" or "DSL".													
Local Network	note : If you select the WAN access type is "Ethernet", Please send line to LAN4 port!													
LAN IPv6	WAN Access Type : ☐ Ethernet ☒ DSL													
Time and Date	DSL SETUP													
Logout	<table border="1"> <thead> <tr> <th>VPI/VCI</th> <th>VLAN ID</th> <th>ENCAP</th> <th>Service Name</th> <th>Protocol</th> <th>State</th> <th>Status</th> <th>Backup3G</th> <th>Action</th> </tr> </thead> <tbody> </tbody> </table>					VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Backup3G	Action
VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Backup3G	Action						
	ETHERNET SETUP													
	<table border="1"> <thead> <tr> <th>VLAN ID</th> <th>Service Name</th> <th>Protocol</th> <th>State</th> <th>Status</th> <th>Action</th> </tr> </thead> <tbody> </tbody> </table>					VLAN ID	Service Name	Protocol	State	Status	Action			
VLAN ID	Service Name	Protocol	State	Status	Action									
	Add Edit Delete													

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

DSL-2750U	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 : 0 (0-255) VCI : 35 (32-65535) Service Category : UBR With PCR Peak Cell Rate : 0 (cells/s) Sustainable Cell Rate : 0 (cells/s) Maximum Burst Size : 0 (cells)				
Time and Date	CONNECTION TYPE				
Logout	Protocol : Bridging Encapsulation Mode : LLC 802.1Q VLAN ID : 0 (0 = disable, 1 - 4094) Priority : 0 (0 - 7) Firewall Enable : ☒ ☐ Enable Proxy Arp				
	Enable Bridge Service : ☒ Service Name : br_0_35_0_1				
	Apply Cancel				

The following table describes the parameters in this page.

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

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

● WAN Access Type: Ethernet

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

Note:

If you select the WAN access type to be **Ethernet**, Please connected the LAN/WAN port of the **2750U** to WAN uplink port of the modem through Ethernet cable.

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																											
Wizard	INTERNET SETUP																															
Internet Setup	Choose "Add", "Edit", or "Delete" to configure WAN interfaces.																															
Wireless	If you want to change WAN access type, you can click on "Ethernet" or "DSL".																															
Local Network	note : If you select the WAN access type is "Ethernet", Please send line to LAN4 port!																															
LAN IPv6	WAN Access Type : ☒ Ethernet ☐ DSL																															
Time and Date	DSL SETUP																															
Logout	<table border="1"> <thead> <tr> <th>VPI/VCI</th> <th>VLAN ID</th> <th>ENCAP</th> <th>Service Name</th> <th>Protocol</th> <th>State</th> <th>Status</th> <th>Backup3G</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="9">ETHERNET SETUP</td> </tr> <tr> <td>VLAN ID</td> <td>Service Name</td> <td>Protocol</td> <td>State</td> <td>Status</td> <td colspan="4">Action</td> </tr> </tbody> </table>					VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Backup3G	Action	ETHERNET SETUP									VLAN ID	Service Name	Protocol	State	Status	Action			
VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Backup3G	Action																								
ETHERNET SETUP																																
VLAN ID	Service Name	Protocol	State	Status	Action																											
Add Edit Delete																																

Click **Add** to go to the next page. Choose Protocol to be **PPP over Ethernet (PPPoE)** in this page.

- **PPPoE**

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	INTERNET SETUP				
Internet Setup	In this page, you can configure an Ethernet-LAN identifier and select a service category.				
Wireless	CONNECTION TYPE				
Local Network	Protocol : PPP over Ethernet (PPPoE)				
LAN IPv6	802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)				
Time and Date	PPP USERNAME AND PASSWORD				
Logout	PPP Username : PPP Password : Confirm PPP Password : Authentication Method : AUTO Dial-up mode : AlwaysOn Inactivity Timeout : 100 (Seconds [0-65535]) MRU Size : 1492 (576~1492) Keep Alive : ☒ Lcp Echo Interval (sec) : 30 Lcp Echo Failure : 5 Use Static IP Address : ☐ IP Address :				
	NETWORK ADDRESS TRANSLATION SETTINGS				
	Enable NAT : ☒ NAT Type : Full Cone Nat Enable WAN Service : ☒ Service Name : pppoe_0_0				
	Apply Cancel				

The following table describes the parameters of this page

Field	Description
Protocol	It displays the protocol type used for this WAN connection.
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.
PPP Username	The correct user name provided by your ISP.
PPP Password	The correct password provided by your ISP
Authentication	To authenticate whether the PPP username and

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

- **Dynamic IP**

Choose Protocol to be **Dynamic IP**, and the following page appears.

INTERNET SETUP

In this page, you can configure an Ethernet-LAN identifier and select a service category.

CONNECTION TYPE

Protocol :

802.1Q VLAN ID : (0 = disable, 1 - 4094)

NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT : ☒

NAT Type :

Enable WAN Service : ☒

Service Name :

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

- **Static IP**

Choose Protocol to be **Static IP**, and the following page appears.

INTERNET SETUP

In this page, you can configure an Ethernet-LAN identifier and select a service category.

CONNECTION TYPE

Protocol :

802.1Q VLAN ID : (0 = disable, 1 - 4094)

WAN IP SETTINGS

WAN IP Address :

WAN Subnet Mask :

Default gateway :

Preferred DNS server :

Alternate DNS server :

NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT : ☒

NAT Type :

Enable WAN Service : ☒

Service Name :

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 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.

- Bridging

Choose Protocol to be **Bridging**, and the following page appears.
It is recommended to keep the settings as default.

INTERNET SETUP	
In this page, you can configure an Ethernet-LAN identifier and select a service category.	
CONNECTION TYPE	
Protocol :	Bridging
802.1Q VLAN ID :	0 (0 = disable, 1 - 4094)
NETWORK ADDRESS TRANSLATION SETTINGS	
Enable Bridge Service :	☒
Service Name :	br_0_0
Apply Cancel	

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-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Wizard	WIRELESS SETTINGS -- WIRELESS BASIC				
Internet Setup	Configure your wireless basic settings.				
Wireless	Wireless Basic				
Local Network	WIRELESS SETTINGS -- WIRELESS SECURITY				
LAN IPv6	Configure your wireless security settings.				
Time and Date	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.

SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
WIRELESS BASIC				
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 NETWORK SETTINGS				
Enable Wireless: ☒ Enable MultiAP Isolation: ☐ Wireless Network Name (SSID) : D-Link Visibility Status : ☒ Visible ☐ Invisible Country/Region : United Arab Emirates Control Sideband: Upper Wireless Channel : Auto Scan 802.11 Mode : 802.11b/g/n Band Width : 40 M 				
Remember your SSID as you will need to configure the same settings on your wireless devices and PC.				
Apply Cancel				

The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select this to turn Wi-Fi on.
Enable MultiAP Isolation	Select this to turn MultiAP isolation on.
Wireless Network Name (SSID)	The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.
Visibility Status	Select Visible , the SSID can be detected. Select

Field	Description
	Invisible , the SSID cannot be detected.
Country	Select the country 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 **QRcode** on the right of the page. This QRcode can help your cellphone connect to the wireless network of **DSL-2750U** automatically by shooting the QRcode with this cellphone.

Note:

A cellphone can not connect to the wireless network by taking photo of QRcode unless installing a QRcode software.

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 :

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

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

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

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	- 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-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
------------------	--------------	-----------------	-------------------	---------------	-------------

[Wizard](#)
[Internet Setup](#)
[Wireless](#)
[Local Network](#)
[LAN IPv6](#)
[Time and Date](#)
[Logout](#)

LOCAL NETWORK

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.

ROUTER SETTINGS

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.

Router IP Address :

Subnet Mask :

Domain Name :

☒ Configure the second IP Address and Subnet Mask for LAN

IP Address :

Subnet Mask :

DHCP SETTINGS (OPTIONAL)

In this page, you can configure the built-in DHCP server to assign IP addresses to the computers on your network.

☒ Enable DHCP Server

DHCP IP Address Range : to

DHCP IP Mask :

DHCP Router IP :

DHCP Lease Time : (seconds)

DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address
Add	Edit	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 :	☐
Computer Name :	
IP Address :	
MAC Address :	

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-2750U	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	STATIC LAN IPV6 ADDRESS CONFIGURATION				
Local Network	IPv6 Interface Address fe80::1				
LAN IPv6	DHCPV6 CONFIGURATION				
Time and Date	Enable DHCPv6 Server ☒ LAN address config mode ☒ Stateless ☐ Stateful Start Interface ID 33 End Interface ID 254 DHCPv6 Lease Time 43200 Use the following DNS server addresses. Get DNS Servers from WAN ☒ Static DNS Servers ☐ Static IPv6 DNS Servers 2111:3c:123:0:c:135:9a:a				
Logout	SITE PREFIX CONFIGURATION				
	Enable RADVD ☒ Auto get prefix from WAN ☒ Static ☐ Site Prefix				
	Apply 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-2750U	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	☐ Automatically synchronize with Internet time server Primary NTP time server: ntp1.dlink.com Secondary NTP time server: Manual setup time: 2012 Year 05 Mon 23 Day 07 Hour 50 Min 24 Sec				
LAN IPv6	TIME CONFIGURATION				
Time and Date	Time Zone: (GMT+04:00) Abu Dhabi, Muscat, Dubai ☒ 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	Apply 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.

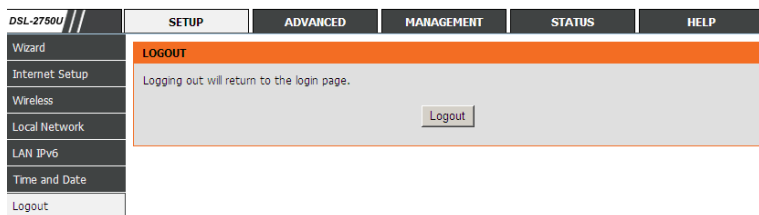
Select **Automatically adjust clock for daylight saving changes** if necessary.

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-2750U	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	ADVANCED WIRELESS -- MAC FILTERING				
3G Configuration	You can configure wireless firewall by denying or allowing designated MAC addresses.				
Parental Control	MAC Filtering				
Filtering Options	ADVANCED WIRELESS -- SECURITY SETTINGS				
QoS Configuration	You can configure security features of the wireless LAN interface.				
Firewall Settings	Security Settings				
DNS	ADVANCED WIRELESS -- WPS SETTING				
Dynamic DNS	You can configure the wireless WPS.				
Network Tools	WPS Setting				
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

3.3.1.1 Advanced Settings

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

DSL-2750U	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 : Auto Multicast Rate : Lower Transmit Power : 100% Beacon Period : 100 (20 ~ 1000) RTS Threshold : 2346 (256 ~ 2346) Fragmentation Threshold : 2345 (256 ~ 2346) DTIM Interval : 1 (1 ~ 255) Preamble Type : long				
3G Configuration	SSID				
Parental Control	Enable Wireless : ☒ Wireless Network Name (SSID) : D-Link Visibility Status : ☒ Visible ☐ Invisible User Isolation : Off WMM Advertise : On Max Clients : 16 (1 ~ 32)				
Filtering Options	GUEST/VIRTUAL ACCESS POINT-1				
QoS Configuration	Enable Wireless Guest Network : ☐ Guest SSID : D-link_GUEST1 Visibility Status : ☒ Visible ☐ Invisible User Isolation : Off WMM Advertise : On Max Clients : 16 (1 ~ 32)				
Firewall Settings	GUEST/VIRTUAL ACCESS POINT-2				
DNS	Enable Wireless Guest Network : ☐ Guest SSID : D-link_GUEST2 Visibility Status : ☒ Visible ☐ Invisible User Isolation : Off WMM Advertise : On Max Clients : 16 (1 ~ 32)				
Dynamic DNS	GUEST/VIRTUAL ACCESS POINT-3				
Network Tools	Enable Wireless Guest Network : ☐ Guest SSID : D-link_GUEST3 Visibility Status : ☒ Visible ☐ Invisible User Isolation : Off WMM Advertise : On Max Clients : 16 (1 ~ 32)				
Routing	Apply Cancel				
Schedules					
NAT					
FTPD Setting					
FTPD 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.

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

Click **Apply** to save the settings.

3.3.1.2 MAC Filtering

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

The screenshot shows a web interface for MAC Address Access Control. At the top, there is an orange header bar with the text "MAC ADDRESS". Below this, a grey box contains the following 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." and "Enter the MAC address of the management station permitted to access this route, and click 'Apply'". Below the grey box is a dark grey header bar with the text "ACCESS CONTROL -- MAC ADDRESSES". The main content area has a checkbox labeled "Enable Access Control Mode". Below the checkbox is a text input field labeled "MAC Address". At the bottom of the form 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 web interface for adding a MAC address. At the top, there is a dark grey header bar with the text "MAC ADDRESS". Below this, the text "MAC Address :" is followed by a text input field. At the bottom of the form 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 : 12345670

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.

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP			
Advanced Wireless	PORT FORWARDING							
Port Forwarding	Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured. Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the Internal Port Start or Internal Port End is not recommended. If the External Port Start or the External Port End changes, the Internal Port Start or Internal Port End automatically changes accordingly.							
DMZ	PORT FORWARDING SETUP							
SAMBA	Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
3G Configuration	Add Edit 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 a virtual server.

PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

WAN Connection(s) :

Server Name :

☒ Select a Service :

☐ Custom Server :

Schedule : [View Available Schedules](#)

Server IP Address(Host Name) :

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

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

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

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

Click **Apply** to save the settings.

3.3.3 DMZ

DMZ is the abbreviation of the Demilitarized Zone. Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible

to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

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

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	DMZ 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. Enter IP address of the computer and click "Apply" to enable the DMZ host. Clear the field of the IP address and click "Apply" to disable the DMZ host.				
Port Forwarding					
DMZ					
SAMBA					
3G Configuration					
Parental Control	DMZ HOST WAN Connection : v Enable DMZ : ☐ DMZ Host IP Address : Apply Cancel				
Filtering Options					
QoS Configuration					
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

Click **Apply** to save the settings.

3.3.4 3G Configuration

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

Note:

It will take over 2 minutes for 2750U to connect the 3G network..

- **3G card without PIN protect**

If the 3G card has no PIN protect function, the page will be shown as the following figure appears.

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP								
Advanced Wireless	Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.												
Port Forwarding	When you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.												
DMZ	3G Status: Ready Inform: CONNECTED, Auto Dialed												
SAMBA													
3G 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>Connected</td> <td>☐</td> <td>undial</td> </tr> </tbody> </table>	Service Name	Protocol	State	Status	Default Gateway	Action	ppp3g	PPPo3G	1	Connected	☐	undial
Service Name	Protocol	State	Status	Default Gateway	Action								
ppp3g	PPPo3G	1	Connected	☐	undial								
Parental Control	Add Edit Delete Pin Manage DongleInfo												
Filtering Options													
QoS Configuration													
Firewall Settings													
DNS													
Dynamic DNS													
Network Tools													
Routing													
Schedules													
NAT													
FTPD Setting													
FTPD Account													
IP Tunnel													
Logout													

Figure 5 Main page

● 3G card with PIN protect

If the 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-2750U User Manual

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP								
Advanced Wireless	Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.												
Port Forwarding	When you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.												
DMZ	3G Status: NeedPinCode Inform: NEED PIN CODE!												
SAMBA													
3G Configuration	<table><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>☐</td><td> dial </td></tr></tbody></table>	Service Name	Protocol	State	Status	Default Gateway	Action	pppo3g	PPPo3G	1	Disconnected	☐	dial
Service Name	Protocol	State	Status	Default Gateway	Action								
pppo3g	PPPo3G	1	Disconnected	☐	dial								
Parental Control	Add Edit Delete Pin Manage DongleInfo												
Filtering Options													
QoS Configuration													
Firewall Settings													
DNS													
Dynamic DNS													
Network Tools													
Routing													
Schedules													
NAT													
FTPD Setting													
FTPD Account													
IP Tunnel													
Logout													

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

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	THE 3G CONFIGURATION				
Port Forwarding	In this page, you can configure the PIN code of the SIM card.				
DMZ	sim card's status is : NEED PIN CODE				
SAMBA	Unlock with PIN code				
3G Configuration	Enter PIN code: Remain times:3				
Parental Control	Apply Cancel				
Filtering Options					
QoS Configuration					
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

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

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	PIN ACTION RESULT:				
Port Forwarding	Action is OK!				
DMZ					
SAMBA					
3G Configuration					
Parental Control					
Filtering Options					
QoS Configuration					
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

3 seconds later, the page will automatically skip to the following page. You can choose to enable or disable the Pin protect function of the 3G card, or change the Pin code.

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	THE 3G CONFIGURATION				
Port Forwarding	In this page, you can configure the PIN code of the SIM card.				
DMZ	sim card's status is : lock enable				
SAMBA	Disable PIN protect ☒				
3G Configuration	Change PIN code ☐				
Parental Control	Enter PIN code: Remain times:3				
Filtering Options	Apply Cancel				
QoS Configuration					
Firewall Settings					
ONS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

- 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 protect function is remain effective.

- Disable PIN Protect

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

PIN ACTION RESULT:
Action is OK!

This page indicates that the PIN protect function is disabled.

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

● Edit an Existing 3G Configuration

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

Note:

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

DSL-2750U User Manual

DSL-2750U //	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP												
Advanced Wireless	Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.																
Port Forwarding	When you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.																
DMZ	3G Status: Ready Inform: DISCONNECT																
SAMBA																	
3G 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>☐</td><td>dial</td></tr></tbody></table>					Service Name	Protocol	State	Status	Default Gateway	Action	pppo3g	PPPo3G	1	Disconnected	☐	dial
Service Name	Protocol	State	Status	Default Gateway	Action												
pppo3g	PPPo3G	1	Disconnected	☐	dial												
Parental Control	Add Edit Delete Pin Manage DongleInfo																
Filtering Options																	
QoS Configuration																	
Firewall Settings																	
DNS																	
Dynamic DNS																	
Network Tools																	
Routing																	
Schedules																	
NAT																	
FTPD Setting																	
FTPD Account																	
IP Tunnel																	
Logout																	

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

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	3G INTERNET SETUP				
Port Forwarding	This screen allows you to configure a 3G Internet connection.				
DMZ	3G USB SETUP				
SAMBA	Enable 3G Service : ☒				
3G Configuration	Country: Bahrain				
Parental Control	Profile Name: Batelco				
Filtering Options	Account:				
QoS Configuration	Password:				
Firewall Settings	Dial_Number: *99#				
DNS	Net Type: Auto				
Dynamic DNS	APN: internet.batelco.c				
Network Tools	OnDemand: ☐				
Routing	Inactivity Timeout: 0 (Seconds [40-65535]. But if 0, we will set default)				
Schedules	Backup delay time: 60 (Seconds [0-600])				
NAT	Recovery delay time: 60 (Seconds [0-600])				
FTPD Setting	Initialization Delay time: 20 (If too small, some 3g dongle will be unsupported)				
FTPD Account	Mode Switch Delay time: 20 (If too small, some 3g dongle will be unsupported)				
IP Tunnel	BackupMechanism: DSL				
Logout	Checking IP address: 8.8.8.8				
	Timeout (in sec.): 1				
	Period time (in sec.): 1				
	Fail Tolerance: 1				
	Apply AutoSet Cancel				

The following table describes the parameters of this page.

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

Field	Description
Delay Time	

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

3.3.5 Parental Control

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

DSL-2750U	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.

3.3.5.1 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.

BLOCK WEBSITE

URL

Schedule

Add

Edit

Delete

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

ADD SCHEDULE RULEURL :
☒ **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)

Apply

Cancel

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

	URL	Schedule
☐	www.xxx.com	Always

Add

Edit

Delete

3.3.5.2 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

BLOCK MAC ADDRESS--BLACKLIST

Username	MAC	Schedule

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 : 44:37:e6:99:43:25
☒ Other MAC Address :

☒ Schedule : always [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**.

3.3.6 Filtering Options

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

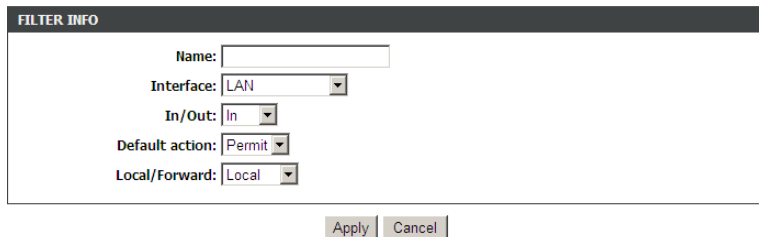
DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	FILTERING OPTIONS -- IP FILTERING				
Port Forwarding	Uses IP address to implement filtering.				
DMZ	IP Filtering				
SAMBA	FILTERING OPTIONS -- BRIDGE FILTERING				
3G Configuration	Uses MAC address to implement filtering. Useful only 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					

3.3.6.1 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.



The screenshot shows a web interface titled "FILTER INFO" in a dark header. Below the header, there are five configuration fields, each with a label and a value in a dropdown menu:

- Name: [Empty text box]
- Interface: [LAN]
- In/Out: [In]
- Default action: [Permit]
- Local/Forward: [Local]

At the bottom right of the form area, there are two buttons: "Apply" and "Cancel".

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: ☐	
Protocol: ALL	
IP Version Type: IPv4	
Action: Permit	
DSCP:	
Packet Length: - (1~65535)	
SOURCE SETTING	
IP Address:	
PrefixLength/Mask:	
DESTINATION SETTING	
FQDN Enabled ☐	
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

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

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

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

Add Filter

Edit Filter

Delete Filter

RULE

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

Add Rule

Edit Rule

Delete Rule

3.3.6.2 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.

Field	Description
Source MAC Address	The MAC address of sender of the message.
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.

3.3.7 QoS Configuration

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

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	QOS GLOBAL OPTIONS				
Port Forwarding	Configure QoS global options.				
DMZ	Configure QoS Global Options				
SAMBA	QOS QUEUE CONFIGURATION				
3G Configuration	Configure QoS Queue.				
Parental Control	Configure QoS Queue				
Filtering Options	QOS CLASSIFICATION CONFIGURATION				
QoS Configuration	Configure QoS Classification.				
Firewall Settings	Configure QoS Classification				
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

3.3.7.1 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

3.3.7.2 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	☒	1	WAN	Delete
2	UP_Q_4	☒	2	WAN	Delete
3	UP_Q_5	☒	3	WAN	Delete
4	UP_Q_6	☒	4	WAN	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.

3.3.7.3 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

Add Classification Rule

LIST

Classify Number	Enable	Classify Condition	Classify Mark	Classify Queue	Operation

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

Advanced Wireless

Port Forwarding

DMZ

Parental Control

Filtering Options

QoS Configuration

Firewall Settings

DNS

Dynamic DNS

Network Tools

Routing

Schedules

Logout

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

Submit
Refresh

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

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

3.3.8 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-2750U	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 ☐				
3G Configuration	Icmp Echo ☒				
Parental Control	Fraggle ☒				
Filtering Options	Echo Chargin ☒				
QoS Configuration	IP Land ☒				
Firewall Settings	Port Scan ☒				
DNS	TCP Flags: Set "SYN FIN" ☒				
Dynamic DNS	TCP Flags: Set "SYN RST" ☒				
Network Tools	TCP Flags: Set "FIN RST" ☒				
Routing	TCP DoS : ☒				
Schedules	TCP DoS Max Rate: 50 (packets/second)				
NAT	Apply Cancel				
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

Click **Apply** to save the settings.

3.3.9 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.

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Advanced Wireless	DNS				
Port Forwarding	Click "Apply" to save the configuration. If you want to make the DNS effective immediately, Please ensure that the WAN connection is the default gateway connection. You can change the default gateway connection in the "Advanced->routing->default gateway" page./p>				
DMZ	DNS SERVER CONFIGURATION				
SAMBA	Wan Connection : ppp3g				
3G Configuration	☒ Obtain DNS server address automatically ☐ Use the following DNS server addresses				
Parental Control	Primary DNS server :				
Filtering Options	Secondary DNS server :				
QoS Configuration	☒ Obtain IPv6 DNS server address automatically ☐ Use the following IPv6 DNS server addresses				
Firewall Settings	Preferred IPv6 DNS server :				
DNS	Alternate IPv6 DNS server :				
Dynamic DNS	Apply Cancel				
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

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.

3.3.10 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 (DynDNS.org or dlinkddns.com).

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

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
------------------	--------------	-----------------	-------------------	---------------	-------------

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
Logout

DYNAMIC DNS

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.

DYNAMIC DNS

Hostname	Username	Service	Interface
Add Edit Delete			

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

ADD DYNAMIC DNS

DDNS provider : dlinkddns.com
Hostname :
Interface : ppp3g
Username :
Password :

Apply
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

Field	Description
	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.

3.3.11 Network Tools

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

DSL-2750U	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	NETWORK TOOLS -- IGMP PROXY				
3G Configuration	Transmission of identical content, such as multimedia, from a source to a number of recipients.				
Parental Control	IGMP Proxy				
Filtering Options	NETWORK TOOLS -- IGMP SNOOPING				
QoS Configuration	Transmission of identical content, such as multimedia, from a source to a number of recipients.				
Firewall Settings	IGMP Snooping				
DNS	NETWORK TOOLS -- MLD CONFIGURATION				
Dynamic DNS	Transmission of identical content, such as multimedia, from a source to a number of recipients.				
Network Tools	MLD Configuration				
Routing	NETWORK TOOLS -- UPNP				
Schedules	Allows you to enable or disable UPnP.				
NAT	Upnp				
FTPD Setting	NETWORK TOOLS -- ADSL				
FTPD Account	Allows you to configure advanced settings for ADSL.				
IP Tunnel	ADSL				
Logout	NETWORK TOOLS -- SNMP				
	Network Tools -- SNMP				
	SNMP				

3.3.11.1 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
☐ 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.

3.3.11.2 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 : IGMP V2

Port Binding Lan1

Enable FastLeaving : ☐

General Query Interval : 150 (seconds)

General Query Response Interval: 20 (*100 milliseconds)

Group Query Interval : 325 (seconds)

Group Query Response Interval: 20 (*100 milliseconds)

Group Query Count : 3

Last Member Query Interval : 1 (seconds)

Last Member Query Count : 0

Apply
Cancel

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.

3.3.11.3 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 :

Apply

Cancel

3.3.11.4 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

Apply

Cancel

3.3.11.5 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.

3.3.11.6 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**
- 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.

3.3.11.7 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

3.3.12 Routing

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

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

3.3.12.1 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 interface. Then, click "Apply" to add the entry to the routing table.

A maximum 3 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 :

Apply

cancel

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.

3.3.12.2 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
--------	-------------	-----------

Add

Edit

Delete

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

IPv6 STATIC ROUTE ADD

Enable : ☐

Destination Network Address :

Use Interface :

Apply

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.

3.3.12.3 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 :choose one Wanconnection and one Lanconnection then bind them.

POLICY ROUTE SETUP

WAN

LAN

Add

Delete

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

WAN INSTANCE AND LAN INSTANCEWAN Connection LAN Connection

Apply

Cancel

3.3.12.4 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 GATEWAYAssigned the Default Gateway : **IPv6 DEFAULT GATEWAY**Assigned the IPv6 Default Gateway :

Apply

Cancel

Click **Apply** to save the settings.

3.3.12.5 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	☐	☐
Lan1	-	1 ▼	Active	☐	☐

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.

3.3.12.6 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
ppp3g		☐

Click **Apply** to save the settings.

3.3.13 Schedules

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

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP					
Advanced Wireless	SCHEDULES									
Port Forwarding	You can use schedule to create scheduling rules to be applied for your firewall. Maximum number of schedule rules: 20									
DMZ	SCHEDULE RULES									
SAMBA	Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop time
3G Configuration	Add Edit 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 :	: minute, 24 hour time)
End Time :	: minute, 24 hour time)
Apply Cancel	

Click **Apply** to save the settings.

3.3.14 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-2750U	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											
3G Configuration	NAT TABLES										
Parental Control	<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"> Add Edit Delete </td> </tr> </tbody> </table>					Name	Internal IP Address	External IP Address	Add Edit Delete		
Name	Internal IP Address	External IP Address									
Add Edit Delete											
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 an NAT server. The page shown in the following figure appears.

NAT SETTINGS	
Entry Name :	
Internal IP Type :	Single IP
Internal IP Address :	
External IP Type :	Single IP
External IP Address :	
Apply Cancel	

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

3.3.15 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-2750U	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 ☐ Off ☒ On				
3G Configuration	Enable FTP Server ☐				
Parental Control	Enable FtpServer for WAN: ☐				
Filtering Options	FTP Server Port 2121				
QoS Configuration	Submit Cancel				
Firewall Settings					
DNS					
Dynamic DNS					
Network Tools					
Routing					
Schedules					
NAT					
FTPD Setting					
FTPD Account					
IP Tunnel					
Logout					

3.3.16 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.

FTP

In this page, you can manage the FTP user information, such as the user name, password, and the corresponding authority.

FTP USER MANAGE

User Name

Password

Rights ☐ View ☐ Upload ☐ Download

ACCOUNT TABLE

No.	User	Password	Rights			Operation
			View	Upload	Download	

3.3.17 IP Tunnel

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

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

3.3.17.14in6 Tunnel

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

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.

IP TUNNEL

Tunnel Name	Mode	Wan interface	Port Binding	Activated	Counter
Add Edit Delete					

DS-LITE IPV4 OVER IPV6 TUNNEL LIST

Mechanism	Dynamic	RemoteIPv6Address	ConnStatus	Select
Add Edit Delete				

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

ADD TUNNEL ITEMS

Tunnel Name:
 Tunnel Mode:
 Wan Interface:
 Lan Interface:

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 enable the settings.

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

DS-LITE IPV4 OVER IPV6 TUNNEL LIST

Mechanism: DualStackLite

Dynamic: 0

RemoteIPv6Address:

Apply

Cancel

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.

3.3.17.2 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.

IP TUNNEL

Tunnel Name	Mode	Wan interface	Lan interface	Activated	Counter
-------------	------	---------------	---------------	-----------	---------

[Add](#) [Edit](#) [Delete](#)

IPv6 RAPID DEPLOYMENT

Mechanism	Dynamic	IPv4MaskLen	Prefix	BorderRelayAddress	ConnStatus	Select
-----------	---------	-------------	--------	--------------------	------------	--------

[Add](#) [Edit](#) [Delete](#)

Click **Add** below the table **IP TUNNEL** 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 enable the settings.

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

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.

3.3.18 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.

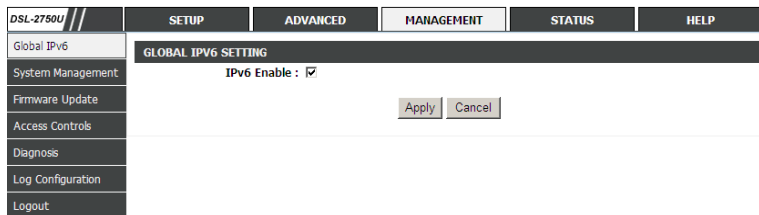
3.4 Management

In the main interface, click **Management** tab to enter the **Management** menu as shown in the following figure. The submenus are **Global IPv6**, **System**

Management, Firmware Update, Access Controls, Diagnosis, Log Configuration and Logout.

3.4.1 Global IPv6

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



3.4.2 System Management

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

DSL-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
System Management	SYSTEM -- REBOOT				
Firmware Update	Click the button below to reboot the router.				
Access Controls	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>				
	Backup Setting				
	SYSTEM -- UPDATE SETTINGS				
	Update settings on the DSL router. You can update them using the configuration files your saved.				
	Settings file Name: Browse...				
	Update Setting				
	SYSTEM -- RESTORE DEFAULT SETTINGS				
	Restore settings on the DSL router to the factory defaults.				
	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-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Global IPv6	FIRMWARE UPDATE Step 1: Obtain an updated firmware image file from your ISP. Step 2: Enter the directory of the image file in the following field or click "Browse" to select the image file. Step 3: Click "Update Firmware" to upload the new image file. 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.				
System Management					
Firmware Update					
Access Controls					
Diagnosis					
Log Configuration					
Logout	FIRMWARE UPDATE Current Firmware Version: ME_1.06 Current Version Date: 03/02/2013-18:43:48 Select File: Browse ... Clear Config: ☐ 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.

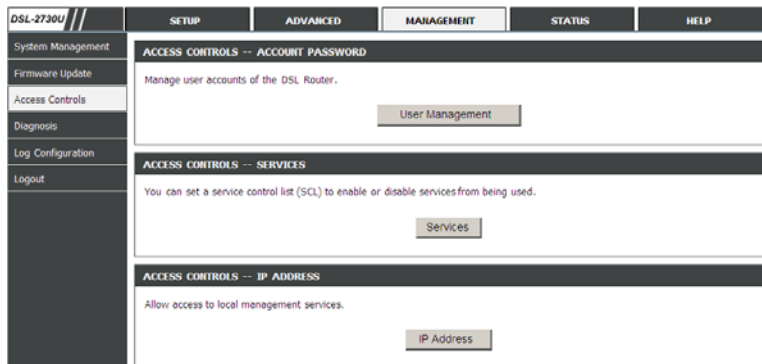
The device loads the file and reboots automatically.

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 Account Password

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:

Apply

Cancel

WEB IDLE TIMEOUT SETTINGS

Web Idle Timeout:

Apply

Cancel

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.

SERVICES

You can set a service control list (SCL) to enable or disable services from being used.

ACCESS CONTROL -- SERVICES

Select WAN Connections

Service

Port Binding

WAN

WAN Access Source Host(IP / Mask) :(Dst Port)

Apply

Cancel

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

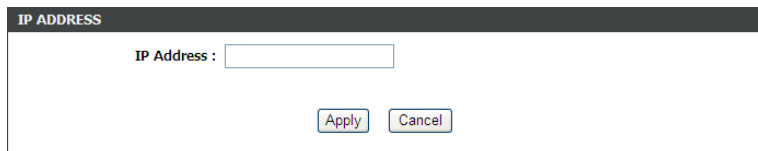
Delete

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.

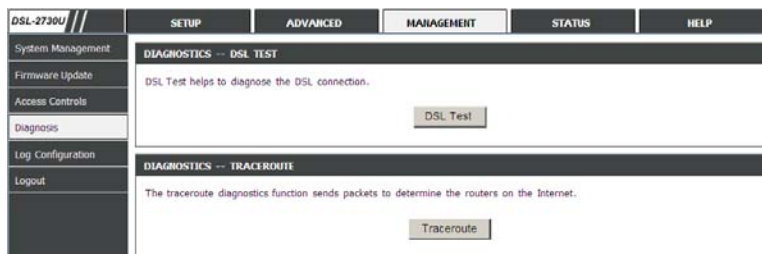
To add an IP address to the IP list, click **Add**. The page shown in the following figure appears.



Click **Apply** to apply the settings.

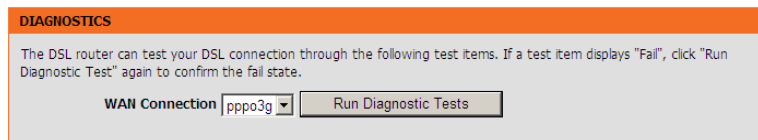
3.4.5 Diagnosis

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 : 192.168.1.1

Max TTL : 30 (1-64)

Wait times : 5000 (>=1ms)

Traceroute

Stop

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-2750U	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. Set the appropriate values and click "Apply" to save the settings of system log. 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."				
Firmware Update	SYSTEM LOG -- CONFIGURATION				
Access Controls	☐ Enable Log Mode : Local Server IP Address : Server UDP Port :				
Diagnosis	Apply Cancel View System Log View Firewall Log				
Log Configuration					
Logout					

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-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
System Management	LOGOUT				
Firmware Update	Logging out will return to the login page. Logout				
Access Controls					
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-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																								
Device Info	DEVICE INFO																												
Wireless Clients	It indicates the current status of all the connections.																												
DHCP Clients																													
IPv6 Status	SYSTEM INFO																												
Logs	Modem Name : DSL-2750U Serial Number : 001ee306cd93 Time and Date : 2012-05-23 03:41:10 Hardware Version : U1 Firmware Version : ME_1.06 System Up Time : 03:41:22																												
Firewall Logs	INTERNET INFO																												
Statistics	Internet Connection Status : ppp3g																												
Route Info	Internet Connection Status: Disconnected Wan service type: Internet Default Gateway: Preferred DNS Server: Alternate DNS Server: Data Time Counter (Second):																												
Logout	Enabled WAN Connections : <table border="1"> <thead> <tr> <th>VPI/VCI</th> <th>Service Name</th> <th>Protocol</th> <th>IGMP</th> <th>QoS</th> <th>IP Address</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </tbody> </table>					VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address																		
VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address																								
	WIRELESS INFO																												
	select wireless : D-Link																												
	MAC Address: 00:1e:e3:06:cd:9c Status: Enable Network Name (SSID): D-Link Visibility: Visible Security Mode: None																												
	LOCAL NETWORK INFO																												
	MAC Address: 00:1e:e3:06:cd:93 IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0 DHCP Server: Enable																												

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-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP										
Device Info	WIRELESS CLIENTS														
Wireless Clients	This page shows authenticated wireless stations and their status.														
DHCP Clients															
IPv6 Status	WIRELESS -- AUTHENTICATED STATIONS														
Logs	<table><tr><td>Mac</td><td>Associated</td><td>Authorized</td><td>SSID</td><td>Interface</td></tr><tr><td>c4:6a:b7:3e:66:7f</td><td>Connected</td><td>None</td><td>D-Link</td><td>wlan0</td></tr></table>					Mac	Associated	Authorized	SSID	Interface	c4:6a:b7:3e:66:7f	Connected	None	D-Link	wlan0
Mac	Associated	Authorized	SSID	Interface											
c4:6a:b7:3e:66:7f	Connected	None	D-Link	wlan0											
Firewall Logs	Refresh														
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-2750U	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																
Device Info	DHCP CLIENTS																				
Wireless Clients	It indicates the current DHCP client of your router.																				
DHCP Clients																					
IPv6 Status	DHCP LEASES																				
Logs	<table><tr><th>Hostname</th><th>MAC Address</th><th>IP Address</th><th>Expires In</th></tr><tr><td>gj1886d</td><td>44:c37:e6:99:43:25</td><td>192.168.1.33</td><td>24731</td></tr><tr><td>android-ddc5b2e466e338f9</td><td>c4:6a:b7:3e:66:7f</td><td>192.168.1.34</td><td>41474</td></tr><tr><td>shousho</td><td>7c:c5:37:97:d7:dd</td><td>192.168.1.36</td><td>41406</td></tr></table>					Hostname	MAC Address	IP Address	Expires In	gj1886d	44:c37:e6:99:43:25	192.168.1.33	24731	android-ddc5b2e466e338f9	c4:6a:b7:3e:66:7f	192.168.1.34	41474	shousho	7c:c5:37:97:d7:dd	192.168.1.36	41406
Hostname	MAC Address	IP Address	Expires In																		
gj1886d	44:c37:e6:99:43:25	192.168.1.33	24731																		
android-ddc5b2e466e338f9	c4:6a:b7:3e:66:7f	192.168.1.34	41474																		
shousho	7c:c5:37:97:d7:dd	192.168.1.36	41406																		
Firewall Logs																					
Statistics																					
Route Info																					
Logout	Refresh																				

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

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-2750U //	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Device Info	LOGS This page allows you to view system logs.				
Wireless Clients					
DHCP Clients	SYSTEM LOG 				
IPv6 Status					
Logs					
Firewall Logs					
Statistics					
Route Info					
Logout					
	Refresh				

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.

DSL-2750U

SETUP ADVANCED MANAGEMENT STATUS HELP

Device Info

Wireless Clients

DHCP Clients

IPv6 Status

Logs

Firewall Logs

Statistics

Route Info

Logout

FIREWALL LOGS

In this page, you can view firewall logs.

FIREWALL LOG

TimeStamp	SourceIP-DestIP	Protocol	port	target
-----------	-----------------	----------	------	--------

Refresh

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-2750U	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>LAN1</td> <td>752.04KB</td> <td>5886</td> <td>0</td> <td>0</td> <td>2.09MB</td> <td>9100</td> <td>0</td> <td>0</td> </tr> <tr> <td>D-Link</td> <td>52.24MB</td> <td>462584</td> <td>0</td> <td>0</td> <td>23.81MB</td> <td>78071</td> <td>0</td> <td>0</td> </tr> </tbody> </table>					Interface	Received				Transmitted				Data	Pkts	Errs	Rx drop	Data	Pkts	Errs	Tx drop	LAN1	752.04KB	5886	0	0	2.09MB	9100	0	0	D-Link	52.24MB	462584	0	0	23.81MB	78071	0	0																																																																											
Interface	Received				Transmitted																																																																																																														
	Data	Pkts	Errs	Rx drop	Data	Pkts	Errs	Tx drop																																																																																																											
LAN1	752.04KB	5886	0	0	2.09MB	9100	0	0																																																																																																											
D-Link	52.24MB	462584	0	0	23.81MB	78071	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>ppp3g</td> <td></td> <td>PPPOE</td> <td>0KB</td> <td></td> <td></td> <td></td> <td>0KB</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>					Service	VPI/VCI	Protocol	Received				Transmitted				Data	Pkts	Errs	Drops	Data	Pkts	Errs	Drops	ppp3g		PPPOE	0KB				0KB																																																																																			
Service	VPI/VCI	Protocol	Received						Transmitted																																																																																																										
			Data	Pkts	Errs	Drops	Data	Pkts	Errs	Drops																																																																																																									
ppp3g		PPPOE	0KB				0KB																																																																																																												
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 colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>Attenuation (0.1dB):</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>Output Power (dBm):</td> <td colspan="2">0.0</td> <td colspan="2">0.0</td> </tr> <tr> <td>Attainable Rate (Kbps):</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>Rate (Kbps):</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>D (interleave depth):</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>Delay (msec):</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>Data Counter:</td> <td colspan="2">0</td> <td>Clear</td> <td>0</td> </tr> <tr> <td></td> <td colspan="2"></td> <td></td> <td>Clear</td> </tr> <tr> <td>HEC Errors:</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>OCD Errors:</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>LCD Errors:</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>CRC Errors:</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>FEC Errors:</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>Total ES</td> <td colspan="2">0</td> <td colspan="2">0</td> </tr> <tr> <td>Total Frames</td> <td colspan="2">0</td> <td colspan="2">510</td> </tr> </tbody> </table>					Mode:	0				Type:	0				Line Coding:	Enable				Status:	Disabled				Up Time:						Downstream		Upstream		SNR Margin (0.1dB):	0		0		Attenuation (0.1dB):	0		0		Output Power (dBm):	0.0		0.0		Attainable Rate (Kbps):	0		0		Rate (Kbps):	0		0		D (interleave depth):	0		0		Delay (msec):	0		0		Data Counter:	0		Clear	0					Clear	HEC Errors:	0		0		OCD Errors:	0		0		LCD Errors:	0		0		CRC Errors:	0		0		FEC Errors:	0		0		Total ES	0		0		Total Frames	0		510	
Mode:	0																																																																																																																		
Type:	0																																																																																																																		
Line Coding:	Enable																																																																																																																		
Status:	Disabled																																																																																																																		
Up Time:																																																																																																																			
	Downstream		Upstream																																																																																																																
SNR Margin (0.1dB):	0		0																																																																																																																
Attenuation (0.1dB):	0		0																																																																																																																
Output Power (dBm):	0.0		0.0																																																																																																																
Attainable Rate (Kbps):	0		0																																																																																																																
Rate (Kbps):	0		0																																																																																																																
D (interleave depth):	0		0																																																																																																																
Delay (msec):	0		0																																																																																																																
Data Counter:	0		Clear	0																																																																																																															
				Clear																																																																																																															
HEC Errors:	0		0																																																																																																																
OCD Errors:	0		0																																																																																																																
LCD Errors:	0		0																																																																																																																
CRC Errors:	0		0																																																																																																																
FEC Errors:	0		0																																																																																																																
Total ES	0		0																																																																																																																
Total Frames	0		510																																																																																																																
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-2750U //	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP																												
Device Info	ROUTE INFO Flags: U - up, I - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).																																
Wireless Clients																																	
DHCP Clients																																	
IPv6 Status																																	
Logs	DEVICE INFO -- ROUTE <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>10.167.64.80</td> <td>0.0.0.0</td> <td>255.255.255.248</td> <td>U</td> <td>0</td> <td>0</td> <td>br0</td> </tr> <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	10.167.64.80	0.0.0.0	255.255.255.248	U	0	0	br0	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																											
10.167.64.80	0.0.0.0	255.255.255.248	U	0	0	br0																											
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																											
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.
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-2750U //	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
Menu	HELP MENU				
Setup	• Setup • Advanced • Management • Status				
Advanced					
Maintenance					
Status	SETUP HELP				
Support	• Wizard • Internet Setup • Wireless • Local Network • Time and Date				
	ADVANCED HELP				
	• Advanced Wireless • Port Forwarding • DMZ • Parental Control • Filtering Options • Firewall Settings • DNS • DDNS • Network Tools • Routing • Schedules				
	MANAGEMENT HELP				
	• System Management • Firmware Update • Access Controls • Diagnosis • Log Configuration				
	STATUS HELP				
	• Device Info • Wireless Clients • DHCP Clients • Logs • Statistics • Route Info				