D-Link®

Version 1.0 | 04/24/2014

User Manual

Wireless N 300 ADSL2+ Modem Router

DSL-2750U

Contents

SAFETY PRECAUTION **1**
INTRODUCTION **1**
SYSTEM REQUIREMENTS **2**
Features 3
INSTALLATION **4**
Before You Begin 4
Installation Notes 4
Information you will need from your ADSL service provider 6
Information you will need about your DSL-2750U Router 7
Information you will need about your LAN or computer 8
Hardware Description and Installation 9
LED Indicators *9*
Best Location for Wireless Operation *11*
Connecting the Router *11*
TCP/IP Configuration On A PC 14
WEB CONFIGURATION **15**
Logging in the Router 15
Setup 16
Wizard *16*
Internet Setup-ADSL WAN *21*
Internet Setup-Ethernet WAN *24*
Wireless *25*
Local Network *28*
LAN IPv6 ..... *30*
Time and Date *30*
Logout *31*
Advanced 32
Advanced Wireless *32*
Port Forwarding *35*
DMZ *37*
SAMBA *37*
3G Configuration *38*
Parental Control *40*
Filtering Options *42*
QoS Configuration *45*
Firewall Setting *47*
DNS *48*
Dynamic DNS *48*
Network Tools *49*
MLD Configuration *50*
Routing *53*
Schedules *55*
NAT *55*
FTPD Setting *56*
FTPD Account *56*
IP Tunnel *56*
Logout *58*
MANAGEMENT 58
Global IPv6 ..... *59*
System Management *59*
Firmware Update *59*
Access Controls *60*
Diagnosis *61*
Log Configuration *62*
Logout *62*
Status 63
Help 63
TROUBLESHOOTING **64**
NETWORKING BASICS **66**
Check Your IP Address 66
Statically Assigning an IP Address 67
TECHNICAL SPECIFICATIONS **68**

Safety Precaution

Follow the following instructions to prevent the device from risks and damage

- Use the power adapter in the package.
- An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid overheating. The holes on the device are designed for heat dissipation to ensure running normally. Do not cover these heat dissipation holes.
- Do not put this device close to a heat source or high temperature place. Avoid the device direct exposing sunshine.
- Do not put this device close to over damp place. Do not spill any fluid on this device.
- Do not connect this device to PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

Introduction

The DSL-2750U supports multiple line modes. With four 10/100 base-T Ethernet interfaces at the user end, the DSL-2740U provides both DSL uplink access with a downstream rate of 24 Mbps and an upstream rate of 1 Mbps and Ethernet uplink access. It also supports 3G connection to the Internet or Intranet for high-end users like net bars and office users. It complies with specifications of IEEE 802.11, 802.11b/g/n, WEP, WPA, and WPA2 security. The WLAN of the device supports 2T2R.

System Requirements

Network Requirement	Available uplink access (DSL uplink or Ethernet uplink)
Clients to be connected	Devices installed a wireless network adapter or 10 base T/100BaseT Ethernet adapter.
Web-based Configuration Utility Requirement	Computer with the following: Windows®, Macintosh, or Linux-based operating system An installed Ethernet adapter Browser Requirements: Microsoft Internet Explorer® v7, Mozilla® Firefox v9.0, Google® Chrome 16.0, or Safari® v4 or higher version. Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Features

The device supports the following features:

- Various line modes
- Two uplink access: DSL and Ethernet uplink access
- External PPPoE dial-up access
- Internal PPPoE/PPPoA dial-up access
- 1483Bridged/1483Routed with dynamic IP or static IP
- Multiple PVCs (the number of PVCs support is eight)
- DHCP server/relay
- Static route
- Network Address Translation(NAT)
- DMZ
- Virtual Server
- Universal plug and play (UPnP)
- Dynamic Domain Name Server(DDNS)
- Network Time Protocol(NTP)
- Firmware upgrading through Web, TFTP, or FTP
- Resetting to the factory defaults through Reset button or Web
- Diagnostic test
- Web interface
- Telnet CLI
- IP/MAC/URL Filter
- Application layer service
- QoS
- Port binding
- Auto upgrade
- Cloud security
- Digital Living Network Alliance (DLNA)
- Wireless network
- 3G network

Installation

This section will guide you through the installation process. Placement of the Router is very important. Do not place the Router in an enclosed area such as a closet, cabinet or in the attic or garage.

Before You Begin

Please read and make sure you understand all the prerequisites for proper installation of your new Router. Have all the necessary information and equipment on hand before beginning the installation.

Installation Notes

In order to establish a connection to the Internet it will be necessary to provide information to the Router that will be stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required. You can print out the two pages below and use the tables to list this information. This way you have a hard copy of all the information needed to setup the Router. If it is necessary to reconfigure the device, all the necessary information can be easily accessed. Be sure to keep this information safe and private.

Low Pass Filters
Since ADSL and telephone services share the same copper wiring to carry their respective signals, a filtering mechanism may be necessary to avoid mutual interference. A low pass filter device can be installed for each telephone that shares the line with the ADSL line. These filters are easy to install passive devices that connect to the ADSL device and/or telephone using a standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

Operating Systems
The DSL-2750U uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, Windows XP, Windows Vista, Windows 7, and Windows 8.

Web Browser
Any common web browser can be used to configure the Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Opera, Microsoft Internet Explorer® version 6.0, Netscape Navigator® version 6.2.3, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)
Any computer that uses the Router must be able to connect to it through the Ethernet port on the Router. This connection is an Ethernet connection and therefore requires that your computer be equipped with an Ethernet port as well. Most notebook computers are now sold with an Ethernet port already installed. Likewise, most fully assembled desktop computers come with an Ethernet NIC adapter as standard. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the Router. If you need to install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

Additional Software
It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using the device as a simple bridge. For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device, not in the Router itself.

If your ADSL service is delivered through a PPPoE or PPPoA connection, the information needed to establish and maintain the Internet connection can be stored in the Router. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

All connections to the Internet require a unique global IP address. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN side of the bridge, such as a PC, a server, a gateway device, such as a router, or similar firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

Information you will need from your ADSL service provider

Username
This is the Username used to log on to your ADSL service provider's network. Your ADSL service provider uses this to identify your account.

Password
This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account.

WAN Setting / Connection Type
These settings describe the method your ADSL service provider uses to transport data between the Internet and your computer. Most users will use the default settings. You may need to specify one of the following WAN Setting and Connection Type configurations (Connection Type settings listed in parenthesis):

- PPPoE/PPPoA (PPPoE LLC, PPPoA LLC or PPPoA VC-Mux)
- Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC Mux)
- IPoA/MER (Static IP Address) (Bridged IP LLC, 1483 Bridged IP VC Mux, 1483 Routed IP LLC, 1483 Routed IP VC-Mux or IPoA)
- MER (Dynamic IP Address) (1483 Bridged IP LLC or 1483 Bridged IP VC-Mux)

Modulation Type
ADSL uses various standardized modulation techniques to transmit data over the allotted signal frequencies. Some users may need to change the type of modulation used for their service. The default DSL modulation (ADSL2+ Multi-Mode) used for the Router automatically detects all types of ADSL, ADSL2 and ADSL2+ modulation.

Security Protocol
This is the method your ADSL service provider will use to verify your Username and Password when you log on to their network. Your Router supports the PAP and CHAP protocols.

VPI
Most users will not be required to change this setting. The Virtual Path Identifier (VPI) is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

VCI
Most users will not be required to change this setting. The Virtual Channel Identifier (VCI) is used in conjunction with the VPI to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Setup window of the web management interface.

Information you will need about your DSL-2750U Router

Username
This is the Username needed to access the Router's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Router is "admin."

Password
This is the Password you will be prompted to enter when you access the Router's management interface. The default Password is "admin." The user may change this.

LAN IP addresses for the DSL-2750U
This is the IP address you will enter into the Address field of your web browser to access the Router's configuration graphical user interface (GUI) using a web browser. The default IP address is **192.168.1.1**. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.

LAN Subnet Mask for the DSL-2750U
This is the subnet mask used by the DSL-2750U and will be used throughout your LAN. The default subnet mask is **255.255.255.0**.

Information you will need about your LAN or computer

Ethernet NIC
If your computer has an Ethernet NIC, you can connect the DSL-2750U to the Ethernet port using an Ethernet cable.

DHCP Client status
Your DSL-2750U ADSL Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-2750U will assign are from 192.168.1.2 to 192.168.1.254. Your computer (or computers) needs to be configured to obtain an IP address automatically (that is, they need to be configured as DHCP clients.)

It is recommended that you backup or record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your DSL-2750U ADSL Router.

Hardware Description and Installation

LED Indicators

Note:

The figures in this document are for reference only.

Figure 1 Front panel

The following table describes the LEDs of the device.

LED	Color	Status	Description
Power	Green	On	The initialization of the system is complete.
	Red	On	The device is initiating.
		Blinking	The firmware is upgrading.
LAN	Green	Off	The Ethernet interface is not properly connected.
		Blinking	The Ethernet interface is properly connected and data is being transmitted.
		On	The Ethernet interface is properly connected, but no data is being transmitted.
2.4GHz	Green	Blinking	The WLAN function is enabled and data is being transmitted on the WLAN.
		On	The WLAN function is enabled, but no data is being transmitted on the WLAN.
		Off	The WLAN function is disabled.
WPS	Green	Blinking	WPS is successfully triggered.
		Solid on for 5 seconds and then turns off	Connection is successfully established between the router and the client through WPS.
USB	Green	On	The 3G or USB flash disk has been connected.
		Blinking	Data is being transmitted.
		Off	USB connection is not established.

LED	Color	Status	Description
DSL	Green	Off	No signal is being detected.
		Blinking	The device is handshaking with the physical layer of the office end.
		On	A connection is set up with the physical layer of the office end.
Internet	Green	Off	The device is under the Bridge mode or powered off.
		On	A connection is set up and no traffic is detected.
		Blinking	Data is being transmitted over Internet.
	Red	On	The device is attempted to become IP connected, but failed.

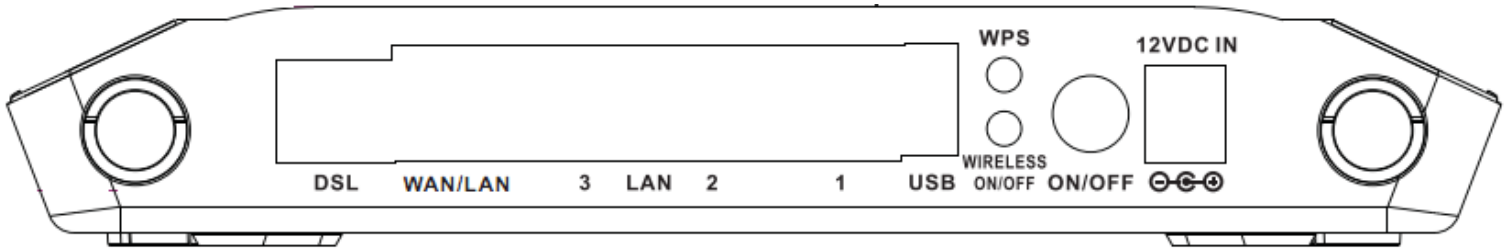


Figure 2 Rear panel

The following table describes the interfaces of the device.

Interface/Button	Description
DSL	RJ-11 interface for connecting the host to the telephone jack on the wall or the **MODEM** interface of the splitter through a telephone line.
WAN/LAN	This Ethernet RJ-45 interface has two functions. ● Worked as a WAN interface that connects to the WAN for Ethernet uplink ● Worked as a LAN interface that connects to the Ethernet interfaces of computers or Ethernet devices.
LAN3/2/1	For a PC or other Ethernet-abled device to join the LAN of 2750U by being connected to this interface with RJ-45 cable.
USB	USB port, for connecting the 3G network card or other USB storage devices.
WPS	Press and hold the button for 5 seconds starts WPS negotiation.
WIRELESS ON/OFF	Press and hold the button for 5 seconds starts WLAN.
ON/OFF	Power switch, which is used to power on or power off the router.
12V DC IN (power)	Interface for connecting the power adapter.
Reset (On the bottom side)	Press and hold the button for 1 second to restore the factory defaults.

Best Location for Wireless Operation

Many environmental factors may affect the effective wireless function of the DSL Router. If this is the first time that you set up a wireless network device, read the following information:
The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, as you may need to view them for troubleshooting.
Designed to go up to 100 meters indoors and up to 300 meters outdoors, wireless LAN lets you access your network from anywhere you want. However, the numbers of walls, ceilings, or other objects that the wireless signals must pass through limit signal range. Typical ranges vary depending on types of materials and background RF noise in your home or business.

Connecting the Router

- **DSL Uplink Connection**

The following figure displays the application diagram for the connection of the device, PC, splitter and telephone sets, when no telephone set is placed before the splitter

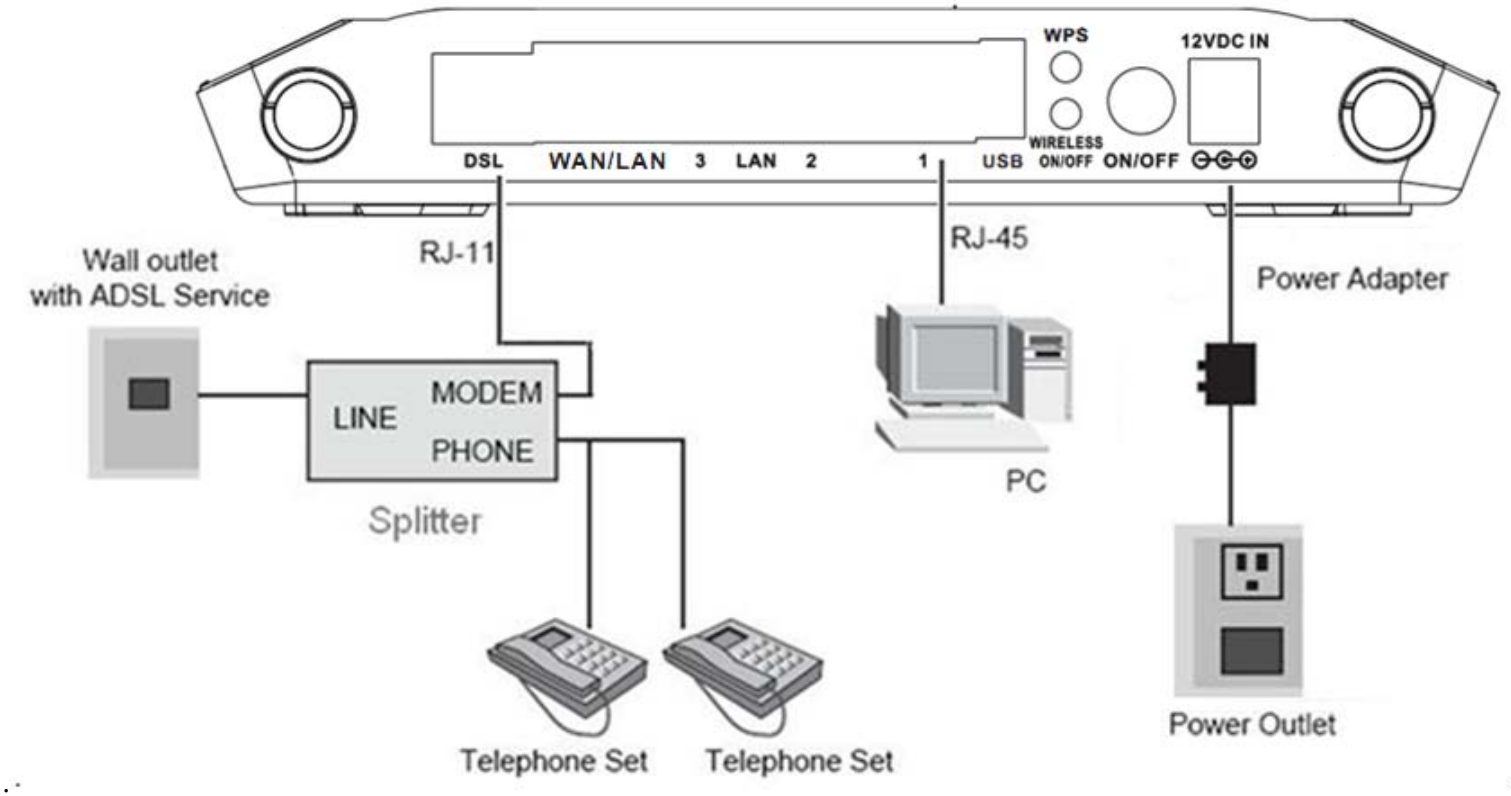


Figure 3 DSL uplink connection

Step 1 Connect the **DSL** port of the router and the Modem port of the splitter through a telephone cable; connect the phone to the phone port of the splitter through a telephone cable; and connect the Line port of the splitter to the uplink telephone jack on the wall.

The spliter has three ports:

- **LINE**: Connect to a wall phone jack (RJ-11 jack)
- **MODEM**: Connect to the Line interface of the router
- **PHONE**: Connect to a telephone set

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

Step 3 Plug the power adapter to the wall outlet and then connect the other end of it to the **Power** (12V DC IN) port of the route.

- **Ethernet Uplink Connection**

The following figure displays the Ethernet uplink connection.

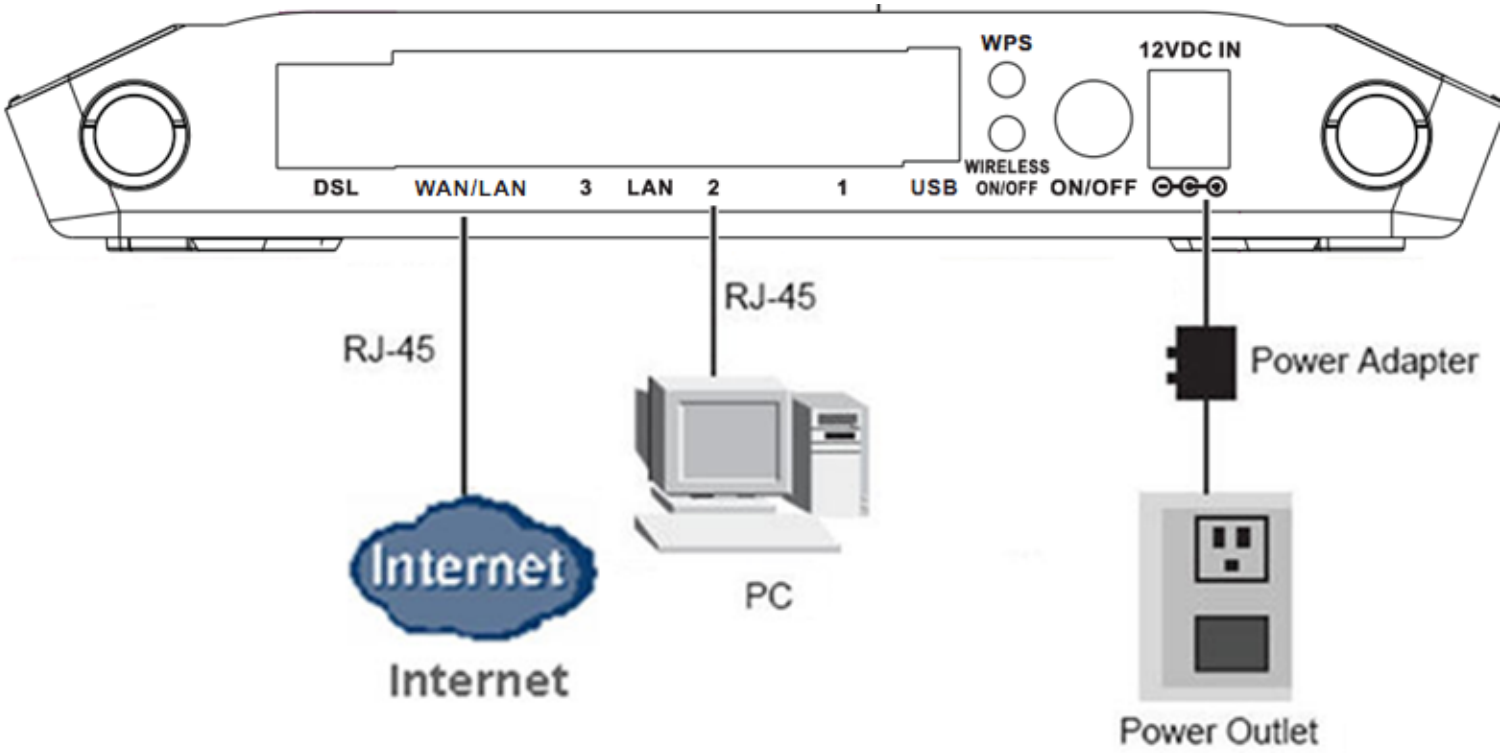


Figure 4 Ethernet uplink connection

Step 1 Connect the LAN interface of the wireless router to your PC with RJ45 Ethernet cable.
Step 2 Connect the WAN/LAN interface of the wireless router to the uplink network device with RJ45 Ethernet cable.
Step 3 Connect the power adapter to the 12V DC IN interface of the wireless router.

TCP/IP Configuration On A PC

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.
The configuration principle is identical but should be carried out differently on each operating system.
The right figure displays the **TCP/IP Properties** dialog box on Windows XP.

TCP/IP configuration steps for Windows XP are as follows:

Step 1 Choose **Start** > **Control Panel** > **Network Connections**.

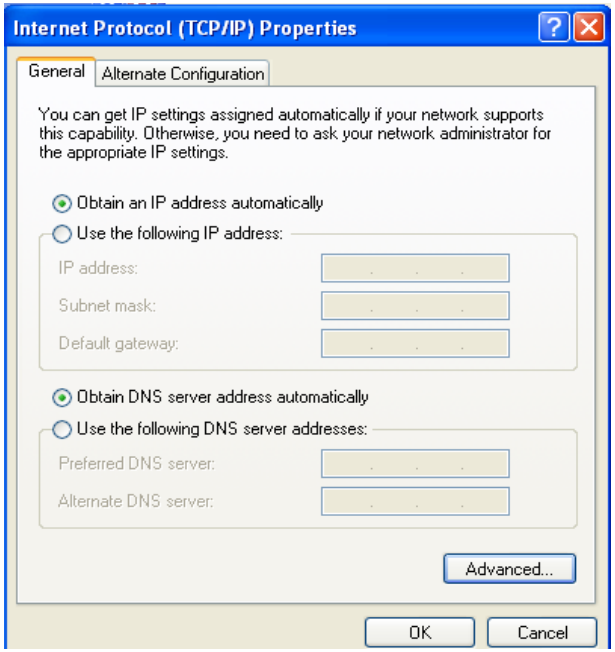
Step 2 Right-click the Ethernet connection icon and choose **Properties**.

Step 3 On the General tab, select the Internet Protocol (TCP/IP) component and click Properties. The Internet Protocol (TCP/IP) Properties window appears.

Step 4 Select the **Obtain an IP address automatically** button.

Step 5 Select the **Obtain DNS server address automatically** button.

Click **OK** to save the settings.



Web Configuration

This chapter describes how to use Web-based management of the DSL router, which allows you to configure and control all of DSL router features and system parameters in a user-friendly GUI.

Logging in the Router

The following description is a detail “How-To” user guide and is prepared for first time users.

Step 1 Open the Internet Explorer (IE) browser, and then go to **http://192.168.1.1**.

Step 2 The Login page is shown as the figure appears on the right. Select **admin** from the drop-down list of username and enter the password. And then click **Login**.

- The default password is **admin**.

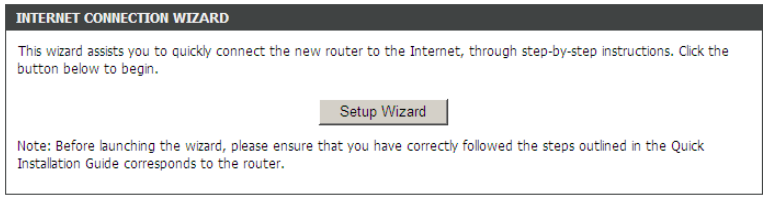
Select **Remember my login info. on this computer**, you only need to enter the password once for the first time logging.

Setup

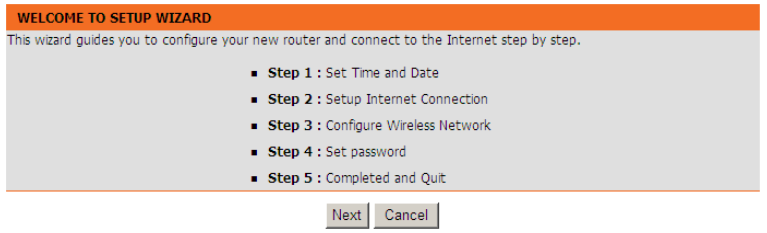
Wizard

Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe these various configuration parameters.
When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. The connection type of your physical WAN device can be Ethernet, DSL, or both. Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or the protocol, such as PPPoA or PPPoE, that you use to communicate over the Internet.

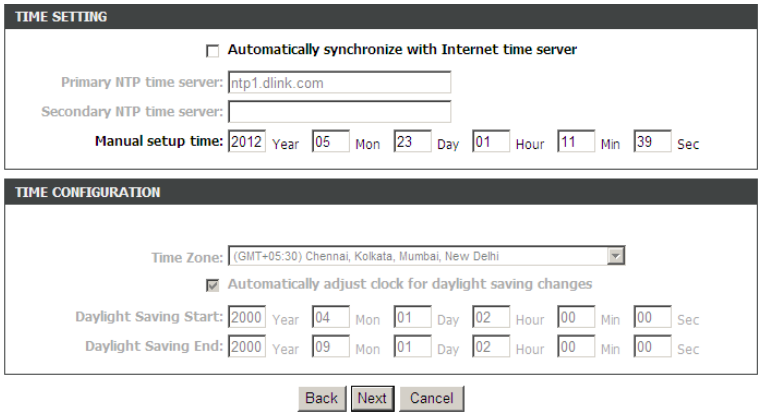
Choose **SETUP** > **Wizard**. The page is shown as the figure appears on the right.



Step 1 Click **Setup Wizard**. The page is shown as the figure appears on the right. There are 5 steps to configure the device. Click **Next** to continue.



Step 2 Set the time and date, and then click **Next**.



Step 3 Configure the Internet connection.

There are 2 types of WAN access: DSL and Ethernet.

- **For DSL WAN access:**

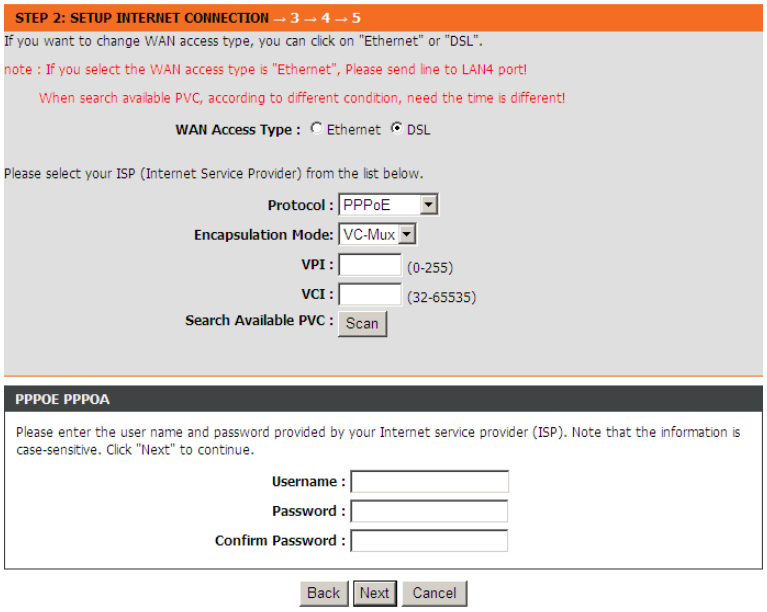
There are 6 types of connection mode: PPPoE, PPPoA, Dynamic IP, Static IP, Bridge, and IPoA.

- **PPPoE/PPPoA**

If the protocol is set to **PPPoE** or **PPPoA**, the page shown as the right figure appears.

1) Choose **DSL** in WAN Access Type.
2) Select **PPPoE** in Protocol.
3) Enter the VPI and VCI provided by your ISP.
4) Enter the Username and Password provided by your ISP.
5) Re-enter the password for confirmation.

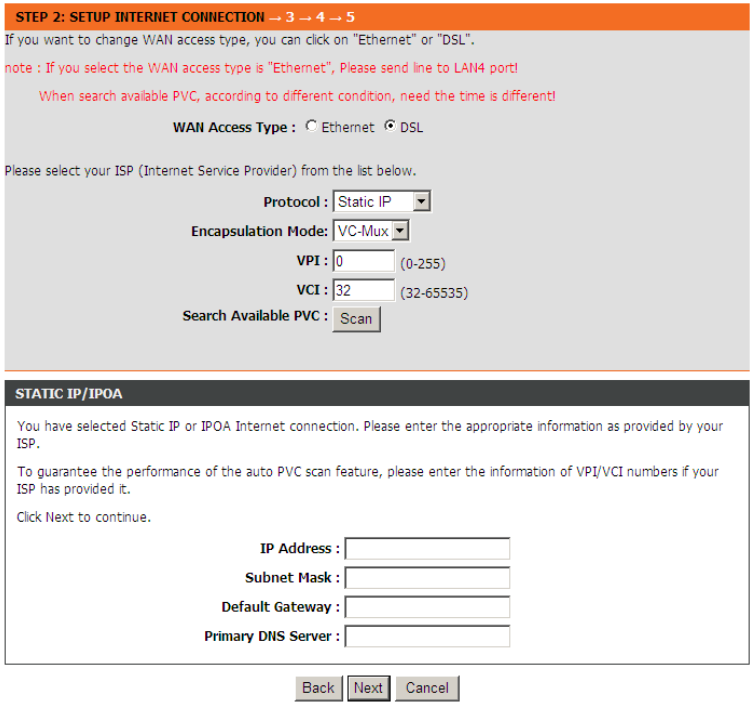
Click **Next** to go to the next page.



- **Static IP/IPoA**

If the protocol is set to **Static IP**, the page shown as the right figure appears.
You can set the parameters in this page as follow:

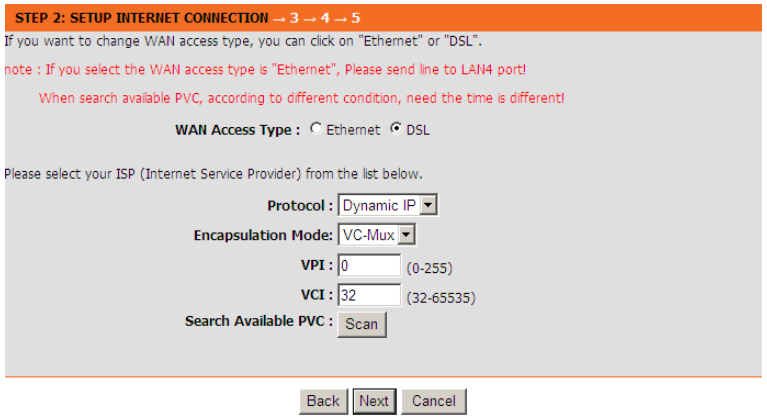
1) Set the protocol to **Static IP**.
2) Choose the Encapsulation Mode provided by your ISP.
3) Enter the **VPI** and **VCI** provided by your ISP.
4) Enter the WAN IP Address, Subnet Mask, Default Gateway, and Primary DNS Server provided by your ISP.



- **Dynamic IP/Bridge**

If the protocol is set to **Dynamic IP/Bridge**, the page shown as the right figure appears.
In this page, enter the connection type, VPI, and VCI provided by your ISP.

After setting, click **Next**.

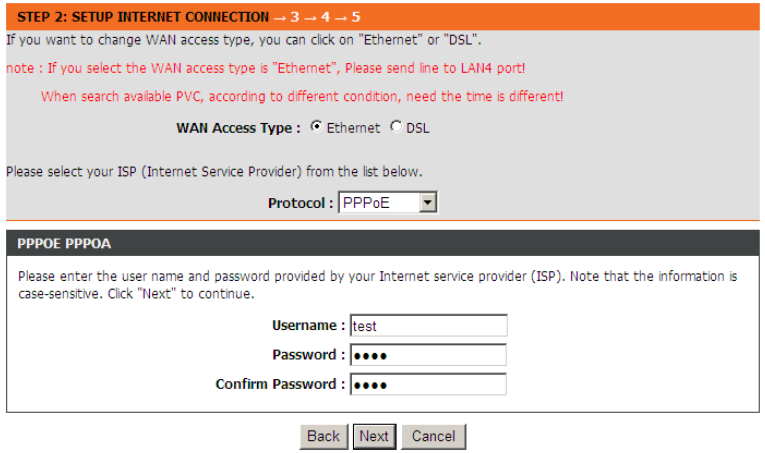


- **For Ethernet WAN access:**

There are 4 types of connection mode: **PPPoE**, **Dynamic IP**, **Static IP**, and **Bridge**.

Note:

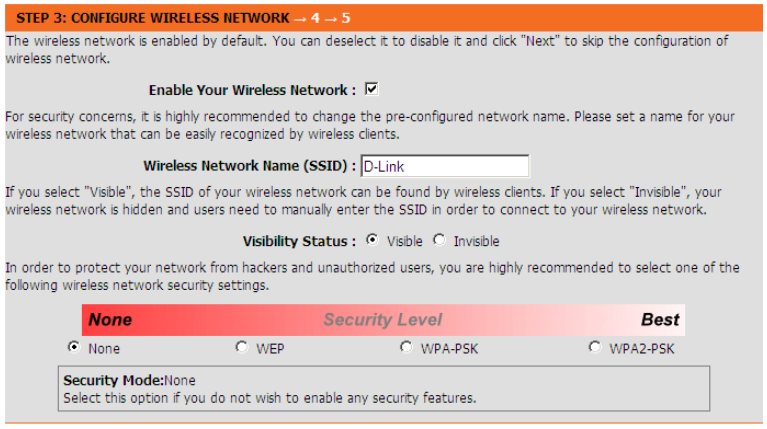
If the selected WAN access type is Ethernet, please connect the WAN/LAN port to the Ethernet uplink jack through a RJ45 cable.



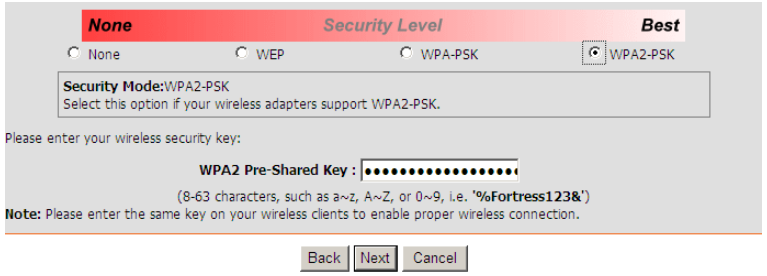
In this page, select protocol according to the Internet service you subscribed from your ISP. And then input the entries with the information provided by your ISP. After setting, click **Next**.

Step 4 Configure the wireless network in this page.

1) Check **Enable Your Wireless Network**.
2) Set the SSID for your wireless network, you can also keep it as default.
3) Choose to display or hide your wireless network.
   - **Visible**: Your wireless network can be detected.
   - **Invisible**: You wireless network cannot be detected. Wireless clients needs to enter the SSID and password manually to join this wireless network.



4) Set the security level. The default security level of wireless network is **None**. Choose an encryption mode for the wireless network. It is recommended to choose **WPA2-PSK**.
5) Enter a new password in **WPA2 Pre-Shared Key**.
6) Click **Next** to go to the next page.



Step 5 Set a new login password. If you want to keep the previous password, click **Skip** to go to next page directly. After setting a new password, click **Next**.

Note:

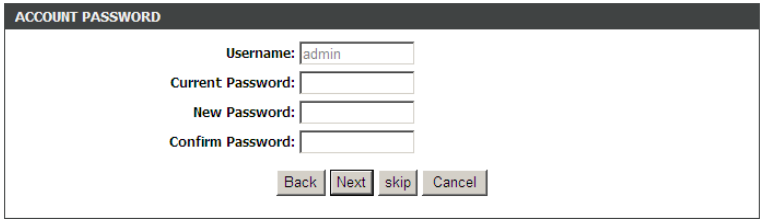
The login password cannot contain a space.

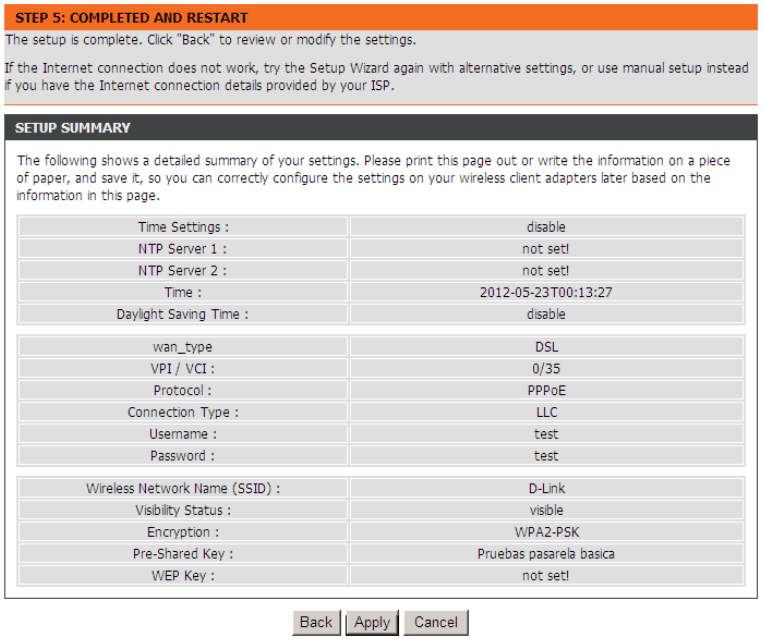
Step 6 View the setup summary.

Click **Apply** to take the setup into effect.

Click **Back** to modify the setup.

Click **Cancel** to cancel the whole setup.





Internet Setup-ADSL WAN

Choose **SETUP** > **Internet Setup**. The page is shown as the figure appears on the right. In this page, you can add or configure WAN interface of your router.

Step 1 Select **DSL** in WAN Access Type.

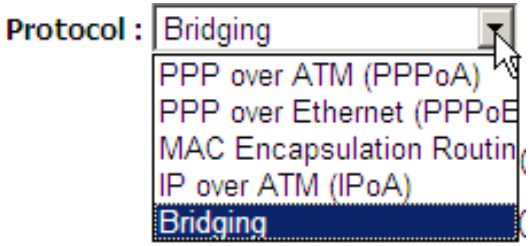
Step 2 Click **Add** to add a PVC.

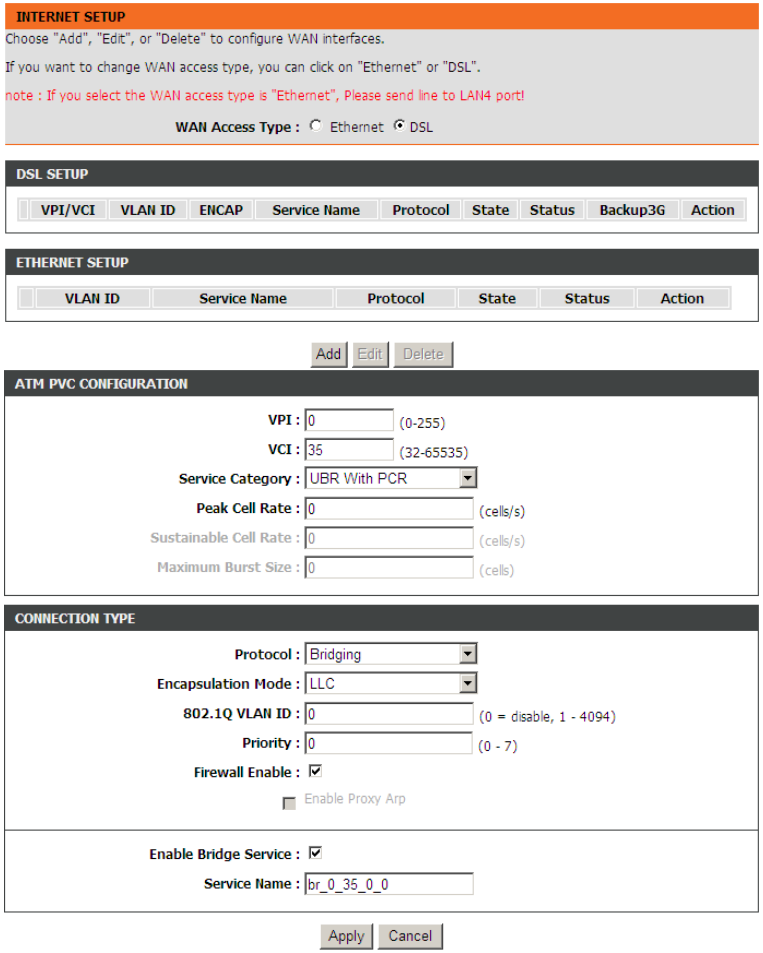
Note:

To access the internet, at least one PVC is required to add.

Step 3 In the VPI and VCI textbox, enter the VPI and VCI value provided by your ISP.

Step 4 In the protocol drop-down list, select the protocol according to the internet service you subscribed from your ISP. There are 5 types of protocols: **PPP over ATM (PPPoA)**, **PPP over Ethernet (PPPoE)**, **MAC Encapsulation Routing (MER)**, **IP over ATM (IPoA)**, **Bridging**.

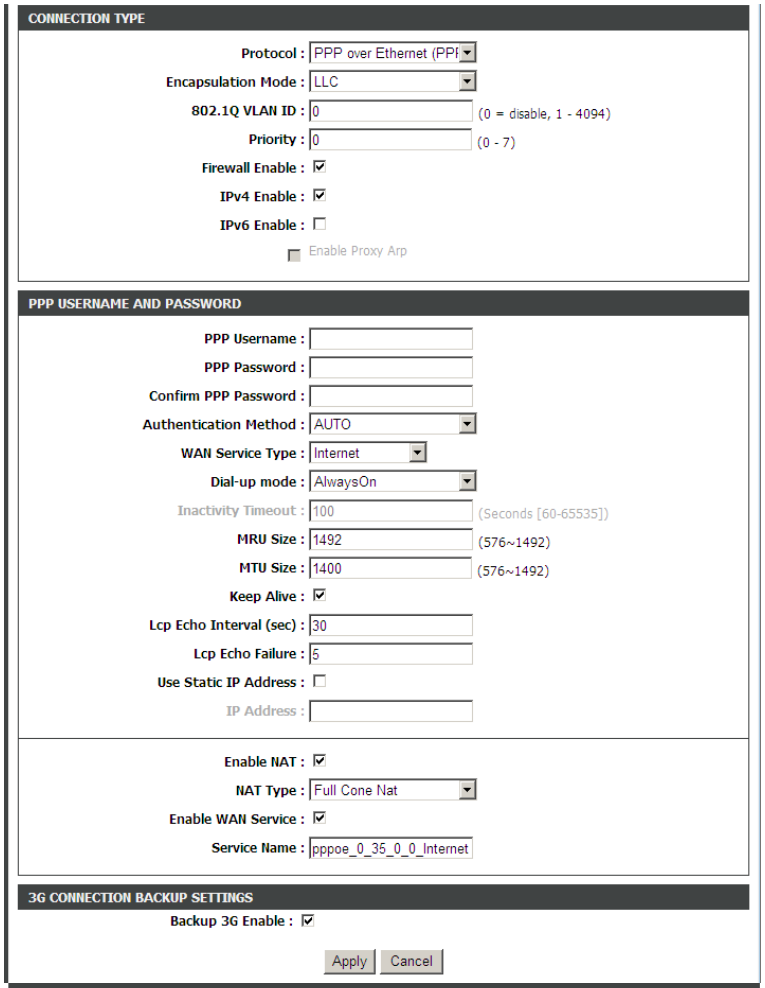




- Adding a PVC in **PPPoE** or **PPPoA** mode

If the protocol is selected to **PPP over Ethernet (PPPoE)** or **PPP over ATM (PPPoA)**, the page shown as the right figure appears.

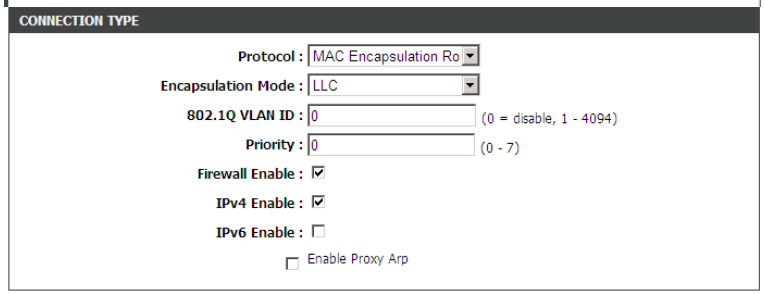
1) In **Protocol** drop-down list, select **PPPoE** (or **PPPoA**).
2) In **Encapsulation** Mode, select an option according to the information provided by your ISP.
3) In the PPP Username and PPP Password textbox, input the Username and password of PPPoE account provided by your ISP.
4) In the **Confirm PPP Password** textbox, re-enter the password.
5) In the **Authentication Method** drop-down list, select **Auto**.
6) In the **WAN Service Type** drop-down list, select **Internet**.
7) In the **Dial-up Mode** drop-down list, select an option as you demand. There are 3 modes available: Continuous, Connect On Demand, Manual.
   - **Continuous**: The system automatically keeps dialing for WAN connection once the connection is off-line.
   - **Connect On Demand**: The system automatically dials for WAN connection once network access request is detected. If no request is sent from the LAN within the IdleTime, the system automatically disconnect from the internet. You can set the Idle Time as you need.
   - **Manual**: Manually dial to connect the WAN once powering on the Router.
8) For other entries which are not mentioned above, you can keep them as defaults.



- Adding a PVC in **MAC Encapsulation Routing (MER)** or **IP Over ATM (IPoA)** mode

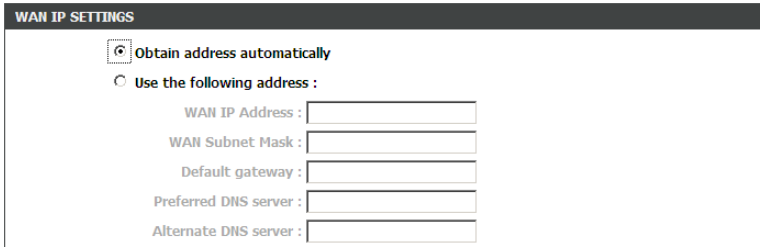
If the protocol is selected to **MAC Encapsulation Routing (MER)**, the page shown as the right figure appears.

1) In **Protocol** drop-down list, select **MAC Encapsulation Routing (MER)**.
2) In **Encapsulation Mode** drop-down list, select an option according to the information provided by your ISP.

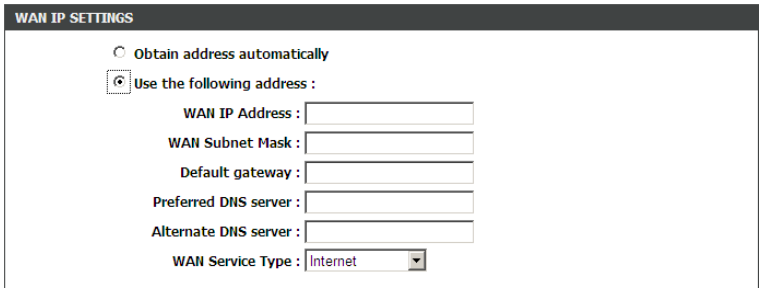


3) In WAN IP Setting section, choose an option according to the information provided by your ISP.

- **Obtain address automatically**: the dynamic WAN IP address will be assigned by your ISP.



- **Use the following address**: A static WAN IP address is provided to you by your ISP. Input the static WAN IP address and other information provided by your ISP.



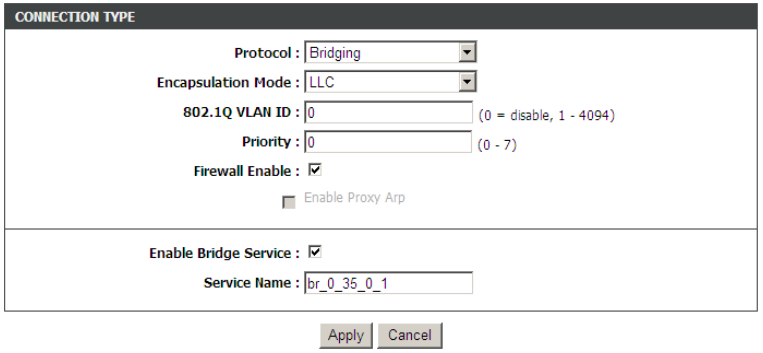
4) For other entries which are not mentioned above, you can keep them as defaults.

- Adding a PVC in **Bridging** mode

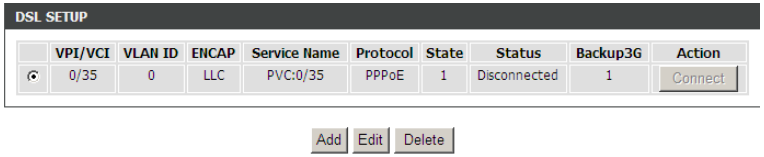
For PVC in Bridging mode, keep the settings as defaults.

Note:

If the connection protocol is in Bridging mode, the connected PC must dial for WAN connection with installed dial-up software.



Step 5 After setting (take adding a PPPoE PVC as an example), click **Apply** and the page skip to the page shown as the right figure appears. You can edit or delete the PVCs in the table.



Internet Setup-Ethernet WAN

Choose **SETUP** > **Internet Setup**. In this page, select **Ethernet** in WAN Access Type. And then the page is shown as the figure appears on the right. In this page, you can add or configure WAN interface of your router.
Click **Add**.

Note:

If the selected WAN access type is Ethernet, please connect the WAN/LAN port to the Ethernet uplink jack through a RJ45 cable.

- Adding a WAN access in **PPPoE** mode:

Step 1 In **Protocol** drop-down list, select **PPP over Ethernet (PPPoE)**.

Step 2 Enter the **PPP Username** and **PPP password** of PPPoE account provided by your ISP.

Step 3 Re-enter the password for confirmation.

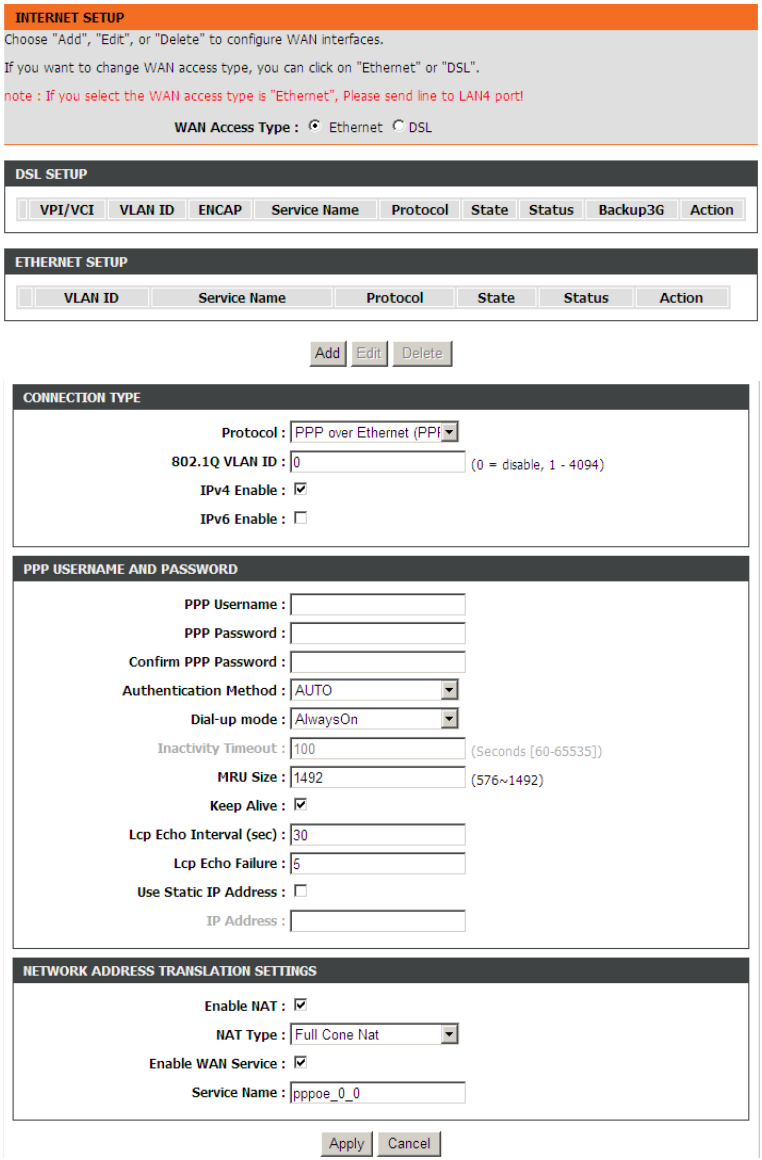
Step 4 Choose a connection type from the Type drop-down list. There are 3 connection types available: **Continuous**, **Connect On Demand**, **Manual**.

Continuous: The system automatically keeps dialing for WAN connection once the connection is off-line.

Connect On Demand: The system automatically dials for WAN connection once network access request is detected. If no request is sent from the LAN within the **IdleTime**, the system automatically disconnect from the internet. You can set the Idle Time as you need.

Manual: Manually dial to connect the WAN once powering on the Router.

Step 5 For the entries that are not mentioned above, keep them as defaults. After setting, click **Add** to add the new channel.

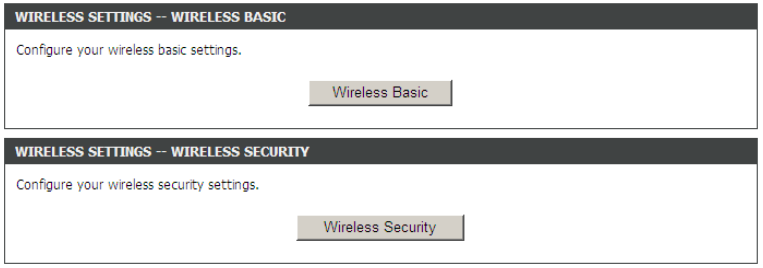


- Adding a WAN access in other modes.

To add a WAN access in other modes, select the corresponding protocol and input the information provided by your ISP.

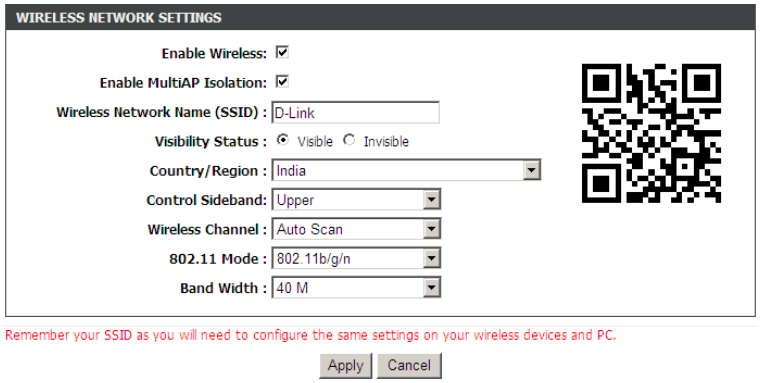
Wireless

This section describes the configuration of 2.4G wireless network.
Choose **SETUP** > **Wireless**. The page shown in the right figure appears. This section contains **Wireless Basic** and **Wireless Security**.



Wireless Basic

Choose **SETUP** > **Wireless** > **Wireless Basic**. The page shown as the right figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.
To configure this page, do as follow:



Step 1 Select **Enable Wireless**.

Step 2 Select **Enable MultiAP Isolation**. After isolate multiAP, the wireless clients connected to the DSL-2750U cannot communicate with each other.

Step 3 In **Wireless Network Name** (SSID) textbox, enter a name for your wireless network. You can also keep it as defaults.

Step 4 Configure **Visibility Status**.

- Select **Visible**, your SSID can be detected by wireless clients automatically.
- Select **Invisible**, the SSID cannot be detected by wireless clients.

Step 5 In **Country/Region** drop-down list, select the country you locate.

Step 6 Keep other entries as defaults.

Click **Apply** to save the settings.

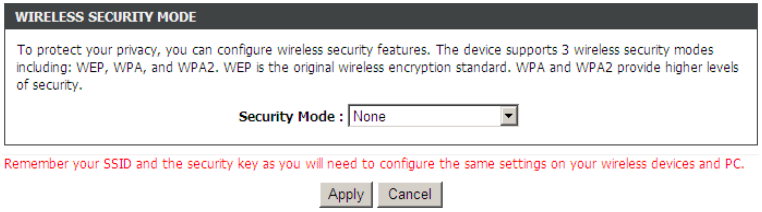
There is a **QRcode** on the right of the page. This QRcode can help your mobile phone connect to the wireless network of DSL-2750U automatically by scan the QRcode with this mobile phone.

Note:

A mobile phone cannot be connected to the wireless network by scanning QRcode unless installing QRcode software.

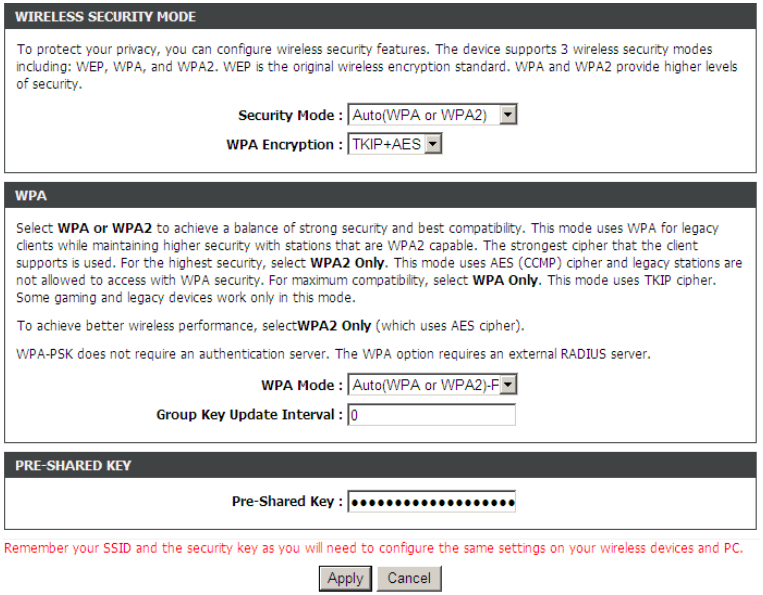
Wireless Security

Choose **SETUP** > **Wireless** > **Wireless Security**. The page shown as the right figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device. Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and wired network.



The default security mode is **None**. If the security mode is set to None, your wireless network can be connected by all wireless clients that can detect the SSID of this network.

If the Security Mode is set to **Auto(WPA or WPA2)**, **WPA only**, or **WPA2 only**,, the page is shown as the right figure appears. Take **Auto(WPA or WPA2)** as an example.



Step 1 In **Security Mode** drop-down list, select **Auto(WPA or WPA2)**.

Step 2 In **WPA Encryption** drop-down list, select **TKIP+AES**.

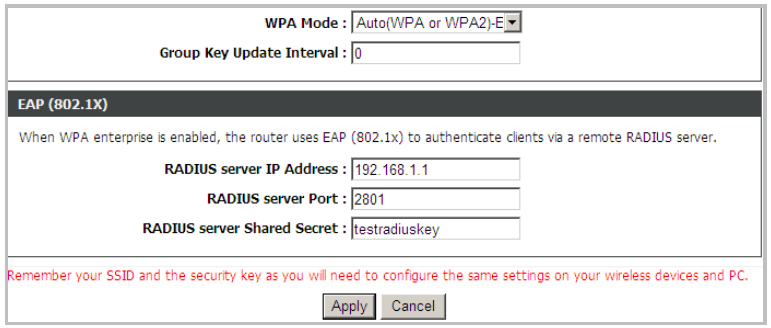
Step 3 Configure the **WPA Mode**.

- **Auto(WPA or WPA2)-PSK**: WPA-PSK does not require an authentication server. You need to set a Pre-shared Key (wireless network password) for your wireless network.

- **Auto(WPA or WPA2)-Enterprise**: When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server. Enter the port, IP address, and password of the Radius server. The wireless clients are required to enter the username and password provided by the Radius server.

Step 4 Set the Group Key Update Interval. For higher security, WPA password is updated periodically. This value is the update interval of the WPA password. You can keep it as default.

Step 5 After setting, click **Apply** to save the settings.



Local Network

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

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

Choose **SETUP** > **Local Network**. The **Local Network** page shown in the right figure appears.

To configure the local network of AC750, do as follow:

Step 1 In the **Router IP Address** textbox, enter the IP address of LAN interface. The default IP address is **192.168.1.1**. The Router IP address is the URL address for logging in the Web configuration page.

Step 2 Enter the subnet mask of LAN interface. If the Router IP address is **192.168.1.1**, the range of subnet mask is from **255.255.0.0** - **255.255.255.254**.

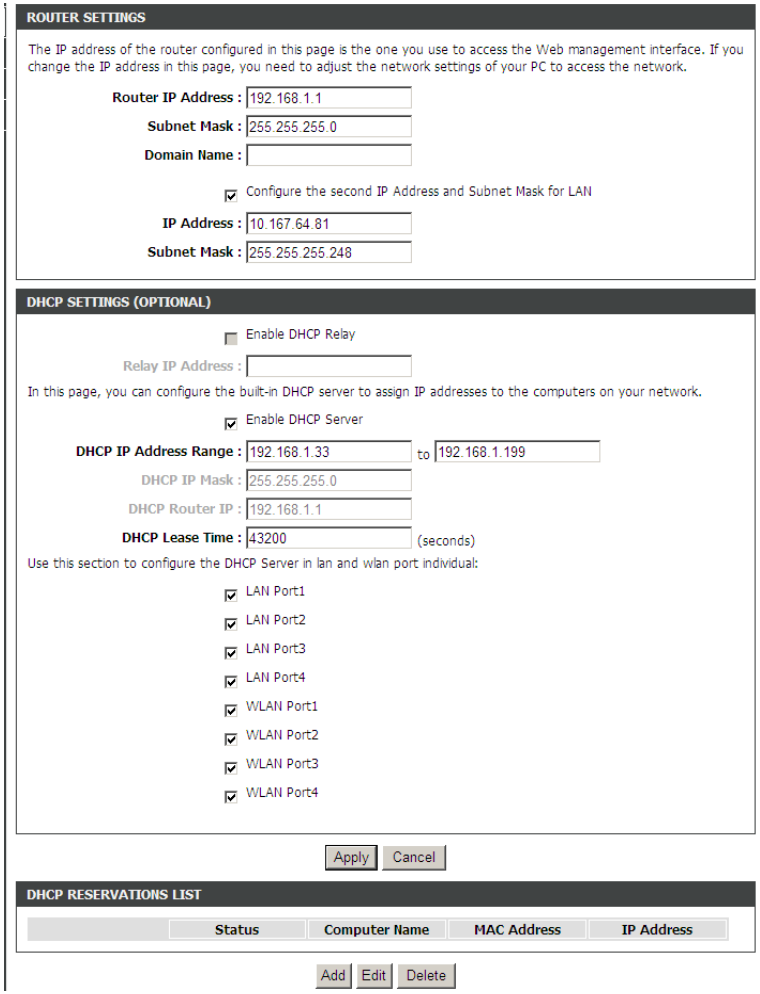
Step 3 In the **Domain Name** textbox, set a domain name. If you leave it blank, a domain name assigned by DHCP from the ISP is used.

Step 4 Select **Configure the second IP Address and Subnet Mask for LAN**. It enables the secondary LAN IP address for your router. It will be used when your primary router IP address is in the same network segment with other LANs. The Secondary router IP address must be in the different network segment from the primary one.

Step 5 Enter the secondary router IP address and subnet mask.

Step 6 Configure DHCP Server.

- **Enable DHCP Relay**: Enable the message to transmit between clients in different network segment.
- **Enable DHCP Server**: Enable the router to assign IP addresses, IP default gateway and DNS Servers to the host.



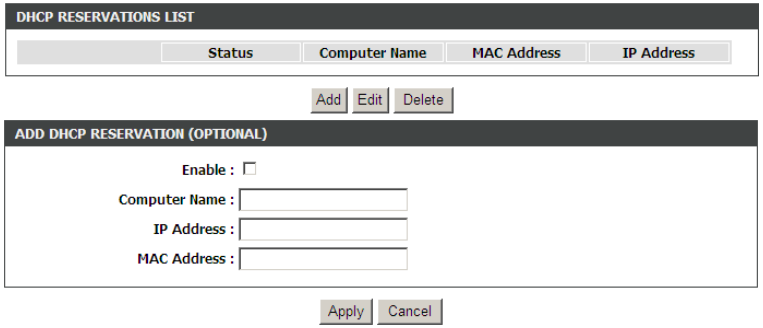
DHCP IP Address Range: It specifies the first IP address in the IP address pool. The router assigns IP address that base on the IP pool range to the host.

DHCP Lease Time: The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.

Step 7 Select the LAN or WAN ports which are going to adopt the setting.

Step 8 Click **Apply** to make the settings take effect.

The **DHCP RESERVATIONS LIST** shown in the right figure appears. It used to reserve a fixed IP address within IP address range for a specified PC. So the DHCP Server will assign that fixed IP address to the specified PC all the time.



Step 1 Click **Add**, the right figure appears.

Step 2 Select **Enable** to enable this DHCP IP address reservation.

Step 3 In the computer name textbox, input the specified computer name.

Step 4 In the IP Address textbox, input an IP address to be assigned to this specified PC. Note: the IP Address must be within the DHCP IP address range.

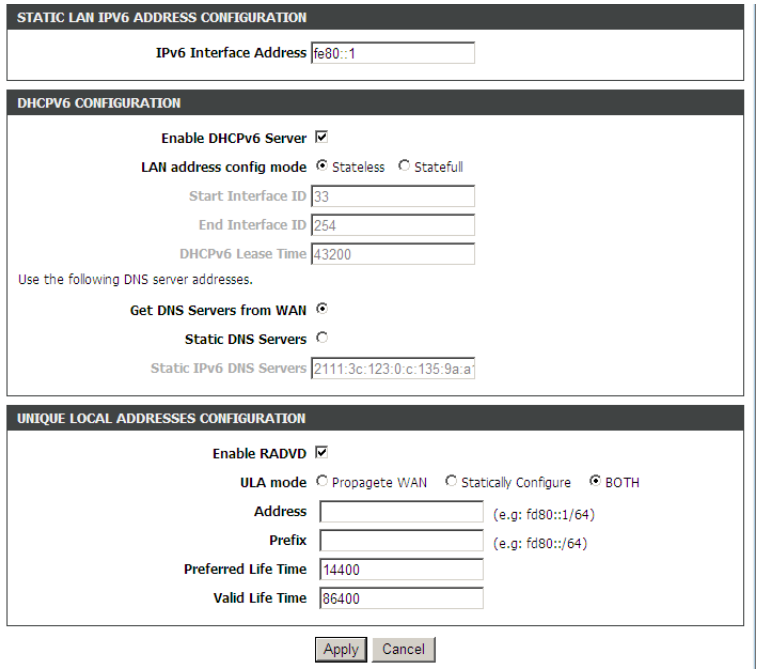
Step 5 In the MAC address textbox, input the MAC address of the specified PC.

Step 6 After setting, click **Apply** to add a DHCP server.

LAN IPv6

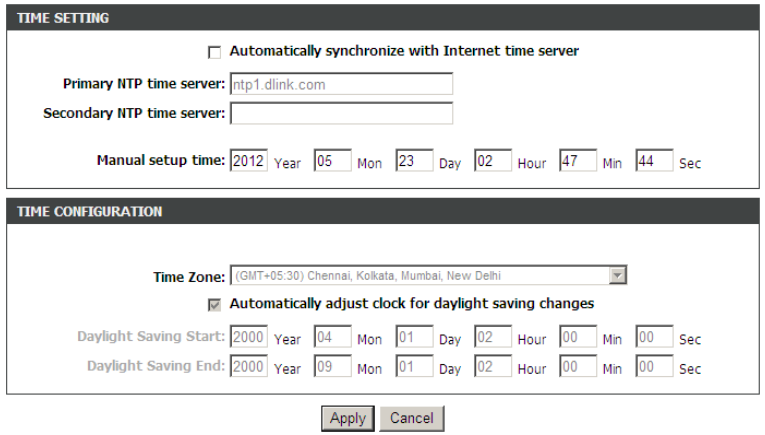
Choose **SETUP** > **LAN IPv6**. The page shown in the right figure appears. This page allows you to configure IPv6 LAN.
The following table describes the parameters of this page.

Field	Description
IPv6 Interface Address	The address through which PCs access the gateway.
Enable DHCPv6 Server	Choose to enable or disable DHCPv6 service.
LAN address config mode	Set the mode address obtaining mode of LAN PCs. You may choose **Stateless** or **Stateful**.
Start/End Interface ID	The address pool using DHCPv6 for address assignment under stateful mode.
DHCPv6 Lease Time	The address lease time using DHCPv6 for address assignment under stateful mode.
Enable RADVD	Choose to enable or disable router advertisement (RADVD) service.



Time and Date

Choose **SETUP** > **Time and Date**. The page shown in the right figure appears. This page allows you to configure IPv6 LAN.
In the **Time and Date** page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.
Select **Automatically synchronize with Internet time servers**.
Enter the specific time server and select the time zone from the corresponding drop-down lists.
Select **Enable Daylight Saving** if necessary. Set the daylight as you want.
Click **Apply** to save the settings.



Logout

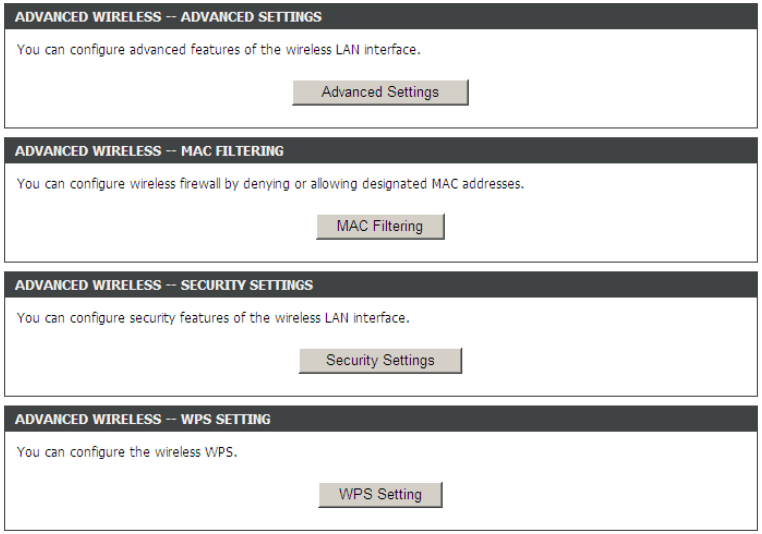
Choose **SETUP** > **Logout**. The page shown in the right figure appears. In this page, you can log out of the configuration page.

Advanced

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

Advanced Wireless

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



Advanced Settings

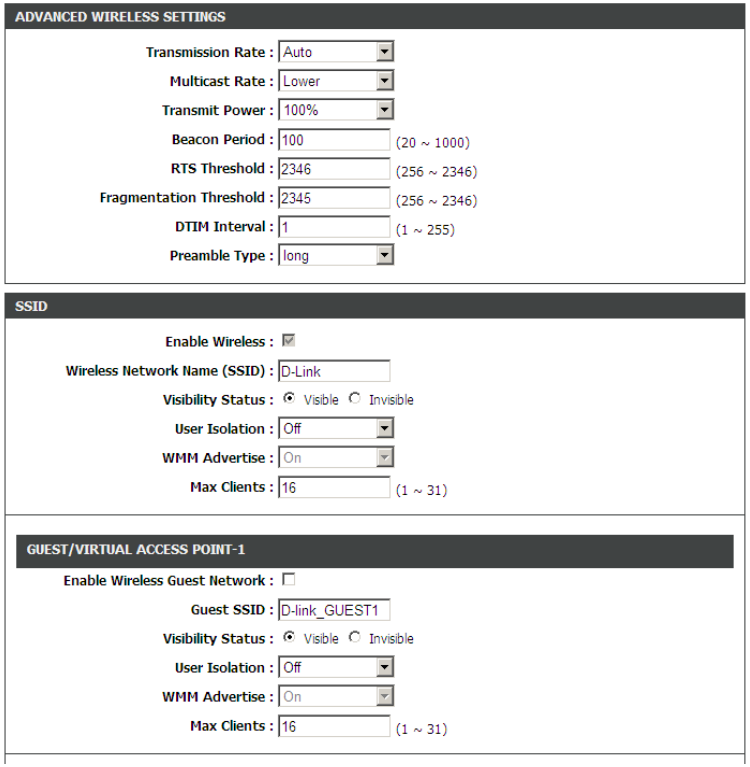
Choose **ADVANCED** > **Advanced Wireless** > **Advanced Settings.** The page shown in the right figure appears. In this page, you can configure guest wireless networks.

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

The router supports multiple SSID. Multiple WLAN SSIDs realizes multiple wireless access points on a single wireless router. Wireless clients being connected to different SSIDs can avoid mutual interference. This function is applied to small office or house joint rent users. For example, 4 departments of a small office are sharing the wireless network of a wireless router, while each department wants to have its own individual WLAN. Multiple WLAN SSIDs function can realize this application.

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

Click **Apply** to save the settings.

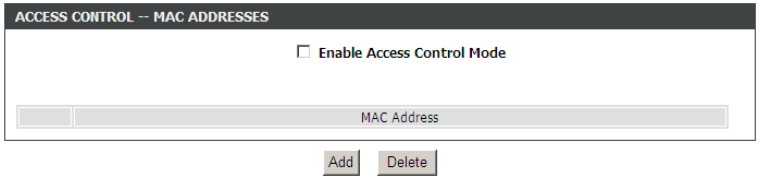


Note:

If you want to know more about the parameters of Advanced Wireless Settings, refer to **HELP** index.

MAC Filtering

Choose **ADVANCED** > **Advanced Wireless** > **MAC Filtering.** The page shown in the right figure appears. This page is used to permit or block access to this router from host with MAC address contained in the **MAC Address** table.

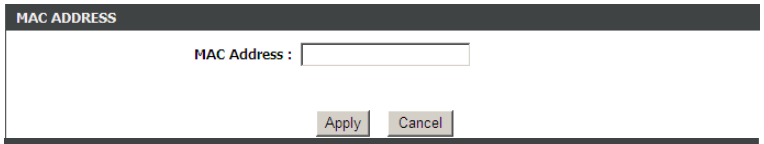


Step 1 Select **Enable Access Control Mode**.

Step 2 Click **Add**. The page shown as the right figure appears.

Step 3 Enter the MAC address of the PC to be filtered.

Step 4 Click **Apply** to add the MAC address.



Security Settings

Choose **ADVANCED** > **Advanced Wireless** > **Security Settings**. In this page, you can set the security for the wireless network.

Step 1 In the **Select SSID** drop-down list, select a SSID to be configured. For example: **D-Link**.

Step 2 In the **Security Mode** drop-down list, select a security encryption mode for the wireless network. It is recommended to select **Auto (WPA or WPA2)**.

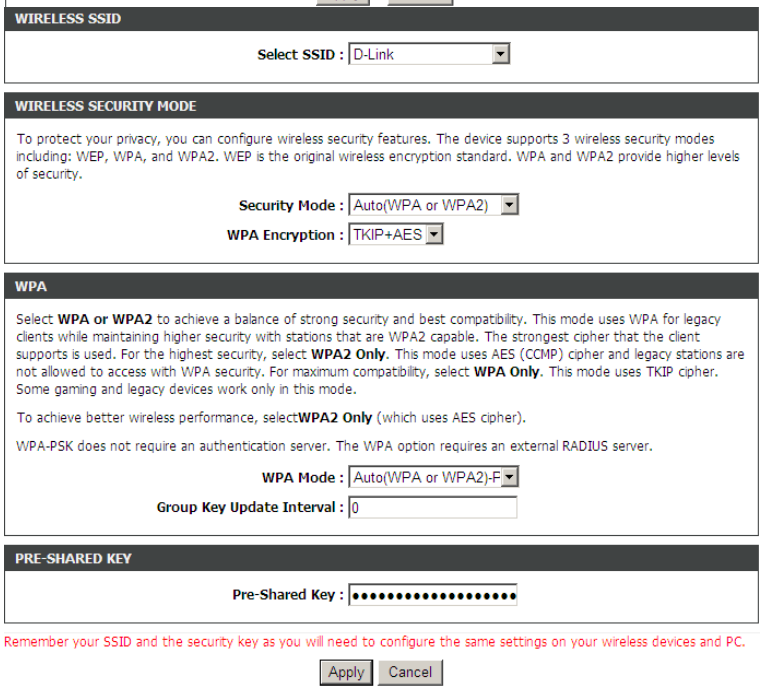
Step 3 In the **WPA Encryption** drop-down list, select **TKIP+AES**.

Step 4 Configure the **WPA Mode**.

- **Auto (WPA or WPA2)-PSK**: set the pre-shared key (password of your wireless network) in the Pre-Shared Key field.
- **Auto (WPA or WPA2)-Enterprise**: enter the port, IP address, and password of the Radius server. The wireless clients are required to enter the username and password provided by the Radius server.

Step 5 Set the **Group Key Update Interval**. For higher security, WPA password is updated periodically. This value is the update interval of the WPA password. You can keep it as default.

Step 6 In **Pre-Shared Key** textbox, set the password for the wireless network.



WPS Settings

Choose **ADVANCED** > **Advanced Wireless** > **WPS Settings**. This page is used to configure WPS settings.

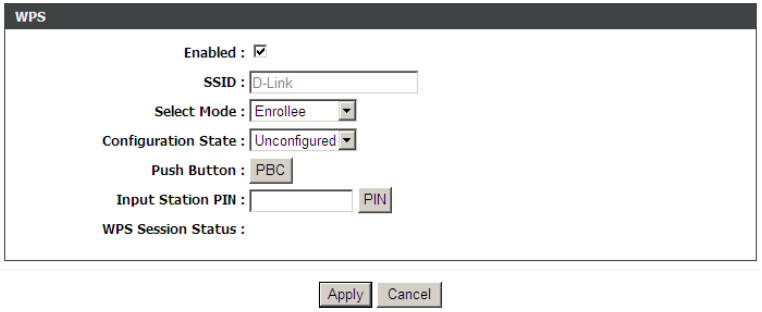
There are 3 methods to realize wireless connection through WPS.

- PBC

Click the **PBC** button in this page. And then click WPS button on the client to be connected within 2 minutes. The connection will be established.

- Based on the PIN of wireless client to be connected.

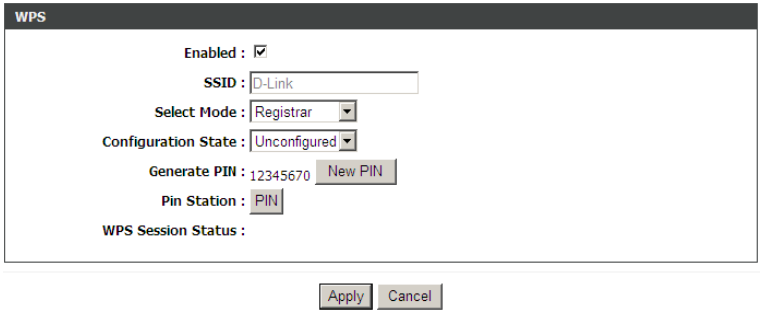
1) Select **Enabled** to enable WPS.



2) In **select Mode** drop-down list, select **Enrollee**.
3) In **Configuration State** drop-down list, select **Unconfigured**.
4) In **Input Station PIN** textbox, input the PIN code of the wireless client to be connected.
5) Click **Apply** to start wireless connection via WPS.

– Based on the PIN of the DSL-2750U.

1) Select **Enabled** to enable WPS.
2) In **select Mode** drop-down list, select **Registrar**.
3) In **Configuration State** drop-down list, select **Unconfigured**.
4) Input the Generate PIN at wireless client to be connected.
5) Click **Apply** to start wireless connection via WPS.

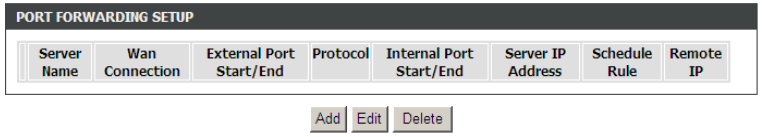


Port Forwarding

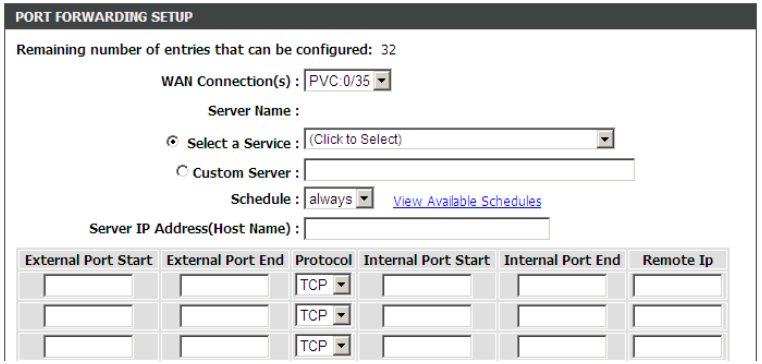
Choose **ADVANCED** > **Port Forwarding**. The page shown in the right figure appears.

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

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

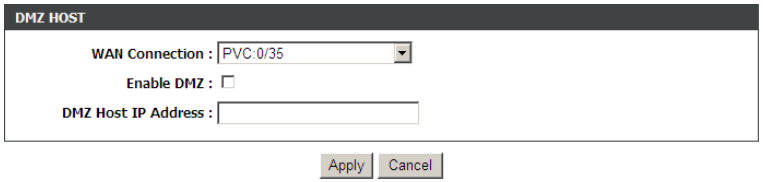


Enter an IP address in the **Server IP Address** field, to appoint the corresponding PC to receive forwarded packets.
The Ports show the ports that you want to open on the device. The **TCP/UDP** means the protocol type of the opened ports.
Click **Apply** to save the settings.



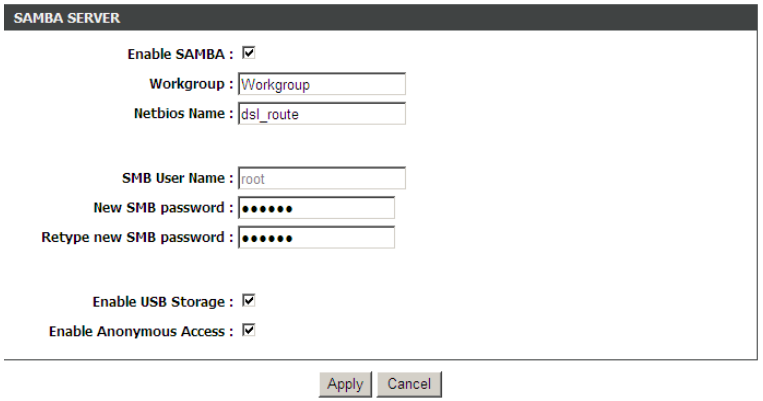
DMZ

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 right figure appears.
Select a WAN connection, input the host IP address.
Click **Apply** to save the settings.



SAMBA

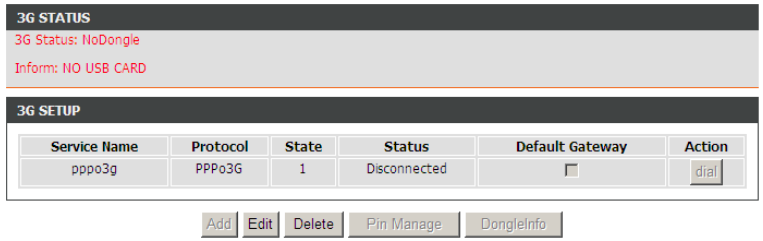
SAMBA enables the workstation in the network to share the USB flash disk connected to the DSL-2750U.
Choose **ADVANCED** > **SAMBA**. The page shown in the right figure appears.
The following table describes the parameters of this page.



Field	Description
Enable SAMBA	Select the check box to enable the samba service
Workgroup	Enter the name of your local area network (LAN).
Netbios Name	Enter your netbios name which is an identifier used by netbios services running on a computer.
New SMB password	Enter your samba password for user root.
Retype new SMB password	Reconfirm your samba password here.
Enable USB Storage	Select the check box to support USB storage.
Enable Anonymous Access	Select the check box to allow anonymous users access.

3G Configuration

Choose **ADVANCED** > **3G Configuration** and the page shown in the right figure appears. (Ensure your 3G card is connected the USB interface of AC750）

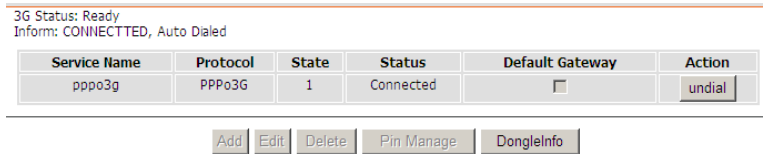


Note:

If you want to know more about the parameters of Advanced Wireless Settings, refer to **HELP** index.

- **3G card without PIN protect**

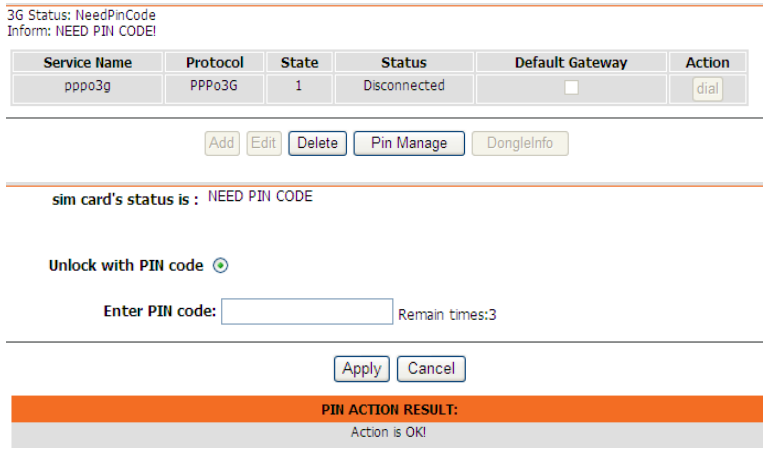
If the 3G card has no PIN protect function, the page will be shown as the right figure appears.



- **3G card with PIN protect**

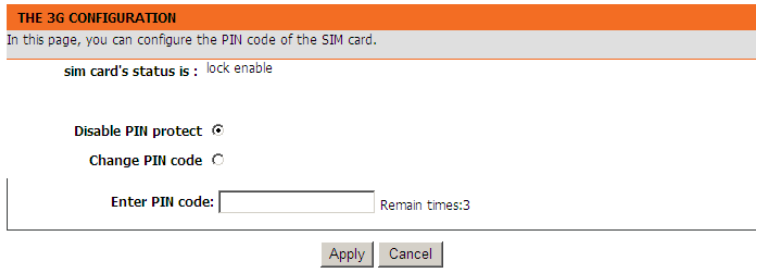
If the 3G card has PIN protect function, the page will be shown as the right figure appears. You'll be required to enter a PIN code which provided by your ISP before connecting to 3G network. Follow the instructions below to authenticate the pin code.

Step 1 Click **Pin Manage**, the right page appears.



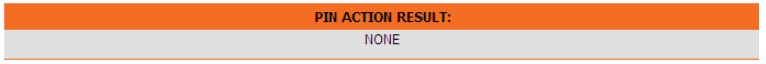
Step 2 Enter the Pin provided by your ISP, then click **Apply**, the right page appears. This page indicates the pin authentication is complete.

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



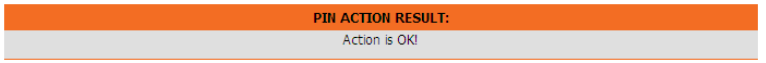
- Keep the PIN Protect

Check **Disable PIN protect**, then click **Apply**. The right page will appear. This page indicates that the PIN protect function is remain effective.



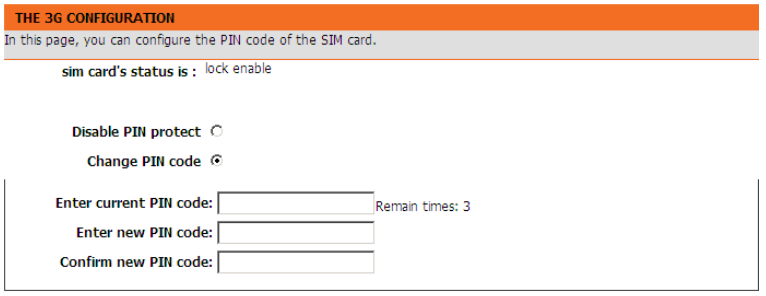
- Disable PIN Protect

Check **Disable PIN protect** and enter the pin in **Enter PIN code field**, then click **Apply**. The right page will appear. This page indicates that the PIN protect function is disabled.

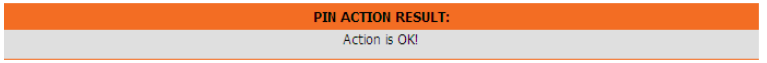


- Change PIN Code

Check **Change PIN code**, and the right page appears. Enter the required PIN code and click **Apply**.



If the operation is successful, the right page will appear.

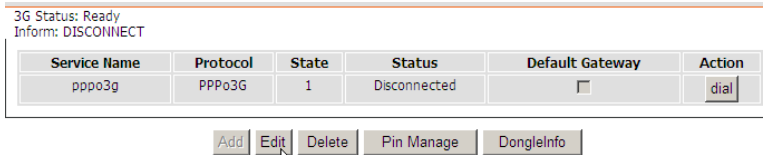


Note:

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

- **Edit an Existing 3G Configuration**

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



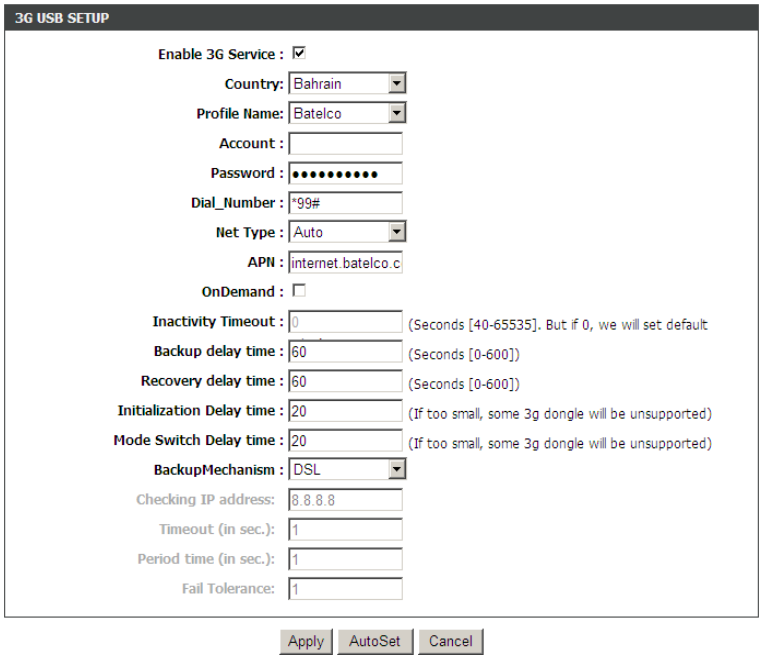
Note:

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

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

The following table describes the parameters of this page.

Field	Description
Country	Choose the country you located in the dropdown list.
Profile Name	Choose the ISP you subscribed service from.
Dial_Number	The number to be dialed to connect to 3G network. It's recommended to keep it as default.
Net Type	Choose the 3G network access type.
Backup Delay Time	The response time for 3G connection dial-up after DSL or Ethernet uplink is disconnected.
Recovery Delay Time	The time interval to re-dial.
Initialize Delay Time	The time for 3G card to initialize.
Mode Switch Delay Time	The time for mode switch.

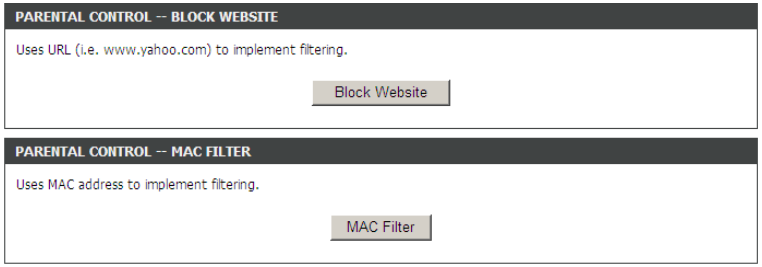


After setting, click Apply to make the settings take effect. Click **AutoSet** to keep the settings as default.

Parental Control

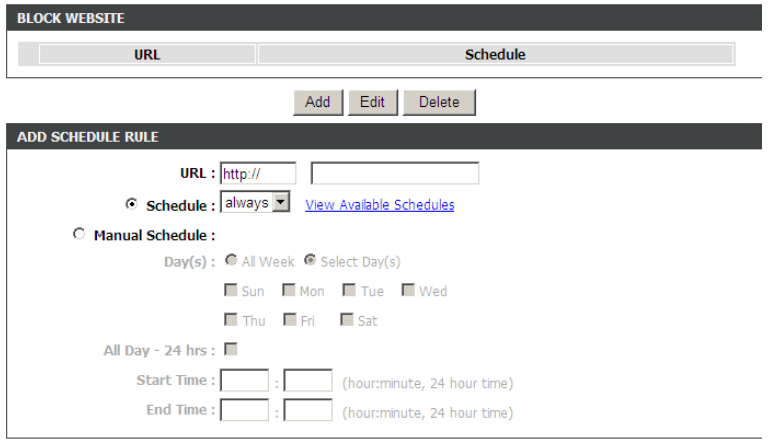
Choose **ADVANCED** > **Parental Control**. The **Parent Control** page shown in the right figure appears.

This page provides two useful tools for restricting the Internet access. **Block Website** 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.



Block Website

Choose **ADVANCED** > **Parental Control** > **Block Website**. The page shown in the right figure appears.



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

Step 1 Enter the website in the URL field.

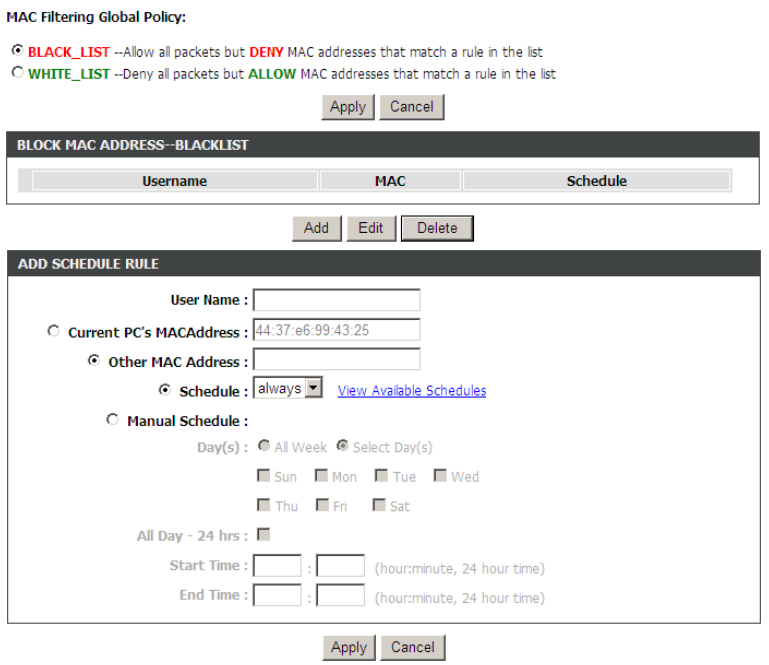
Step 2 Select the corresponding time and days.

Step 3 Click **Apply**.

MAC Filter

Choose **ADVANCED** > **Parental Control** > **MAC Filter**. The page shown in the right figure appears.

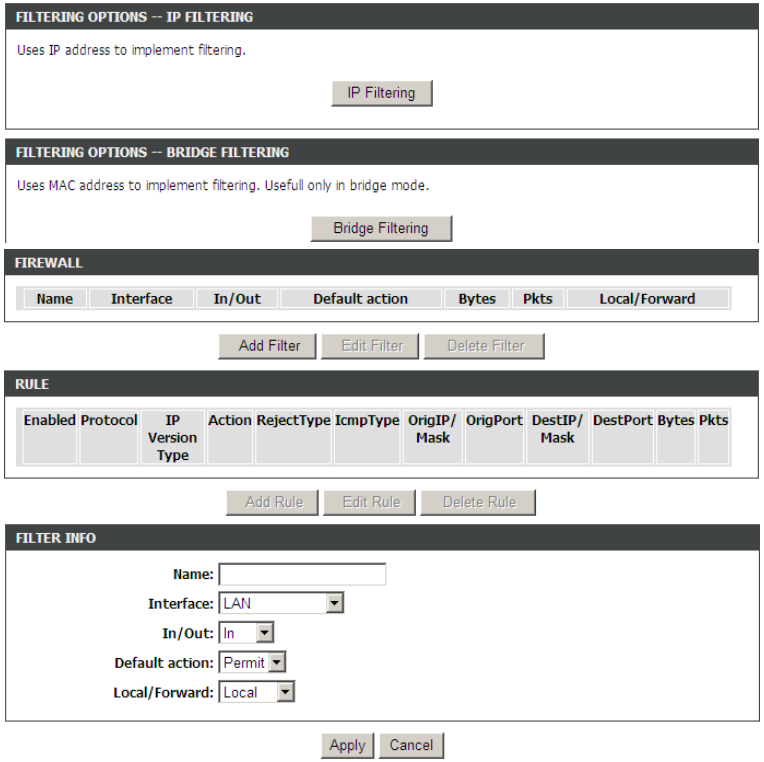
Choose **BLACK_LIST** or **WHITE_LIST**, and then click **Add**.



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

Filtering Options

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



IP Filtering

Choose **ADVANCED** > **Filtering Options** > **IP Filtering**. The page shown in the right figure appears. In this page, you may configure IP firewall function.
Click **Add Filter**.

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

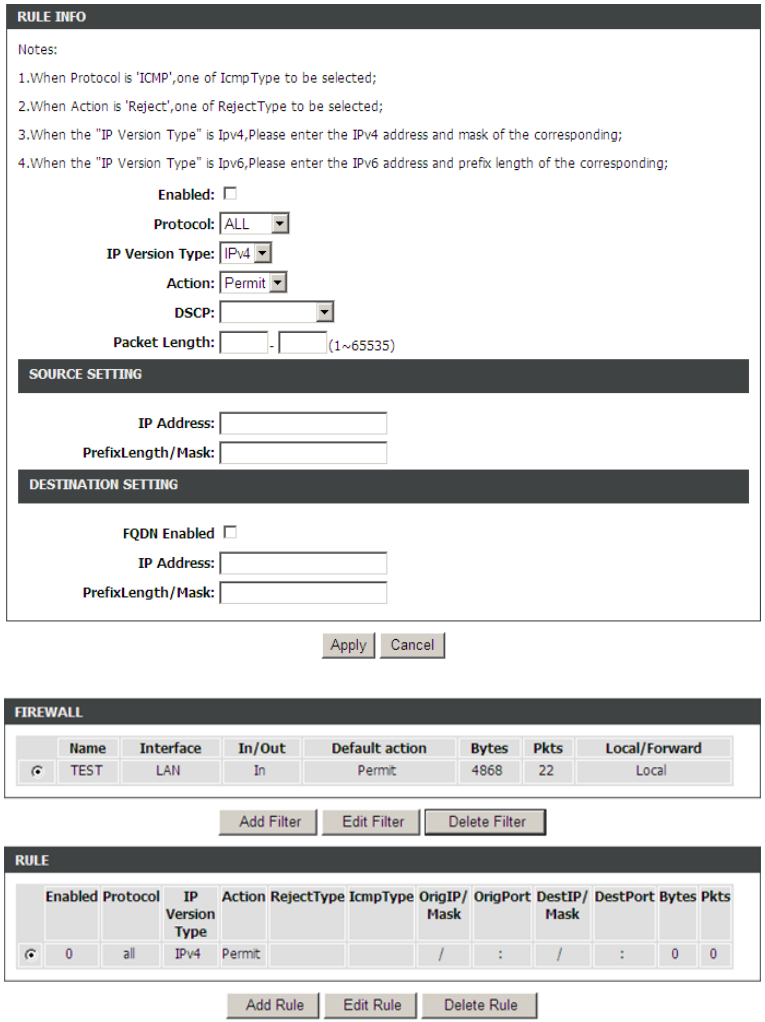
Note:

The settings are applicable only when the firewall is enabled.

After adding a filter, click **Add Rule**.
The following table describes the parameters of this page.

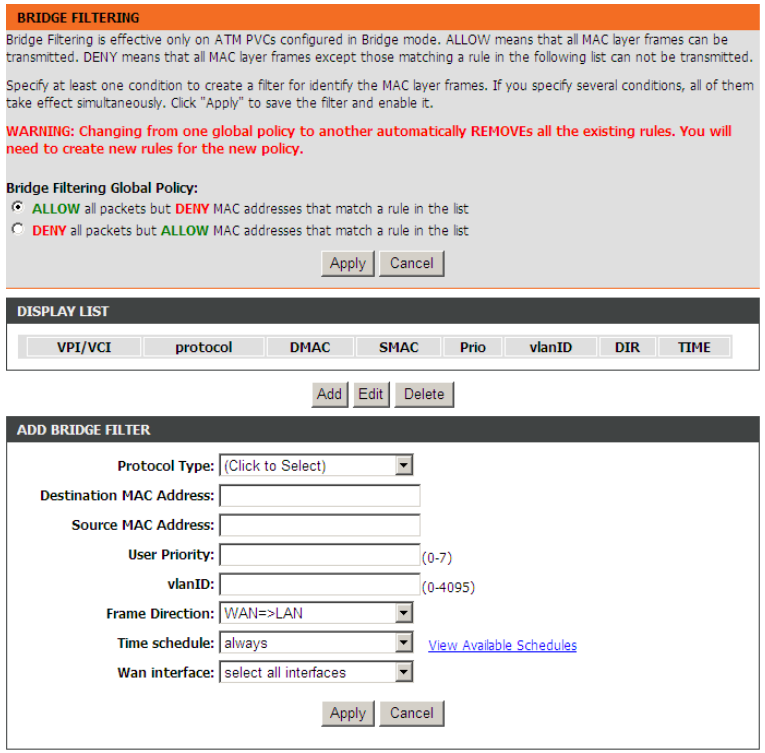
Field	Description
Enable	Tick in the box to enable a firewall rule.
Protocol	Choose a protocol corresponding to the rule. You may choose **TCP**, **UDP** or **ICMP**.
Action	The action when the rule is matched. **Permit** means allowing the message to pass, **Drop** means discarding messages without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

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



Bridge Filtering

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



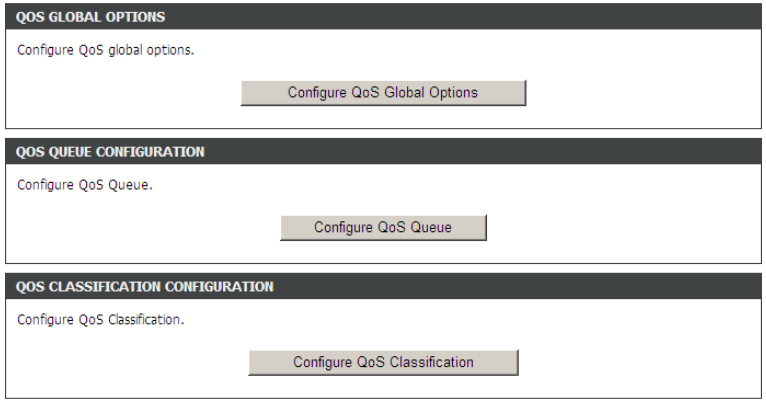
Click **Add** to add a bridge filter. The page shown in the right figure appears. The following table describes the parameters of this page.

Field	Description
Protocol Type	Choose a third-layer protocol type for bridge filtering from the drop-down list. You may choose **PPPoE**, **IPv4**, **IPv6**, **AppleTalk**, **IPX**, or **NetBEUI**.
Destination MAC Address	The MAC address of sendee of the message.
Source MAC Address	The MAC address of sender of the message.
Frame Direction	Choose the sending direction as **WAN to LAN** or **LAN to WAN**.
Time schedule	Choose the filtering strategy as **always** or **never**.
Wan interface	Set an effective interface for the bridge filtering rule.

Click **Apply** to save the settings.

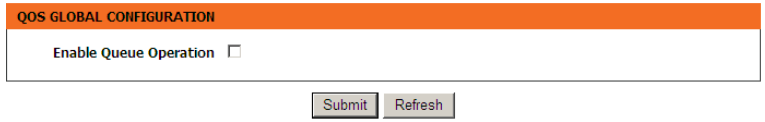
QoS Configuration

Choose **ADVANCED** > **QoS Configuration**. The page shown in the right figure appears. The QoS Configuration contains 3 parts: **Configure QoS Global Options**, **Configure QoS Queue**, **Configure QoS Classification**.



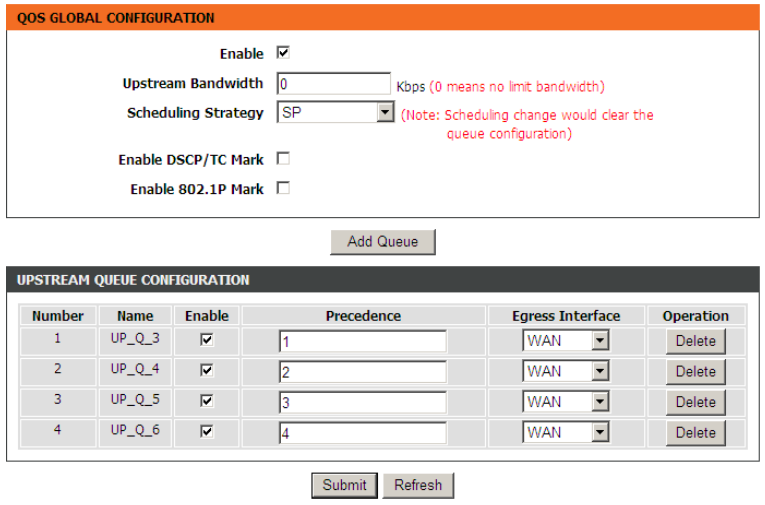
Configure QoS Global Options

Choose **ADVANCED** > **QoS Configuration** > **Configure QoS Global Options**. The page shown in the right figure appears. You can tick in the checkbox and then click **Submit** to enable queuing operation.



Configure QoS Queue

Choose **ADVANCED** > **QoS Configuration** > **Configure QoS Queue**. The page shown in the right right appears. In this page, you can set QoS flow control. The following table describes the parameters of this page.



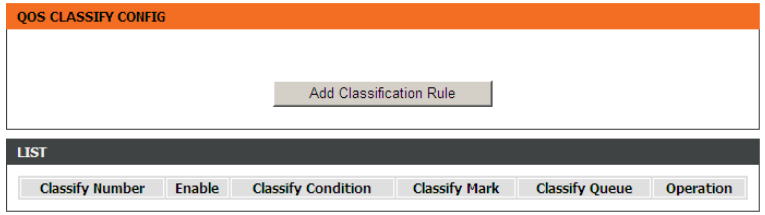
Field	Description
Enable	Tick in the box to enable queue.
Upstream Bandwidth	Total bandwidth for upstream flow.
Scheduling Strategy	Scheduling algorithm of QoS queue.
Enable DSCP/TC Mark	You may tick in the box to permit DSCP/TC Mark.
Enable 802.1P Mark	You may tick in the box to permit 802.1P Mark.

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

Configure QoS Classification

Choose **ADVANCED** > **QoS Configuration** > **Configure QoS Classification**. The page shown in the right appears. In this page, you can configure QoS queue rule.

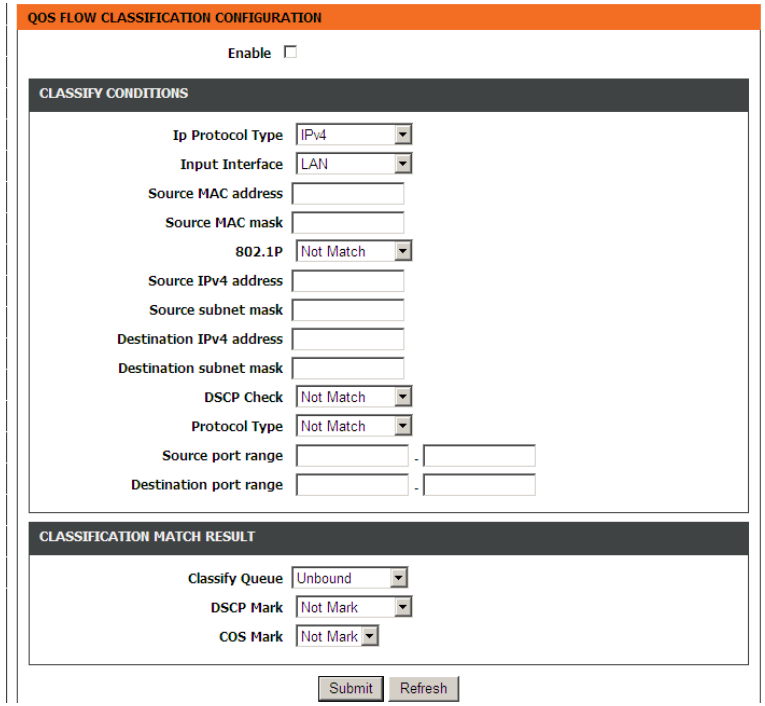
Click **Add Classification Rule**.

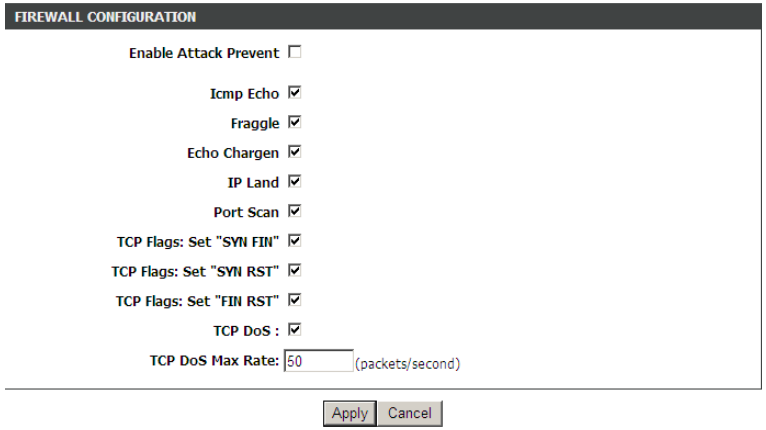


The following table describes the parameters of this page.

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

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

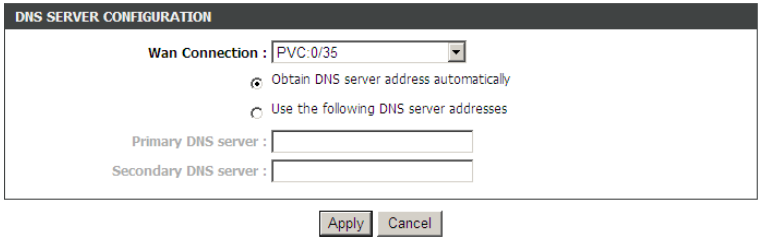




Firewall Setting

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

DNS



Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4.

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

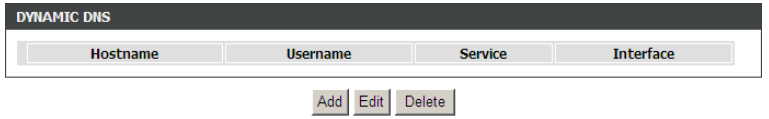
Choose **ADVANCED** > **DNS**. The page shown in the right figure appears.

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

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

Click **Apply** to save the settings.

Dynamic DNS



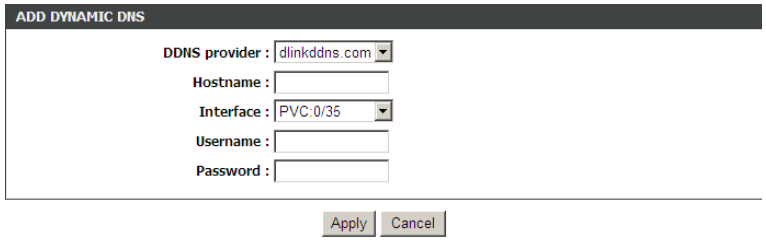
The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of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

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

Click **Add** to add dynamic DNS.

The following table describes the parameters of this page.

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



Click **Apply** to save the settings.

Network Tools

Port Mapping

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

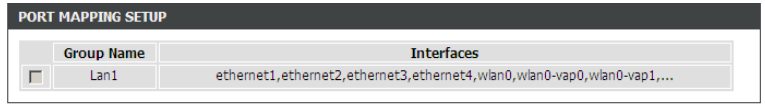
Click **Add** to add port mapping.

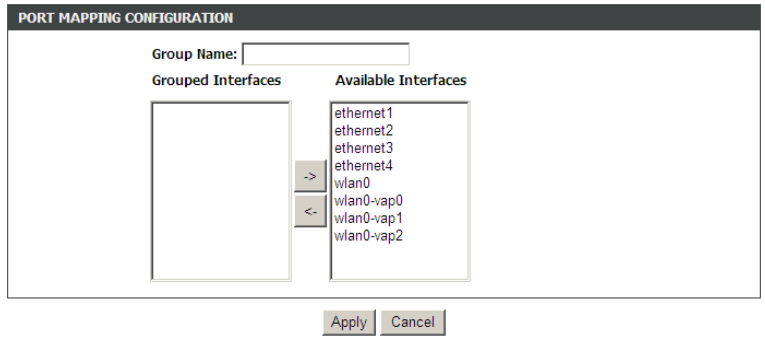
The procedure for creating a mapping group is as follows:

Step 1 Enter the group name.

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

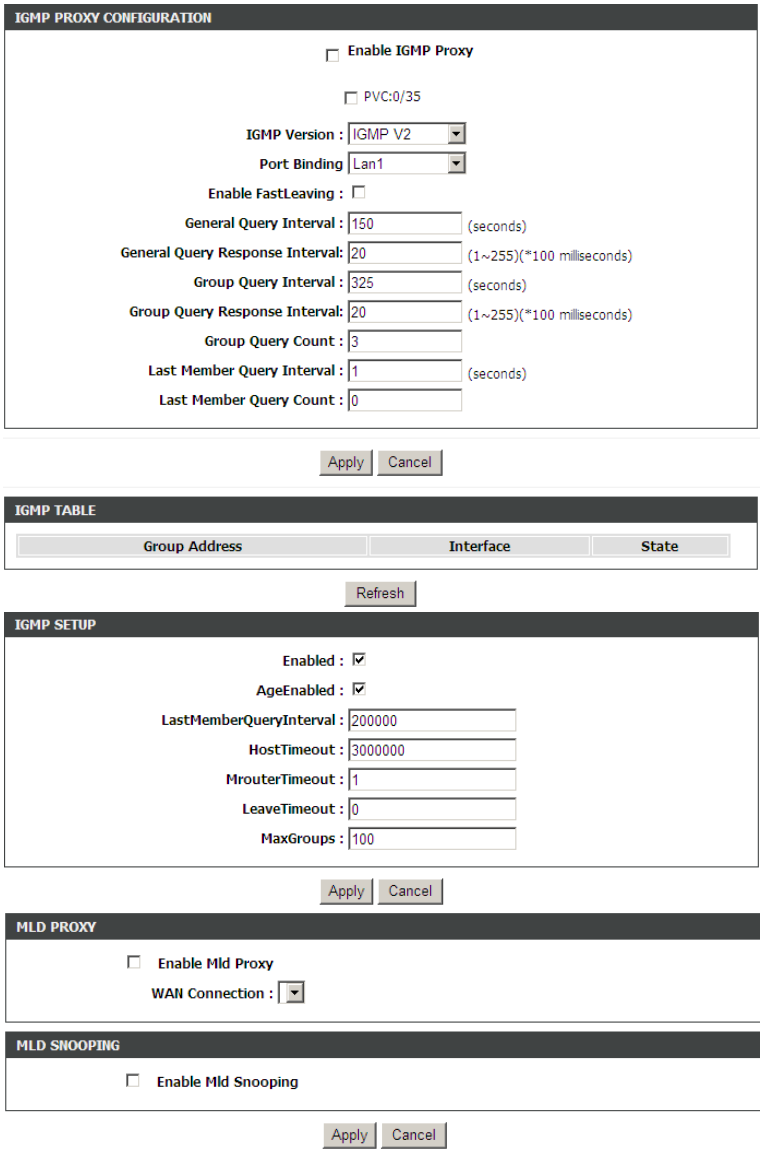
Step 3 Click **Apply** to save the settings.





IGMP Proxy

Choose **ADVANCED** > **Network Tools** > **IGMP Proxy**. The page shown in the right figure appears.
IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.



IGMP Snooping

Choose **ADVANCED** > **Network Tools** > **IGMP Snooping**. The page shown in the right figure appears.
When IGMP Snooping is enabled, the multicast data transmits through the specific LAN port which has received the request report.

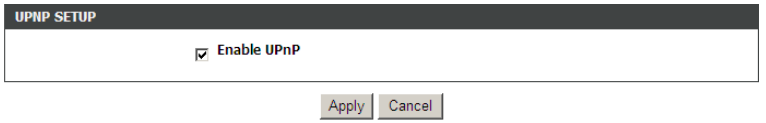
MLD Configuration

Choose **ADVANCED** > **Network Tools** > **MLD Configuration**. The page shown in the right figure appears. This section allows you to configure the MLD Setup settings of your Router . Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

UPNP

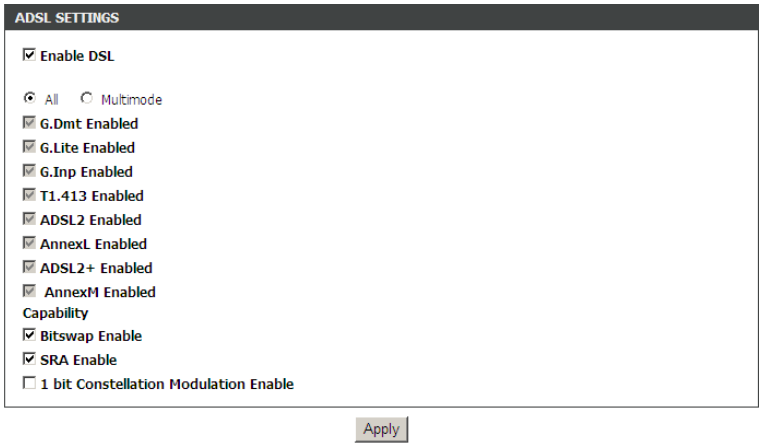
Choose **ADVANCED** > **Network Tools** > **UPnP**. The page shown in the right

figure appears.
In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.
UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.
Click **Apply** to save the settings.



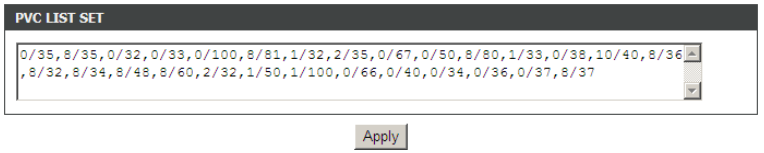
ADSL

Choose **ADVANCED** > **Network Tools** > **ADSL**. The page shown in the right figure appears.
In this page, it is recommended to keep it as defaults. The device negotiates the modulation mode with DSLAM.
Click **Apply** to save the settings.



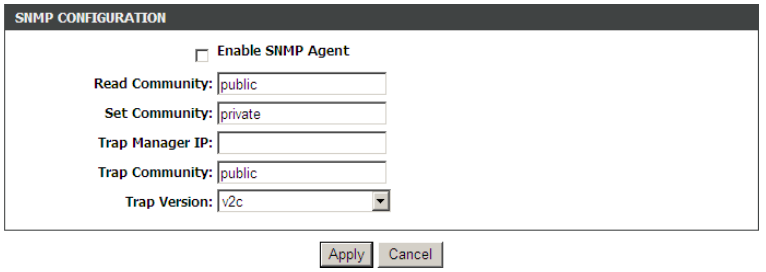
Default PVC

Choose **ADVANCED** > **Network Tools** > **Default PVC**. The page shown in the right figure appears.
Set the default PVC, which you think mostly appears. Input the PVC such as 0/32, 8/81, 0/35…



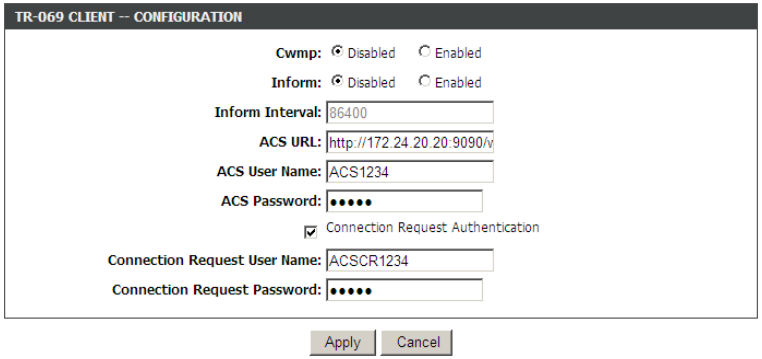
SNMP

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



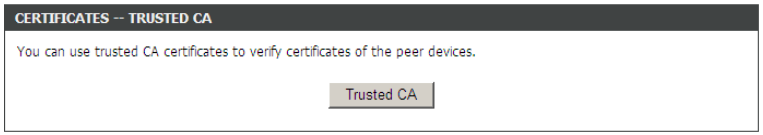
TR-069

Choose **ADVANCED** > **Network Tools** > **TR-069**. The page shown in the right figure appears. In this page, In this page, you can configure the TR069 CPE.



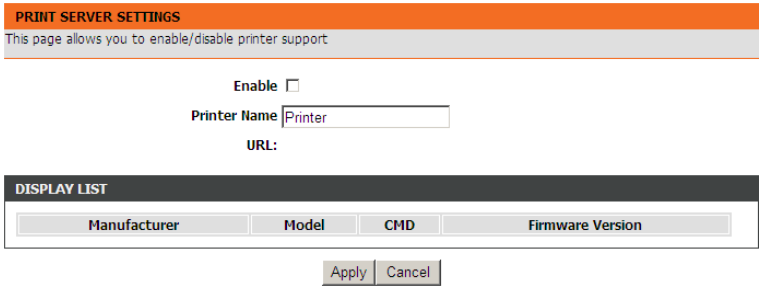
Certificates

Choose **ADVANCED** > **Network Tools** > **Certificates**. The page shown in the right figure appears. You can import certificates in this page.



Printer

Choose **ADVANCED** > **Network Tools** > **Printer**. The page shown in the right figure appears. This page allows you to enable/disable printer support.



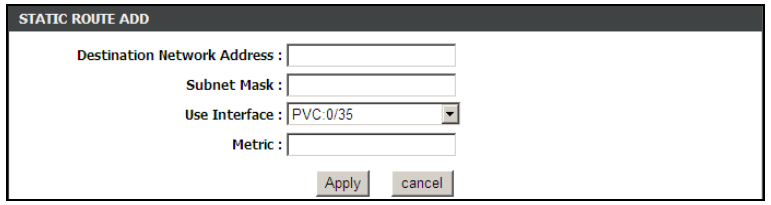
Routing

Static Routing

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

Click **Add** to add a static route.

The following table describes the parameters of this page.



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

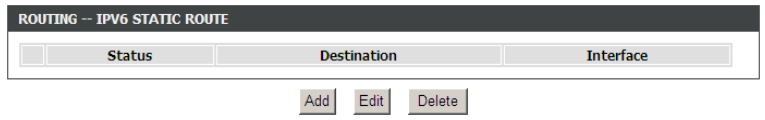
Click **Apply** to save the settings.

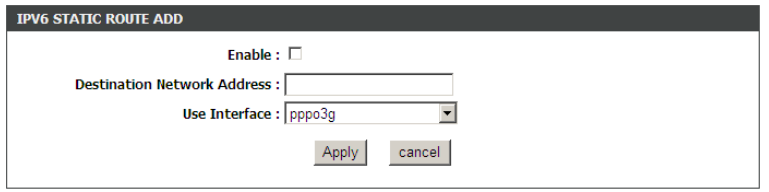
IPv6 Static Routing

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

Click **Add** to add a static route.

The following table describes the parameters of this page.





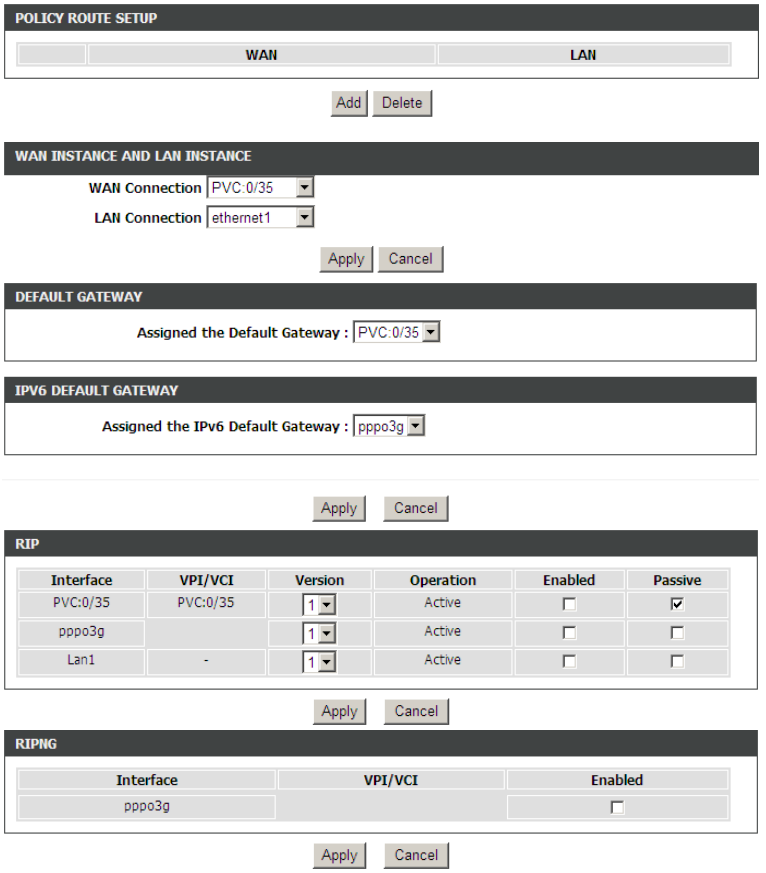
Field	Description
Destination Network Address	The destination IP address of the static route.
Use Gateway IP Address	The gateway IP address of the static route.
Use Interface	The interface name of the static route.

Click **Apply** to save the settings.

Policy Route

Choose **ADVANCED** > **Routing** > **Policy Route**. The page shown in the right figure appears. The policy route binds one WAN connection and one LAN interface.

Click **add**, the page shown in the right figure appears. Choose one WAN connection and at least one LAN connection to bind together, and then click **Apply** to finish the settings.



Default Gateway

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

Click **Apply** to save the settings.

RIP

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

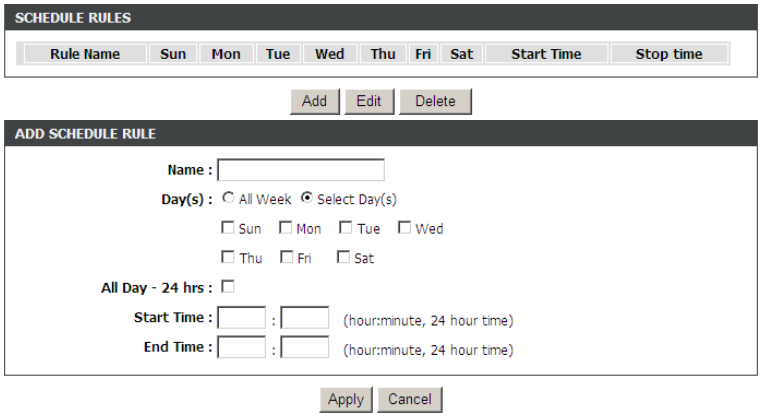
RIPng

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

Click **Apply** to save the settings.

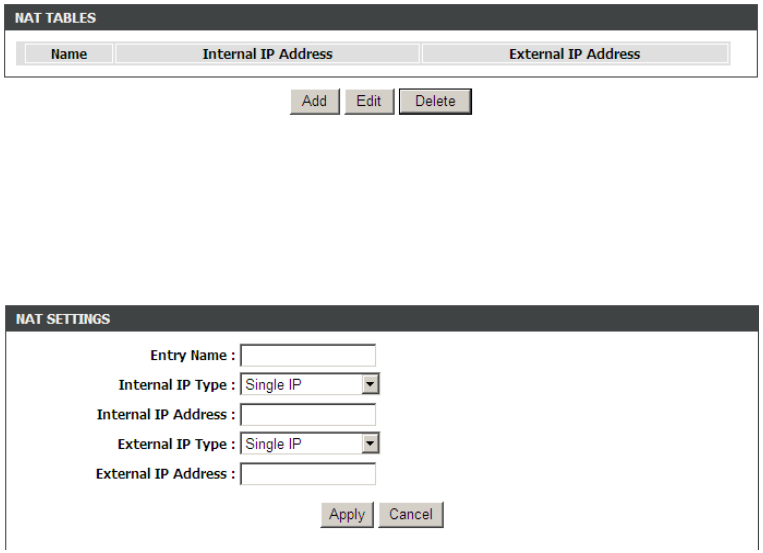
Schedules

Choose **ADVANCED** > **Schedules**. The page shown in the right figure appears.
Click **Add** to add schedule rule.
Click **Apply** to save the settings.



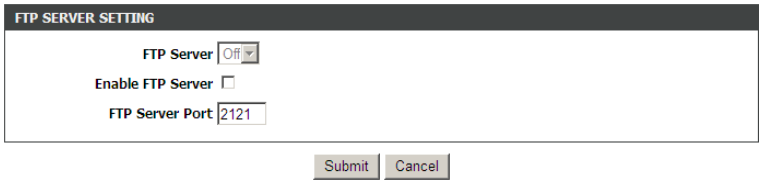
NAT

Choose **ADVANCED** > **NAT**. The page shown in the right figure appears.
Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts.
In this page, you are allowed to add, edit or remove a virtual server entry.
Click **Add** to add an NAT server.
After setting, click **Apply** to make the settings take effect.



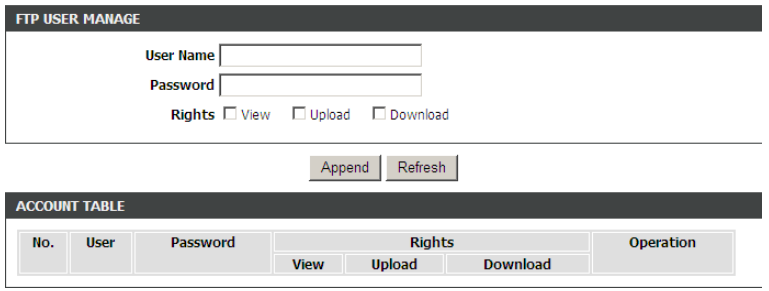
FTPD Setting

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



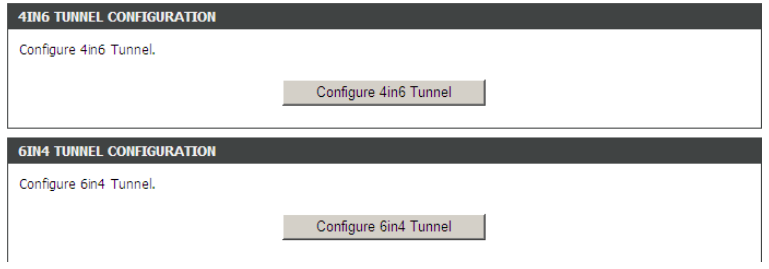
FTPD Account

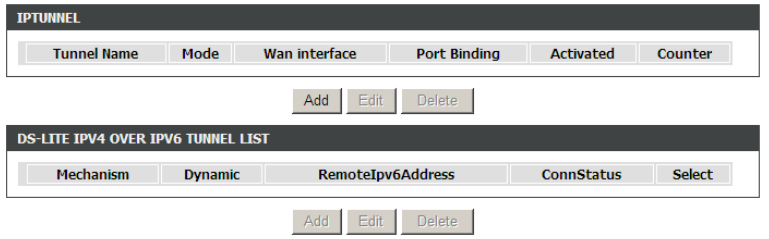
Choose **ADVANCED** > **FTPD Account**. The page shown in the right figure appears. In this page, you can manage the FTP user information, such as the user name, password, and the corresponding authority.

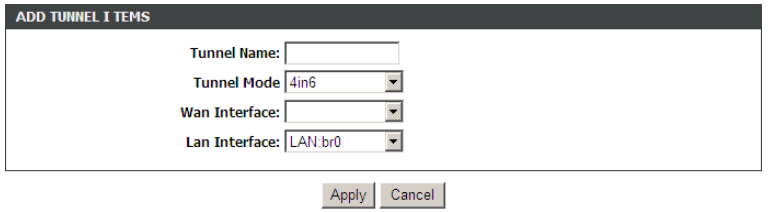


IP Tunnel

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







Configure 4in6 Tunnel

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

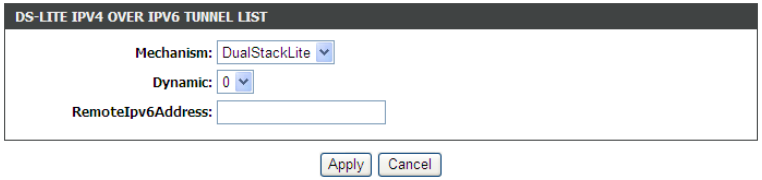
Click **Add** below the table **IPTUNNEL** to add tunnel items.

The following table describes the parameters of this page.

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

Click **Apply** to enable the settings.
Click **Add** below the table **DS-Lite IPv4 over IPv6 Tunnel List** to add a DS-Lite item，which is a 4in6 tunnel.
The following table describes the parameters of this page.

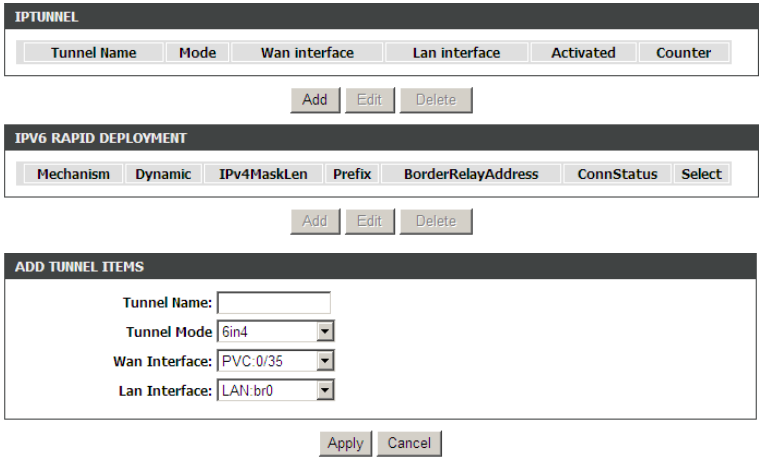
Field	Description
Mechanism	The tunnel type is DS-Lite, which is 4in6 tunnel.
Dynamic	Set the obtaining mode of remote IPv6 addresses. You can select **0** or **1**.
RemoteIpv6Address	Set the remote end IPv6 address of the tunnel.



Configure 6in4 Tunnel

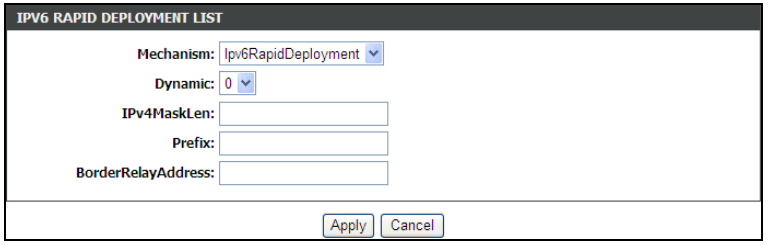
Choose **ADVANCED** > **IP Tunnel** > **Configure 6in4 Tunnel**. The page shown in the right figure appears. In this page, you can configure IPv6 penetration through IPv4 network. When only IPv4 access is provided by your ISP, you can access the Internet via IPv4 and IPv6.
Click **Add** below the table **IPTUNNEL** to add tunnel items.
The following table describes the parameters of this page.

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



Click **Apply** to enable the settings.
Click **Add** below the table **IPv6 Rapid Deployment** to add a 6RD item, which is a 6in4 tunnel.
The following table describes the parameters of this page.

Field	Description
Mechanism	The tunnel type is 6RD, which is a 6in4 tunnel.
Dynamic	Set the obtaining mode of Border Relay Address. You may choose **0** or **1**.

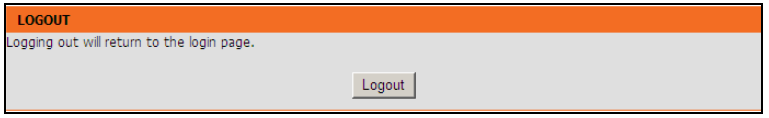


IPv4MaskLen	Set the subnet mask digits of the IPv4 address of the local WAN interface.
Prefix	Set the IPv6 prefix of the 6RD tunnel.
BorderRelayAddress	Set the Border Relay IPv4 address at the remote end.

Click **Apply** to enable the settings.

Logout

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



MANAGEMENT

In the main interface, click **Management** tab to enter the **Management** menu. The submenu of the Management contains **Global IPv6**, **System Management**, **Firmware Update**, **Access Controls**, **Diagnosis**, **Log Configuration** and **Logout**.

Global IPv6

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

System Management

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

In this page, you can reboot device, back up the current settings to a file, update settings from the file saved previously and restore the factory defaults.

The buttons in this page are described as follows:

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

Note:

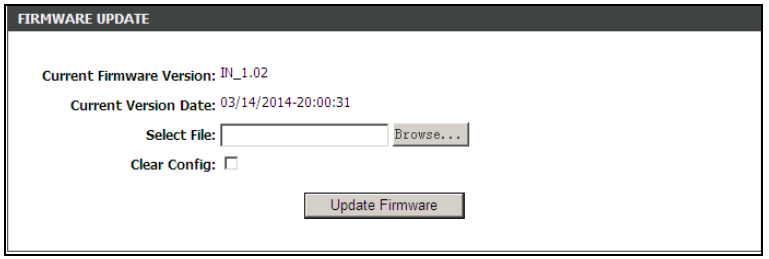
Do not turn off your device or press the Reset button while an operation in this page is in progress.

Firmware Update

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

To update the firmware, take the following steps.

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



Step 2 Select **Clear Config**.

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

The device loads the file and reboots automatically.

Note:

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

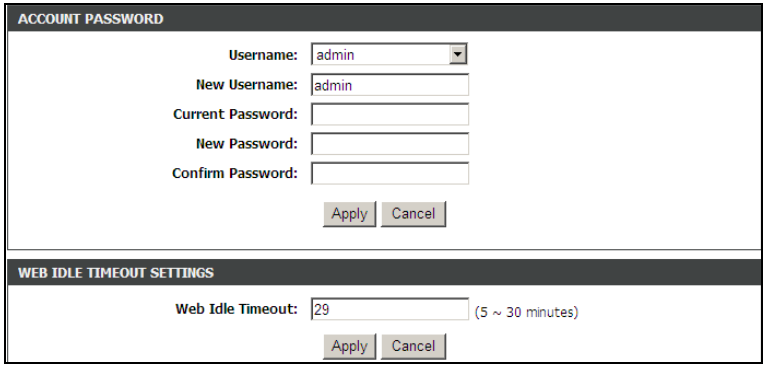
Access Controls

User Management

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

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

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

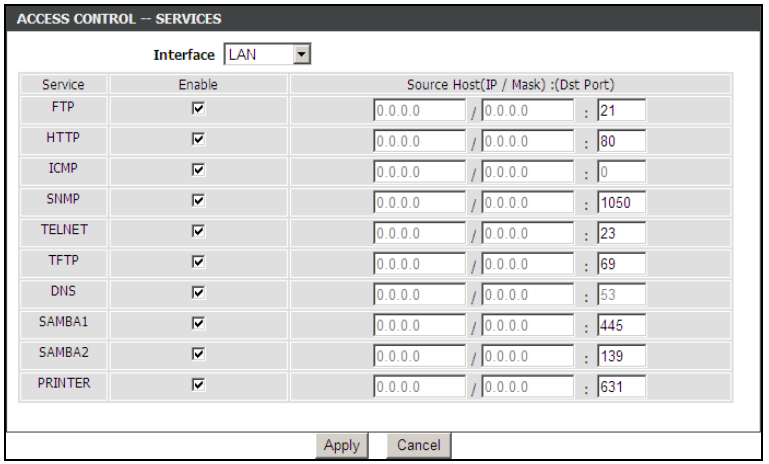


Services

Choose **MANAGEMENT** > **Access Controls** > **Services**. The page shown in the right figure appears.

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

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



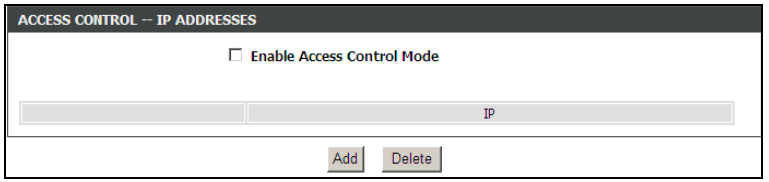
Note:

If you disable HTTP service, you cannot access the configuration page of

the device any more.

IP Address

Choose **MANAGEMENT** > **Access Controls** > **IP Address**. The page shown in the right figure appears.
In this page, you can configure the IP address for access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.
Select **Enable Access Control Mode** to enable ACL.



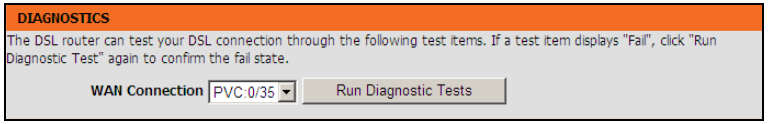
Note:

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

Diagnosis

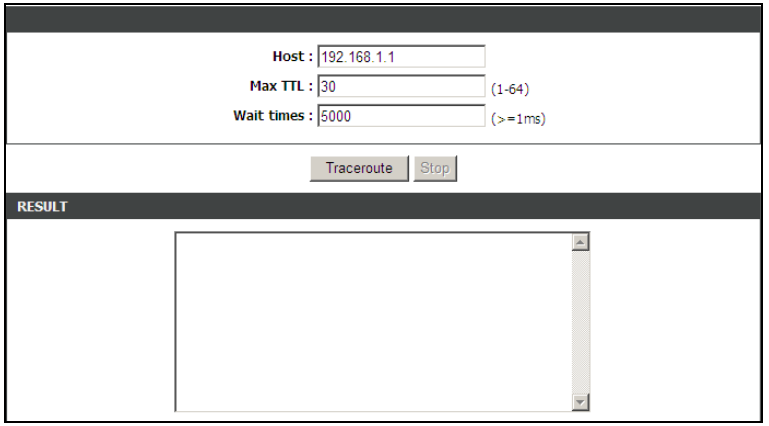
DSL Test

Choose **MANAGEMENT** > **Diagnosis** > **DSL Test**. The page shown in the right figure appears. In this page, you can test your DSL connection by clicking **Run Diagnosis Tests**.



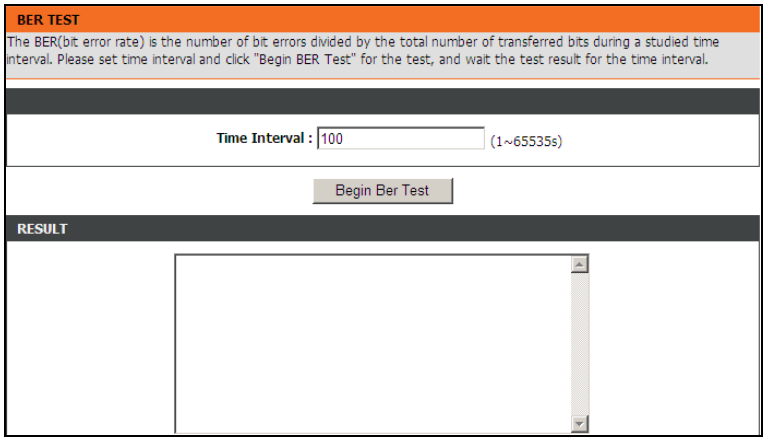
Traceroute

Choose **MANAGEMENT** > **Diagnosis** > **Traceroute**. The page shown in the right figure appears. In this page, you can determine the routers on the Internet by sending packets.



BER Test

Choose **MANAGEMENT** > **Diagnosis** > **BER Test**. The page shown in the right figure appears. In this page, you can test the bit error rate.
The BER(bit error rate) is the number of bit errors divided by the total number of transferred bits during a studied time interval. Please set time interval and click **Begin BER Test** for the test, and wait the test result for the time interval.

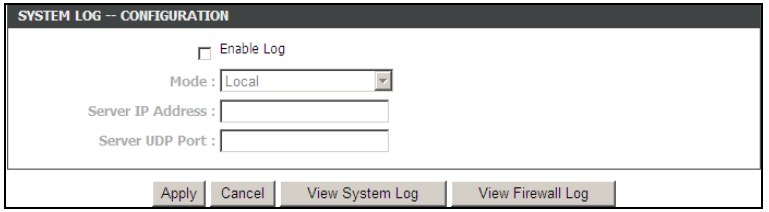


Log Configuration

Choose **MANAGEMENT** > **Log Configuration**. The **System Log** page shown in the right figure appears.
This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. Available event severity levels are as follows: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. In this page, you can enable or disable the system log function.
To log the events, take the following steps.

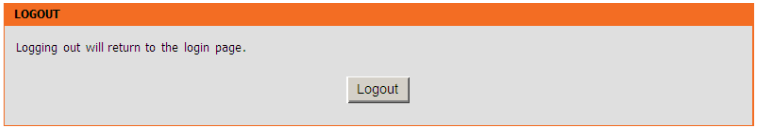
Step 1 Select **Enable Log** check box.
Step 2 Select the display mode from the Mode drop-down list.
Step 3 Enter the Server IP Address and Server UDP Port if the Mode is set to **Both** or **Remote**.
Step 4 Click **Apply** to apply the settings.

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



Logout

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



Status

In the main interface, click **Status** tab to enter the **Status** menu. The submenus are **Device Info**, **Wireless Clients**, **DHCP clients**, **IPv6 Status**, **Logs**, **Firewall logs**, **Statistics**, **Route Info** and **Logout**. You can view the system information and monitor performance.

Help

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

Troubleshooting

This chapter provides solutions to problems that might occur during the installation and operation of the DSL-2750U. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

1. How do I configure my DSL-2750U Router without the CD-ROM?

Step 1 Connect your PC to the Router using an Ethernet cable.
Step 2 Open a web browser and enter the address http://192.168.1.1
Step 3 The default username is ‘admin’ and the default password is ‘admin’.
Step 4 If you have changed the password and cannot remember it, you will need to reset the Router to the factory default setting (see question 2), which will set the password back to ‘admin’.

2. How do I reset my Router to the factory default settings?

Step 1 Ensure the Router is powered on.
Step 2 Press and hold the reset button on the back of the device for approximately 1 second.
Step 3 This process should take around 1 to 2 minutes.

Note:
Resetting the Router to the factory default settings will erase the current configuration settings.

3. What can I do if my Router is not working correctly?

There are a few quick steps you can take to try and resolve any issues:
Step 1 Follow the directions in Question 2 to reset the Router.
Step 2 Check that all the cables are firmly connected at both ends.
Step 3 Check the LEDs on the front of the Router. The Power indicator should be on, the Status indicator should flash, and the DSL and LAN

indicators should be on as well.

Step 4 Please ensure that the settings in the Web-based configuration manager, e.g. ISP username and password, are the same as the settings that have been provided by your ISP.

4. Why can't I get an Internet connection?

For ADSL ISP users, please contact your ISP to make sure the service has been enabled/connected by your ISP and that your ISP username and password are correct.

5. What can I do if my Router can't be detected by running the installation CD?

Step 1 Ensure the Router is powered on.

Step 2 Check that all the cables are firmly connected at both ends and all LEDs are working correctly.

Step 3 Ensure only one network interface card on your PC is activated.

Step 4 Click on **Start** > **Control Panel** > **Security Center** to disable the firewall.

Note:

There is a potential security issue if the firewall is disabled on your PC. Please remember to turn it back on once you have finished the whole installation procedure. This will enable you to surf the Internet without any problems.

Networking Basics

Check Your IP Address

After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

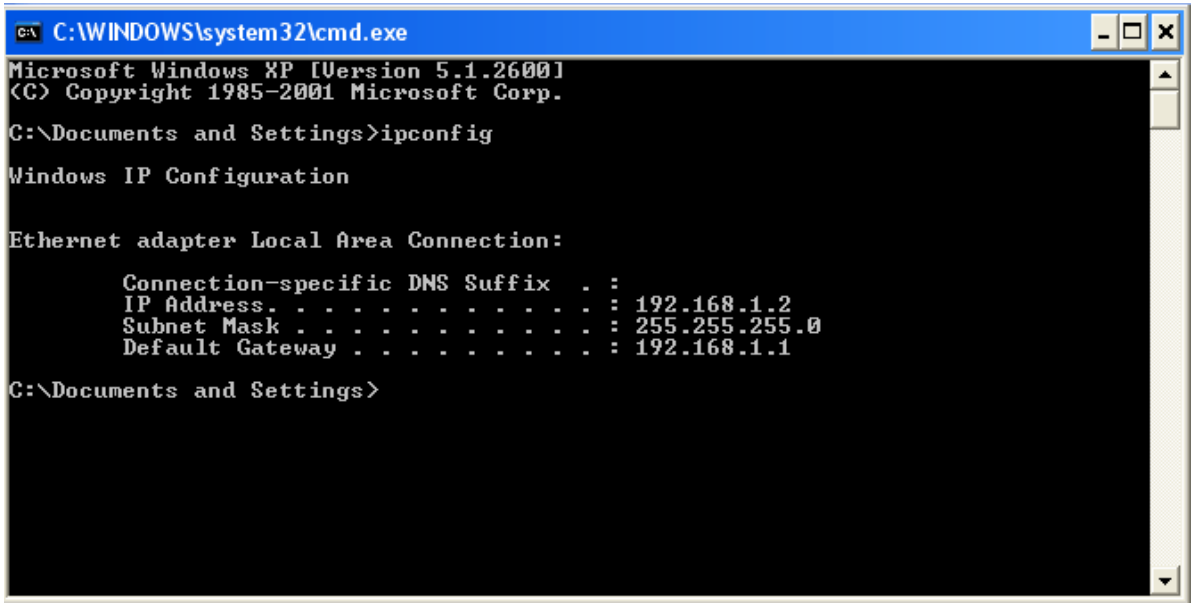
Click on **Start** > **Run**. In the run box type ***cmd*** and click on the **OK** button.

At the prompt, type ***ipconfig*** and press **Enter**.

This will display the IP address, subnet mask and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.



Statically Assigning an IP Address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

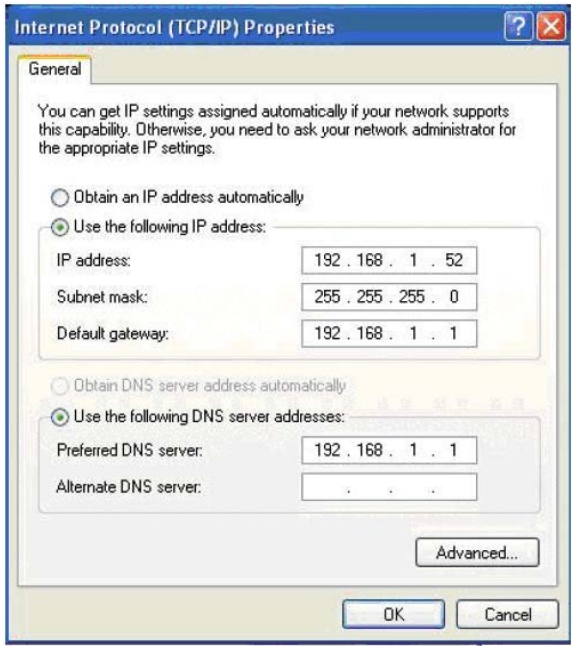
Step 1
Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.
Windows® 2000 - From the desktop, right-click on the **My Network Places** > **Properties**.

Step 2
Right-click on the **Local Area Connection** which represents your network adapter and select the **Properties** button.

Step 3
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button.

Step 4
Click on the **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.
Example: If the router's LAN IP address is 192.168.1.1, make your IP address 192.168.1.X where X is a number between 2 and 254. Make sure that the number you choose is not in use on the network. Set the Default Gateway to be the same as the LAN IP address of your router (192.168.1.1).

Set the Primary DNS to be the same as the LAN IP address of your router (192.168.1.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.



Step 5
Click on the **OK** button twice to save your settings.

Technical Specifications

ADSL Standards

- ANSI T1.413 Issue 2
- ITU G.992.1 (G.dmt) AnnexA
- ITU G.992.2 (G.lite) Annex A
- ITU G.994.1 (G.hs)
- ITU G.992.5 Annex A

ADSL2 Standards

- ITU G.992.3 (G.dmt.bis) Annex A
- ITU G.992.4 (G.lite.bis) Annex A

ADSL2+ Standards

- ITU G.992.5 (ADSL2+)

Protocols

- IEEE 802.1d Spanning Tree
- TCP/UDP
- ARP
- RARP
- ICMP
- RFC1058 RIP v1
- RFC1213 SNMP v1 & v2c
- RFC1334 PAP
- RFC1389 RIP v2
- RFC1577 Classical IP over ATM
- RFC1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)
- RFC1661 Point to Point Protocol
- RFC1994 CHAP
- RFC2131 DHCP Client / DHCP Server
- RFC2364 PPP over ATM
- RFC2516 PPP over Ethernet

Data Transfer Rate

- G.dmt full rate downstream: up to 8 Mbps / upstream: up to 1 Mbps
- G.lite: ADSL downstream up to 1.5 Mbps / upstream up to 512 Kbps
- G.dmt.bis full rate downstream: up to 12 Mbps / upstream: up to 12 Mbps
- ADSL full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps

Media Interface

- ADSL interface: RJ-11 connector for connection to 24/26 AWG twisted pair telephone line
- LAN interface: RJ-45 port for 10/100BASE-T Ethernet connection