D-Link DSL-2730E

Wireless N 150 ADSL2+ Modem Router

User Manual

D-Link®
Building Networks for People

RECYCLABLE

2013/04/12

Ver. 1.00

Contents

1 Introduction 1
1.1 Packing List 1
1.2 Safety Precautions 1
1.3 LEDs and Interfaces 2
1.4 System Requirements 4
1.5 Features 4
2 Hardware Installation 6
3 Web Configuration 7
3.1 Accessing the Device 7
3.2 Setup 9
3.2.1 Wizard 9
3.2.2 Local Network 15
3.2.3 Internet Setup 24
3.2.4 Wireless Setup 31
3.2.5 Time and Date 36
3.3 Advanced 37
3.3.1 Advanced Wireless 38
3.3.2 Access Control List 43
3.3.3 Port Triggering 46
3.3.4 Port Forwarding 48
3.3.5 DMZ 49
3.3.6 Parental Control 49
3.3.7 Filtering Options 52
3.3.8 DoS Settings 55
3.3.9 DNS 56
3.3.10 Dynamic DNS 58
3.3.11 Network Tools 60
3.3.12 Routing 72
3.3.13 NAT 76
3.4 Maintenance 80
3.4.1 System 80
3.4.2 Firmware Update 82
3.4.3 Password 82

3.4.4 Diagnostics 83
3.4.5 System Log 86
3.4.6 Logout 88
3.5 Status 88
3.5.1 Device Info 88
3.5.2 Wireless Clients 90
3.5.3 DHCP Clients 90
3.5.4 ADSL Driver 91
3.5.5 Statistics 91
3.5.6 Route Info 92
3.6 Help 93

1 Introduction

The DSL-2730E 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 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 1T1R.

1.1 Packing List

- 1 x DSL-2730E
- 1 x external splitter
- 1 x power adapter
- 1 x telephone cables (RJ-11)
- 1 x Ethernet cable (RJ-45)
- 1 x QIG

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.
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

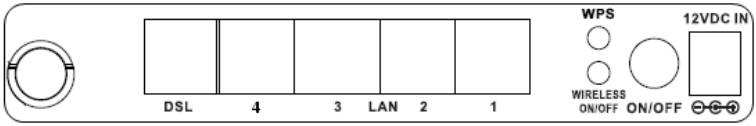


Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
	Antenna position
DSL	RJ-11 interface that connects to the telephone set through the telephone cable.
LAN4/3/2/1	Ethernet RJ-45 interfaces that connect to the Ethernet interfaces of computers or Ethernet devices.
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: 12V DC, 500mA.
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 installed on your PC
- A hub or switch (attached to several PCs through one of Ethernet interfaces on the device)
- Operating system: Windows Vista, Windows 7, Windows 98SE, Windows 2000, Windows ME or Windows XP
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or Firefox 1.5 or higher

1.5 Features

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

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

2 Hardware Installation

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

The splitter has three ports:

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

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

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

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

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

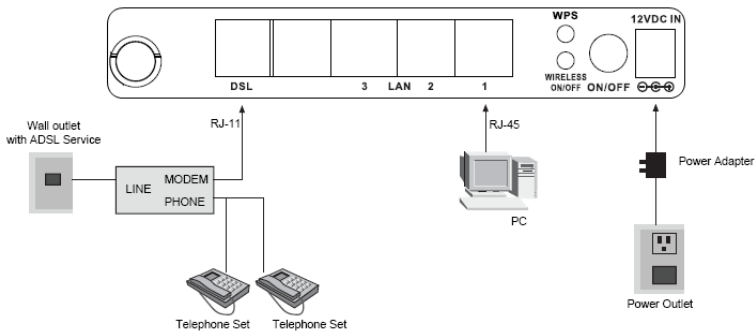


Figure 3 Connection diagram

3 Web Configuration

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

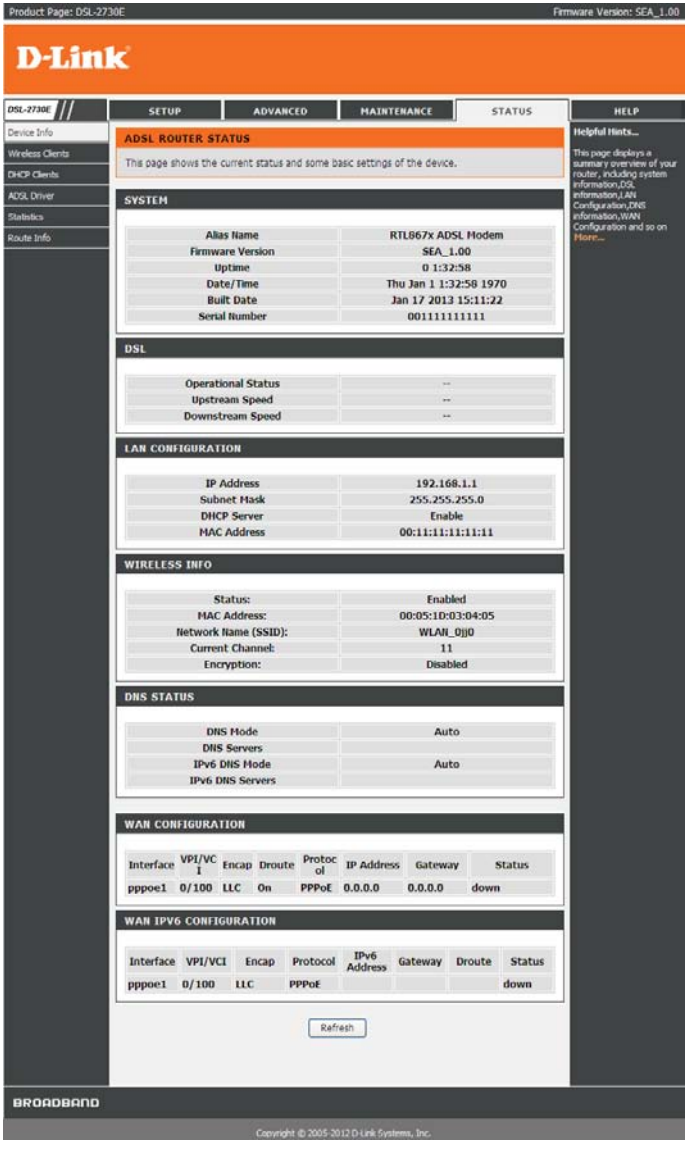
3.1 Accessing the Device

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

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

Step 2 The **Login** page shown in the following figure appears. Enter the user name and password. The user name and password of the super user are **admin** and **admin**.

If you log in as the super user successfully, the page shown in the following figure appears. This page displays a summary overview of the router, including the system information, DSL information, LAN Configuration, DNS information and WAN Configuration.


Product Page: DSL-2730E
Firmware Version: SEA_1.00
D-Link
DSL-2730E
SETUP
ADVANCED
MAINTENANCE
STATUS
HELP
Device Info
Wireless Clients
DHCP Clients
ADSL Driver
Statistics
Route Info
ADSL ROUTER STATUS
This page shows the current status and some basic settings of the device.
SYSTEM
Alias Name RTL867x ADSL Modem
Firmware Version SEA_1.00
Uptime 0 1:32:58
Date/Time Thu Jan 1 1:32:58 1970
Built Date Jan 17 2013 15:11:22
Serial Number 001111111111
DSL
Operational Status --
Upstream Speed --
Downstream Speed --
LAN CONFIGURATION
IP Address 192.168.1.1
Subnet Mask 255.255.255.0
DHCP Server Enable
MAC Address 00:11:11:11:11:11
WIRELESS INFO
Status: Enabled
MAC Address: 00:05:1D:03:04:05
Network Name (SSID): WLAN_0jj0
Current Channel: 11
Encryption: Disabled
DNS STATUS
DNS Mode Auto
DNS Servers
IPv6 DNS Mode Auto
IPv6 DNS Servers
WAN CONFIGURATION
Interface VPI/VCI Encap Droute Protocol IP Address Gateway Status
pppoe1 0/100 LLC On PPPoE 0.0.0.0 0.0.0.0 down
WAN IPV6 CONFIGURATION
Interface VPI/VCI Encap Protocol IPv6 Address Gateway Droute Status
pppoe1 0/100 LLC PPPoE down
Refresh
Helpful Hints...
This page displays a summary overview of your router, including system information,DSL information,LAN Configuration,DNS information,WAN Configuration and so on
More...
BROADBAND
Copyright © 2005-2012 D-Link Systems, Inc.

3.2 Setup

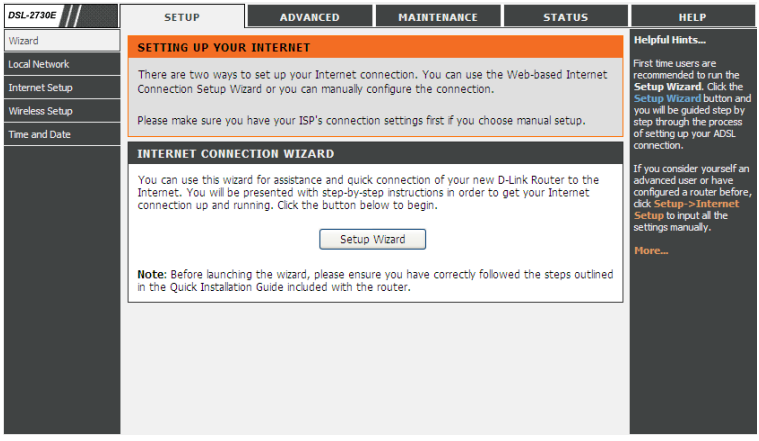
In the main interface, click **Setup** tab to enter the **Setup** menu as shown in the following figure. The submenus are **Wizard**, **Local Network**, **Internet Setup**, **Wireless Setup** and **Time and Date**.

3.2.1 Wizard

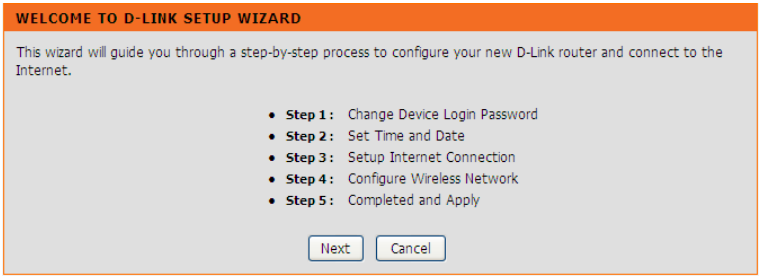
Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe configuration parameters. When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Your physical WAN device 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 that you are connected to the Internet using a static or dynamic IP address, and the protocol you use to communicate over the Internet, i.e. PPPoA or PPPoE.

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

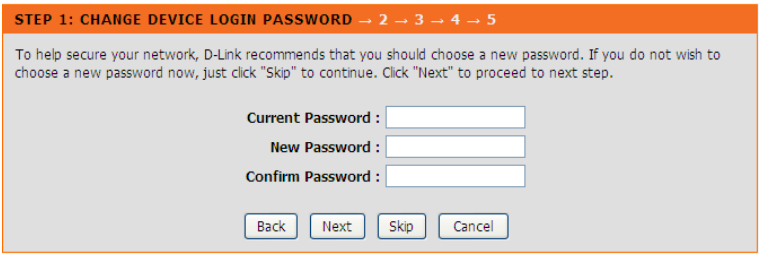


Click **Setup Wizard**. The page shown in the following figure appears.

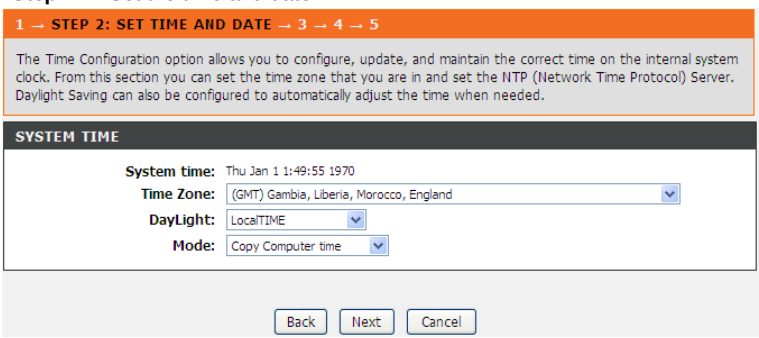


There are 5 steps to configure the device. Click **Next** to continue.

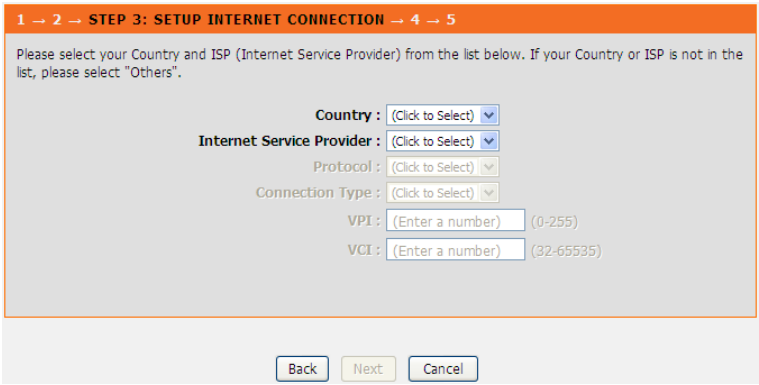
Step 1 Change the device login password.



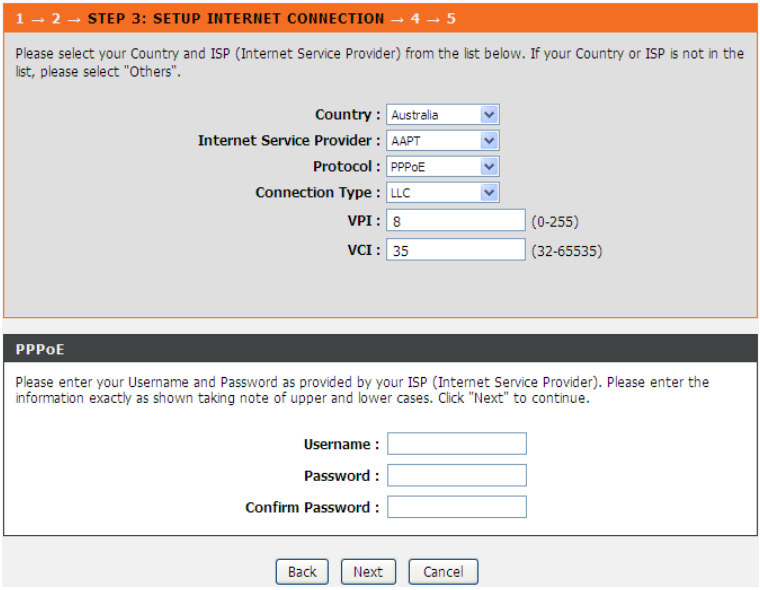
Step 2 Set the time and date.



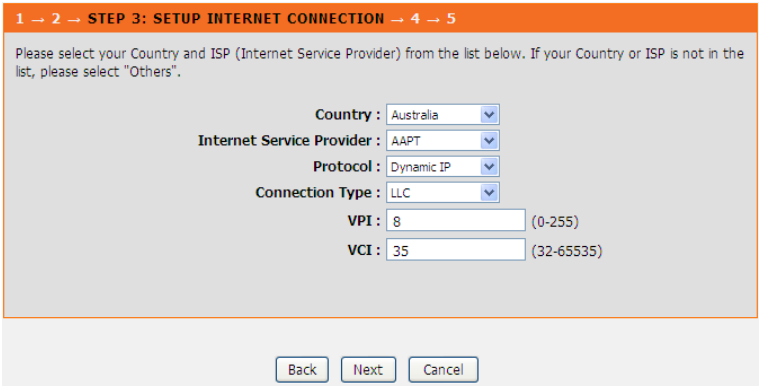
Step 3 Configure the Internet connection.



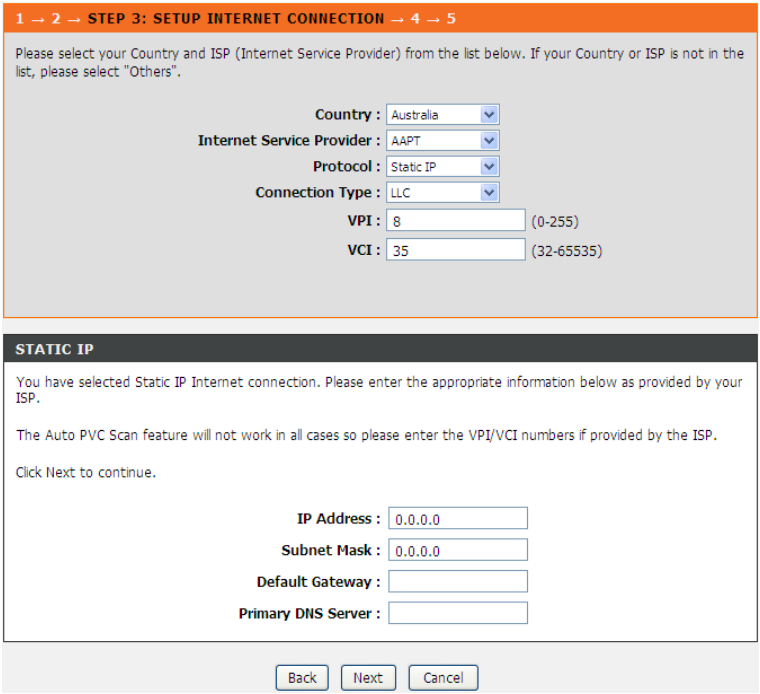
If the internet service you subscribed is **PPPoE** or **PPPoA**, you can choose the **Protocol** to be **PPPoE** or **PPPoA**. Set the VPI and VCI. Enter the user name and password provided by your ISP.



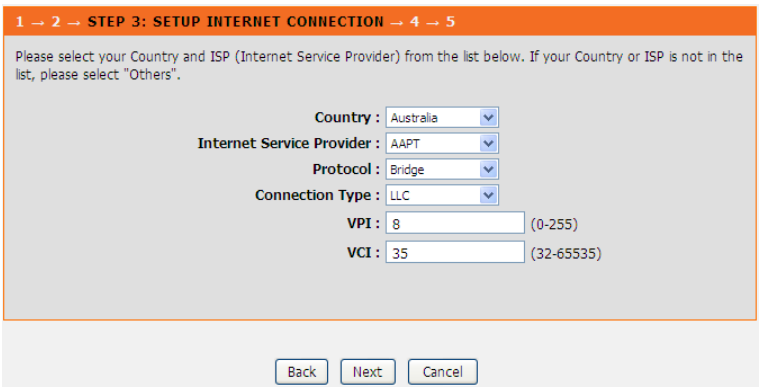
If the internet service you subscribed is **Dynamic IP**, you can choose **Protocol** to be **Dynamic IP**. The page shown in the following figure appears.



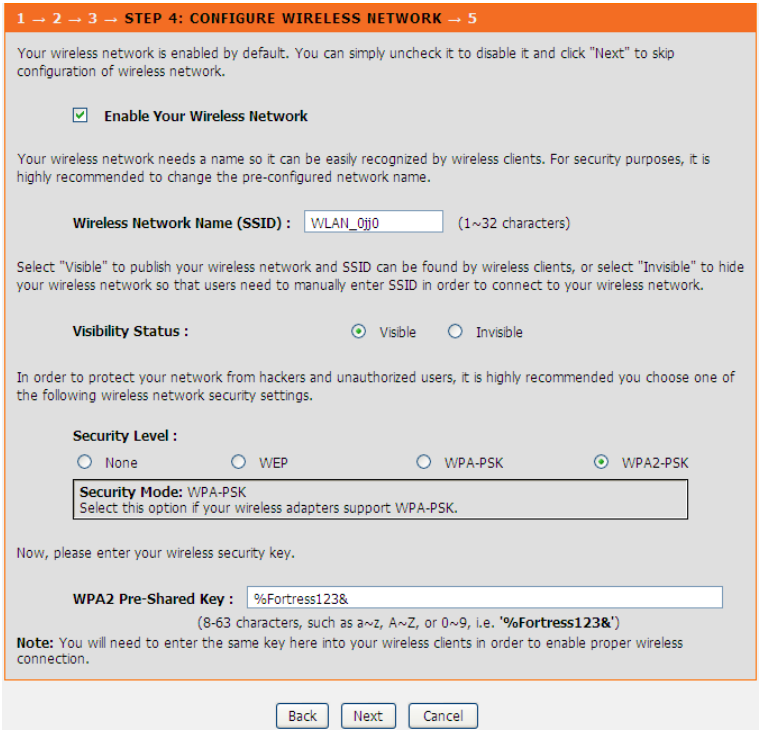
If the Protocol is **Static IP**, you can choose **Protocol** to be **Static IP**. The page shown in the following figure appears. Enter the **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS Server** provided by your ISP.



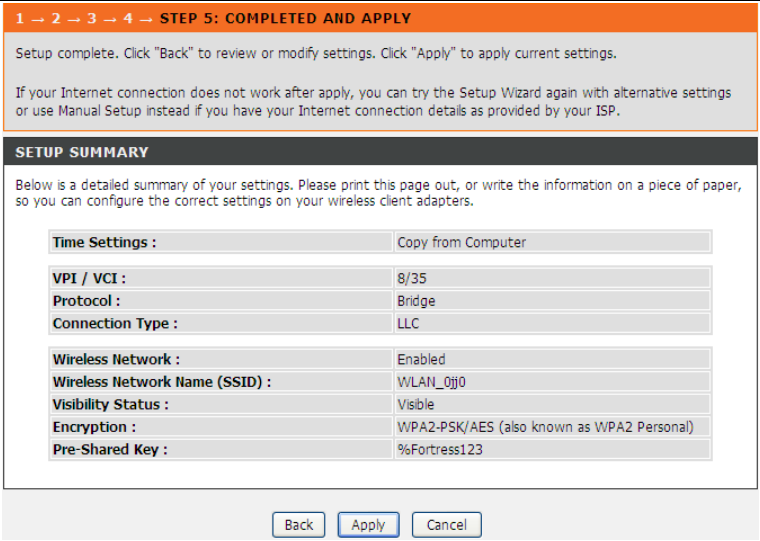
If the Protocol is **Bridge**, the page shown in the following figure appears.



Step 4 Configure the wireless network.



Step 5 Complete and apply the settings. 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.

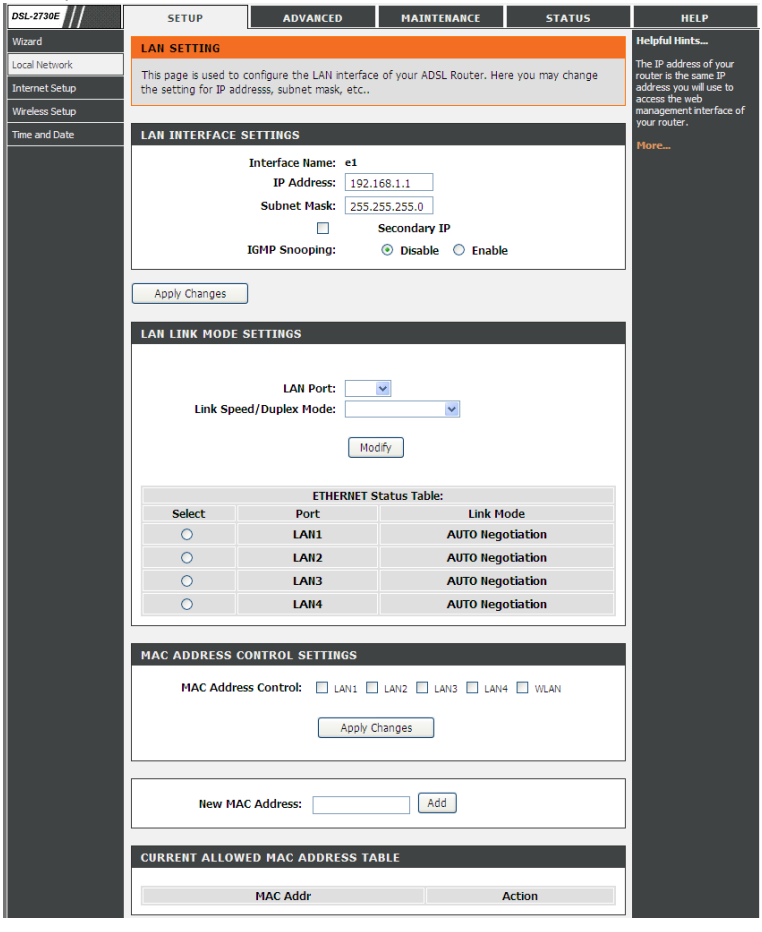
3.2.2 Local Network

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.

3.2.2.1 LAN Interface

Choose **Setup** > **Local Network** > **LAN Interface**. The **LAN Setting** page shown in the following figure appears. You may configure the LAN interface, for example, the IP address and subnet mask.

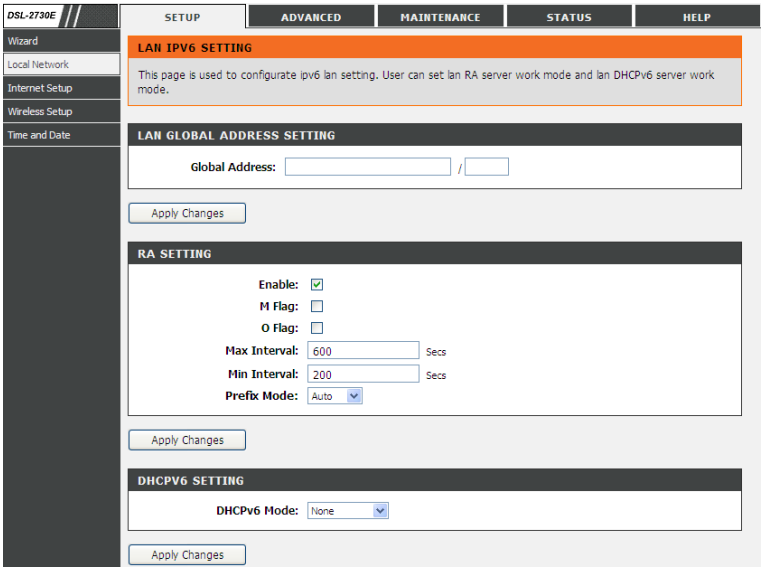


The following table describes the parameters in this page.

Field	Description
IP Address	Enter the IP address of LAN interface. It is recommended to use an address from a block reserved for private use. This address block is 192.168.1.1- 192.168.1.254.
Subnet Mask	Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.0.0-255.255.255.254.
Secondary IP	Select it to enable the secondary LAN IP address. The two LAN IP addresses must be in different subnets.
LAN Port	You may choose the LAN interface you want to configure.
Link Speed/ Duplex Mode	You may select one mode from the drop-downlist: **100Mbps/FullDuplex**, **100Mbps/Half Duplex**, **10Mbps/FullDuplex**, **10Mbps/Half Duplex** and **Auto Negotiation**.
MAC Address Control	It is the access control based on MAC address. Select it, and the host whose MAC address is listed in the **Current Allowed MAC Address Table** can access the modem.
Add	Enter MAC address, and then click this button to add a new MAC address.

3.2.2.2 LAN IPv6 Interface

Choose **Setup** > **Local Network** > **LAN IPv6 Interface**. The **LAN IPv6 Setting** page shown in the following figure appears. You may set LAN RA server work mode and LAN DHCPv6 server work mode.



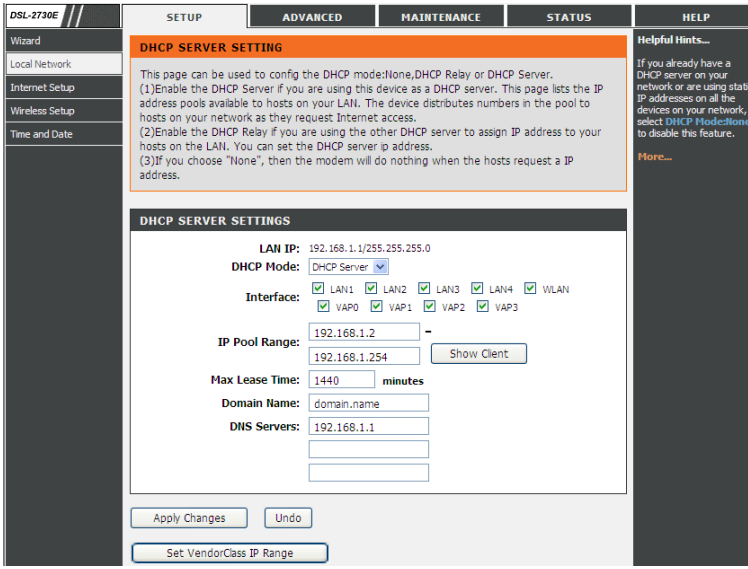
The following table describes the parameters of this page.

Field	Description
Global Address	Specify the LAN global ipv6 address. It can be assigned by ISP.
Enable	Enable or disable the Router Advertisement feature.
M Flag	Enable or disable the “Managed address configuration” flag in RA packet.
O Flag	Enable or disable the “Other configuration” flag in RA packet.
Prefix Mode	Specify the RA feature prefix mode: “Auto”: the RA prefix will use WAN dhcp-pd prefix; “Manual”: user will specify the prefix address, length, preferred time and valid time.
DHCPv6 Mode	Specify the dhcpv6 server mode: “None”: close dhcpv6 server; “Manual”: dhcpv6 server is opened and user

Field	Description
	specifies the dhcpv6 server address pool and other parameters. “Auto”: dhcpv6 server is opened and it use WAN dhcp-pd prefix to generate address pool.

3.2.2.3 DHCP Server

Choose **Setup** > **Local Network** > **DHCP Server**. The **DHCP Server Setting** page shown in the following figure appears. You may configure the DHCP mode.

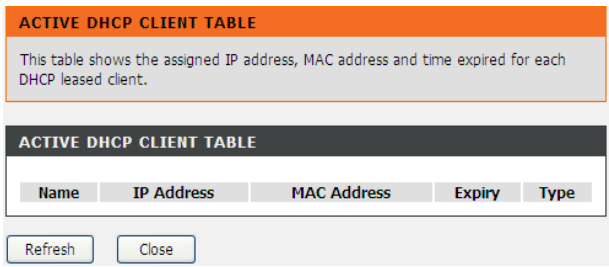


The following table describes the parameters of this page.

Field	Description
DHCP Mode	If set to **DHCP Server**, the router can assign IP addresses, IP default gateway and DNS servers to the host in Windows95, Windows NT and other

Field	Description
	operation systems that support the DHCP client.
IP Pool Range	It specifies the first and last IP addresses in the IP address pool. The router assigns IP address in the IP pool range to the host.
Max Lease Time	The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
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 server.
DNS Servers	You can configure the DNS server ip addresses for DNS Relay.

Click the button **Show Client** to display the page **Active DHCP Client Table** as shown below. It shows the IP addresses assigned to DHCP clients.

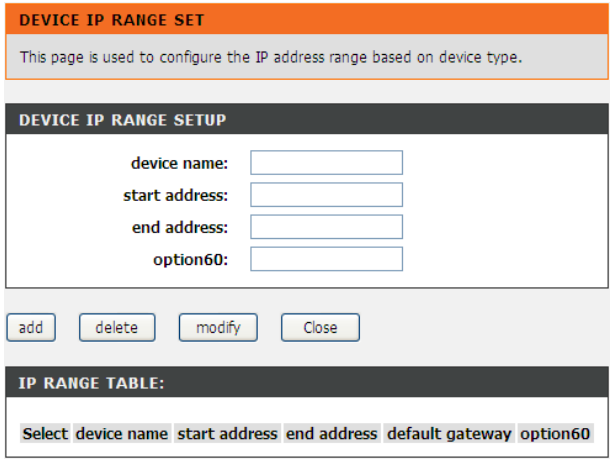


The following table describes the parameters and buttons in this page:

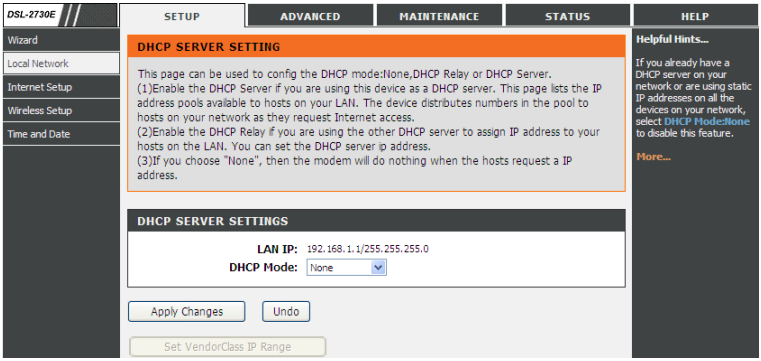
Field	Description
IP Address	It displays the IP address assigned to the DHCP client from the router.
MAC Address	It displays the MAC address of the DHCP client. Each Ethernet device has a unique MAC address.

Field	Description
	The MAC address is assigned at the factory and it consists of six pairs of hexadecimal character, for example, 00-A0-C5-00-02-12.
Expiry	It displays the lease time. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Refresh	Click it to refresh this page.

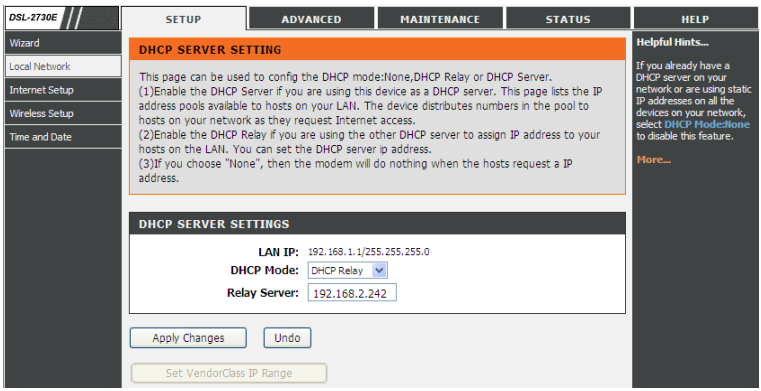
Click the button **Set VendorClass IP Range** to display the page **Device IP Range Set**. In this page, you can configure the IP address range based on the device type.



In the **DHCP Mode** field, choose **None**. The page shown in the following figure appears.



In the **DHCP Mode** field, choose **DHCP Relay**. The page shown in the following figure appears.

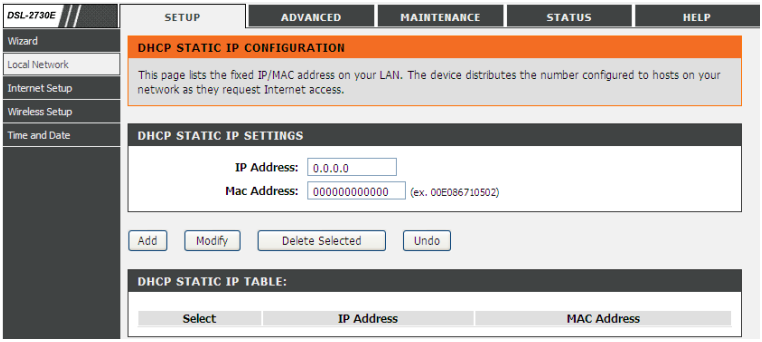


The following table describes the parameters and buttons of this page:

Field	Description
DHCP Mode	If set to **DHCP Relay**, the router acts a surrogate DHCP Server and relays the DHCP requests and responses between the remote server and the client.
Relay Server	Enter the DHCP server address provided by your ISP.
Apply Changes	Click it to save the settings of this page.

3.2.2.4 DHCP Reserved

Choose **Setup** > **Local Network** > **DHCP Reserved**. The **DHCP Static IP Configuration** page appears. This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.



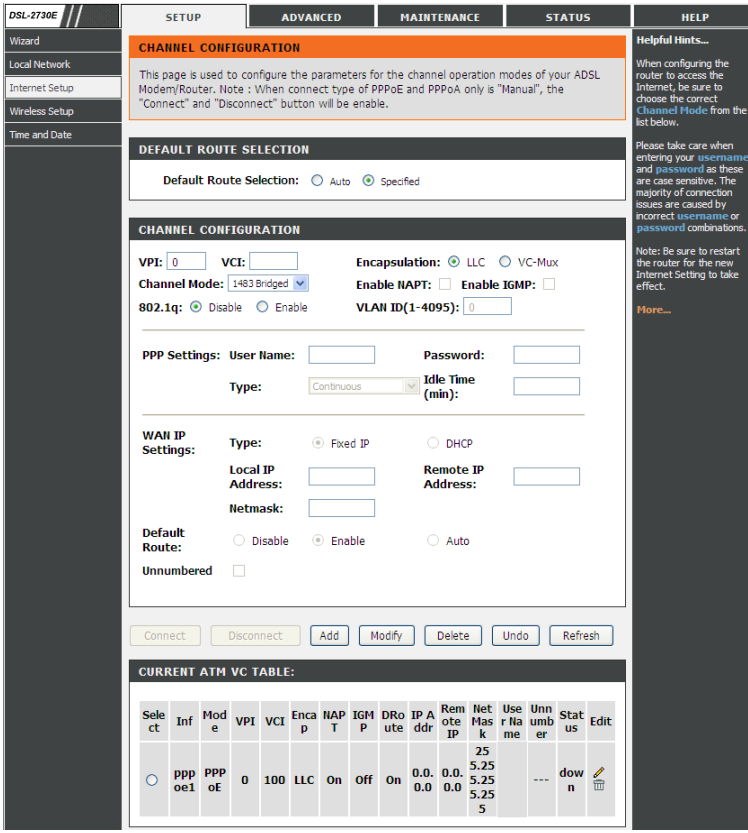
The following table describes the parameters of this page.

Field	Description
IP Address	Enter the specified IP address in the IP pool range, which is assigned to the host.
Mac Address	Enter the MAC address of a host on the LAN.
Add	After entering the IP address and MAC address, click this button to add them to the DHCP Static IP Table.
Delete Selected	Select a row in the DHCP Static IP Table, then click it, this row is deleted.
Undo	Click it to refresh this page.
DHCP Static IP Table	It shows the assigned IP address based on the MAC address.

3.2.3 Internet Setup

3.2.3.1 Channel Config

Choose **Setup** > **Internet Setup** > **Channel Config**. The **Channel Configuration** page appears. You may configure the parameters for the channel operation modes of your ADSL Router.

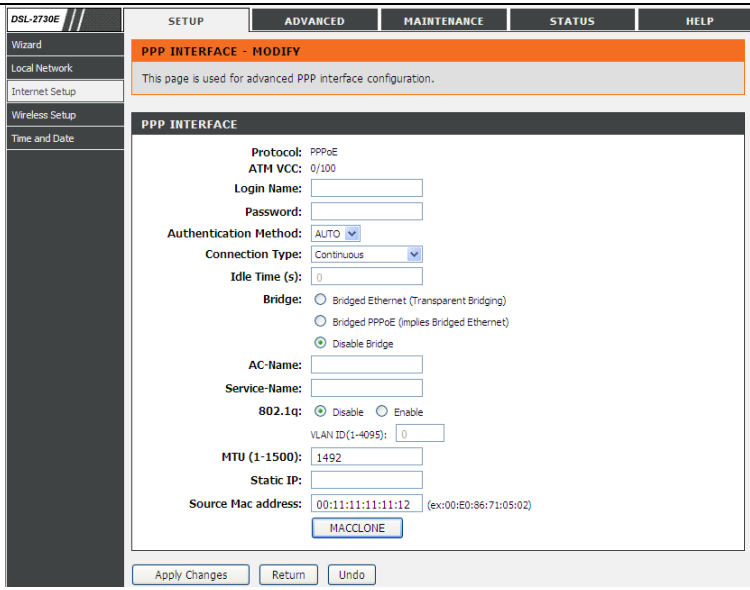


The following table describes the parameters of this page.

Field	Description
Default Route Selection	You can select **Auto** or **Specified**.
VPI	The virtual path between two points in an ATM network, ranging from **0** to **255**.
VCI	The virtual channel between two points in an ATM network, ranging from **32** to **65535** (**1** to **31** are reserved for known protocols)
Encapsulation	You can choose **LLC** and **VC-Mux**.
Channel Mode	You can choose **1483 Bridged**, **1483 MER**, **PPPoE**, **PPPoA**, **1483 Routed** or **IPoA**.
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is enabled.
Enable IGMP	You can enable or disable Internet Group Management Protocol (IGMP) function.
802.1q	You can select **Disable** or **Enable**. If enabled, you need to enter the VLAN ID.
VLAN ID	The value ranges from **1** to **4095**.
IP Protocol	When any channel mode except 1483 Bridged is selected, select an IP protocol from **IPv4/IPv6**, **IPv4** and **IPv6**.
PPP Settings	
User Name	Enter the correct user name for PPP dial-up, which is provided by your ISP.
Password	Enter the correct password for PPP dial-up, which is provided by your ISP.
Type	You can choose **Continuous**, **Connect on Demand** or **Manual**.
Idle Time (min)	If the type is set to **Connect on Demand**, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the

Field	Description
	user continuously, the router automatically disconnects the PPPoE connection.
WAN IP Settings	
Type	You can choose **Fixed IP** or **DHCP**. ● If select **Fixed IP**, you should enter the local IP address, remote IP address and subnet mask. ● If select **DHCP**, the router is a DHCP client, the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Remote IP Address	Enter the IP address of gateway provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Default Route	Routing table entry is not clearly specified in the routing, as to any network prefix forwarding address.
Unnumbered	Select this checkbox to enable IP unnumbered function.
IPv6 WAN Setting	
Address Mode	When the channel mode is not set to **1483 Bridged**, configure this interface as supportting Slaac or Static to generate wan ipv6 addresses.
Enable DHCPv6 Client	You may enable or disable dhcpv6 client on this interface. After enabling it, user may specify the dhcpv6 client request an address or prefix.

After a PPPoE ATM VC is added to the table, click in the **PPPoE** mode, the page shown in the following figure appears. In this page, you can configure parameters of this PPPoE PVC.



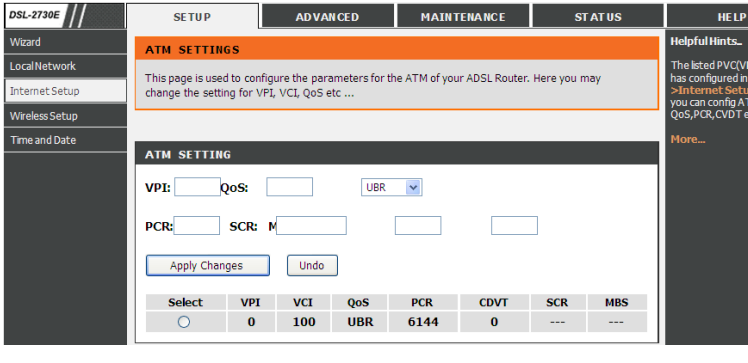
The following table describes the parameters and buttons of this page:

Field	Description
Protocol	It displays the protocol type used for this WAN connection.
ATM VCC	The ATM virtual circuit connection assigned for this PPP interface (VPI/VCI).
Login Name	The user name provided by your ISP.
Password	The password provided by your ISP.
Authentication Method	You can choose **AUTO**, **CHAP**, or **PAP**.
Connection Type	You can choose **Continuous**, **Connect on Demand**, or **Manual**.
Idle Time (s)	If choose **Connect on Demand**, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
Bridge	You can select **Bridged Ethernet**, **Bridged**

Field	Description
	PPPoE, or **Disable Bridge**.
AC-Name	The accessed equipment type.
Service-Name	The service name.
802.1q	You can select **Disable** or **Enable**. After enable it, you need to enter the VLAN ID. The value ranges from 1 to 4095.
Source Mac address	The MAC address you want to clone.
MAC Clone	Click it to enable the MAC Clone function with the MAC address that is configured.
Apply Changes	Click it to save the settings of this page temporarily.
Return	Click it to return to the **Channel Configuration** page.
Undo	Click it to refresh this page.

3.2.3.2 ATM Settings

Choose **Setup** > **Internet Setup** > **ATM Settings**. The **ATM Settings** page appears. You may configure the parameters for the ATM of your ADSL Router. Here you may change the setting for VPI, VCI and QoS, etc.

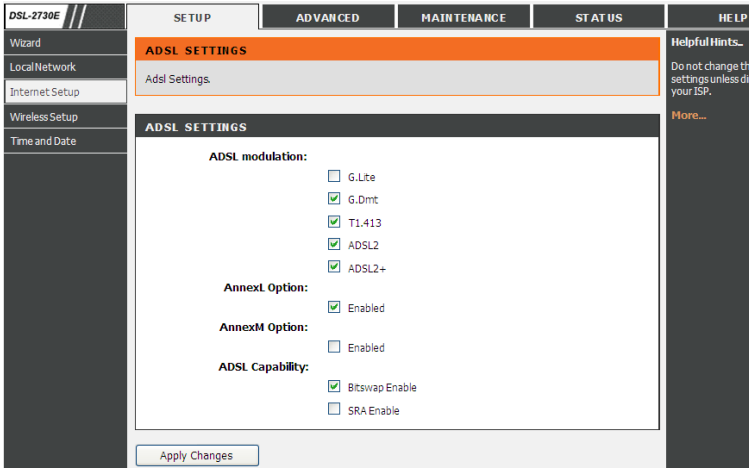


The following table describes the parameters of this page.

Field	Description
VPI	The virtual path identifier of the ATM PVC.
VCI	The virtual channel identifier of the ATM PVC.
QoS	The QoS category of the PVC. You can choose **UBR**, **CBR**, **rt-VBR**, or **nrt-VBR**.
PCR	Peak cell rate (PCR) is the maximum rate at which cells can be transmitted along a connection in the ATM network. Its value ranges from 1 to 65535.
CDVT	Cell delay variation tolerance (CDVT) is the amount of delay permitted between ATM cells (in microseconds). Its value ranges from 0 to 4294967295.
SCR	Sustained cell rate (SCR) is the maximum rate that traffic can pass over a PVC without the risk of cell loss. Its value ranges from 0 to 65535.
MBS	Maximum burst size (MBS) is the maximum number of cells that can be transmitted at the PCR. Its value ranges from 0 to 65535.

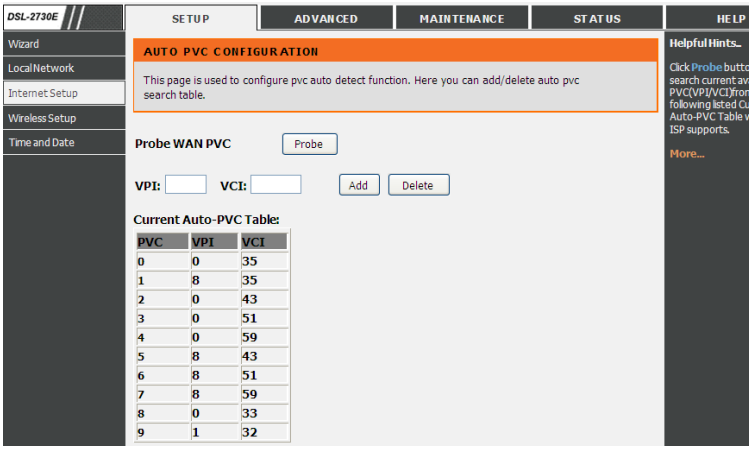
3.2.3.3 ADSL Settings

Choose **Setup** > **Internet Setup** > **ADSL Settings**. The **ADSL Settings** page appears. This page contains a modulation and capability section to be specified by your ISP. Consult with your ISP to select the correct settings for each. Click **Apply Changes** to finish.



3.2.3.4 PVC Auto Search

Choose **Setup** > **Internet Setup** > **PVC Auto Search**. The **Auto PVC Configuration** page appears. You may configure PVC auto detect function. Here you can add/delete auto PVC search table.

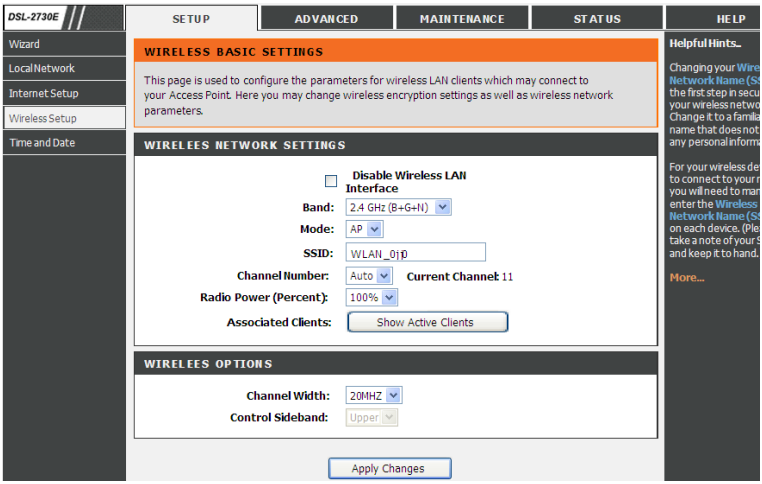


3.2.4 Wireless Setup

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

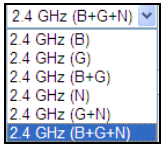
3.2.4.1 Wireless Basics

Choose **Setup** > **Wireless Setup** > **Wireless Basics**. The **Wireless Basic Settings** page appears. You may configure the parameters for wireless LAN clients, which may connect to your access point. Here you may change wireless encryption settings as well as wireless network parameters.

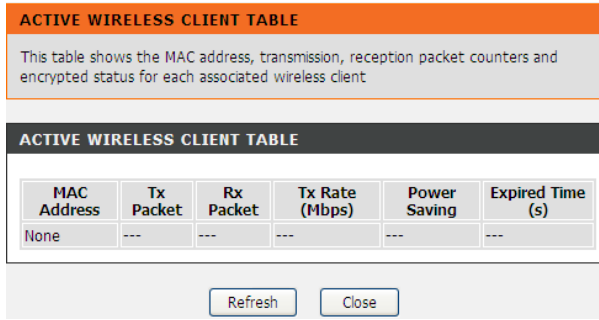


The following table describes the parameters in this page.

Field	Description
Band	Choose the working mode of the modem. You can choose from the drop-down list.

Field	Description
	
Mode	Choose the network model of the modem, which is varied according to the software. By default, the network model of the modem is **AP**.
SSID	The service set identification (SSID) is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the modem.
Channel Number	Choose a channel from the drop-down list box. A channel is the radio frequency used by 802.11b/g wireless devices. There are 13 channels (from 1 to 13) available depending on the geographical area. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. Interference and degrading performance occurs when radio signal from different APs overlap.
Radio Power (Percent)	You can choose the transmission power of the radio signal. The default one is **100%**. It is recommended to choose the default value**100%**.
Show Active Clients	Click it to view the information of the wireless clients connected to the modem.
Channel Width	Select the appropriate band of **20MHZ** or **40MHZ** according to your subscribed broadband service.
Control Sideband	Choose the channel selection mode as **Upper** or **Lower**.

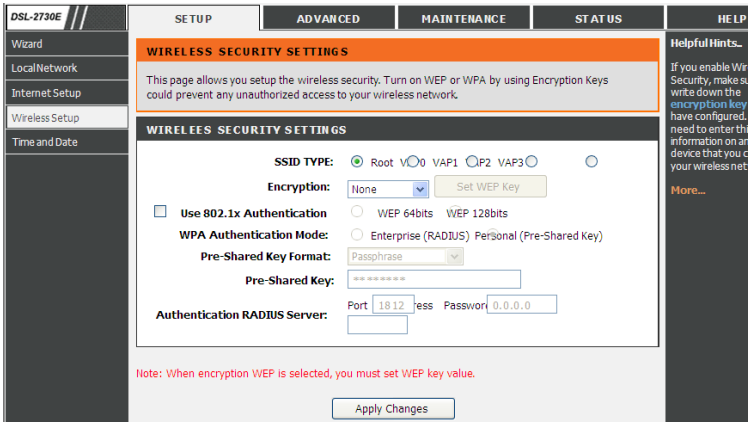
Click the button **Show Active Clients** to view the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.



Click **Apply Changes** to save the settings.

3.2.4.2 Wireless Security

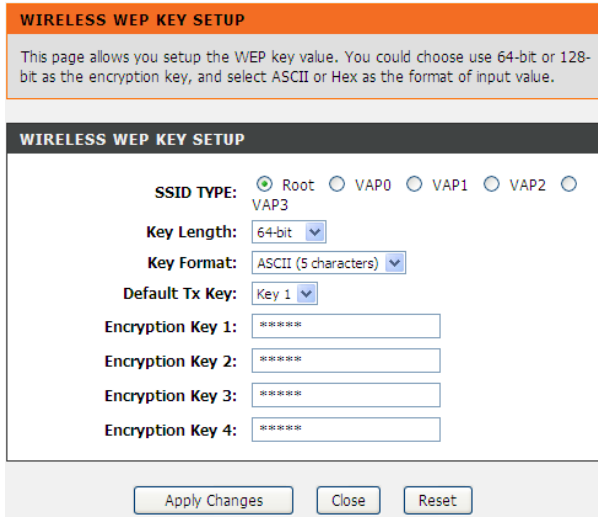
Choose **Setup** > **Wireless Setup** > **Wireless Security**. The **Wireless Security Settings** page appears. Turn on WEP or WPA using encryption keys could prevent any unauthorized access to your wireless network.



The following table describes the parameters of this page:

Field	Description
Encryption	Configure the wireless encryption mode. You can choose **None**, **WEP**, **WPA (TKIP)**, **WPA (AES)**, **WPA2 (AES)**, **WPA2 (TKIP)** or **WPA2 Mixed**. ● 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 WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2. Key differences between WPA and WEP are in user authentication and improved data encryption.
Set WEP Key	It is available when you set the encryption mode to **WEP**. Click it, the **Wireless WEP Key Setup** page appears.
WPA Authentication Mode	● Select **Personal (Pre-Shared Key)**, enter the pre-shared key in the **Pre-Shared Key** field. ● Select **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. If the encryption is set to **WEP**, the modem uses 802.1 X authentication, which is Radius authentication.

Click **Set WEP Key**, and the page **Wireless WEP Key Setup** appears. You can choose a 64-bit or 128-bit encryption key, and select ASCII or Hex format for input values.



The following describes the parameters of this page:

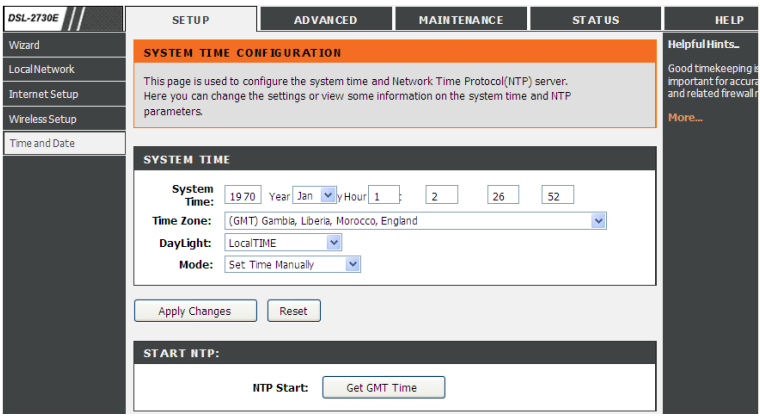
Field	Description
Key Length	Choose the WEP key length. You can Choose **64-bit** or **128-bit**.
Key Format	● If you choose **64-bit**, you can choose ASCII (5 characters) or Hex (10 characters). ● If you choose **128-bit**, you can choose ASCII (13 characters) or Hex (26 characters).
Default Tx Key	Choose the index of WEP Key. You can choose **Key 1**, **Key 2**, **Key 3** or **Key 4**.
Encryption Key 1 to 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. ● If you choose **64-bit** and **ASCII (5 characters)**, enter any 5 ASCII characters. ● If you choose **64-bit** and **Hex (10 characters)**, enter any 10 hexadecimal characters. ● If you choose **128-bit** and **ASCII (13**

Field	Description
	characters), enter any 13 ASCII characters. ● If you choose **128-bit** and **Hex (26 characters)**, enter any 26 hexadecimal characters.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click **Save** in the lower left corner.

Click **Apply Changes** to save the settings.

3.2.5 Time and Date

Choose **Setup** > **Time and Date**. The **System Time Configuration** page appears. In the 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.

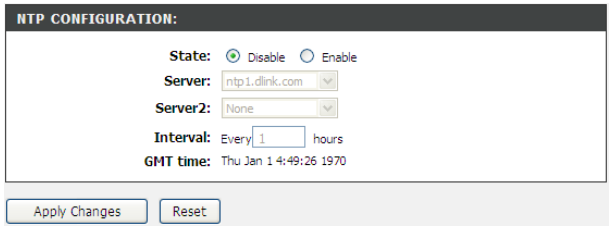


The following table describes the parameters in this page.

Field	Description
System Time	Displays the time currently maintained by the router. If this is incorrect, use the following options to configure the time correctly.

Field	Description
Time Zone	Select your local time zone from the dropdown list.
Daylight	Adjust the clock for daylight savings time.
Mode	To synchronize the time automatically with the Internet or your own computer, you may select **Set Time Manually**, **Copy Computer Time** or **Set NTP Server Manually**.
Get GMT Time	Synchronize to Greenwich Mean Time.

When the mode is set to **Set NTP Server Manually**, the following page will appear.



The following table describes the parameters in this page.

Field	Description
State	Select **Enable** to synchronize the time automatically with Internet or your own computer.
Server	Select a Network Time Server for synchronization from the dropdown list. You may set two servers.
Interval	Specify the interval for synchronization with the time server.

3.3 Advanced

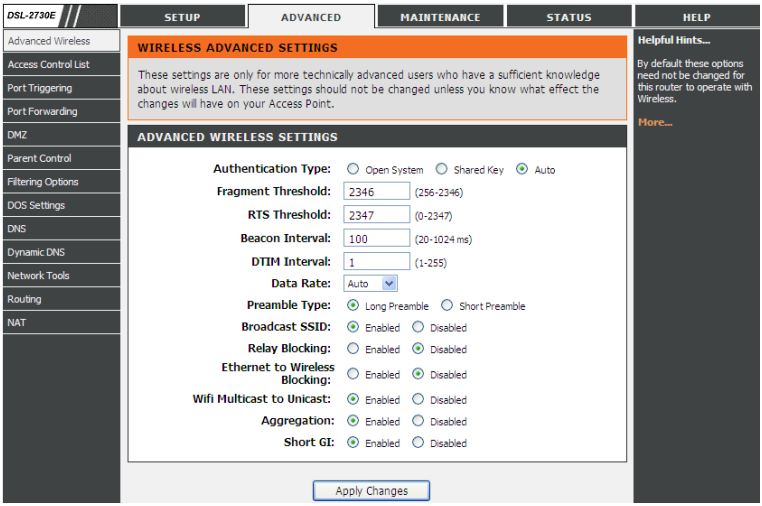
This section includes advanced features for network management, security and administrative tools to manage the device. You can view status and other information used to examine performance and for troubleshooting.

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.

3.3.1.1 Advanced Settings

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



The following table describes the parameters in this page.

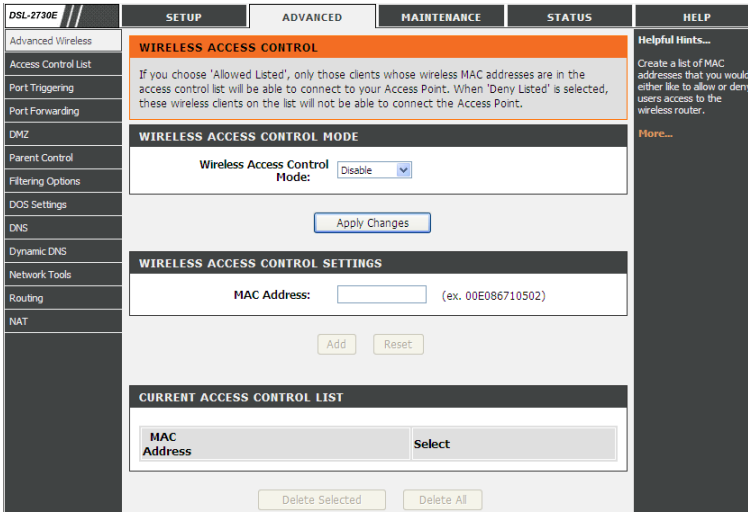
Field	Description
Fragment Threshold	Used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.

Field	Description
RTS Threshold (Request to Send Threshold)	Determines the packet size of a transmission through the use of the router to help control traffic flow.
Beacon Interval	A packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).
DTIM Interval	Sets the wake-up interval for clients in power-saving mode.
Preamble Type	This is the length of the CRC (Cyclic Redundancy Check) block for communication between the router and wireless clients. High network traffic areas should select Short preamble type.
Broadcast SSID	With Disabled selected, no wireless clients will be able to see your wireless network when they scan to see what's available.

Click **Apply Changes** to save the settings.

3.3.1.2 Access Control

Choose **Advanced** > **Advanced Wireless** > **Access Control**. The page shown in the following figure appears. Incoming connection can be filtered on your wireless router based on their MAC addresses.

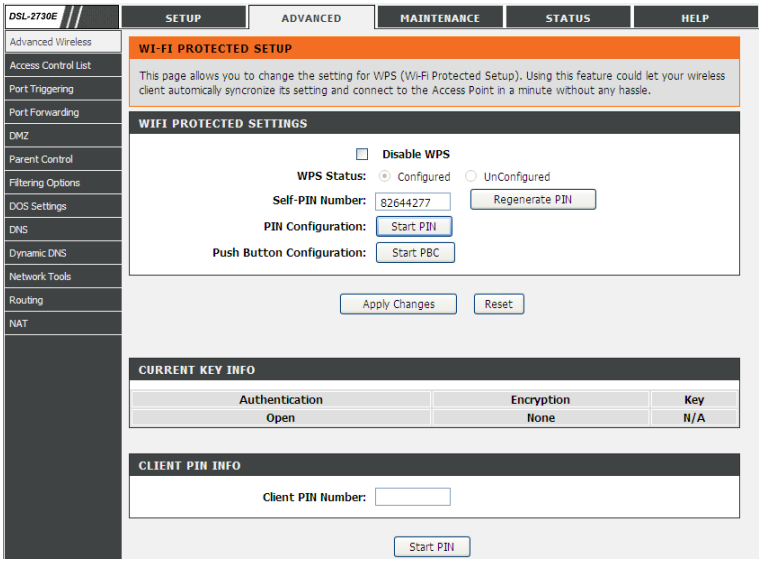


Set the Wireless Access Control Mode to **Allow Listed** to enable white list function. Only the devices whose MAC addresses are listed in the **Current Access Control List** can access the modem.

Set the Wireless Access Control Mode to **Deny Listed** to enable black list function. The devices whose MAC addresses are listed in the **Current Access Control List** are denied to access the modem.

3.3.1.3 WPS

Choose **Advanced** > **Advanced Wireless** > **WPS**. The page shown in the following figure appears. With this feature, your wireless client automically syncronize its setting and connect to the Access Point.



There are two methods for the wireless client to establish connection with the modem through WPS.

For one method, click **Regenerate PIN** to generate a new PIN, and then click **Start PBC**. In the wireless client tool, enter the PIN which is generated by the modem to start connection. The client will automatically establish the connection with the modem through the encryption mode, and you need not to enter the key.

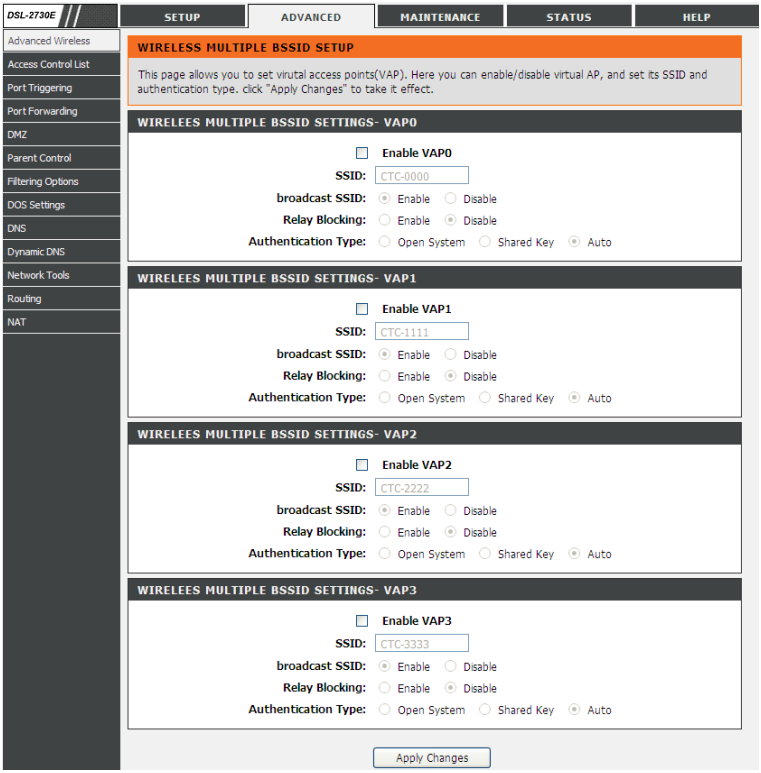
For the other method, the wireless client generates PIN. In the above figure, enter PIN of the wireless client in the **Client PIN Number** field, then click **Start PIN** to establish the connection.

Note:

The wireless client establishes the connection with the modem through WPS negotiation. The wireless client must support WPS.

3.3.1.4 MBSSID

Choose **Advanced** > **Advanced Wireless** > **MBSSID**. The page shown in the following figure appears. In this page, you can set virutal access points (VAP), its SSID and authentication type.



The device supports four virtual access points (VAPs). It is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same name. Enter a descriptive name that is used when the wireless client is connecting to the modem.

3.3.2 Access Control List

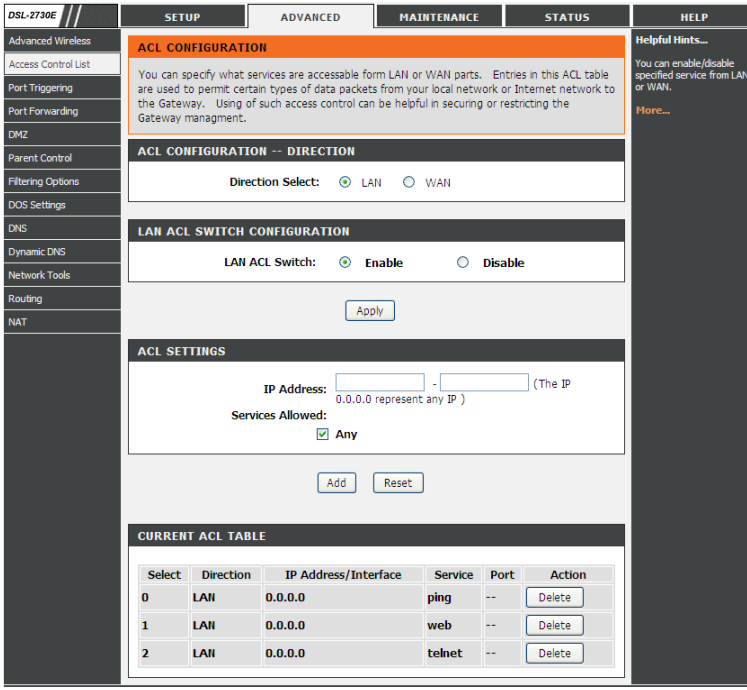
Multiple connections are required by some applications, for example, internet games, video conferencing and Internet telephony. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network.

3.3.2.1 Access Control List

Choose **Advanced** > **Access Control List** > **Access Control List**. The page shown in the following figure appears. In this page, you can permit the data packets from LAN or WAN to access the router. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.

Note:

If you select **Enable** in ACL capability, ensure that your host IP address is in ACL list before it takes effect.

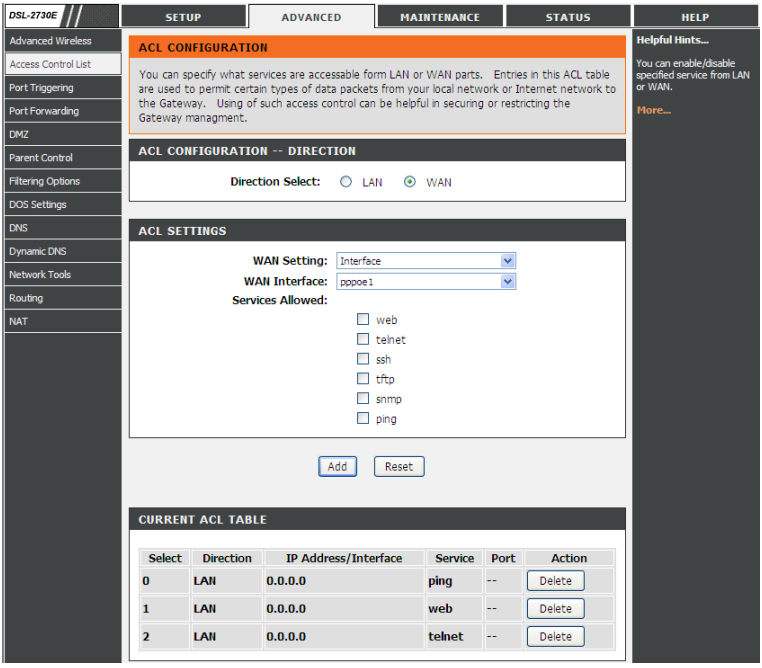


The following table describes the parameters and buttons of this page:

Field	Description
Direction Select	Select the router interface. You can select **LAN** or **WAN**. In this example, **LAN** is selected.
LAN ACL Switch	Select it to enable or disable ACL function.
IP Address	Enter the IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can access the router.
Services Allowed	You can choose the following services from LAN: **Web**, **Telnet**, **SSH**, **TFTP**, **SNMP** and **PING**. You can also choose all the services.
Add	After setting the parameters, click it to add an entry

Field	Description
	to the **Current ACL Table**.
Reset	Click it to refresh this page.

When the direction of data packets is set to **WAN**, the page shown in the following figure appears.



The following table describes the parameters and buttons of this page:

Field	Description
Direction Select	Select the router interface. You can select **LAN** or **WAN**. In this example, **WAN** is selected.
WAN Setting	You can choose **Interface** or **IP Address**.
WAN Interface	Choose the interface that permits data packets from WAN to access the router.

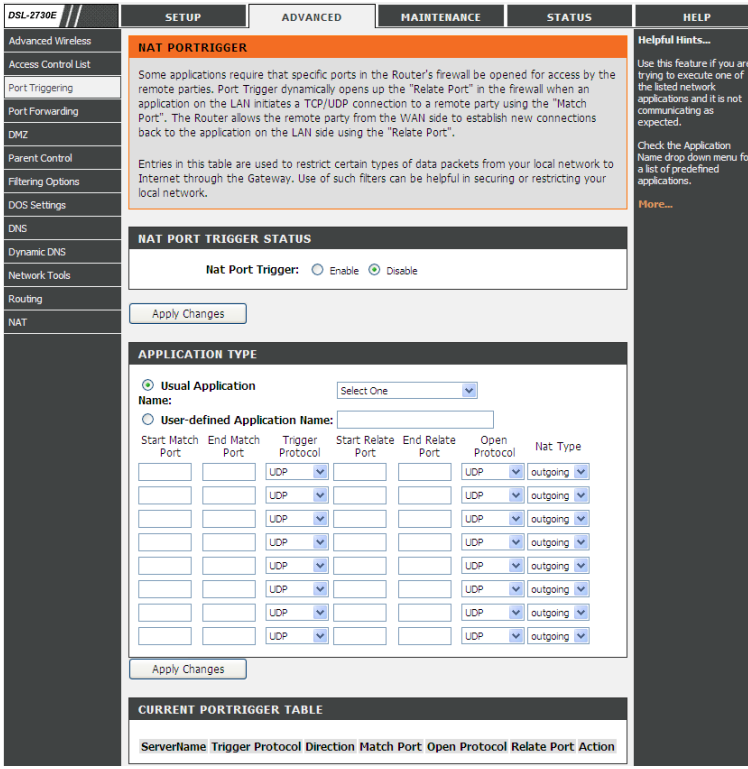
Field	Description
Services Allowed	You can choose the following services from WAN: **Web**, **Telnet**, **SSH**, **TFTP**, **SNMP** and **PING**. You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the **Current ACL Table**.
Reset	Click it to refresh this page.

3.3.2.2 Access Control List IPv6

Choose **Advanced** > **Access Control List** > **Access Control List IPv6**. The page shown in the following figure appears. For configuration method, refer to *3.3.2.1 Access Control List*.

3.3.3 Port Triggering

Choose **Advanced** > **Port Triggering**. The page shown in the following figure appears. Port Triggering is a special form of Port Forwarding in which it requires an outgoing connection before allowing incoming connections on a single or multiple ports. Port Triggering is mostly used when your computer is behind a NAT router. It gives more flexibility than static port forwarding because you don't need to set it up for a specific computer.



Click the **Usual Application Name** drop-down menu to choose the application you want to set up for port triggering. When you have chosen an application the default Trigger settings will populate the table below.

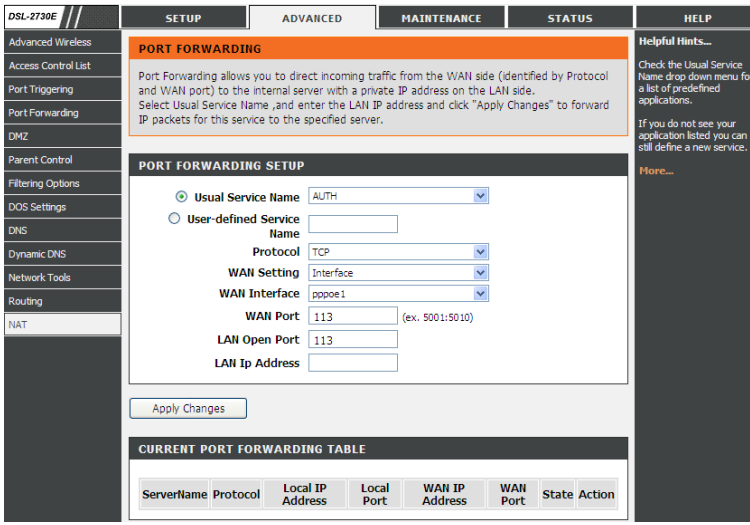
If the application you want to set up isn't listed, click the **User-defined Application Name** radio button and type in a name for the trigger in the Custom application field. Configure the **Start Match Port**, **End Match Port**, **Trigger Protocol**, **Start Relate Port**, **End Relate Port, Open Protocol** and **Nat type**.

Click the **Apply changes** button to finish.

3.3.4 Port Forwarding

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

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



Click the **Usual Service Name** drop-down menu to choose the service you want to set up for port forwarding. When you have chosen a service, the default settings will populate the table below.

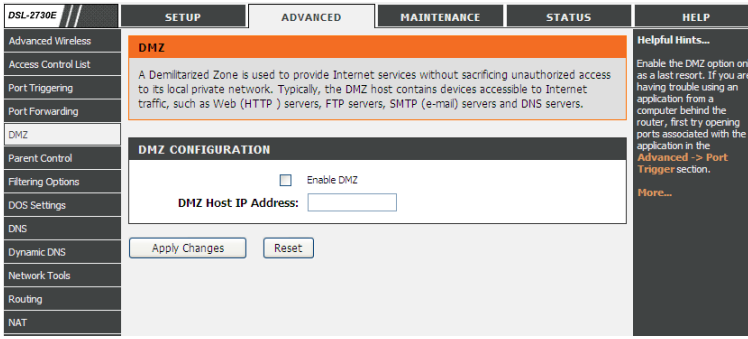
If the service you want to set up isn't listed, select the **User-defined Service Name** radio button and type in a service name. Configure the **Protocol**, **WAN Setting**, **WAN Interface**, **WAN Port**, **LAN Open Port** and **LAN IP Address**.

Click the **Apply changes** button to finish.

3.3.5 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.



In the DMZ Host IP Address, input the LAN IP address of the LAN computer that you want to have unrestricted Internet communication. If this computer obtains its address automatically using DHCP, then you may want to make a static reservation on the Setup-->Local Network-->DHCP Reserved page so that the IP address of the DMZ computer does not change.

Click **Apply** to save the settings.

3.3.6 Parental Control

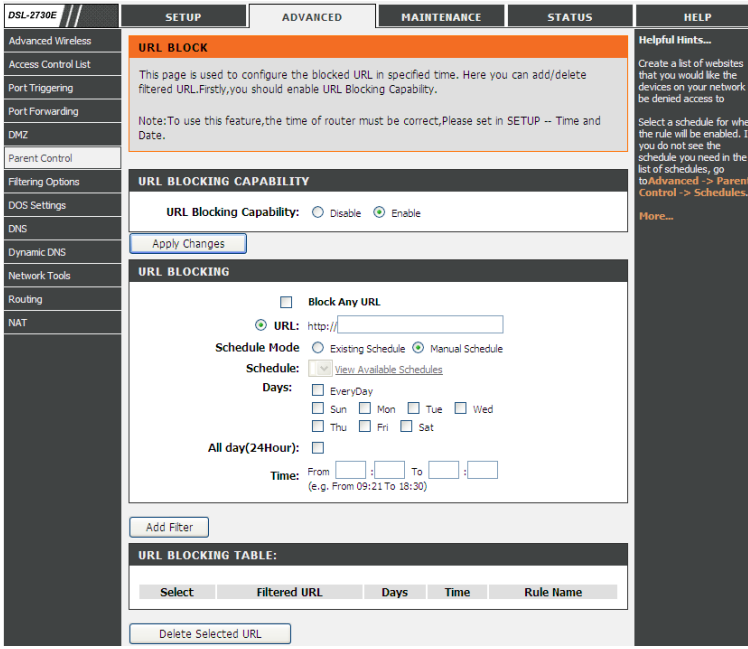
You may create a list of websites that you would like the devices on your network to be denied access to. **URL Block** allows you to quickly create a list of all websites that you wish to stop users from accessing. **MAC Filter** allows you to control when clients or PCs connected to the device are allowed to access the Internet.

3.3.6.1 URL Block

Choose **Advanced** > **Parental Control** > **URL Block**. The **URL Block** page shown in the following figure appears. You may deny certain websites from being accessed during the "schedule" you specified. Here you can add/delete filtered URL.

Note:

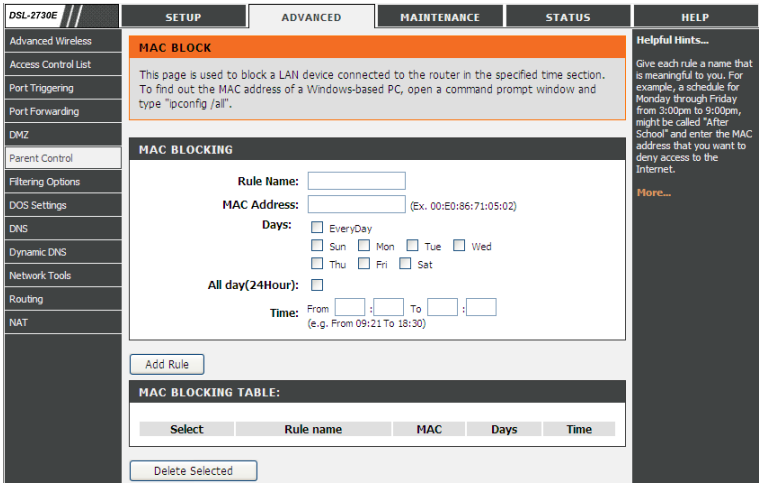
To use this feature, the time of router must be correct. Please set in 3.2.5 Time and Date.



In the field **Schedule Mode**, you may select an existing schedule schedule for when the rule will be enabled, or manually set a schedule. After setting, click **Add Filter** to add the URL into the **URL Blocking Table**. To add schedules, refer to 3.3.6.3 Schedules.

3.3.6.2 MAC Block

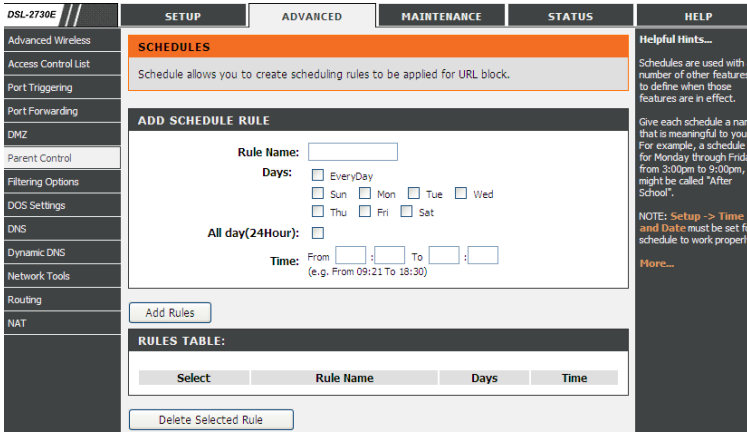
Choose **Advanced** > **Parental Control** > **MAC Block**. The **URL Block** page shown in the following figure appears. You may block a LAN device connected to the router in the specified time section.



In the field **Rule Name**, input a name that is meaningful to you, then enter a MAC address that you want to deny access to the Internet, and set the days and hours, and click Add Rule to add the MAC into the **MAC Blocking Table**.

3.3.6.3 Schedules

Choose **Advanced** > **Parental Control** > **Schedules**. The **Schedules** page shown in the following figure appears. You may add or delete scheduling rules to be applied for URL block.



In the field **Rule Name**, give the schedule a name that is meaningful to you, such as "Weekday rule". Set the **Day(s)** and time field, and click **Add Rules** to save the new rule in the following Rules Table.

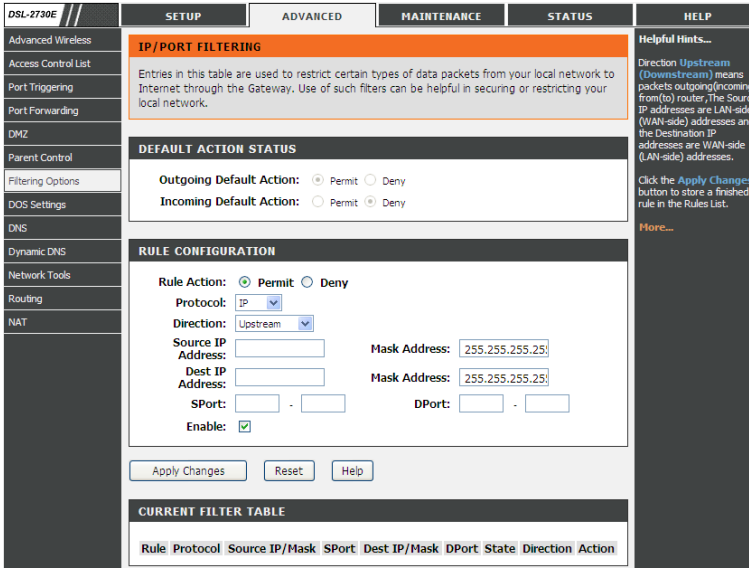
3.3.7 Filtering Options

Filters can be configured to manage your incoming and outgoing traffic.

3.3.7.1 IP/Port Filter

When you use the Port Triggering or Port Forwarding features to open specific ports to traffic from the Internet, you could be increasing the exposure of your LAN to cyberattacks from the Internet. In these cases, you can limit that exposure by specifying the IP addresses of Internet hosts that you trust to access your LAN through the ports that you have opened.

Choose **Advanced** > **Filtering Options** > **IP/Port Filter**. The **IP/Port Filtering** page shown in the following figure appears.



Direction **Upstream (Downstream)** means packets outgoing (incoming) from (to) router. The Source IP addresses are LAN-side (WAN-side) addresses and the Destination IP addresses are WAN-side (LAN-side) addresses. Select the rule action, specify at least one of the following criteria: protocol, source/destination IP address, subnet mask and source/destination port.

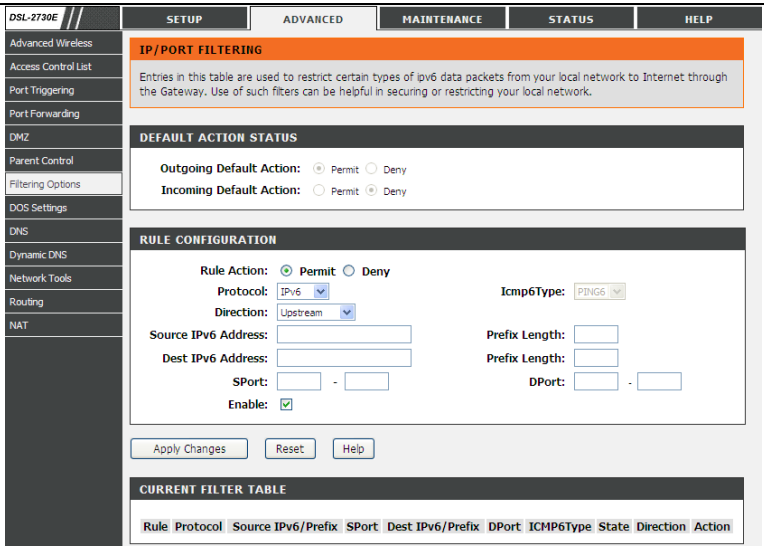
Click the **Apply Changes** to save a finished rule in the Rules List. The **Current Filter Table** shows detailed information about each created IP filter.

Note:

The settings only apply when the firewall is enabled.

3.3.7.2 IPv6/Port Filter

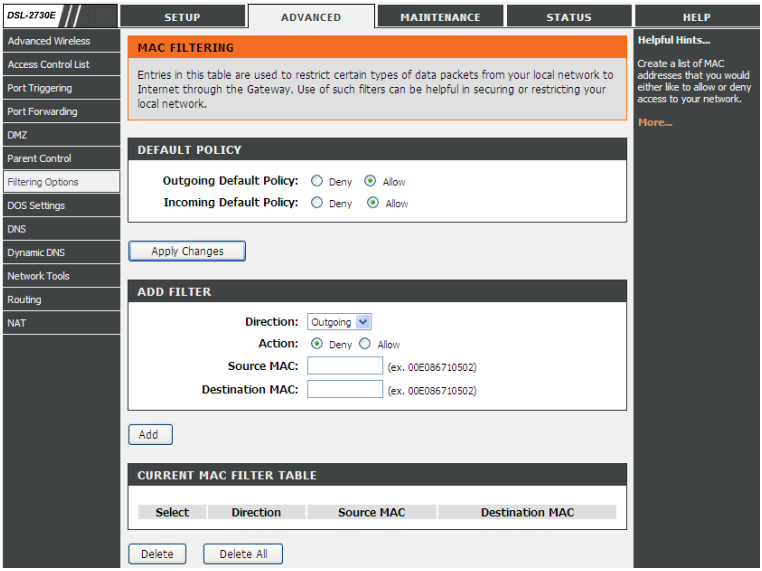
Choose **Advanced** > **Filtering Options** > **IPv6/Port Filter**. The **IP/Port Filtering** page shown in the following figure appears. You may restrict certain types of ipv6 data packets between LAN-side and WAN-side.



For detailed configuration, you may refer to 3.3.7.1IP/Port Filter.

3.3.7.3 MAC Filter

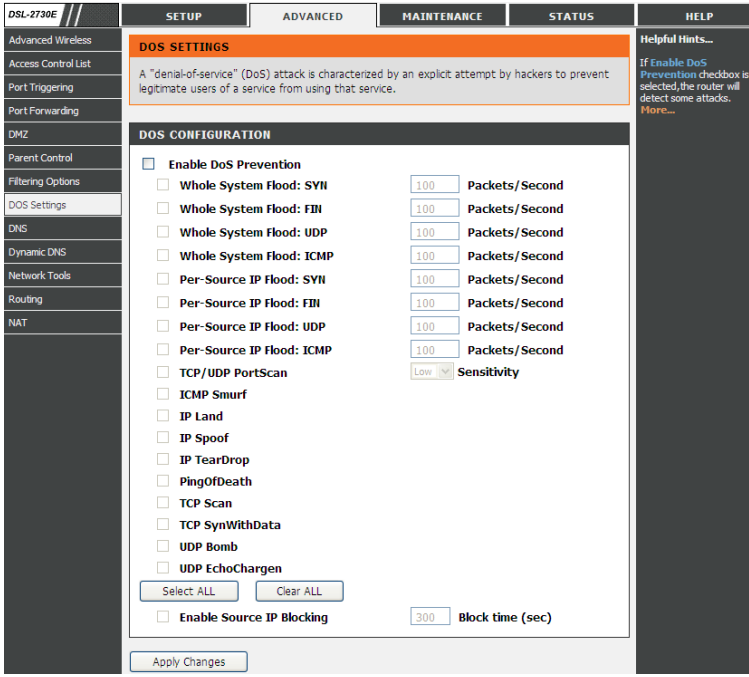
Choose **Advanced** > **Filtering Options** > **MAC Filter**. The **MAC Filtering** page shown in the following figure appears. You may create a list of MAC addresses that you would either like to allow or deny access to your network.



3.3.8 DoS Settings

Denial-of-Service Attack (DoS attack) is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

Choose **Advanced** > **DoS Settings**. The **DOS Settings** page shown in the following figure appears. Select the **Enable DoS Prevention** checkbox, select the options below, and click **Apply Changes** to finish.

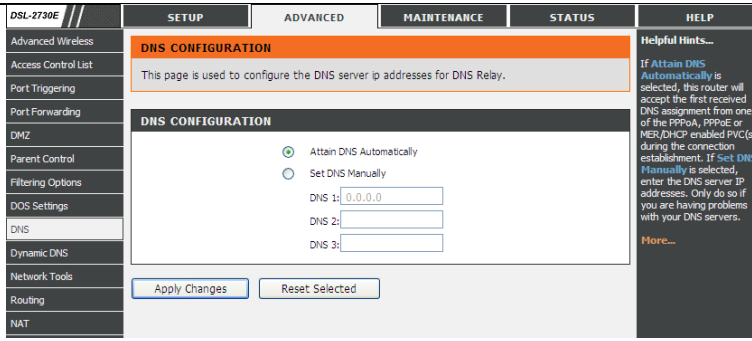


3.3.9 DNS

Domain Name System (DNS) is an Internet service that translates the URL/domain name into the corresponding IP address. Since URL/Domain Names are alphabetical, they are easier to remember. But the Internet is based on IP address. For example, the URL/Domain Name www.dlink.com is actually 192.168.0.123.

3.3.9.1 DNS

Choose **Advanced** > **DNS** > **DNS**. The **DNS Configuration** page shown in the following figure appears. You may configure the ip addresses of DNS servers for DNS Relay.

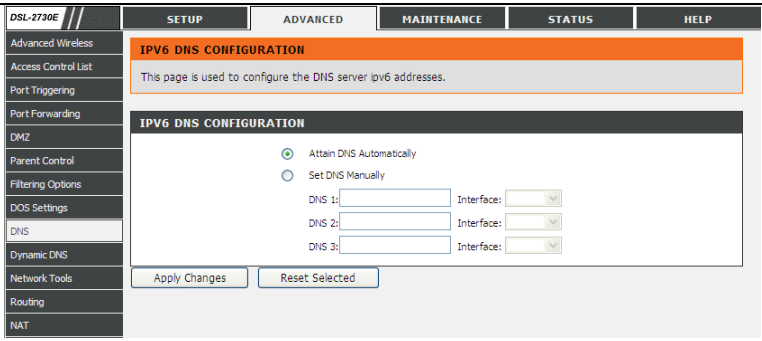


The following table describes the parameters and buttons of this page:

Field	Description
Attain DNS Automatically	Select it, the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it, enter the IP addresses of the primary and secondary DNS server.
Apply Changes	Click it to save the settings of this page.
Reset Selected	Click it to start configuring the parameters in this page.

3.3.9.2 IPv6 DNS

Choose **Advanced** > **DNS** > **IPv6 DNS**. The **IPv6 DNS Configuration** page shown in the following figure appears. You may configure the ipv6 addresses of DNS servers.



The following table describes the parameters and buttons of this page.

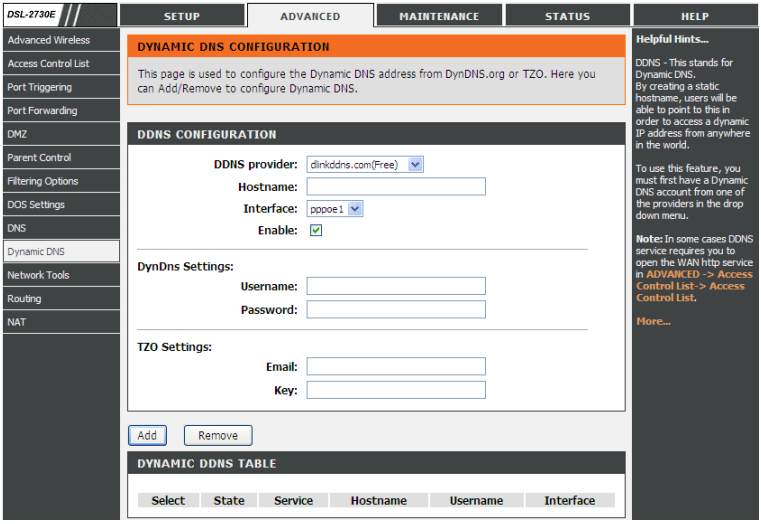
Field	Description
Attain DNS Automatically	Select it, the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it, enter the IP addresses and choose the WAN interface of the primary, the secondary and the tertiary DNS server.
Interface	The router accepts received packet assignment from one of the PPPoA, PPPoE or MER enabled PVC(s).
Apply Changes	Click it to save the settings of this page.
Reset Selected	Click it to start configuring the parameters in this page.

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 (DyndDNS.org or dlinkddns.com).

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



The following table describes the parameters and buttons of this page.

Field	Description
DDNS provider	Select a dynamic DNS service provider from the pull-down list.
Hostname	Enter the host name that you registered with your DDNS service provider.
Username	Enter the username provided by your service provider.
Password	Enter the password provided by your service provider.

Note:

In some cases DDNS service requires you to open the WAN http service. Refer to Access Control List-> Access Control List.

Click **Add** to save the settings to the **Dynamic DDNS Table**.

3.3.11 Network Tools

The router provides following tools: **Port Mapping**, **IGMP Proxy**, **IP QoS**, **UPnP**, **SNMP**, **TR-069**, **Software Forbidden**, **ARP Binding** and **Client Limit**.

3.3.11.1 Port Mapping

Port Mapping supports a single (LAN) port or multiple (LAN) ports to be formed as a group and mapped to a PVC (which is associated w/ a VLAN). As a result, each group of LAN ports will perform as an independent (logical) network (like a broadcast domain) among whom traffic broadcast would be prevented. This feature is useful while you would like to form multiple independent (logical) networks for multimedia applications at home. For instance, you can map PVC1 to port 1~3 to create a network (broadcast domain) for PCs for Internet, and map PVC2 to port 4 to create another network (broadcast domain) for IPTV service (devices). By using this feature (w/ multiple PVCs), data traffic and IPTV traffic would not affect each other.

Choose **Advanced** > **Network Tools** > **Port Mapping**. The **Port Mapping Configuration** page shown in the following figure appears.

Follow the steps to manipulate a mapping group.

Step 1 Select a group from the table.

Step 2 Select interfaces from the available WAN and LAN interface groups and add it to the interface group list using the arrow buttons to manipulate the required mapping of the ports.

Step 3 Click **Apply** button to save the changes.

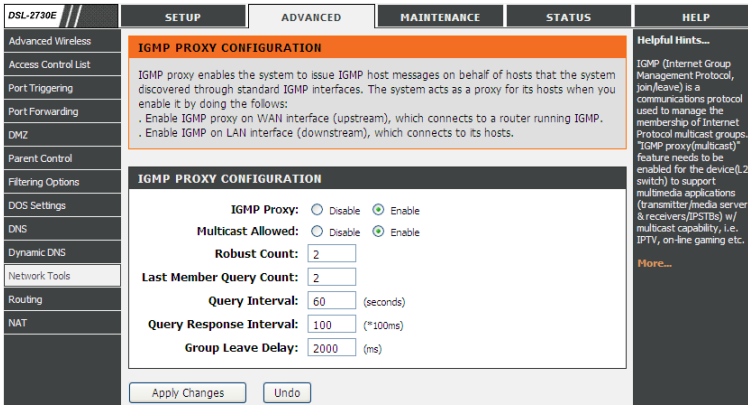
Note:

The selected interfaces will be removed from their existing groups and added to the new group.

3.3.11.2 IGMP Proxy

IGMP allows support for efficient multicasting -- transmission of identical content, such as multimedia, from a source to a number of recipients. 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.

Choose **Advanced** > **Network Tools** > **IGMP Proxy**. The **IGMP Proxy Configuration** page shown in the following figure appears.



The following table describes the parameters and buttons of this page.

Field	Description
Multicast allowed	Enable multicast proxy, only for route mode.
Robust Count	Allows tuning for the expected packet loss on a link. It determines how many times a startup query should be xmitted.
Last Member Query Count	This parameter specifies the times the device sends the query message.

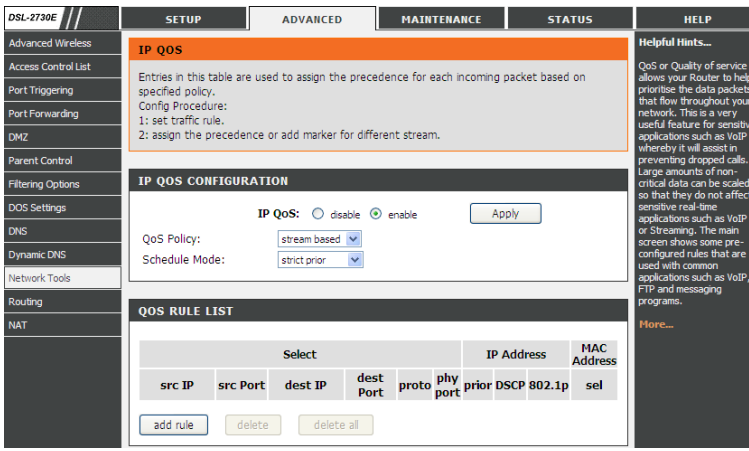
Field	Description
Query Interval	The device sends query messages to check IGMP user periodically. The unit is second.
Query Response Interval	The device waits for the IGMP user's reply. The unit is 100 * millisecond.
Group Leave Delay	The duration for the modem to cease forwarding multicast packets after a corresponding IGMP "Leave Group" message has been successfully offered to the modem.

Click **Apply Changes** to save the settings.

3.3.11.3 IP QoS

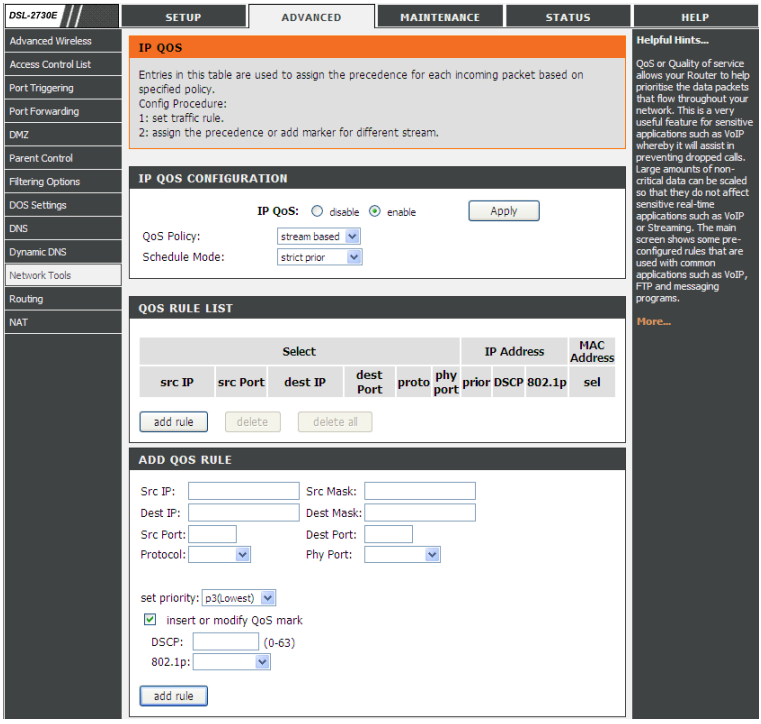
Quality of Service is a feature that allows you to allocate or guarantee the throughput or speed of Internet for certain computers. This is a very useful feature for sensitive applications such as VoIP whereby it will assist in preventing dropped calls. Large amounts of non-critical data can be scaled so that they do not affect sensitive real-time applications such as VoIP or Streaming.

Choose **Advanced** > **Network Tools** > **IP QoS**. The **IP QoS** page shown in the following figure appears.



Step 1 Enable IP QoS and click **Apply** to enable IP QoS function.

Step 2 Click **add rule** to add a new IP QoS rule. The page shown in the following figure appears.



The following table describes the parameters and buttons of this page.

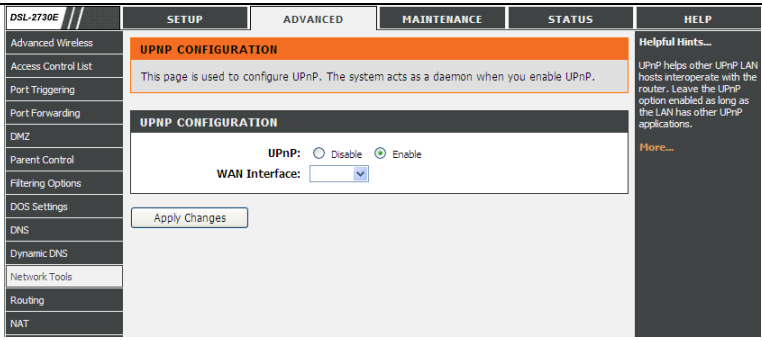
Field	Description
QoS Policy	You can choose **stream based**, **802.1p based**, or **DSCP based**.
Schedule Mode	You can choose **strict prior** or **WFQ (4:3:2:1)**.
Source IP	The IP address of the source data packet.
Source Mask	The subnet mask of the source IP address.
Destination IP	The IP address of the destination data packet.
Destination Mask	The subnet mask of the destination IP address.
Source Port	The port of the source data packet.
Destination Port	The port of the destination data packet.
Protocol	The protocol responding to the IP QoS rules. You can choose **TCP**, **UDP**, or **ICMP**.
Phy Port	The LAN interface responding to the IP QoS rules.
Set priority	The priority of the IP QoS rules. P0 is the highest priority and P3 is the lowest.
802.1p	You can choose from **0** to **7**.
Delete	Select a row in the **QoS rule list** and click it to delete the row.
Delete all	Select all the rows in the **QoS rule list** and click it to delete the rows.

Click **add rule** to add it to the **QoS Rule List**.

3.3.11.4 UpnP

UPnP (Universal Plug and Play) is a networking architecture that provides compatibility among networking equipment, software, and peripherals. This router has optional UPnP capability, and can work with other UPnP devices and software. The system acts as a daemon when you enable UPnP. Leave the UPnP option enabled as long as the LAN has other UPnP applications.

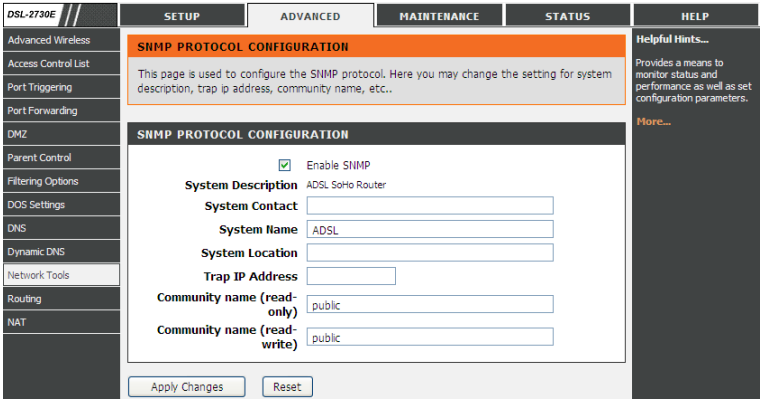
Choose **Advanced** > **Network Tools** > **UPnP**. The **UPnP Configuration** page shown in the following figure appears.



3.3.11.5 SNMP

SNMP (Simple Network Management Protocol) provides a means to monitor status and performance and set configuration parameters. It enables a management station to configure, monitor and receive trap messages from network devices.

Choose **Advanced** > **Network Tools** > **SNMP**. The **SNMP Protocol Configuration** page shown in the following figure appears. You may change the settings for system description, trap ip address and community name.



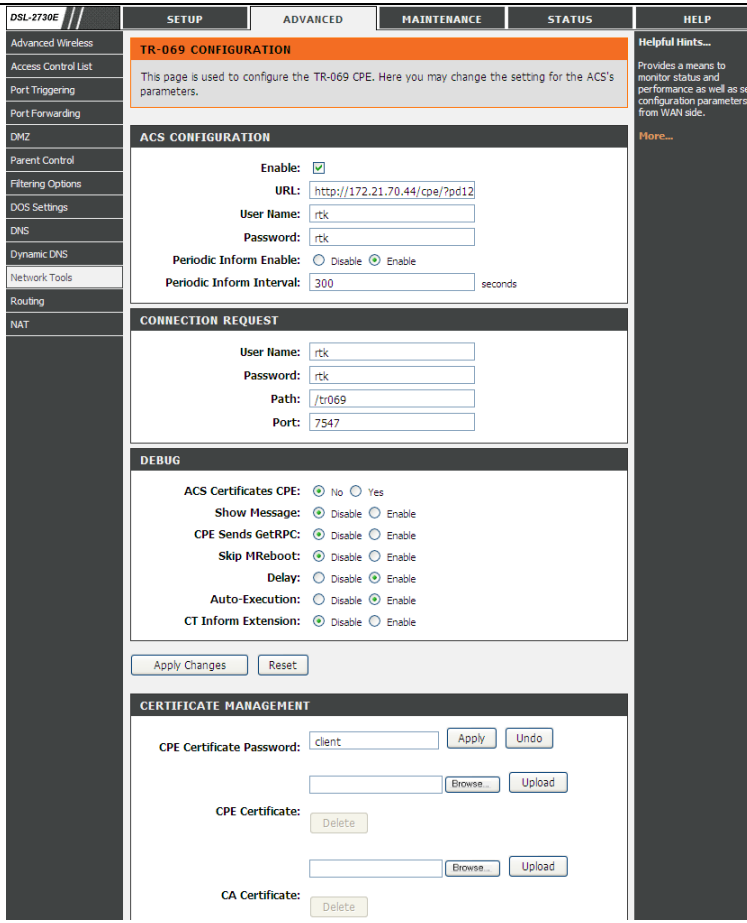
The following table describes the parameters of this page:

Field	Description
Enable SNMP	Select it to enable SNMP function. You need to enable SNMP, and then you can configure the parameters of this page.
Trap IP Address	Enter the trap IP address. The trap information is sent to the corresponding host.
Community Name (Read-only)	The network administrators must use this password to read the information of this router.
Community Name (Read-Write)	The network administrators must use this password to configure the information of the router.

3.3.11.6 TR-069

TR-069 is a WAN management protocol. It is a bidirectional SOAP/HTTP based protocol providing the communication between the ADSL router and an Auto Configuration Server (ACS) to monitor status and performance and to set configuration parameters from WAN side.

Choose **Advanced** > **Network Tools** > **TR-069**. The **TR-069 Configuration** page shown in the following figure appears. You may change change the setting for the ACS's parameters.



The following table describes the parameters of this page:

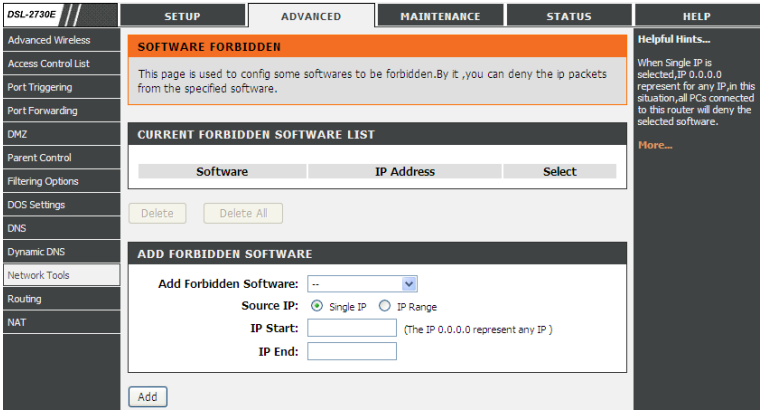
Field	Description
ACS Configuration	
URL	The URL of the auto-configuration server to connect to.
User Name	The user name for logging in to the ACS.

Field	Description
Password	The password for logging in to the ACS.
Periodic Inform Enable	Select **Enable** to periodically connect to the ACS to check configuration updates.
Periodic Inform Interval	Specify the amount of time between connections to ACS.
Connection Request	
User Name	The connection username provided by TR-069 service.
Password	The connection password provided by TR-069 service.
Debug	
Show Message	Select **Enable** to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select **Enable**, the router contacts the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto-Execution	Specify whether to automatically start the TR-069 after the router is powered on.
CT Inform Extension	Specify support China Telecom extension inform type or not.
Certificate Management	
CPE Certificate Password	The certificate password of the router.
CPE Certificate	Enter the CPE Certificate file. Click it to browse and upload the certificate for the router.
CA Certificate	Click it to browse and upload the CA certificate for the router.

3.3.11.7 Software Forbidden

Choose **Advanced** > **Network Tools** > **Software Forbidden**. The **Software Forbidden** page shown in the following figure appears. You may config some software to be forbidden to deny the ip packets of it.

To forbid one specified PC (or some PCs) from using an application, select the application you want to prohibit, and input a single IP address or IP addresses in range. When Single IP is selected, IP 0.0.0.0 represent for any IP. In this situation,all PCs connected to this router will deny the selected software.

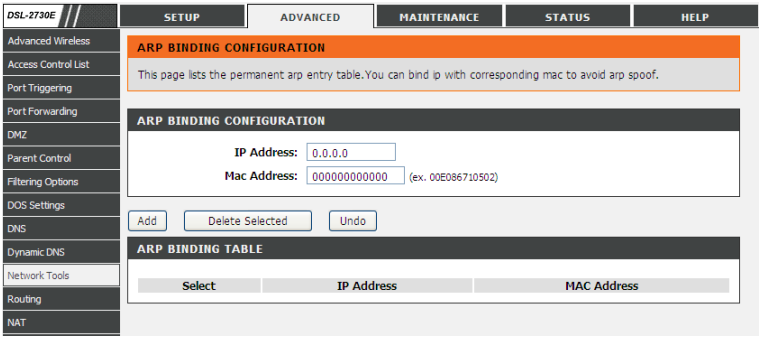


The following table describes the parameters and buttons of this page:

Field	Description
Current Forbidden Software List	A list of currently forbidden applications for accessing the network.
Add Forbidden Software	Select an application to be forbidden from accessing the network.

3.3.11.8 ARP Binding

This function realizes the binding of IP addresses and MAC addresses to avoid ARP address cheats. Choose **Advanced** > **Network Tools** > **ARP Binding**. The **ARP Binding Configuration** page shown in the following figure appears.

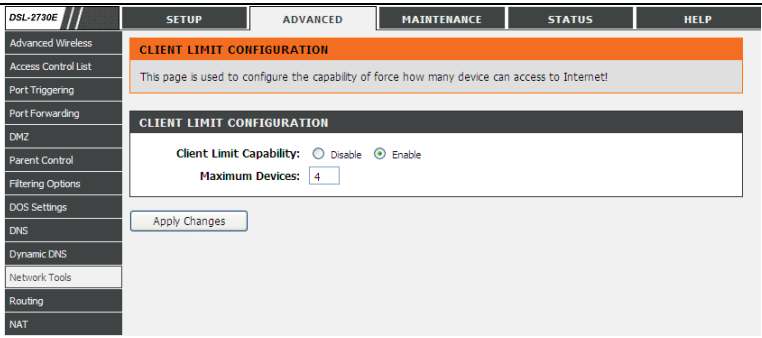


The following table describes the parameters and buttons of this page:

Field	Description
IP Address	An IP address to be bound.
Mac Address	An MAC address to be bound.
Add	Click this icon to add an ARP binding.
Delete Selected	Delete a selected setting from the lsit.
Undo	Reconfigure the above setting.
ARP Binding Table	A list of all the current ARP binding settings.

3.3.11.9 Client Limit

Choose **Advanced** > **Network Tools** > **Client Limit**. The **Client Limit Configuration** page shown in the following figure appears. You may configure the capability of forcing how many devices can access to the Internet.

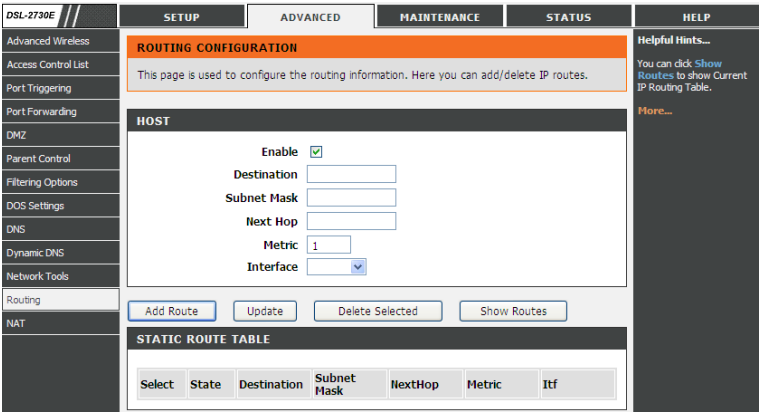


3.3.12 Routing

Under this menu, static route, default gateway and RIP type routing configurations can be performed.

3.3.12.1 Static Route

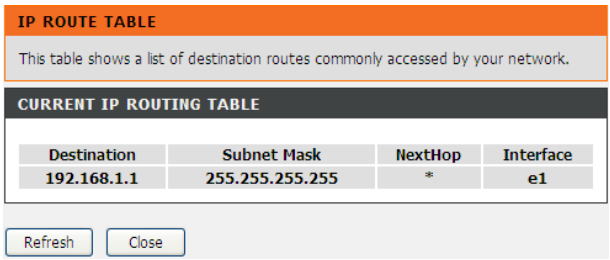
Choose **Advanced** > **Routing** > **Static Route**. The **Routing Configuration** page shown in the following figure appears. This page is used to configure the routing information. You may add or delete IP routes.



The following table describes the parameters and buttons of this page:

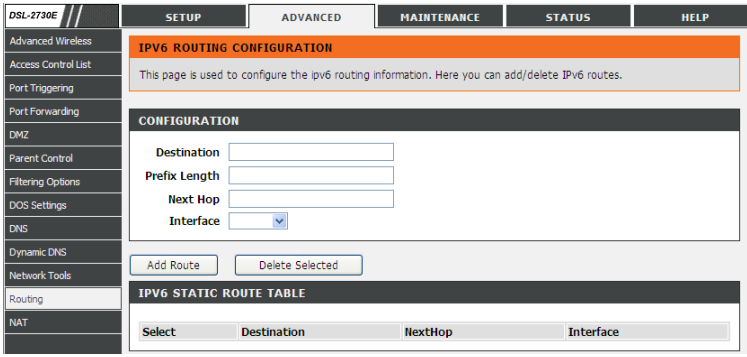
Field	Description
Enable	Select it to use static IP routes.
Destination	Enter the IP address of the destination device.
Subnet Mask	Enter the subnet mask of the destination device.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Metric	The metric cost for the destination.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the **Static Route Table**.
Update	Select a row in the **Static Route Table** and modify the parameters. Then click it to save the settings temporarily.
Delete Selected	Select a row in the **Static Route Table** and click it to delete the row.
Show Routes	Click it, the **IP Route Table** appears. You can view a list of destination routes commonly accessed by your network.
Static Route Table	A list of the previously configured static IP routes.

Click **Show Routes**, the page shown in the following figure appears. The table shows a list of destination routes commonly accessed by your network.



3.3.12.2 IPv6 Static Route

Choose **Advanced** > **Routing** > **IPv6 Static Route**. The **IPv6 Routing Configuration** page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.



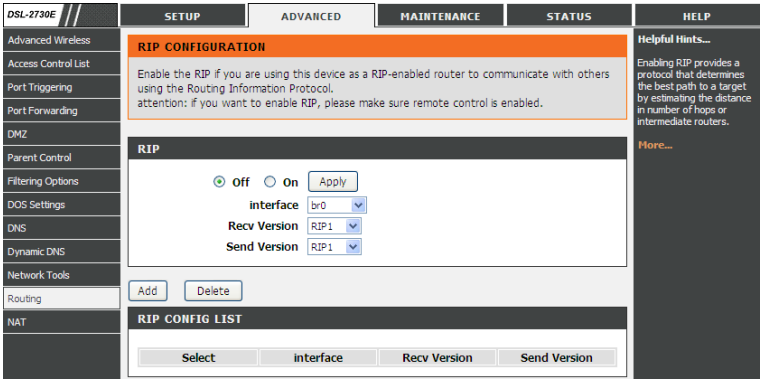
The following table describes the parameters and buttons of this page.

Field	Description
Destination	Enter the IPv6 address of the destination device.
Prefix Length	Enter the prefix length of the IPv6 address.
Next Hop	Enter the IP address of the next hop in the IPv6 route to the destination address.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the **IPv6 Static Route Table**.
Delete Selected	Select a row in the **IPv6 Static Route Table** and click it to delete the row.

3.3.12.3 RIP

Enable this function if you are using this device as a RIP-enabled router to communicate with others using Routing Information Protocol (RIP). This page is used to select the interfaces on your devices that use RIP, and the version of the protocol used.

Choose **Advanced** > **Routing** > **IPv6 Static Route**. The **IPv6 Routing Configuration** page shown in the following figure appears.



The following table describes the parameters and buttons of this page:

Field	Description
RIP	Select **Enable**, the router communicates with other RIP-enabled devices.
Apply	Click it to save the settings of this page.
Interface	Choose the router interface that uses RIP.
Receive Version	Choose the interface version that receives RIP messages. You can choose **RIP1**, **RIP2**, or **Both**. ● Choose **RIP1** indicates the router receives RIP v1 messages. ● Choose **RIP2** indicates the router receives RIP v2 messages. ● Choose **Both** indicates the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose **RIP1** or **RIP2**. ● Choose **RIP1** indicates the router broadcasts RIP1 messages only. ● Choose **RIP2** indicates the router multicasts RIP2 messages only.

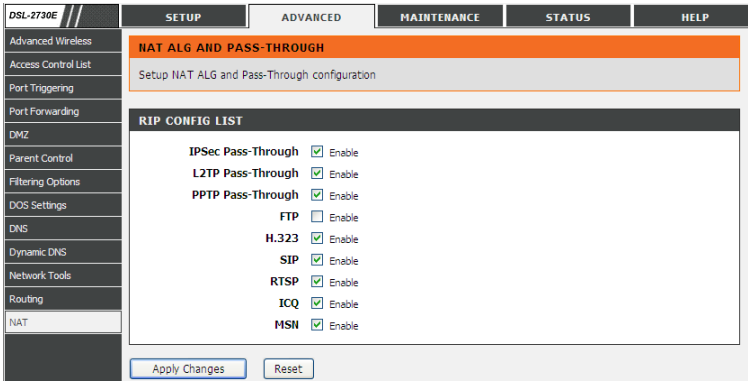
Field	Description
Add	Click it to add the RIP interface to the **Rip Config List**.
Delete	Select a row in the **Rip Config List** and click it to delete the row.

3.3.13 NAT

Under this menu, NAT ALG (Application Layer Gateway), NAT Exclude IP, NAT Forwarding, FTP ALG Config and NAT IP Mapping can be performed.

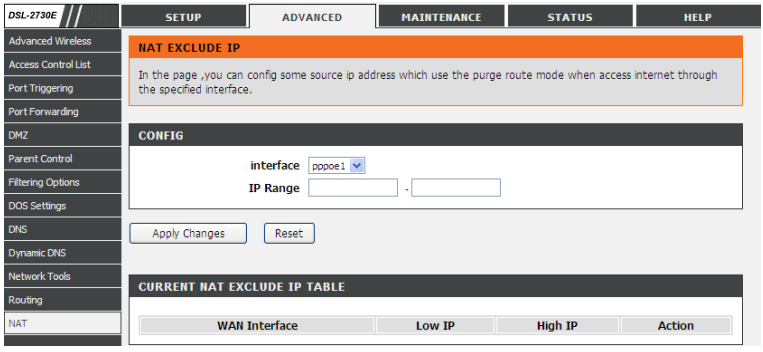
3.3.13.1 NAT ALG

Choose **Advanced** > **NAT** > **NAT ALG**. The **NAT ALG and Pass-Through** page shown in the following figure appears. Choose the NAT ALG and Pass-Through options, and then click **Apply Changes**.



3.3.13.2 NAT Exclude IP

Choose **Advanced** > **NAT** > **NAT Exclude IP**. The **NAT EXCLUDE IP** page shown in the following figure appears. In the page, you can configure some source IP addresses which use the purge route mode when accessing the Internet through the specified interface.

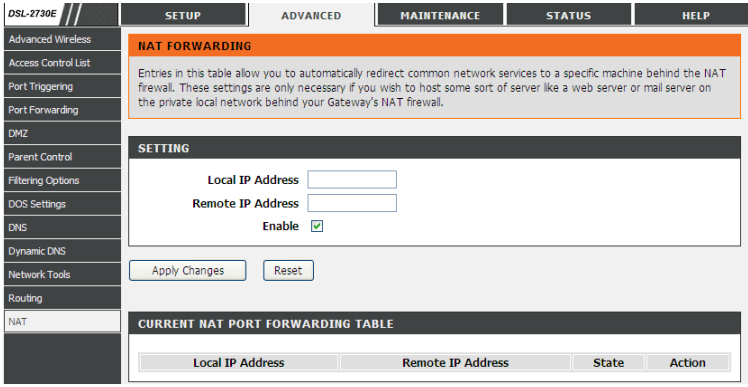


3.3.13.3 NAT Forwarding

Choose **Advanced** > **NAT** > **NAT Forwarding**. The **NAT Forwarding** page shown in the following figure appears.

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Under 1483MER or 1483Routed mode, if NAPT (Network Address Port Translation) is enabled, the **Local IP Address** is configured as 192.168.1.3 and the **Remote IP Address** is configured as 202.32.0.2, the PC with the LAN IP192.168.1.3 will use 202.32.0.2 when it is connected to the Internet via the router without NAPT control.



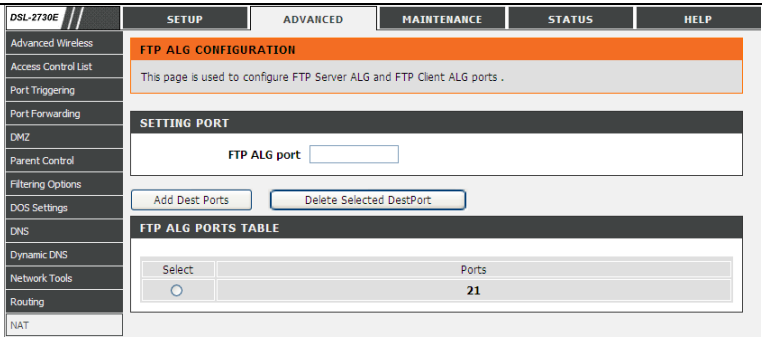
The following table describes the parameters and buttons of this page:

Field	Description
Local IP Address	Input a local IP address.
Remote IP Address	Input a remote IP address
Enable	Enable the current configured rule.
Apply Changes	Submit the configurations.
Reset	Cancel the modification and reconfigure the settings.
Current NAT Port Forwarding Table	Current configuration rule list.

3.3.13.4 FTP ALG Config

The common port for FTP connection is port 21, and a common ALG monitors the TCP port 21 to ensure NAT pass-through of FTP. By enabling this function, when the FTP server connection port is not a port 21, the FTP ALG module will be informed to monitor other TCP ports to ensure NAT pass-through of FTP.

Choose **Advanced** > **NAT** > **FTP ALG Config**. The **FTP ALG Configuration** page shown in the following figure appears.



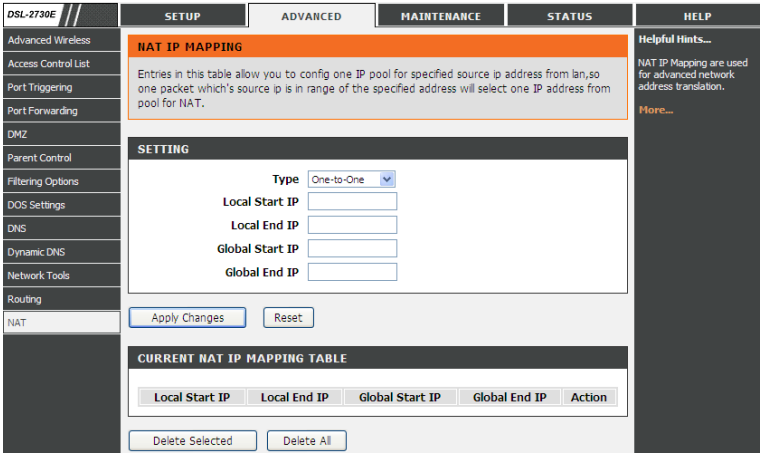
The following table describes the parameters and buttons of this page:

Field	Description
FTP ALG port	Set an FTP ALG port.
Add Dest Ports	Add a port configuration.
Delete Selected DestPort	Delete a selected port configuration from the list.

3.3.13.5 NAT IP Mapping

Choose **Advanced** > **NAT** > **NAT IP Mapping**. The **NAT IP Mapping** page shown in the following figure appears.

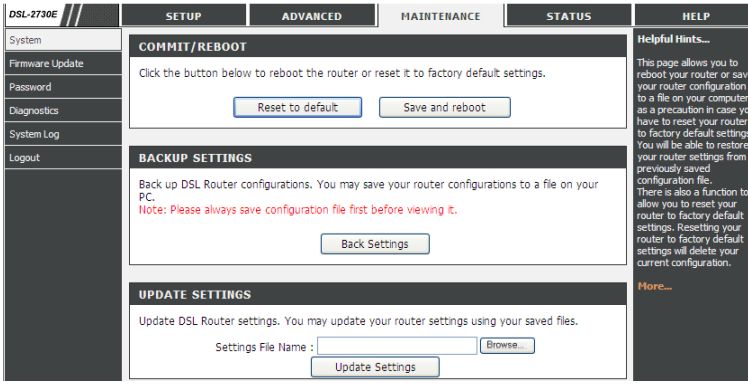
Entries in the **Current NAT IP Mapping Table** allow you to configure one IP pool for a specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.



3.4 Maintenance

3.4.1 System

Choose **Maintenance** > **System**. The page shown in the following figure appears. In this page you can reboot your router or save your router configuration to a file on your computer in case you have to reset your router to factory default settings. You can restore your router settings from a previously saved configuration file. You may also reset your router to factory default settings. Resetting your router to factory default settings will delete your current configuration.



The following table describes the parameters and buttons of this page:

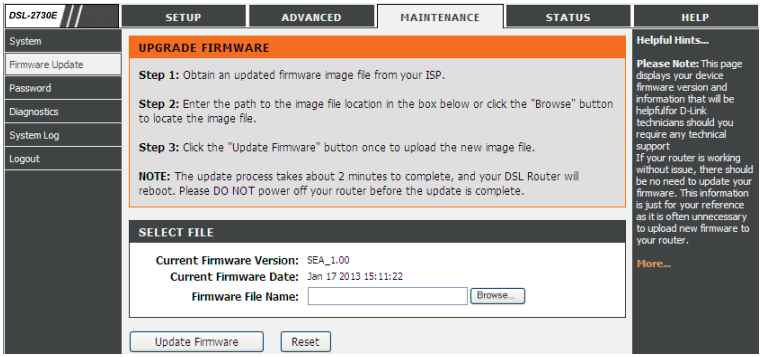
Field	Description
Reset to default	This option restores all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. All settings will be lost. If you want to save your router configuration settings, use the **Backup Settings** option below.
Save and reboot	This will save all your settings and restart the router.
Back settings	Save your configurations in a file on your computer so that it may be accessed again later if your current settings are changed. Be sure to save the configuration before performing a firmware update.
Update settings	Click **Browse** to select the configuration file of device and click **Update Settings** to begin restoring the device configuration.

Note:

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

3.4.2 Firmware Update

Choose **Maintenance** > **Firmware Update**. The page shown in the following figure appears. This page displays your device firmware version and information that will be helpfulfor D-Link technicians should you require any technical support.



The procedure for updating the firmware is as follows.

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

Step 2 Click **Update Firmware** to update the configuration file.

Step 3 Wait for the router to reboot. This can take another minute or more.

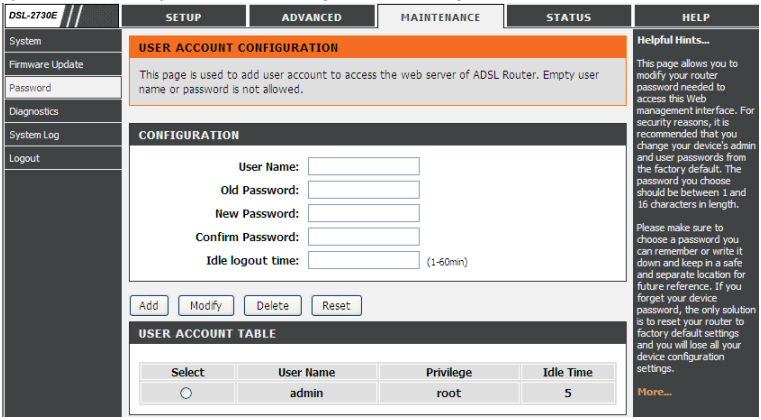
Note:

Some firmware updates reset the configuration options to the factory defaults. Before performing an update, be sure to save the current configuration. Refer to 3.4.1 System.

3.4.3 Password

Choose **Maintenance** > **Password**. The page shown in the following figure appears. You may modify your router password needed to access this Web management interface. For security reasons, it is recommended that you change the default admin and user passwords of the router. The password you choose should be between 1 and 16 characters in length. If you forget your device

password, the only solution is to reset your router to factory default settings and you will lose all your device configuration settings.



The following table describes the parameters and buttons of this page:

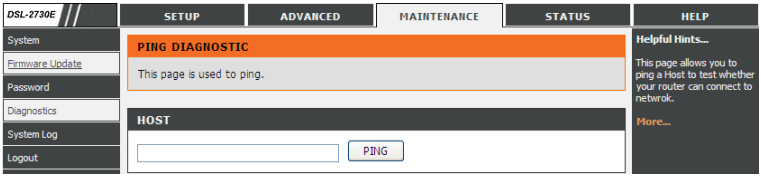
Field	Description
Root	The root account is fixed, having full access to the Web-based management interface.
User	The user account has the previlege to view configuration settings and statistics and update the router's firmware.

3.4.4 Diagnostics

Choose **Maintenance** > **Diagnostics**. The page shown in the following figure appears. Your router is capable of testing your DSL connection. If a test displays a fail status, click “Rerun Diagnostic Tests” at the bottom of this page to make sure the fail status is consistent.

3.4.4.1 Ping Diagnostic

Choose **Maintenance** > **Diagnostics** > **Ping**. The page shown in the following figure appears. This page allows you to ping a Host to test whether your router can be connected to the netwrok.

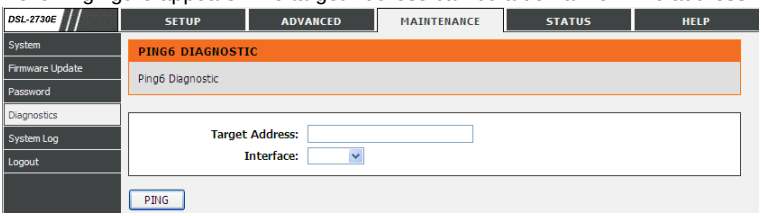


The following table describes the parameter and button of this page:

Field	Description
Host	Enter the valid IP address or domain name.
Ping	Click it to start to Ping.

3.4.4.2 Ping6

Choose **Maintenance** > **Diagnostics** > **Ping6**. The page shown in the following figure appears. The target Address can be a domain or IPv6 address.

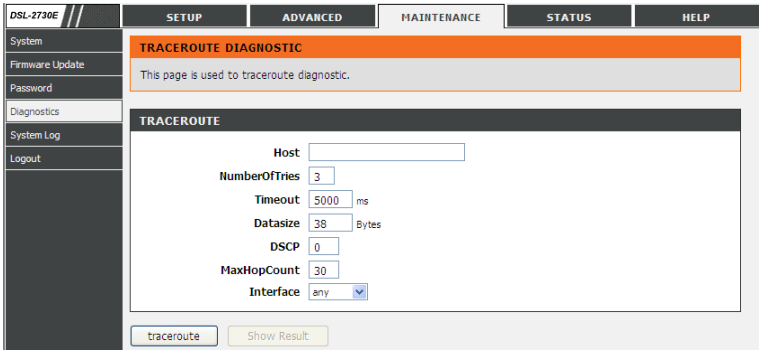


The following table describes the parameter and button of this page:

Field	Description
Target Address	Enter an IP address for Ping6 diagnosis.
Interface name	Enter an interface through which the Ping6 diagnosis is performed.

3.4.4.3 Traceroute

Choose **Maintenance** > **Diagnostics** > **Traceroute**. The page shown in the following figure appears. You can track the route path through the information which is from your computer to the other side host on the Internet.

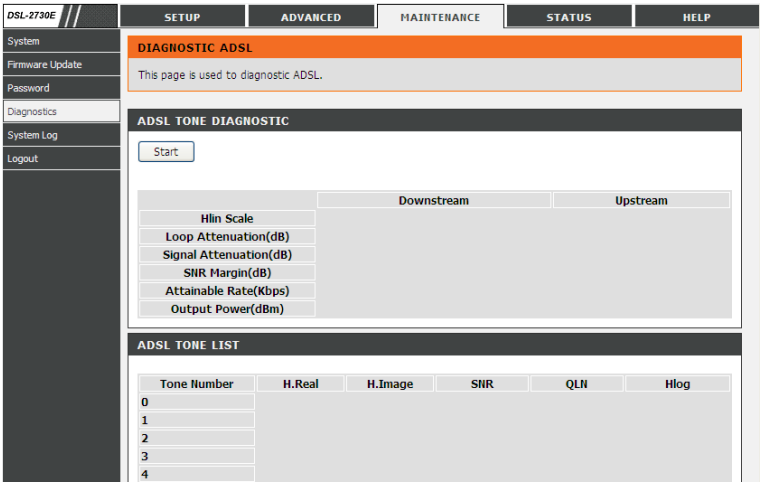


The following table describes the parameters and buttons of this page.

Field	Description
Host	Enter the destination host address for diagnosis.
NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Datasize	Packet size.
DSCP	Differentiated Services Code Point, You should set a value between 0-63.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.
Traceroute	Click start traceroute.

3.4.4.4 ADSL

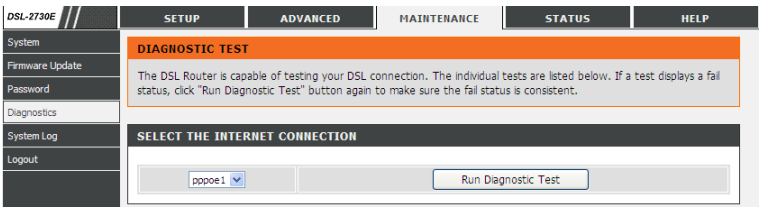
Choose **Maintenance** > **Diagnostics** > **ADSL**. The page shown in the following figure appears. It is used for ADSL tone diagnostics.



Click **Start** to start ADSL tone diagnostics.

3.4.4.5 Diag Test

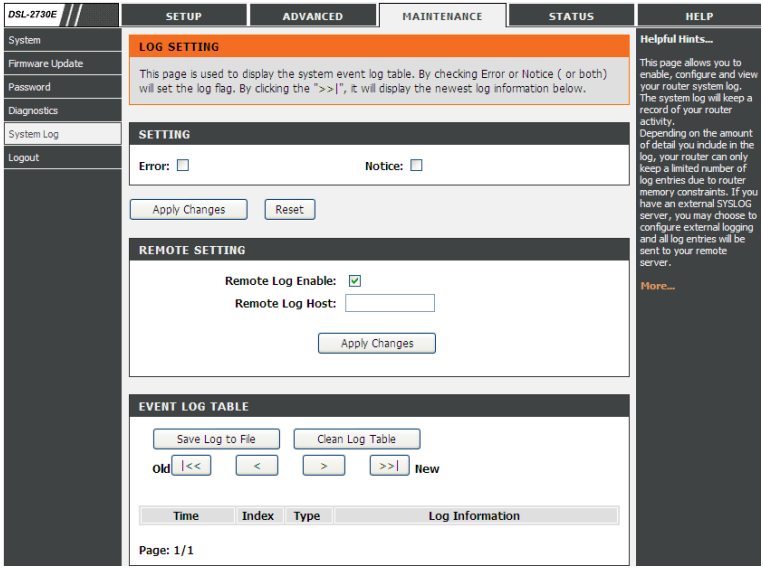
Choose **Maintenance** > **Diagnostics** > **Diag Test**. The page shown in the following figure appears. In this page, you can test the DSL connection. You can also view the LAN status connection and ADSL connection.



3.4.5 System Log

Choose **Maintenance** > **System Log**. The page shown in the following figure appears. This section when enabled allows the system to begin logging events based on the selected log level.

The router can only keep a limited number of log entries due to router memory constraints. If you have an external SYSLOG server, you may choose to configure external logging and all log entries will be sent to your remote server.

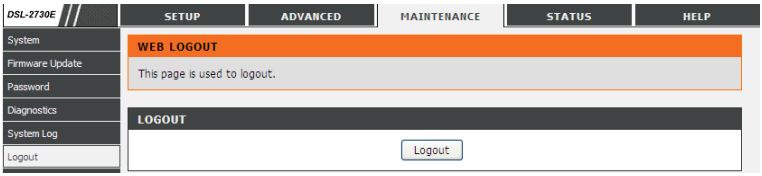


The following table describes the parameters and buttons of this page.

Field	Description
Error	When the system is likely to result in a module abnormity, the system generates an Error log.
Notice	When the system is under attack or logged in, or port status changes, the system generates a Notice log.
Remote Log Host	Send system log to remote host, maybe a domain or an IP.
Save Log to File	You can save current log table to a file.

3.4.6 Logout

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

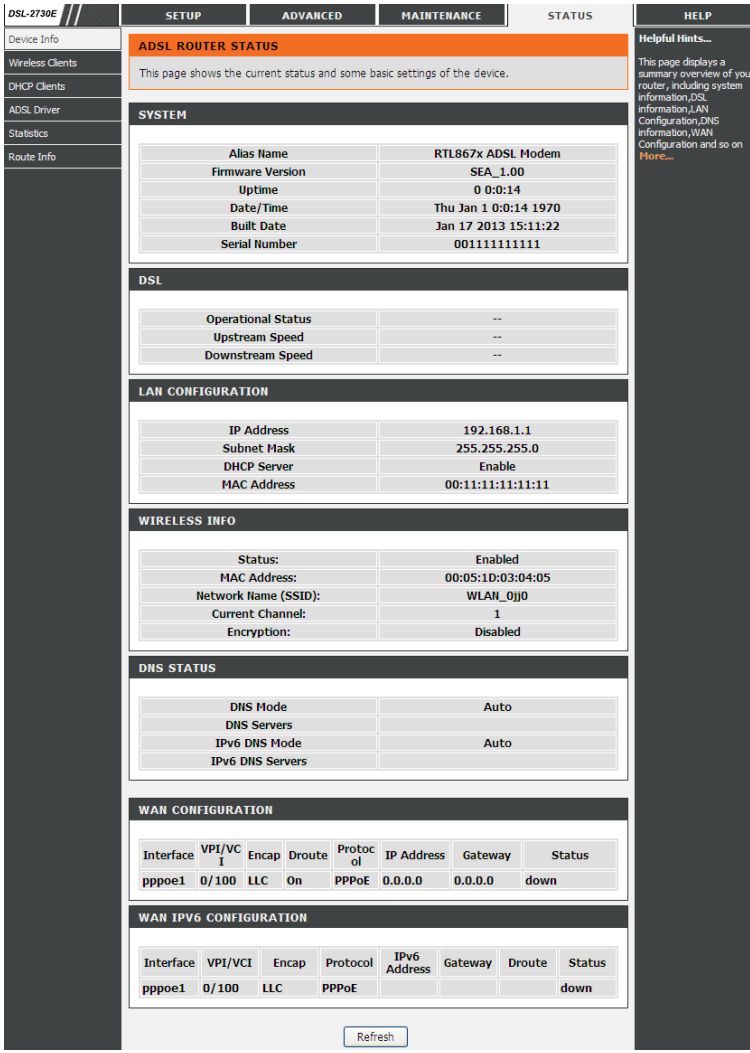


3.5 Status

You can view the system information and monitor performance

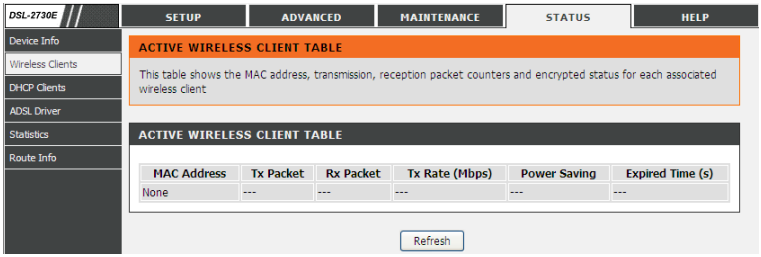
3.5.1 Device Info

Choose **Status** > **Device Info**. The page shown in the following figure appears. This page displays a summary overview of your router, including system information, DSL information, LAN Configuration, DNS information, WAN Configuration and so on.


DSL-2730E
SETUP
ADVANCED
MAINTENANCE
STATUS
HELP
Device Info
Wireless Clients
DHCP Clients
ADSL Driver
Statistics
Route Info
ADSL ROUTER STATUS
This page shows the current status and some basic settings of the device.
SYSTEM
Alias Name RTL867x ADSL Modem
Firmware Version SEA_1.00
Uptime 0 0:0:14
Date/Time Thu Jan 1 0:0:14 1970
Built Date Jan 17 2013 15:11:22
Serial Number 001111111111
DSL
Operational Status --
Upstream Speed --
Downstream Speed --
LAN CONFIGURATION
IP Address 192.168.1.1
Subnet Mask 255.255.255.0
DHCP Server Enable
MAC Address 00:11:11:11:11:11
WIRELESS INFO
Status: Enabled
MAC Address: 00:05:1D:03:04:05
Network Name (SSID): WLAN_0jj0
Current Channel: 1
Encryption: Disabled
DNS STATUS
DNS Mode Auto
DNS Servers
IPv6 DNS Mode Auto
IPv6 DNS Servers
WAN CONFIGURATION
Interface VPI/VCI Encap Droute Protocol IP Address Gateway Status
pppoe1 0/100 LLC On PPPoE 0.0.0.0 0.0.0.0 down
WAN IPV6 CONFIGURATION
Interface VPI/VCI Encap Protocol IPv6 Address Gateway Droute Status
pppoe1 0/100 LLC PPPoE down
Refresh
Helpful Hints...
This page displays a summary overview of your router, including system information,DSL information,LAN Configuration,DNS information,WAN Configuration and so on
More...

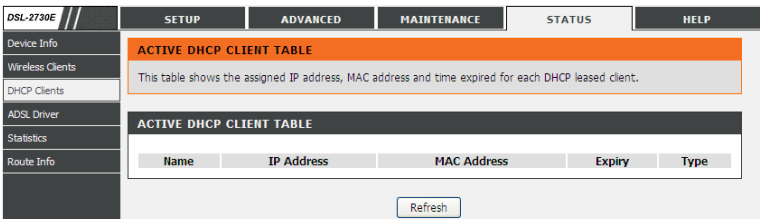
3.5.2 Wireless Clients

Choose **Status** > **Wireless Clients**. The page shown in the following figure appears. This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.



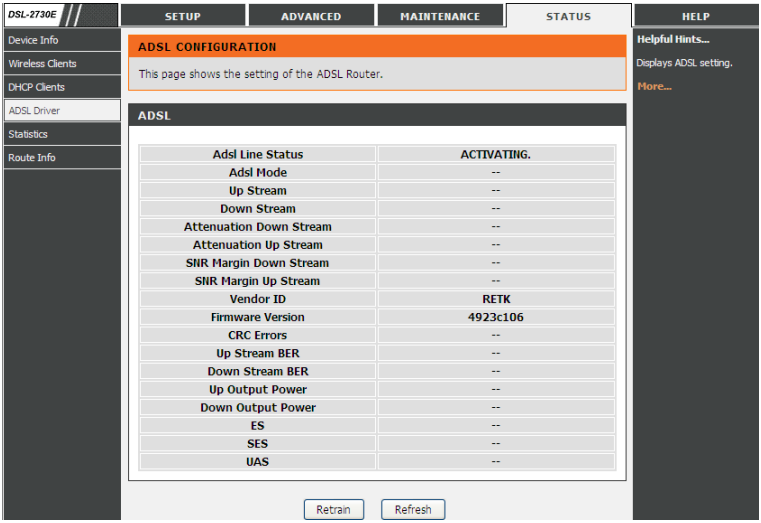
3.5.3 DHCP Clients

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



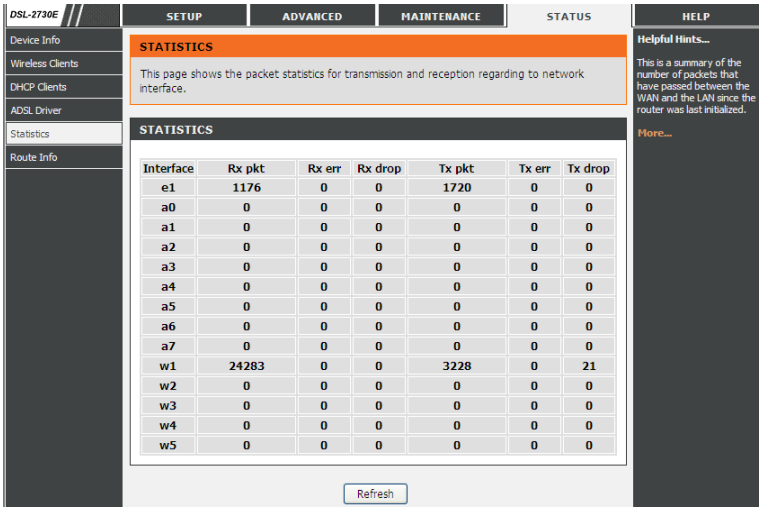
3.5.4 ADSL Driver

Choose **Status** > **ADSL Driver**. The page shown in the following page appears. This page displays all ADSL statistics information, including link down or on, downstream and upstream, type, line coding and so on.



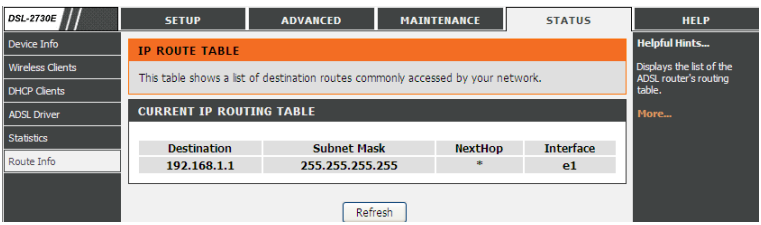
3.5.5 Statistics

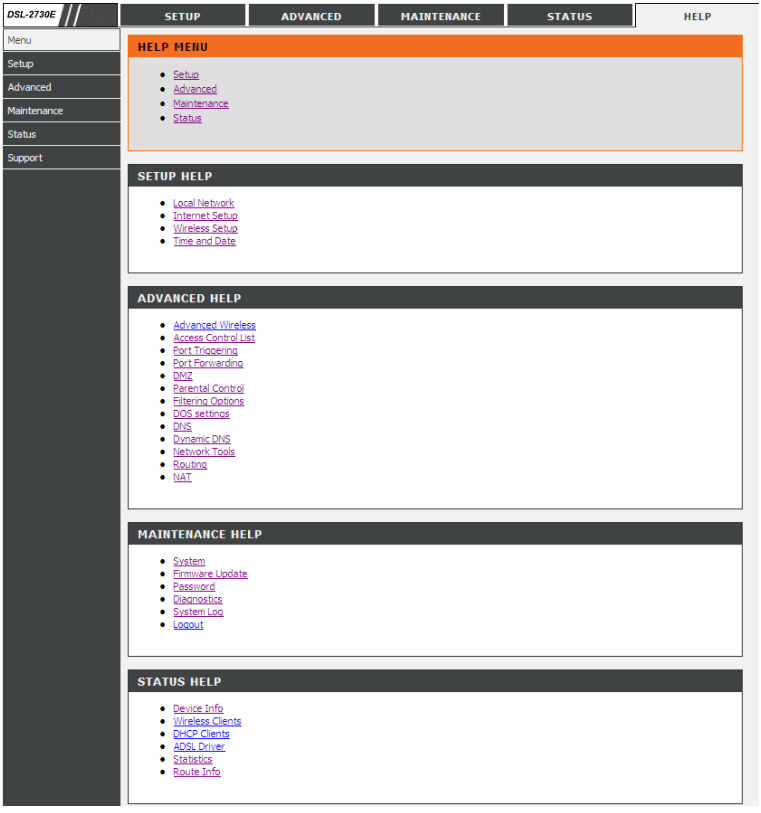
Choose **Status** > **Statistics**. The page shown in the following page appears. This is a summary of the number of packets that have passed between the WAN and the LAN since the router was last initialized.



3.5.6 Route Info

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



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 link to view corresponding information.