



User Manual

Wireless N 300 ADSL2+ Modem Router

Table of Contents

SAFETY PRECAUTION	1	TROUBLESHOOTING	70
INTRODUCTION	1	NETWORKING BASICS	72
SYSTEM REQUIREMENTS	2	Check Your IP Address	72
Features.....	3	Statically Assigning an IP Address	73
INSTALLATION	4	TECHNICAL SPECIFICATIONS	74
Before You Begin.....	4		
Installation Notes.....	4		
Information you will need from your ADSL service provider.....	6		
Information you will need about your DSL-2740U ADSL 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		
Accessing the Router.....	15		
SETUP	16		
Wizard-ADSL WAN.....	16		
Internet Setup-ADSL WAN	22		
Wizard-Ethernet WAN.....	29		
Internet Setup-Ethernet WAN	33		
Local Network.....	37		
Wireless Setup.....	41		
Time and Date	44		
ADVANCED	45		
Advanced Wireless.....	45		
Access Control List.....	49		
Port Triggering	51		
Port Forwarding.....	52		
DMZ.....	52		
Parental Control.....	53		
Filtering Options.....	55		
DoS Settings.....	57		
DNS.....	57		
Dynamic DNS	59		
Network Tools	60		
Routing	62		
NAT.....	65		
MAINTENANCE	67		
System.....	67		
Firmware Update	68		
Password.....	68		
Diagnostics	68		
System Log.....	69		
Logout.....	69		

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-2740U supports multiple line modes. With four 10/100 base-T Ethernet interfaces at the user end, the device provides high-speed ADSL broadband connection to the Internet or Intranet for high-end users like net bars and office users. The DSL-2740U supports both DSL uplink access and Ethernet uplink access. It provides high performance access to the Internet with a downstream rate of 24 Mbps and an upstream rate of 1 Mbps. 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	<p>Computer with the following: Windows®, Macintosh, or Linux-based operating system An installed Ethernet adapter</p> <p>Browser Requirements: Microsoft Internet Explorer® v7, Mozilla® Firefox v9.0, Google® Chrome 16.0, or Safari® v4 or higher version.</p> <p>Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.</p>

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
- Digital Living Network Alliance (DLNA)
- Wireless 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-2740U 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-2740U ADSL 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-2740U

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-2740U

This is the subnet mask used by the DSL-2740U 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-2740U to the Ethernet port using an Ethernet cable.

DHCP Client status

Your DSL-2740U 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-2740U 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-2740U 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 powered on.
		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.
 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.
	Green	Off	The device is under the Bridge mode or powered off.
		On	A connection is set up and no traffic is detected.

LED	Color	Status	Description
Internet	Red	On	The authentication of the PPP dial-up is failed or MER is failed to obtain the correct IP address.
		Off	The WLAN function is disabled.
		Blinking	A connection is set up and data is being transmitted.
		Off	No signal is detected.

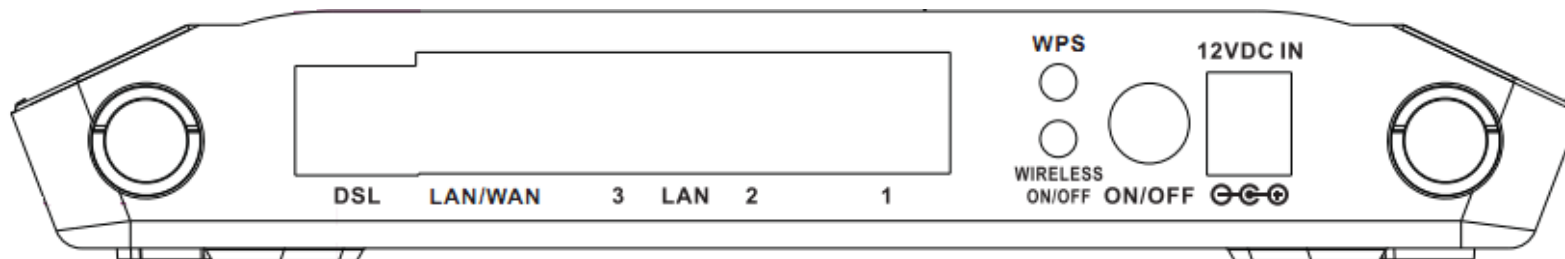


Figure 2 Rear panel

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.
LAN/WAN	This Ethernet RJ-45 interface has two functions. <ul style="list-style-type: none"> ● 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 2740U by being connected to this interface with RJ-45 cable.
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 host.
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.

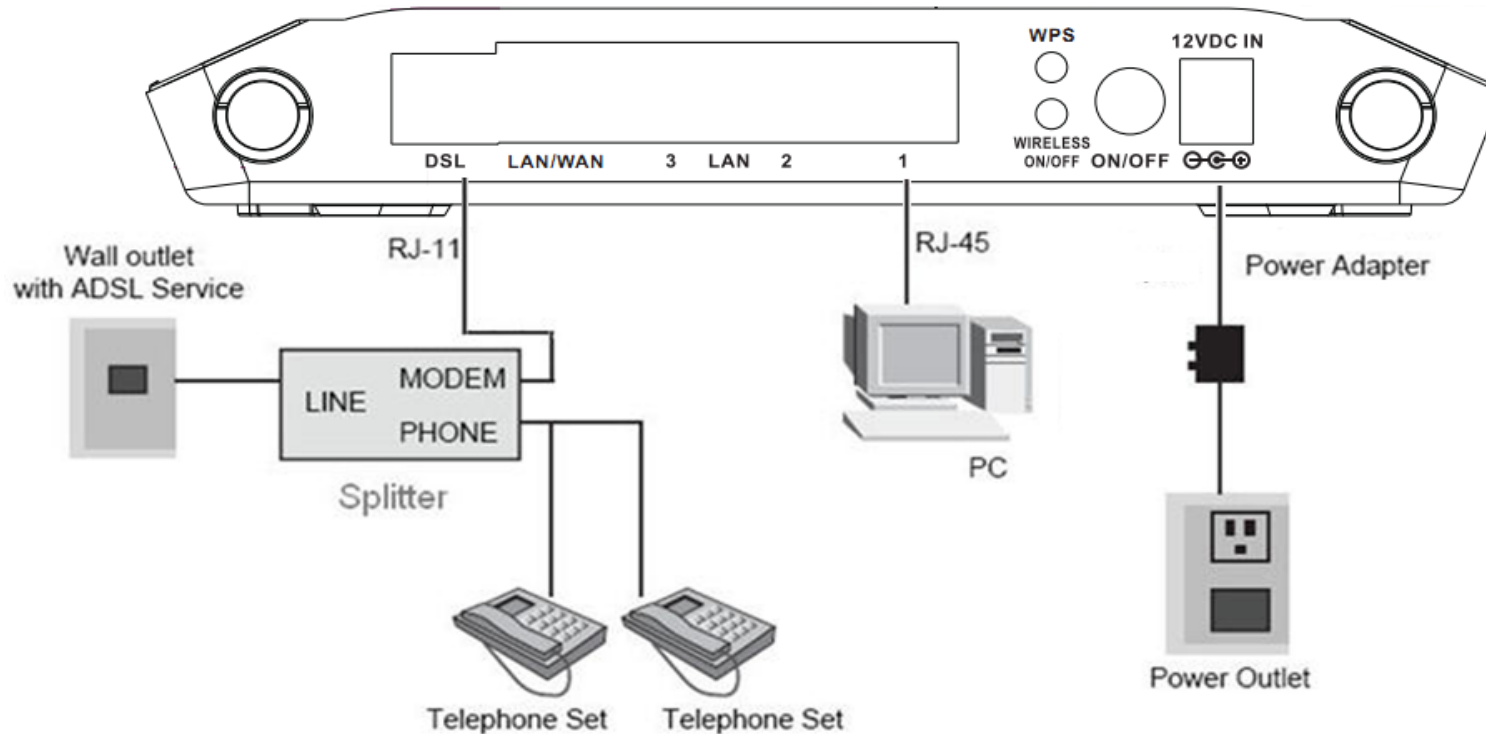


Figure 3 DSL uplink connection

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 splitter 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.

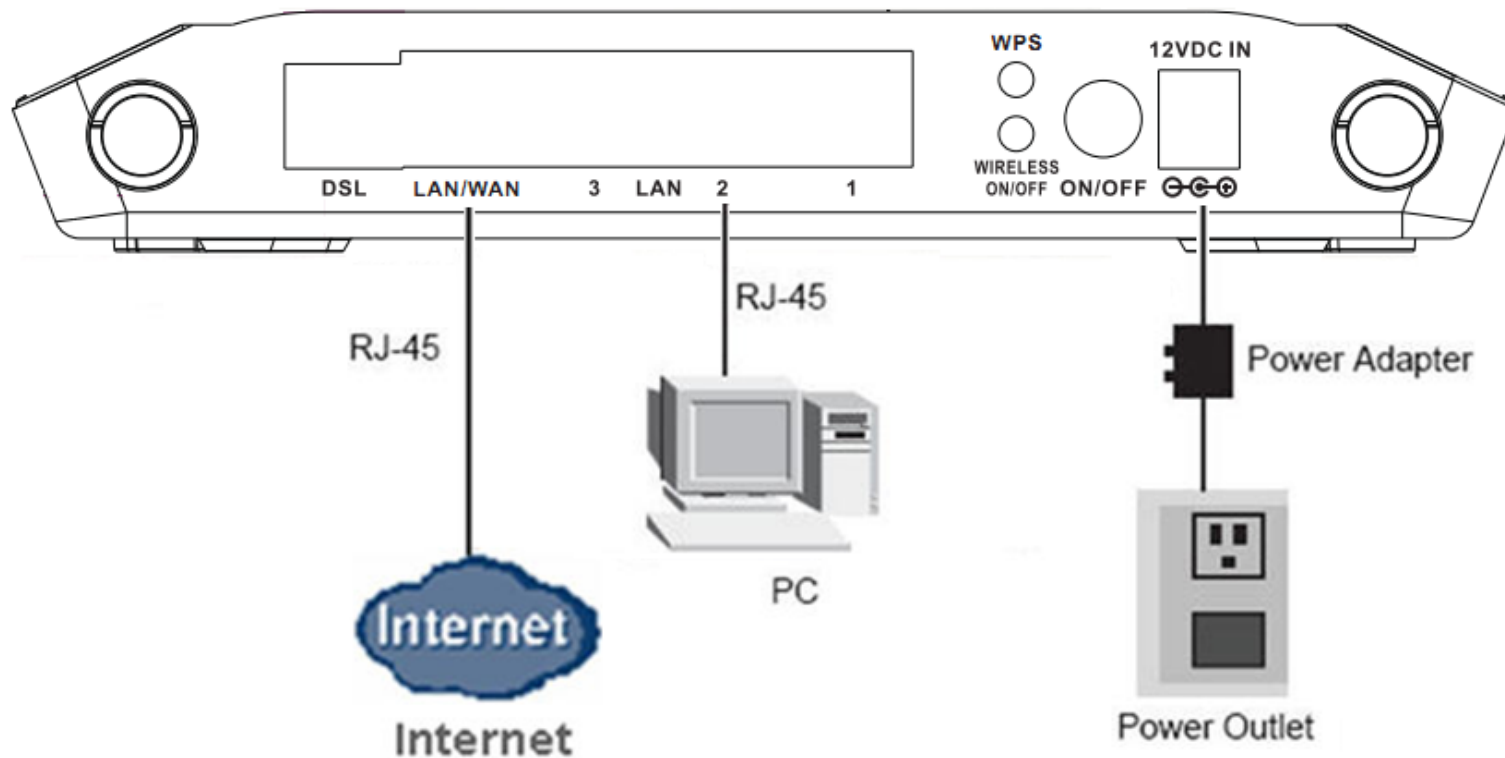


Figure 4 Ethernet uplink connection

- Step 1** Connect the **LAN** interface of the wireless router to your PC with RJ45 Ethernet cable.
- Step 2** Connect the **LAN/WAN** 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 following 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**.

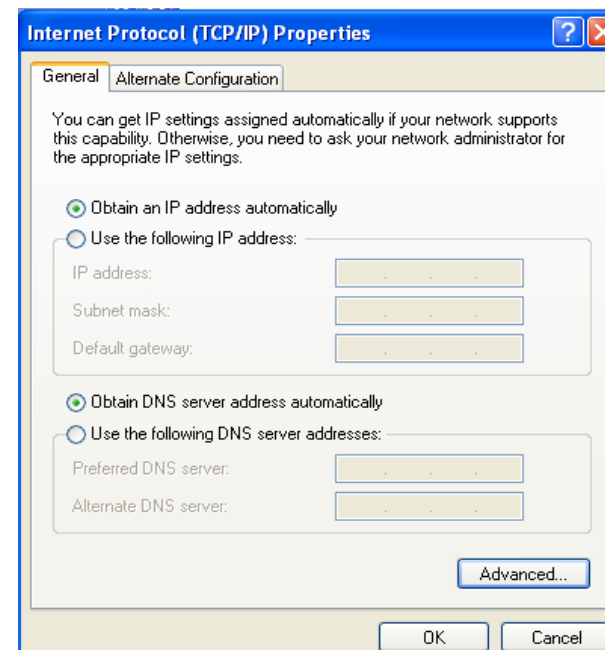
Step 2 Right-click the Ethernet connection icon and choose **Properties**.

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.



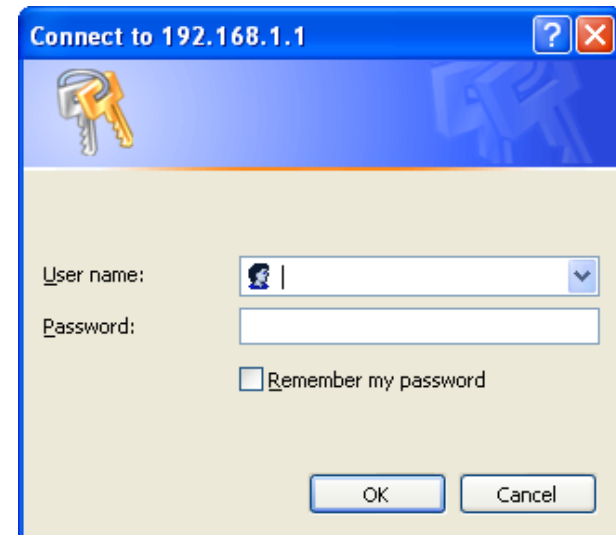
Web Configuration

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.

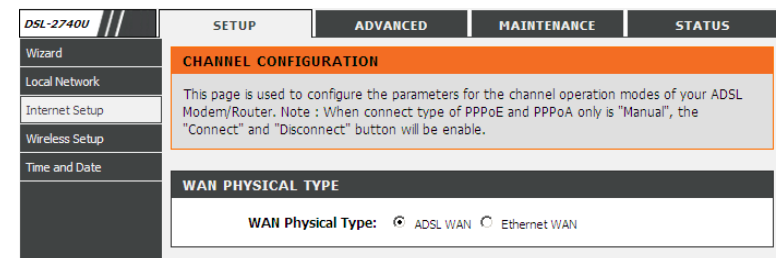
Accessing the Router

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. Enter the username and password. And then click **OK**.
- The default username and password are **admin** and **admin**.



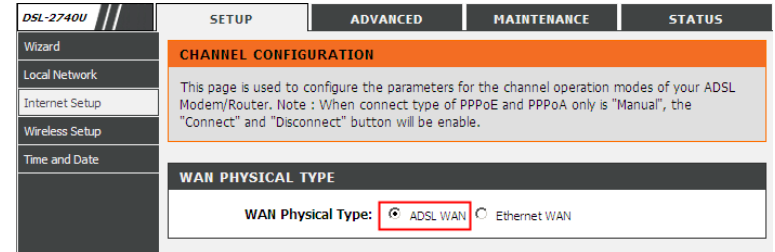
- Step 3** After logging in the web configuration page, choose **SETUP > Internet Setup > Channel Config**. The page is shown as the figure appears on the right. In this page, choose the **WAN Physical Type** according to the Internet service provided by your ISP. There are 2 types of WAN connection: **ADSL WAN** and **Ethernet WAN**.



SETUP

- **For users of ADSL Connection.**

If the Internet service provided by your ISP is in ADSL uplink mode, in **SETUP > Internet Setup > Channel Config** page, choose **ADSL WAN**.

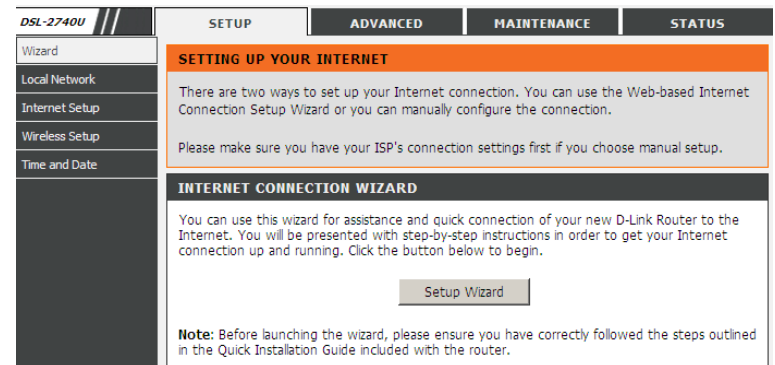


Wizard-ADSL WAN

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.

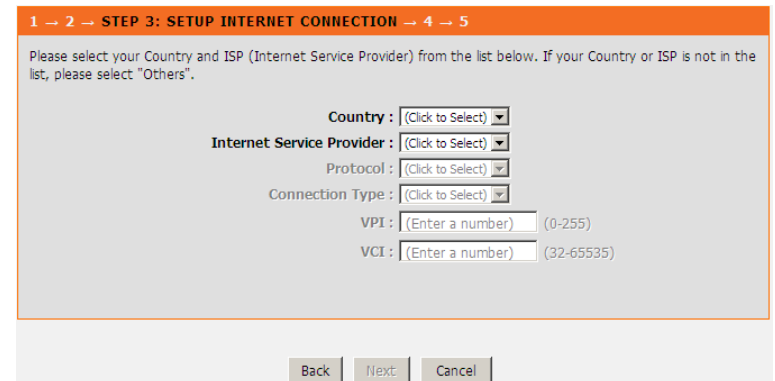
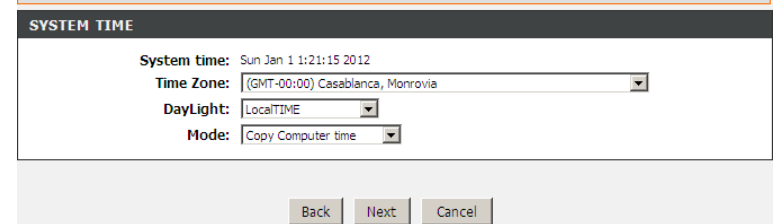
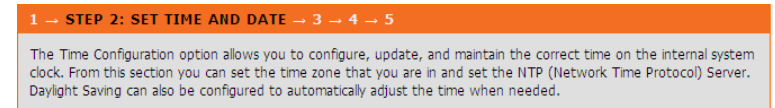
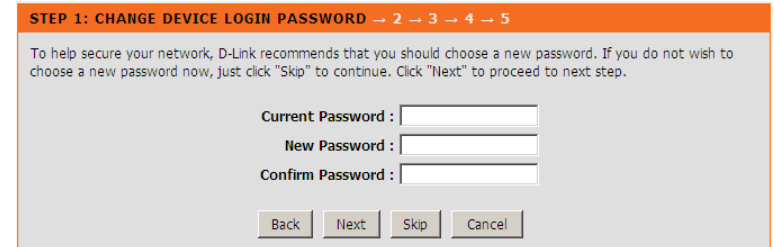
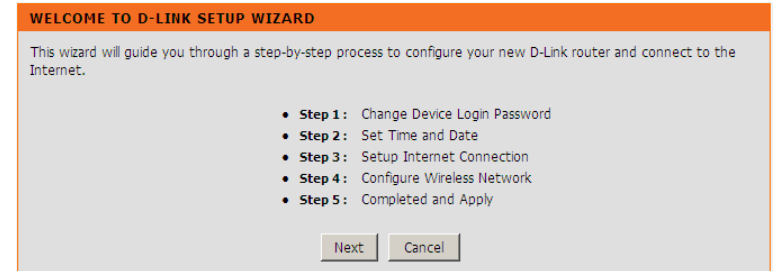
Step 2 Change the Login password (The default Login password is **admin.**), and then click **Next**.

Step 3 If you do not change the Login password, click **Skip** to go to the next page.

Step 4 Set the system time and mode, and then click **Next**.

Step 5 In this page, you can set the WAN interface.

Step 6 There are types of Protocols to connect to internet in the drop-down list of **protocol**. According to your subscribed service from your ISP, select the protocols.



- **PPPoE/PPPoA**

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

You can set the parameters in this page as follow:

- 1) Set the country that you are locating.
- 2) Choose the ISP (Internet Service Provider) where you subscribed the internet service.
- 3) Set the protocol to **PPPoE** or **PPPoA**.
- 4) Choose the connection type provided by your ISP from the **Connection Type** drop-down list.
- 5) Enter the **VPI** and **VCI** provided by your ISP.
- 6) Enter the Username and Password provided by your ISP.
- 7) Re-enter the password for confirmation.

1 → 2 → **STEP 3: SETUP INTERNET CONNECTION** → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :

Internet Service Provider :

Protocol :

Connection Type :

VPI : (0-255)

VCI : (32-65535)

PPPoE

Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.

Username :

Password :

Confirm Password :

- **Static IP**

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 country that you are locating.
- 2) Choose the ISP you subscribed the internet service from.
- 3) Set the protocol to **Static IP**.
- 4) Choose the connection type provided by your ISP from the **Connection Type** drop-down list.
- 5) Enter the **VPI** and **VCI** provided by your ISP.
- 6) 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**.

1 → 2 → **STEP 3: SETUP INTERNET CONNECTION** → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :

Internet Service Provider :

Protocol :

Connection Type :

VPI : (0-255)

VCI : (32-65535)

STATIC IP

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

The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP.

Click Next to continue.

IP Address :

Subnet Mask :

Default Gateway :

Primary DNS Server :

1 → 2 → **STEP 3: SETUP INTERNET CONNECTION** → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :

Internet Service Provider :

Protocol :

Connection Type :

VPI : (0-255)

VCI : (32-65535)

Step 7 Configure the wireless network in this page.

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

1 → 2 → 3 → **STEP 4: CONFIGURE WIRELESS NETWORK** → 5

Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.

Enable Your Wireless Network

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless Network Name (SSID) : (1~32 characters)

Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.

Visibility Status : Visible Invisible

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

Security Level :
 None WEP WPA-PSK WPA2-PSK

Security Mode: WPA-PSK
Select this option if your wireless adapters support WPA-PSK.

Now, please enter your wireless security key.

WPA2 Pre-Shared Key :
(8-63 characters, such as a~z, A~Z, or 0~9, i.e. "%Fortress123&")

Note: You will need to enter the same key here into your wireless clients in order to enable proper wireless connection.

Step 8 Click **Apply** to apply the current settings and finished the setup of the DSL-2740U router. Click **Back** to review or modify settings.

 **Note:**

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

1 → 2 → 3 → 4 → **STEP 5: COMPLETED AND APPLY**

Setup complete. Click "Back" to review or modify settings. Click "Apply" to apply current settings.

If your Internet connection does not work after apply, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

SETUP SUMMARY

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	Copy from Computer
VPI / VCI :	0/32
Protocol :	PPPoE
Connection Type :	LLC
Username :	test
Password :	test
Wireless Network :	Enabled
Wireless Network Name (SSID) :	D-Link
Visibility Status :	Visible
Encryption :	WPA2-PSK/AES (also known as WPA2 Personal)
Pre-Shared Key :	%Fortress123

Back
Apply
Cancel

Internet Setup-ADSL WAN

Channel Configuration

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

To access the internet, at least one PVC in PPPoE or 1483 MER mode is required to add.

The screenshot shows the WAN Physical Type configuration page. It is divided into three main sections: WAN PHYSICAL TYPE, DEFAULT ROUTE SELECTION, and CHANNEL CONFIGURATION. At the bottom, there are several action buttons: Connect, Disconnect, Add, Modify, Delete, Undo, and Refresh.

WAN PHYSICAL TYPE

WAN Physical Type: ADSL WAN Ethernet WAN

DEFAULT ROUTE SELECTION

Default Route Selection: Auto Specified

CHANNEL CONFIGURATION

VPI: VCI: Encapsulation: LLC VC-Mux
Channel Mode: Enable NAPT: Enable IGMP:
802.1q: Disable Enable VLAN ID(1-4095):

PPP Settings: User Name: Password:
Type: Idle Time (min):

WAN IP Settings: Type: Fixed IP DHCP
Local IP Address: Remote IP Address:
Netmask:

Default Route: Disable Enable Auto
Unnumbered

Connect Disconnect Add Modify Delete Undo Refresh

- Adding a PVC in **PPPoE** mode, do as follow:

- Step 1** Set the Default Route Selection to **Auto**.
- Step 2** Input VPI/VCP value and select Encapsulation mode provided by your ISP. The VPI/VCP value of the new PVC must be different from the PVCs which exist in **Current ATM VC Table**.
- Step 3** Set the channel mode to **PPPoE**.
- Step 4** Enter the **User name** and **password** of PPPoE account provided by your ISP.
- Step 5** Choose a connection type from the Type drop-down list. There are 3 connection types available: **Continuous**, **Connect On Demand**, **Manual**.
- Step 6** **Continuous**: The system automatically keeps dialing for WAN connection once the connection is off-line.
- Step 7** **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.
- Step 8** **Manual**: Manually dial to connect the WAN once powering on the Router.
- Step 9** After setting, click **Add** to add the new PVC in PPPoE mode in Current ATM VC Table.

DEFAULT ROUTE SELECTION

Default Route Selection: Auto Specified

CHANNEL CONFIGURATION

VPI: VCI: Encapsulation: LLC VC-Mux

Channel Mode: Enable NAPT: Enable IGMP:

802.1q: Disable Enable VLAN ID(1-4095):

IP Protocol:

PPP Settings: User Name: Password:

Type: Idle Time (min):

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address: Remote IP Address:

Netmask:

Default Route: Disable Enable Auto

Unnumbered

- Adding a PVC in **1483 MER** mode, do as follow:

- Step 1** Set the Default Route Selection to **Auto**.
- Step 2** Input VPI/VCP value and select Encapsulation mode provided by your ISP. The VPI/VCP value of the new PVC must be different from the PVCs which exist in Current ATM VC Table.
- Step 3** Set the channel mode to **1483 MER**.
- Step 4** According to the internet service provided by your ISP, choose the WAN connection type. For static IP user, choose **Fixed IP**. For dynamic IP user, choose **DHCP**.
- Step 5** If the Type is set to Fixed IP, enter the Local IP Address, Remote IP Address, and Netmask provided by your ISP.
- Step 6** After setting, click **Add** to add the new PVC in PPPoE mode in Current ATM VC Table.

DEFAULT ROUTE SELECTION

Default Route Selection: Auto Specified

CHANNEL CONFIGURATION

VPI: VCI: Select 1483MER from the drop-down list

Encapsulation: LLC VC-Mux

Channel Mode: 1483 MER Enable NAPT: Enable IGMP:

802.1q: Disable Enable VLAN ID(1-4095):

IP Protocol: Ipv4

PPP Settings: User Name: Password:

Type: Continuous Idle Time (min):

Choose the type provided by your ISP

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address: Remote IP Address:

Netmask:

Need to fill up for Fixed IP type.

Default Route: Disable Enable Auto

Unnumbered

CURRENT ATM VC TABLE:

Select	Inf	Mod e	VPI	VCI	Enca p	NAP T	IGM P	DRo ute	IP A ddr	Rem ote IP	Net Mas k	Use r Na me	Unn umber	Stat us	Edit
<input type="radio"/>	ppp	PPP	0	35	LLC	On	Off	Off	0.0.0.0	0.0.0.0	25 5.25 5.25 5.25 5	---	Down	<input type="button" value="Edit"/>	

After adding a PPPoE PVC to the table, click in the **PPPoE** mode, the page shown in the following figure appears. In this page, you can modify parameters of this PPPoE PVC.

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

Field	Description
Protocol	It displays the protocol type used for this WAN connection.
ATM VCC	The ATM virtual circuit connection assigned for this PPP interface (VPI/VCI).
Login Name	The user name provided by your ISP.
Password	The password provided by your ISP.
Authentication Method	You can choose AUTO , CHAP , or PAP .
Connection Type	You can choose Continuous , Connect on Demand , or Manual .
Idle Time (s)	If choose Connect on Demand , you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
Bridge	You can select Bridged Ethernet , Bridged PPPoE , or Disable Bridge .
AC-Name	The accessed equipment type.
Service-Name	The service name.
802.1q	You can select Disable or Enable . After enable it, you need to enter the VLAN ID. The value ranges from 1 to 4095.
MTU	Maximum Transmission Unit. Sometimes you must modify this function to access network successfully.
Static IP	If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
Source Mac address	The MAC address you want to clone.
MACCLONE	Click it to enable the MAC Clone function with the MAC

address that is configured.

ATM Settings

Choose **SETUP > Internet Setup > ATM Settings**. The page is shown as the figure appears on the right. In this page, you can configure the parameters of the ATM, including QoS, PCR, CDVT, SCR, and MBS. After setting, click **Apply Changes** to save the settings.

The following table describes the parameters of this page:

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

ADSL Settings

Choose **SETUP > Internet Setup > ADSL Settings**. The page shown in the following figure appears. In this page, you can select the DSL modulation. Mostly, you need to remain this factory default settings. The router supports these modulations: **G.Lite**, **G.Dmt**, **T1.413**, **ADSL2**, **ADSL2+**, and **AnnexL**. The router negotiates the modulation modes with the DSLAM.

PVC Auto Search

Choose **SETUP > Internet Setup > PVC Auto Search**. The page shown in the following figure appears. This page is used to configure PVC auto detect function, you can add or delete auto-pvc.

ADSL SETTINGS

ADSL modulation:

- G.Lite
- G.Dmt
- T1.413
- ADSL2
- ADSL2+

AnnexL Option:

- Enabled

AnnexM Option:

- Enabled

ADSL Capability:

- Bitswap Enable
- SRA Enable

Probe WAN PVC

VPI: VCI:

CURRENT AUTO-PVC TABLE

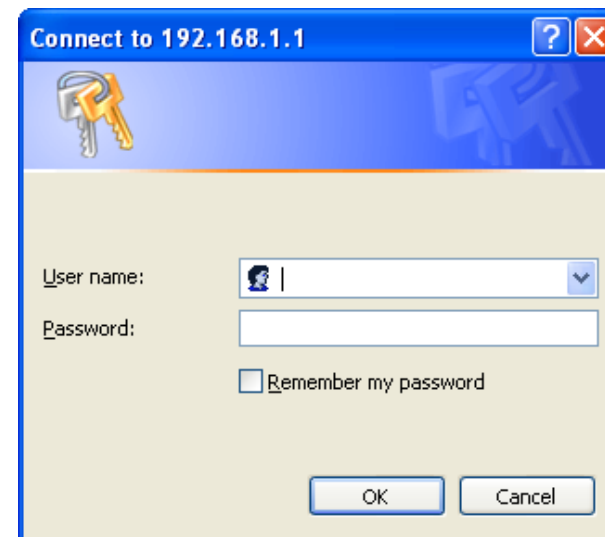
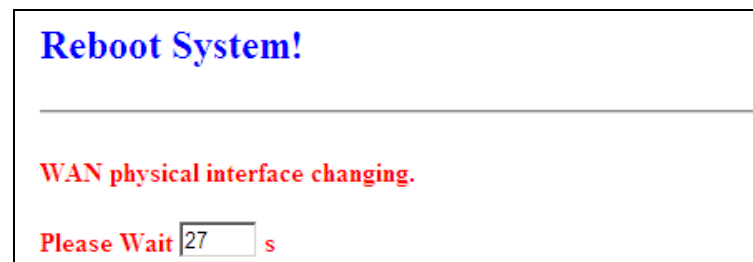
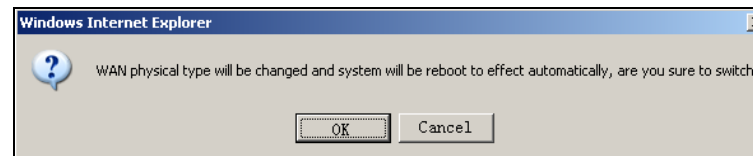
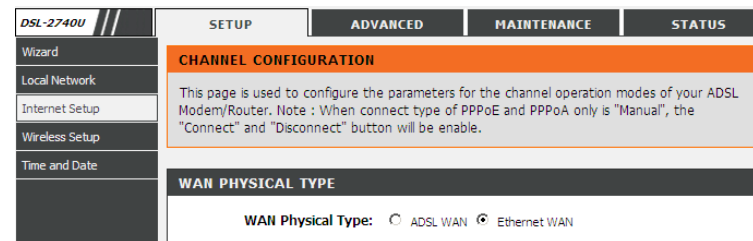
PVC	VPI	VCI
0	0	35
1	8	35
2	0	43
3	0	51
4	0	59
5	8	43
6	8	51
7	8	59

- **For users of Ethernet Connection.**

Step 1 If the Internet service provided by your ISP is in Ethernet uplink mode, in **SETUP > Internet Setup > Channel Config** page, choose **Ethernet WAN**.

Step 2 A dialog box prompts to reboot the router. Click **OK**. And then a pop-up dialog box shows the process of rebooting system.

Step 3 When the rebooting system finished, a login window pops up. Input the username and password to log in the web configuration page.



Wizard-Ethernet WAN

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 Change the Login password (The default Login password is **admin.**), and then click **Next**.

Step 3 If you do not change the Login password, click **Skip** to go to the next page.

Step 4 Set the system time and mode, and then click **Next**.

The figure consists of three screenshots from the D-Link web configuration interface:

- INTERNET CONNECTION WIZARD**: The top screenshot shows the main wizard page. It includes a "Setup Wizard" button and a note: "Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router."
- WELCOME TO D-LINK SETUP WIZARD**: The middle screenshot shows the welcome page. It lists five steps:
 - Step 1: Change Device Login Password
 - Step 2: Set Time and Date
 - Step 3: Setup Internet Connection
 - Step 4: Configure Wireless Network
 - Step 5: Completed and Apply
 There are "Next" and "Cancel" buttons at the bottom.
- STEP 1: CHANGE DEVICE LOGIN PASSWORD**: The bottom screenshot shows the password change step. It has a progress indicator "1 → 2 → 3 → 4 → 5". The text says: "To help secure your network, D-Link recommends that you should choose a new password. If you do not wish to choose a new password now, just click 'Skip' to continue. Click 'Next' to proceed to next step." There are three input fields for "Current Password", "New Password", and "Confirm Password", and "Back", "Next", "Skip", and "Cancel" buttons.

Step 5 In this page, you can set the WAN interface.

Step 6 There are types of Protocols to connect to internet in the drop-down list of **protocol**. According to your subscribed service from your ISP, select the protocols.

- **PPPoE**

If the protocol is set to **PPPoE**, the page shown as the right figure appears. Input the Username and Password of your Internet service account provided by your ISP.

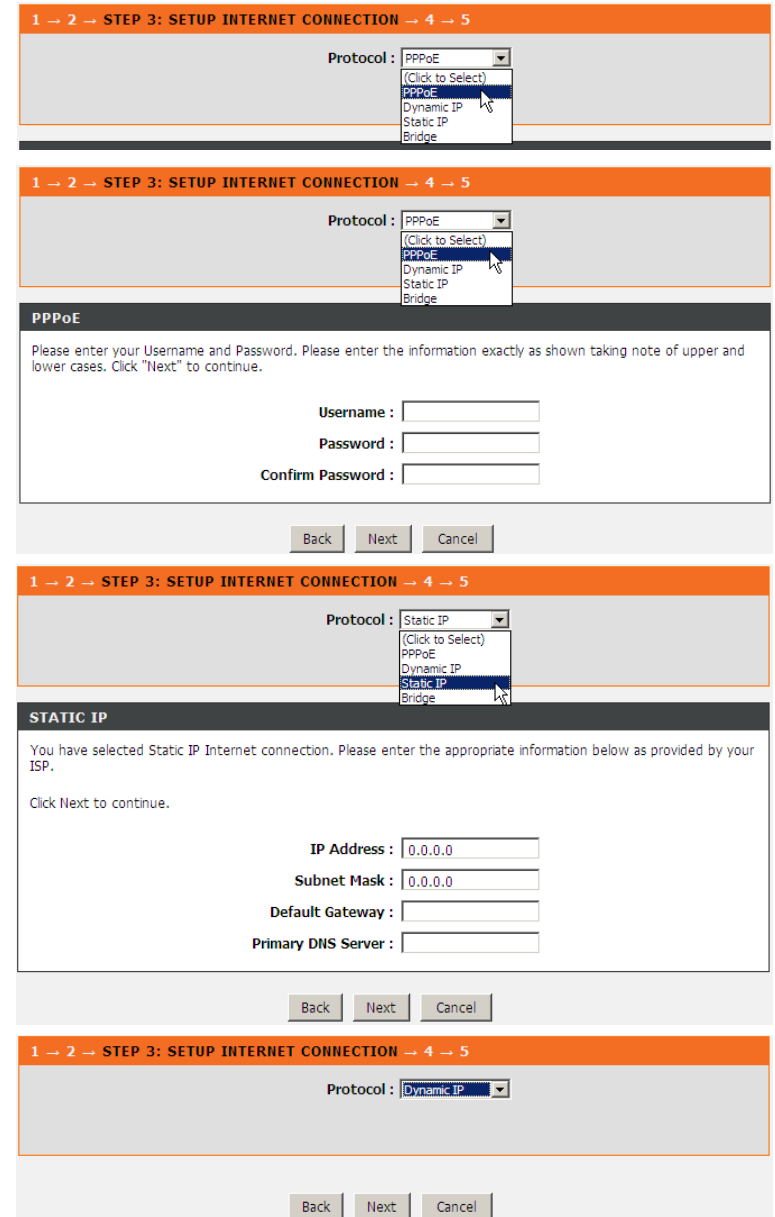
- **Static IP**

If the protocol is set to **Static IP**, the page shown as the right figure appears. Input the information of your Internet service account provided by your ISP.

- **Dynamic IP/Bridge**

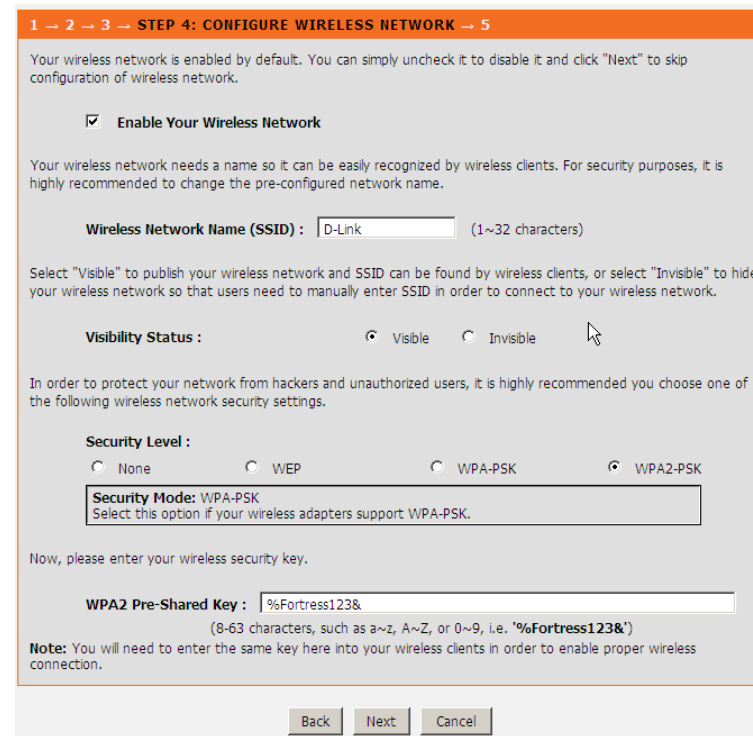
If the protocol is set to **Dynamic IP/Bridge**, the page shown as the right figure appears. You do not need to do any configuration in this step.

After setting, click **Next**.



Step 7 Configure the wireless network in this page.

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



Step 8 Click **Apply** to apply the current settings and finished the setup of the DSL-2740U router. Click **Back** to review or modify settings.

 **Note:**

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

1 → 2 → 3 → 4 → **STEP 5: COMPLETED AND APPLY**

Setup complete. Click "Back" to review or modify settings. Click "Apply" to apply current settings.

If your Internet connection does not work after apply, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

SETUP SUMMARY

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	Copy from Computer
VPI / VCI :	0/32
Protocol :	PPPoE
Connection Type :	LLC
Username :	test
Password :	test
Wireless Network :	Enabled
Wireless Network Name (SSID) :	D-Link
Visibility Status :	Visible
Encryption :	WPA2-PSK/AES (also known as WPA2 Personal)
Pre-Shared Key :	%Fortress123

Back
Apply
Cancel

Internet Setup-Ethernet WAN

Channel Configuration

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

WAN PHYSICAL TYPE

WAN Physical Type: ADSL WAN Ethernet WAN

DEFAULT ROUTE SELECTION

Default Route Selection: Auto Specified

CHANNEL CONFIGURATION

Channel Mode: Enable NAPT: Enable IGMP:

802.1q: Disable Enable VLAN ID(1-4095):

PPP Settings: User Name: Password:

Type: Idle Time (min):

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address: Remote IP Address:

Netmask:

Default Route: Disable Enable Auto

Unnumbered

CURRENT ATM VC TABLE:

Select	Inf	Mode	NAPT	IGMP	DRout e	IP Ad dr	Remo te IP	NetMa sk	User N ame	Statu s	Edit

- Adding a channel **PPPoE** mode, do as follow:

- Step 1** Set the Default Route Selection to **Specified**.
- Step 2** Set the channel mode to **PPPoE**.
- Step 3** Enter the **User name** and **password** of PPPoE account provided by your ISP.
- 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** After setting, click **Add** to add the new channel.

DEFAULT ROUTE SELECTION

Default Route Selection: Auto Specified

[Choose PPPoE](#)

CHANNEL CONFIGURATION

Channel Mode: (Dropdown menu options: Bridge, DHCP(Static IP), PPPoE)

802.1q: Disabled Enabled

Enable NAPT: Enable IGMP:

VLAN ID(1-4095):

IP Protocol: (Dropdown menu options: Ipv4, Ipv6)

[Input information provided by your ISP.](#)

PPP Settings: User Name: Password:

Type: (Dropdown menu options: Continuous, Connect On Demand, Manual) Idle Time (min):

WAN IP Settings: Type: Fixed IP DHCP

Local IP Address: Remote IP Address:

Netmask:

Default Route: Disable Enable Auto

Unnumbered

Connect Disconnect Add Modify Delete Undo Refresh

CURRENT ATM VC TABLE:

Select	Inf	Mode	NAPT	IGMP	DRout e	IP Ad dr	Remo te IP	NetMa sk	User N ame	Statu s	Edit
--------	-----	------	------	------	---------	----------	------------	----------	------------	---------	------

- Adding a channel in **DHCP(Static IP)** mode, do as follow:

- Step 1** Set the Default Route Selection to **Specified**.
- Step 2** Set the channel mode to **DHCP(Static IP)**.
- Step 3** According to the internet service provided by your ISP, choose the WAN connection type. For dynamic IP user, choose **DHCP**. For static IP user, choose **Fixed IP**.
- Step 4** If the Type is set to Fixed IP, enter the Local IP Address, Remote IP Address, and Netmask provided by your ISP.
- Step 5** After setting, click **Add** to add the new channel.

DEFAULT ROUTE SELECTION

Default Route Selection: Auto Specified

[Choose DHCP\(Static IP\)](#)

CHANNEL CONFIGURATION

Channel Mode: DHCP(Static IP) Bridge
DHCP(Static IP)
PPPoE Enable NAPT: Enable IGMP:

802.1q: Dis ... VLAN ID(1-4095):

IP Protocol:

PPP Settings: User Name: Password:

Type: Idle Time (min):

WAN IP Settings: Type: Fixed IP DHCP Choose the type based on the information provided by your ISP.

Local IP Address: Remote IP Address:

Netmask:

Default Route: Disable Enable Auto Entries needed to fill up in Fixed IP mode.

Unnumbered

CURRENT ATM VC TABLE:

Select	Inf	Mode	NAPT	IGMP	DRout e	IP Ad dr	Remo te IP	NetMa sk	User N ame	Statu s	Edit
<input type="radio"/>	pppoe 2	PPPoE	On	Off	On	0.0.0. 0	0.0.0. 0	255.2 55.25 5.255	test	Down	✎ 🗑

CURRENT ATM VC TABLE:

Select	Inf	Mode	NAPT	IGMP	DRout e	IP Ad dr	Remo te IP	NetMa sk	User N ame	Statu s	Edit
<input type="radio"/>	pppoe 2	PPPoE	On	Off	On	0.0.0. 0	0.0.0. 0	255.2 55.25 5.255	test	Down	✎ 🗑

After adding a channel to the table, click in the **PPPoE** mode, the page shown in the following figure appears. In this page, you can modify parameters of this channel in PPPoE mode.

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

Field	Description
Protocol	It displays the protocol type used for this WAN connection.
Login Name	The user name provided by your ISP.
Password	The password provided by your ISP.
Authentication Method	You can choose AUTO , CHAP , or PAP .
Connection Type	You can choose Continuous , Connect on Demand , or Manual .
Idle Time (s)	If choose Connect on Demand , you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
AC-Name	The accessed equipment type.
Service-Name	Enter the service name.
802.1q	You can select Disable or Enable . After enable it, you need to enter the VLAN ID. The value ranges from 1 to 4095.
MTU	Maximum Transmission Unit. Sometimes you must modify this function to access network successfully.
Static IP	If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
Source Mac address	The MAC address you want to clone.
MACCLONE	Click it to enable the MAC Clone function with the MAC address that is configured.

PPP INTERFACE

Protocol: PPPoE

Login Name:

Password:

Authentication Method:

Connection Type:

Idle Time (s):

AC-Name:

Service-Name:

802.1q: Disable Enable

VLAN ID(1-4095):

MTU (1-1500):

Static IP:

Source Mac address: (ex:00:E0:86:71:05:02)

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 network segment.

LAN Interface

Choose **SETUP > Local Network > LAN Interface**. The page is shown as the figure appears on the right. In this page, you can set the LAN IP address, working mode, and MAC address control.

- Step 1** In the **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 set to **255.255.255.0**.
- Step 3** Select Secondary IP. Input a secondary IP address and subnet mask.
- Step 4** **Secondary IP** 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.

Secondary IP

IP Address:

Subnet Mask:

- Step 5** Set IGMP Snooping. You can keep the default settings.
- Step 6** Set the LAN Link Mode for each LAN port. It is recommended to keep it as defaults.

LAN INTERFACE SETTINGS

Interface Name: **e1**

IP Address:

Subnet Mask:

Secondary IP

IGMP Snooping: Disable Enable

LAN LINK MODE SETTINGS

LAN Port:

Link Speed/Duplex Mode:

ETHERNET Status Table:

Select	Port	Link Mode
<input type="radio"/>	LAN1	AUTO Negotiation
<input type="radio"/>	LAN2	AUTO Negotiation
<input type="radio"/>	LAN3	AUTO Negotiation
<input type="radio"/>	LAN4	AUTO Negotiation

MAC ADDRESS CONTROL SETTINGS

MAC Address Control: LAN1 LAN2 LAN3 LAN4 WLAN

New MAC Address:

CURRENT ALLOWED MAC ADDRESS TABLE

MAC Addr	Action

LAN IPv6 Interface

Choose **SETUP > Local Network > LAN IPv6 Interface**. The page shown in the right figure appears. This page allows you to configure IPv6 LAN. User can set LAN RA server work mode and LAN DHCPv6 server work mode.

The following table describes the parameters of this page.

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

The screenshot shows the configuration interface for the LAN IPv6 interface. It is divided into three main sections:

- LAN GLOBAL ADDRESS SETTING:** Contains a 'Global Address' field with a placeholder for IP address and a slash for a subnet mask. Below it is an 'Apply Changes' button.
- RA SETTING:** Contains several options:
 - 'Enable': checked.
 - 'M Flag': unchecked.
 - 'O Flag': checked.
 - 'Max Interval': 600 Secs.
 - 'Min Interval': 200 Secs.
 - 'Prefix Mode': set to 'Auto'.
 - 'ULA Enable': unchecked.
 - 'RA DNS Enable': unchecked.
 Below this section is another 'Apply Changes' button.
- DHCPV6 SETTING:** Contains:
 - 'DHCPv6 Mode': set to 'Auto Mode'.
 - 'IPv6 Address Suffix Pool': set to '::1' - '::ffff' (with a note '(ex. :1:1:1:1 or ::1)').
 - 'IPv6 DNS Mode': set to 'Auto'.
 Below this section is a final 'Apply Changes' button.

DHCP Server

Choose **SETUP > Local Network > DHCP Server**. This page allows you to configure the DHCP server.

There are 3 types of DHCP Modes: **DHCP Server**, **DHCP Relay**, and **None**.

To configure the DHCP Server, do as follow:

– **DHCP Server**

DHCP Server: If you are using 2740U as a DHCP server, select **DHCP Server**. The 2740U will assign IP address to the hosts connected to the 2740U.

- Step 1** Select **DHCP Server** from the DHCP Mode.
- Step 2** Select interfaces using the DHCP Mode set in **Step 1**.
- Step 3** Set the **IP pool 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. You can keep it as defaults.
- Step 4** Set the **default gateway**. You can keep it as defaults: **192.168.1.1**.
- Step 5** Set the **Max lease time**. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
- Step 6** Set the Domain Name and DNS Servers. You can keep it as defaults.
- Step 7** After setting, click **Apply Changes** to save the settings.

– **DHCP Relay**

DHCP Relay: If you are using the other DHCP server to assign IP address to your hosts on the LAN, enable the **DHCP Relay**. You can set the DHCP server IP address. The DHCP Relay enables the message to transmit between clients in different network segment.

- Step 1** Select **DHCP Relay** from the DHCP Mode.
- Step 2** Set the **Relay Server**. You can keep it as defaults.
- Step 3** After setting, click **Apply Changes** to save the settings.

DHCP Reserved

Choose **SETUP > Local Network > DHCP Reserved**. The page shown in the right figure appears. This page allows you to reserve IP address for PC specified in this page.

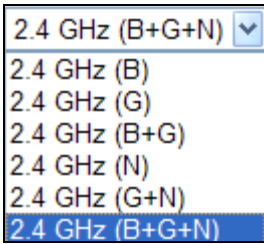
Select	IP Address	MAC Address
--------	------------	-------------

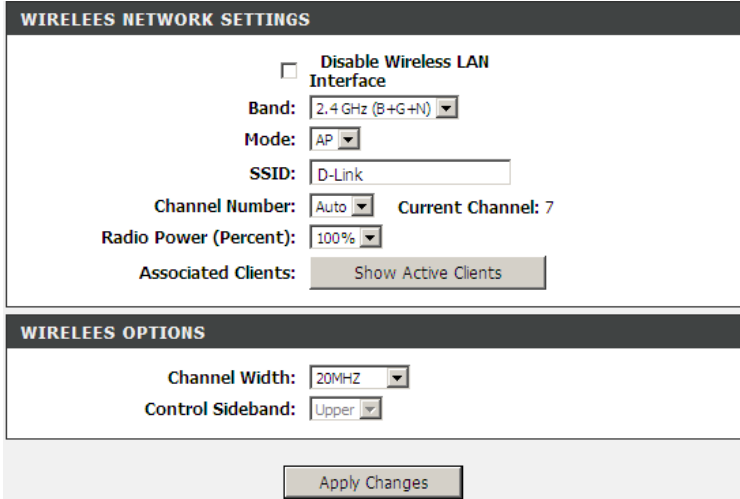
Wireless Setup

Wireless Basics

Choose **SETUP > Wireless Setup > Wireless Basics**. The page is shown as the figure appears on the right. In this page, you can configure the wireless settings for your router.

The following table describes the parameters of this page:

Field	Description
Band	<p>Choose the adapted band of the modem from the drop-down list.</p> 
Mode	<p>Set the working mode of the device. The mode may vary from software to software. By default, the network mode of the modem is AP.</p>
SSID	<p>Set a name for the wireless network of your device. Wireless stations associating to the modem must have the same SSID.</p>
Channel Number	<p>A channel is the radio frequency used by 802.11b/g/n wireless devices. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. Interference and degrading performance occurs when radio signal from different APs overlap. Choose a channel from the drop-down list box.</p>
Radio Power	<p>Choose the transmission power of the radio signal. It is recommended to leave the default setting. The default</p>



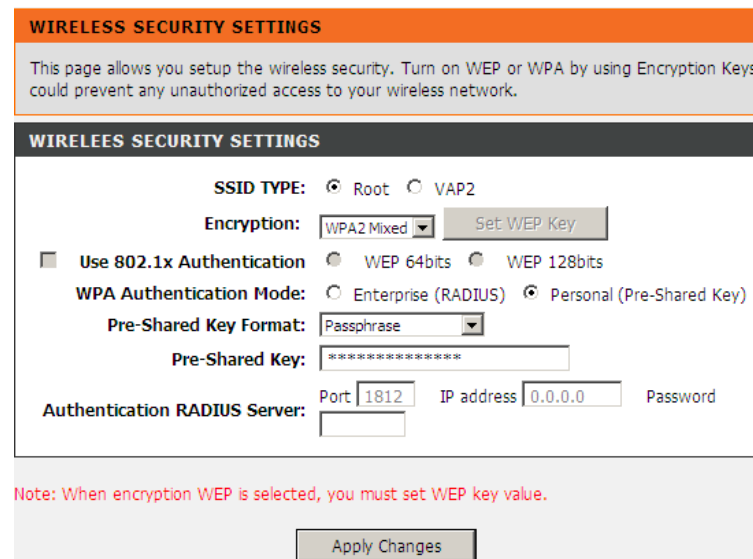
	setting is 100% .
Show Active Clients	Click it to view the information of the wireless clients that are connected to the modem.
Channel Width	You can select 20MHZ, 40MHZ or 20/40MHZ .
Control Sideband	Only when choose 40MHZ for Channel Width, you can set this parameter. You can choose Upper or Lower from the drop-down list.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click Save in the lower left corner.

Wireless Security

Choose **SETUP > Wireless Setup > Wireless Security**. The page is shown as the figure appears on the right. In this page, you can configure the security for your wireless network.

The following table describes the parameters of this page:

Field	Description
Encryption	<p>Configure the wireless encryption mode. You can choose None, WEP, WPA (TKIP), WPA (AES), WPA2 (AES), WPA2 (TKIP), or WPA2 Mixed.</p> <ul style="list-style-type: none"> ● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network. ● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft. ● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes a connection with the modem through WPA or WPA2.
Set WEP Key	It is available when you set the encryption mode to WEP . Click it, the Wireless WEP Key Setup page appears.



WPA Authentication Mode	<ul style="list-style-type: none"> ● Select Personal (Pre-Shared Key), enter the pre-shared key in the Pre-Shared Key field. ● Select Enterprise (RADIUS), enter the port, IP address, and password of the Radius server. You need to enter the username and password provided by the Radius server when the wireless client connects the modem.
-------------------------	---

After setting, click **Apply Changes** to save the settings.

Set the **Encryption** to be **WEP**, then click **Set WEP Key**, and the following page appears.

 **Note:**

If the encryption is set to be **WEP**, the WPS function will be disabled.

The following describes the parameters of this page:

Field	Description
Key Length	Choose the WEP key length. You can Choose 64-bit or 128-bit .
Key Format	<ul style="list-style-type: none"> ● If you choose 64-bit, you can choose ASCII (5 characters) or Hex (10 characters). ● If you choose 128-bit, you can choose ASCII (13 characters) or Hex (26 characters).
Default Tx Key	Choose the index of WEP Key. You can choose Key 1 , Key 2 , Key 3 , or Key 4 .
Encryption Key 1 to 4	<p>The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission.</p> <ul style="list-style-type: none"> ● If you choose 64-bit and ASCII (5 characters), enter any 5 ASCII characters. ● If you choose 64-bit and Hex (10 characters), enter any 10 hexadecimal characters. ● If you choose 128-bit and ASCII (13 characters), enter

	<p>any 13 ASCII characters.</p> <ul style="list-style-type: none"> ● If you choose 128-bit and Hex (26 characters), enter any 26 hexadecimal characters.
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click Save in the lower left corner.

Time and Date

Choose **SETUP > Time and Date**. The page is shown as the figure appears on the right.

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

SYSTEM TIME

System Time: Year Month Day Hour min sec

Time Zone:

DayLight:

Mode:

START NTP:

NTP Start:

ADVANCED

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

Advanced Wireless

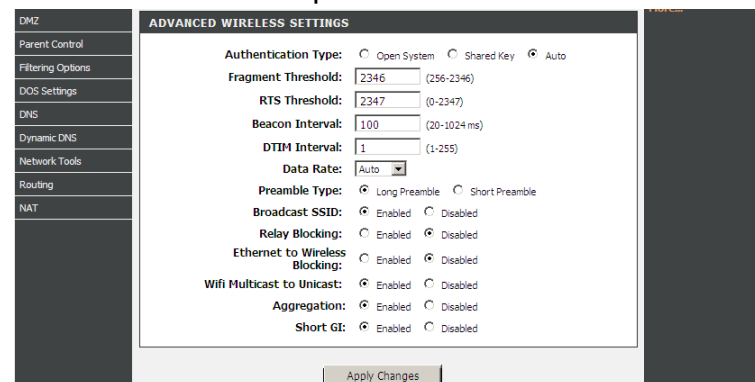
This function is used to modify the standard 802.11 wireless radio settings. It is recommended not to change the default settings, because incorrect settings may impair the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

Wireless Advanced

Choose **ADVANCED >Advanced Wireless >Wireless Advanced**. The page shown as the figure appears on the right. In this page, you can configure the wireless advanced parameters. It is recommended to use the default parameters.

The following table describes parameters in this page:

Field	Description
Authentication Type	It is recommended to keep it as defaults.
Fragmentation Threshold	Set the threshold of fragmentation length. If the length of a packet is greater than the value, the packet is automatically fragmented into several packets. Because too many packets lead to low performance of the wireless network, the value of Fragmentation Threshold cannot be too small. The default value is 2346.
RTS Threshold	Set the CTS/RTS threshold. If the length of a packet is greater than the value, the router sends an RTS frame to the destination station to negotiate. After receiving the RTS frame, the wireless station responds with a Clear to Send (CTS) frame to the router, indicating that they can communicate with each other. The default value is 2346.
Data Rate	Choose the transmission rate of the wireless data from the dropdown list.
Preamble Type	<ul style="list-style-type: none"> ● Long Preamble: It means this card always use long preamble. ● Short Preamble: It means this card can support short



	preamble capability.
Broadcast SSID	Select whether the modem broadcasts SSID or not. You can select Enable or Disable . <ul style="list-style-type: none"> ● Select Enable, the SSID can be detected. ● Select Disable to hide SSID, the wireless clients cannot find the SSID. You need to enter the SSID and password of the wireless network manually.
Relay Blocking	Wireless isolation. Select Enable , the wireless clients that are connected to the modem cannot intercommunication.
Ethernet to Wireless Blocking	Whether the wireless network can communicate with the Ethernet network or not.
Wifi Multicast to Unicast	Enable it to using unicast to transmit multicast packet

After setting, click **Apply Changes** to save the settings.

Access Control

Choose **ADVANCED >Advanced Wireless > Access Control**. The page shown as the figure appears on the right. If you choose **Allowed Listed**, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When **Deny Listed** is selected, these wireless clients on the list will not be able to connect the Access Point.

The screenshot shows the 'WIRELESS ACCESS CONTROL MODE' section with a dropdown menu set to 'Disable' and an 'Apply Changes' button. Below it is the 'WIRELESS ACCESS CONTROL SETTINGS' section with a 'MAC Address' input field (example: 00E086710502) and 'Add' and 'Reset' buttons. The 'CURRENT ACCESS CONTROL LIST' section features a table with 'MAC Address' and 'Select' columns, and 'Delete Selected' and 'Delete All' buttons at the bottom.

WPS

Choose **ADVANCED >Advanced Wireless > WPS**. The page shown as the figure appears on the right. If you choose Allowed Listed, only those clients whose

wireless MAC addresses are in the access control list will be able to connect to your Access Point. When Deny Listed is selected, these wireless clients on the list will not be able to connect the Access Point.

There are 3 methods to realize wireless connection through WPS.

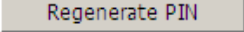
- PBC

Click the **Start 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 2740U.

- 1) Do not select **Disable WPS**.
- 2) Click **Start PIN** button beside **Pin Configuration**.
- 3) Input the Device PIN (a random code displayed in this page) in the WPS application interface of the client to be connected. Take this device for example, the Device PIN is **71221045**. And then click **PIN** on the client.
- 4) After setting, click **Apply Changes**.

 **Note:**

If you want to change the PIN, click **Regenerate PIN**  button in this page.

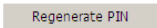
- Based on the PIN of the client to be connected.


- 1) Do not select **Disable WPS**.
- 2) Find the PIN of the client to be connected. Input this PIN in the **Client PIN Number** in this page. And then click **Start PIN** button below.


WIFI PROTECTED SETTINGS

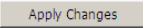

Disable WPS

WPS Status: Configured UnConfigured

Self-PIN Number: 

PIN Configuration: 

Push Button Configuration: 


 

CURRENT KEY INFO

Authentication	Encryption	Key
WPA2 PSK	TKIP+AES	meuoveloXwifi

CLIENT PIN INFO

Client PIN Number:



MBSSID

Choose **ADVANCED >Advanced Wireless > MBSSID**. The page shown as the figure appears on the right. This page allows you to set virtual access points (VAP). Here you can enable/disable virtual AP, and set its SSID and authentication type. click **Apply Changes** to take it into effect.

The screenshot displays the 'WIRELEES MULTIPLE BSSID SETTINGS' configuration page, which is organized into four distinct sections for VAP0, VAP1, VAP2, and VAP3. Each section contains the following settings:

- Enable VAP:** A checkbox that is currently unchecked for all four VAPs.
- SSID:** A text input field containing 'D-Link_Guest1' for VAP0, 'D-Link_Guest2' for VAP1, 'D-Link_Guest3' for VAP2, and 'D-Link_Guest4' for VAP3.
- broadcast SSID:** Radio buttons for 'Enable' and 'Disable', with 'Enable' selected for all VAPs.
- Relay Blocking:** Radio buttons for 'Enable' and 'Disable', with 'Disable' selected for all VAPs.
- Authentication Type:** Radio buttons for 'Open System', 'Shared Key', and 'Auto', with 'Open System' selected for all VAPs.

At the bottom of the page, there is a button labeled 'Apply Changes'.

Access Control List

Access Control List

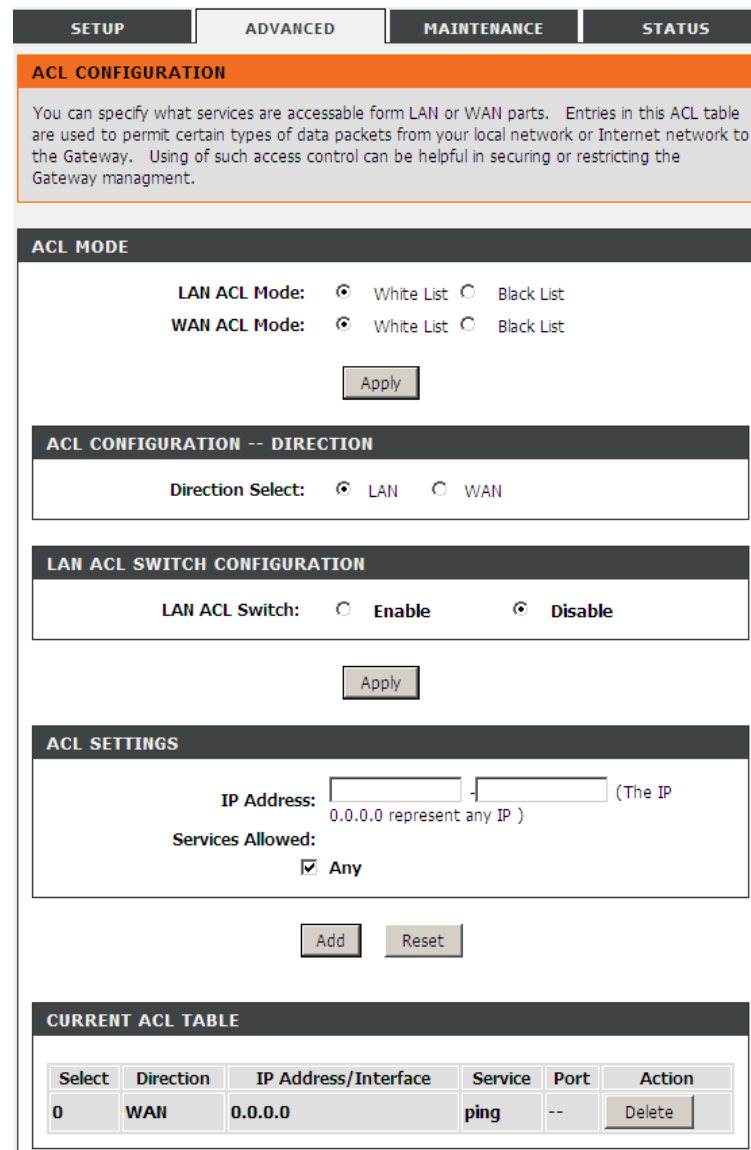
Choose **ADVANCED >Access Control List**. The page shown as the figure appears on the right. In this page, you can permit the data packets from LAN or WAN to access the router in IPv4 protocol. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.

 **Note:**

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

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

Field	Description
ACL Mode	<ul style="list-style-type: none"> White List: permit certain types of data packets from your local network or Internet network to the Gateway. Black List: block certain types of data packets from your local network or Internet network to the Gateway.
Direction Select	Select the router interface. You can select LAN or WAN . In this example, LAN is selected.
LAN ACL Switch	Select it to enable or disable ACL function.
IP Address	Enter the IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can access the router.
Services Allowed	You can choose the following services from LAN: Web, Telnet, SSH, FTP, TFTP, SNMP, or PING . You can select Any to choose all the services.
Add	After setting the parameters, click it to add an entry to the Current ACL Table .



ACL CONFIGURATION

You can specify what services are accessible from LAN or WAN parts. Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway. Using of such access control can be helpful in securing or restricting the Gateway management.

ACL MODE

LAN ACL Mode: White List Black List
 WAN ACL Mode: White List Black List

Apply

ACL CONFIGURATION -- DIRECTION

Direction Select: LAN WAN

LAN ACL SWITCH CONFIGURATION

LAN ACL Switch: Enable Disable

Apply

ACL SETTINGS

IP Address: - (The IP 0.0.0.0 represent any IP)
 Services Allowed: Any

Add Reset

CURRENT ACL TABLE

Select	Direction	IP Address/Interface	Service	Port	Action
0	WAN	0.0.0.0	ping	--	Delete

Reset	Click it to refresh this page.
-------	--------------------------------

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

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

Field	Description
Direction Select	Select the router interface. You can select LAN or WAN . In this example, WAN is selected.
WAN Setting	You can choose Interface or IP Address .
WAN Interface	Choose the interface that permits data packets from WAN to access the router.
Services Allowed	You can choose the following services from WAN: Web, Telnet, SSH, FTP, TFTP, SNMP or PING .
Add	After setting the parameters, click it to add an entry to the Current ACL Table .
Reset	Click it to refresh this page.

The screenshot shows the 'ACL CONFIGURATION -- DIRECTION' page. At the top, 'Direction Select' has radio buttons for 'LAN' and 'WAN', with 'WAN' selected. Below this is the 'ACL SETTINGS' section, which includes a 'WAN Setting' dropdown menu set to 'Interface', a 'WAN Interface' dropdown menu set to 'pppoe1', and a 'Services Allowed' section with checkboxes for 'web', 'telnet', 'ssh', 'ftp', 'tftp', 'snmp', and 'ping'. At the bottom of the settings section are 'Add' and 'Reset' buttons. Below the settings is the 'CURRENT ACL TABLE' section, which contains a table with one entry:

Select	Direction	IP Address/Interface	Service	Port	Action
0	WAN	0.0.0.0	ping	--	Delete

Access Control List IPv6

Choose **ADVANCED > Access Control List > Access Control List IPv6**. In this page, you can permit the data packets from LAN or WAN to access the router in IPv6 protocol. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.

For the parameters description in this page, you can refer to the description of **Access Control List**.

Port Triggering

Choose **ADVANCED > Port Triggering**. The page shown as the figure appears on the right.

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

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

When you have finished, click the **Apply changes** button.

NAT PORT TRIGGER STATUS

Nat Port Trigger: Enable Disable

APPLICATION TYPE

Usual Application Select One ▾

User-defined Application Name:

Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾
<input type="text"/>	<input type="text"/>	UDP ▾	<input type="text"/>	<input type="text"/>	UDP ▾	outgoing ▾

CURRENT PORTTRIGGER TABLE

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action

Port Forwarding

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

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by Protocol and WAN port) to the internal server with a private IP address on the LAN side.

Select Usual Service Name, and enter the LAN IP address and click **Apply Changes** to forward IP packets for this service to the specified server.

PORT FORWARDING SETUP

Usual Service Name: AUTH

User-defined Service Name:

Protocol: TCP

WAN Setting: Interface

WAN Interface: pppoe1

WAN Port: 113 (ex. 5001:5010)

LAN Open Port: 113

LAN Ip Address:

CURRENT PORT FORWARDING TABLE

Select	Server Name	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action

DMZ

Choose **ADVANCED > DMZ** to go to the following page. The page shown as the figure appears on the right.

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.

DMZ CONFIGURATION

WAN Interface: pppoe1

DMZ Host IP Address:

CURRENT DMZ TABLE:

Select	WAN Interface	DMZ Ip

Parental Control

URL Block

Choose **ADVANCED > Parental Control > URL Block**. The page is shown as the figure appears on the right. This page is used to configure the blocked URL in specified time. Here you can add/delete filtered URL Firstly. You should enable URL Blocking Capability.

Note:

To use this feature, the time of router must be correct. Please set the system time in **SETUP > Time and Date**.

To set URL Block, do as follow:

Step 1 Set the URL to be blocked.

- To block all websites, select **Block Any URL**.
- To block a certain website, select **Keyword**, and then input the URL address or keyword of the URL.

Step 2 Set the Schedule Mode.

- Existing Schedule: You can use the schedules already set.
- Manual Schedule: Manually set a time. The URL will be blocked during this time.

Step 3 After setting, click **Add Filter** to save an URL filter in **URL Blocking Table**.

URL BLOCKING CAPABILITY

URL Blocking Capability: Disable Enable

URL BLOCKING

Block Any URL

Keyword:

Schedule Mode Existing Schedule Manual Schedule

Schedule:

Days: EveryDay
 Sun Mon Tue Wed
 Thu Fri Sat

All day(24Hour):

Time: From : : To : :
(e.g. From 09:21 To 18:30)

URL BLOCKING TABLE:

Select	Filtered URL	Days	Time	Rule Name
<input type="button" value="Delete Selected URL"/>				

Online Time Limit

Choose **ADVANCED > Parental Control > Online Time Limit**. The page is shown as the figure appears on the right. This page is used to manage the time of surf Internet, after enable this feature, only the specific PCs can surf Internet in specific time segment

 **Note:**

To use this feature, the time of router must be correct. Please set the system time in **SETUP > Time and Date**.

Schedules

Choose **ADVANCED > Parental Control > Schedules**. The page is shown as the figure appears on the right. It allows you to create scheduling rules to be applied for URL block.

 **Note:**

To use this feature, the time of router must be correct. Please set the system time in **SETUP > Time and Date**.

ONLINE TIME LIMIT

Online Time Limit: Enable Disable

Date: Everyday
 Mon Tues Wed Thur Fri Sat
 Sun

Time: All day(24Hour)
 Start Time End Time (ex. 09:45)

Specific PC: IP Address MAC Address

IP Address: --

MAC Address: (ex. 00:E0:86:71:05:02)

CURRENT ONLINE TIMELIMIT TABLE:

Select	Date	Starting Time	Ending Time	MAC Address	IP Address	Action
<input type="button" value="Delete All"/>						

ADD SCHEDULE RULE

Rule Name:

Days: Everyday
 Sun Mon Tue Wed
 Thu Fri Sat

All day(24Hour):

Time: From : To :
 (e.g. From 09:21 To 18:30)

RULES TABLE:

Select	Rule Name	Days	Time
<input type="button" value="Delete Selected Rule"/>			

Filtering Options

IP/Port Filter

Choose **ADVANCED > Filter Options > IP/Port Filter** to go to the following page. The page shown as the figure appears on the right. The IP/Port Filter in this page is based on IPv4 protocol.

Entries in the table are used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.

For example, select protocol as **IP**, rule action as **Deny**, direction as **Downstream** and fill the **Source IP/Dest IP**, which means downstream IP packets matching the source IP address and the destination IP address cannot enter the internal network.

DEFAULT ACTION STATUS

Outgoing Default Action: Permit Deny
 Incoming Default Action: Permit Deny

RULE CONFIGURATION

Rule Action: Permit Deny
 Protocol:
 Direction:
 Source IP Address: Mask Address:
 Dest IP Address: Mask Address:
 SPort: - DPort: -
 Enable:

CURRENT FILTER TABLE

Rule	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action

IPv6/Port Filter

Choose **ADVANCED > Filter Options > IPv6/Port Filter** to go to the right page. The page shown as the figure appears on the right. The IP/Port Filter in this page is based on IPv6 protocol.

For the parameter descriptions in this page, please refer to **ADVANCED > Filter Options > IP/Port Filter**.

MAC Filter

Choose **ADVANCED > Filter Options > MAC Filter** to go to the following page. Entries in the table are used to restrict certain types of data packets from your local network to Internet through the gateway. These filters are helpful in securing or restricting your local network.

DEFAULT ACTION STATUS

Outgoing Default Action: Permit Deny
 Incoming Default Action: Permit Deny

RULE CONFIGURATION

Rule Action: Permit Deny
 Protocol: IPv6 Icmp6Type: PING6
 Direction: Upstream
 Source IPv6 Address: Prefix Length:
 Dest IPv6 Address: Prefix Length:
 SPort: - DPort: -
 Enable:

CURRENT FILTER TABLE

Rule	Protocol	Source IPv6/Prefix	SPort	Dest IPv6/Prefix	DPort	ICMP6Type	State	Direction	Action

DEFAULT POLICY

Outgoing Default Policy: Deny Allow
 Incoming Default Policy: Deny Allow

ADD FILTER

Direction: Outgoing
 Action: Deny Allow
 Source MAC: (ex. 00E086710502)
 Destination MAC: (ex. 00E086710502)

CURRENT MAC FILTER TABLE

Select	Direction	Source MAC	Destination MAC

DoS Settings

Choose **ADVANCED > DoS Settings**. A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

DOS CONFIGURATION

Enable DoS Prevention

- Whole System Flood: SYN** Packets/Second
- Whole System Flood: FIN** Packets/Second
- Whole System Flood: UDP** Packets/Second
- Whole System Flood: ICMP** Packets/Second
- Per-Source IP Flood: SYN** Packets/Second
- Per-Source IP Flood: FIN** Packets/Second
- Per-Source IP Flood: UDP** Packets/Second
- Per-Source IP Flood: ICMP** Packets/Second
- TCP/UDP PortScan** Sensitivity
- ICMP Smurf**
- IP Land**
- IP Spoof**
- IP TearDrop**
- PingOfDeath**
- TCP Scan**
- TCP SynWithData**
- UDP Bomb**
- UDP EchoChargen**

Enable Source IP Blocking **Block time (sec)**

DNS

DNS

Domain Name System (DNS) is an Internet service that translates the domain name into IP address. Because the domain name is alphabetic, it is easier to remember. The Internet, however, is based on IP addresses. Every time you use a domain name, DNS translates 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 has 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 > DNS**. The page shown in the figure appears on the right. The DNS in this page is based on IPv4 protocol.

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

Field	Description
Attain DNS Automatically	Select it, the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it, enter the IP addresses of the primary and secondary DNS server.

DNS CONFIGURATION

This page is used to configure the DNS server ip addresses for DNS Relay.

DNS CONFIGURATION

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Apply Changes
Reset Selected

IPv6 DNS

Choose **ADVANCED > DNS > IPv6 DNS**. The DNS in this page is based on IPv6 protocol. For the parameter description in this page, please refer to **ADVANCED > DNS > DNS**.

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.

Choose **ADVANCED > Dynamic DNS**. The page is shown as the page appears on the right.

The following table describes the parameters of this page:

Field	Description
DDNS provider	Choose the DDNS provider name. You can choose DynDNS.org or TZO .
Host Name	The DDNS identifier.
Interface	The WAN interface of the router.
Enable	Enable or disable DDNS function.
Username	The name provided by DDNS provider.
Password	The password provided by DDNS provider.
Email	The email provided by DDNS provider.
Key	The key provided by DDNS provider.

DDNS CONFIGURATION

DDNS provider:

Hostname:

Interface:

Enable:

DynDns Settings:

Username:

Password:

TZO Settings:

Email:

Key:

DYNAMIC DDNS TABLE

Network Tools

Port Mapping

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

The procedure for manipulating a mapping group is as follows:

- Step 1** Select **Enable** to enable this function.
- Step 2** Select a group from the table.
- Step 3** Select interfaces from the WAN and LAN interface list and add them to the grouped interface list using the arrow buttons to manipulate the required mapping of the ports.

Click **Apply** to save the changes.

IGMP Proxy

Choose **ADVANCED > Network Tools > IGMP Proxy**, the page shown in the figure appears on the right. 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.

PORT MAPPING CONFIGURATION

Port Mapping: Disable Enable

WAN

Interface group

LAN

Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap2,pppoe1	Enabled
Group1 <input type="radio"/>	wlan-vap3,pppoe2	Enabled
Group2 <input type="radio"/>		--
Group3 <input type="radio"/>		--
Group4 <input type="radio"/>		--

IGMP PROXY CONFIGURATION

IGMP Proxy: Disable Enable

Multicast Allowed: Disable Enable

Robust Count:

Last Member Query Count:

Query Interval: (seconds)

Query Response Interval: (*100ms)

Group Leave Delay: (ms)

IP QoS

Choose **ADVANCED > Network Tools > IP QoS**. Entries in the **QoS Rule List** are used to assign the precedence for each incoming packet based on physical LAN port, TCP/UDP port number, source IP address, destination IP address and other information.

UPnP

Choose **ADVANCED > Network Tools > UPnP**. The page shown in the figure appears on the right. This page is used to configure UPnP. The system acts as a daemon after you enable it.

SNMP

Choose **ADVANCED > Network Tools > SNMP**. The page shown in the figure appears on the right. You can configure the SNMP parameters.

The following table describes the parameters of this page:

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

Community Name (Read-Write)	The network administrators must use this password to configure the information of the router.
-----------------------------	---

Software Forbidden

Choose **ADVANCED > Network Tools > Software Forbidden**. The page shown in the figure appears on the right. This interface realizes application control. Select an application from the drop-down list to prohibit the application from accessing network resources.

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

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

ART Binding

Choose **ADVANCED > Network Tools > ART Binding**. The page shown in the figure appears on the right. This page lists the permanent ARP entry table. You can bind IP with corresponding MAC to avoid ARP spoof.

Client Limit

Choose **ADVANCED > Network Tools > Client Limit**. The page shown in the figure appears on the right. This page is used to configure the capability of forcing how many devices can access to the Internet.

Routing

Static Route

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

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

CURRENT FORBIDDEN SOFTWARE LIST

Software	Select

Delete Delete All

ADD FORBIDDEN SOFTWARE

Add Forbidden Software: --

Add

ARP BINDING CONFIGURATION

IP Address: 0.0.0.0

Mac Address: 000000000000 (ex. 00E086710502)

Add Delete Selected Undo

ARP BINDING TABLE

Select	IP Address	MAC Address

CLIENT LIMIT CONFIGURATION

Client Limit Capability: Disable Enable

Apply Changes

Field	Description
Enable	Select it to use static IP routes.
Destination	Enter the IP address of the destination device.
Subnet Mask	Enter the subnet mask of the destination device.
Next Hop	Enter the IP address of the next hop in the IP route to the destination device.
Metric	The metric cost for the destination.
Interface	The interface for the specified route.
Static Route Table	A list of the previously configured static IP routes.

HOST

Enable

Destination

Subnet Mask

Next Hop

Metric

Interface

STATIC ROUTE TABLE

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf

IP ROUTE TABLE

This table shows a list of destination routes commonly accessed by your network.

CURRENT IP ROUTING TABLE

Destination	Subnet Mask	NextHop	Interface
192.168.1.1	255.255.255.255	*	e1
192.168.182.1	255.255.255.255	*	e1

CONFIGURATION

Destination

Prefix Length

Next Hop

Interface

IPv6 STATIC ROUTE TABLE

Select	Destination	NextHop	Interface

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

IPv6 Static Route

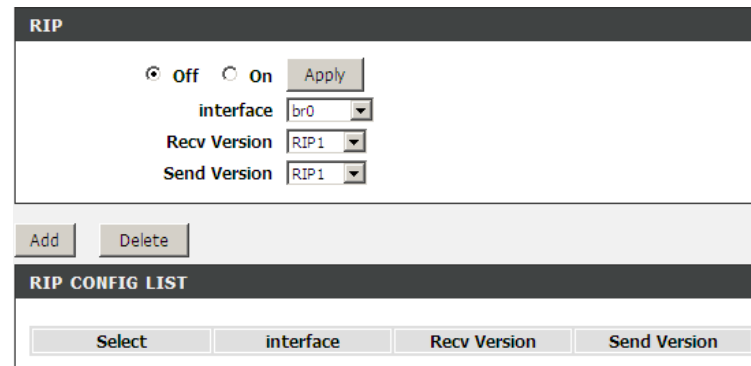
Choose **ADVANCED > Routing > IPv6 Static Route**. The page shown in the figure appears on the right. This page is used to configure the routing information. You can add or delete IP routes.

RIP

Choose **ADVANCED > Routing > RIP**. The page shown in the figure appears on the right. If you are using this device as a RIP-enabled router to communicate with others using Routing Information Protocol (RIP), enable RIP. This page is used to select the interfaces on your devices that use RIP, and the version of the protocol used.

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

Field	Description
Off/On	Select Enable , the router communicates with other RIP-enabled devices.
Interface	Choose the router interface that uses RIP.
Recv Version	Choose the interface version that receives RIP messages. You can choose RIP1 , RIP2 , or Both . <ul style="list-style-type: none"> ● Choose RIP1 indicates the router receives RIP v1 messages. ● Choose RIP2 indicates the router receives RIP v2 messages. ● Choose Both indicates the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose RIP1 or RIP2 . <ul style="list-style-type: none"> ● Choose RIP1 indicates the router broadcasts RIP1 messages only. ● Choose RIP2 indicates the router multicasts RIP2 messages only.
Add	Click it to add the RIP interface to the Rip Config List .
Delete	Select a row in the Rip Config List and click it to delete the row.



NAT

NAT ALG

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

NAT Exclude IP

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

NAT Forwarding

Choose **ADVANCED > NAT > NAT Forwarding**. The page shown in the figure appears on the right. Under 1483MER or 1483Routed mode, if NAPT (Network Address Port Translation) is enabled, the **Local IP Address** is configured as 192.168.1.3 and the **Remote IP Address** is configured as 202.32.0.2, the PC with the LAN IP192.168.1.3 will use 202.32.0.2 when it is connected to the Internet via the router without NAPT control.

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

Field	Description
Local IP Address	Input a local IP address.
Remote IP Address	Input a remote IP address
Enable	Enable the current configured rule.

RIP CONFIG LIST

IPSec Pass-Through Enable

L2TP Pass-Through Enable

PPTP Pass-Through Enable

FTP Enable

H.323 Enable

SIP Enable

RTSP Enable

ICQ Enable

MSN Enable

CONFIG

interface

IP Range -

CURRENT NAT EXCLUDE IP TABLE

WAN Interface	Low IP	High IP	Action

SETTING

Local IP Address

Remote IP Address

Enable

CURRENT NAT PORT FORWARDING TABLE

Local IP Address	Remote IP Address	State	Action

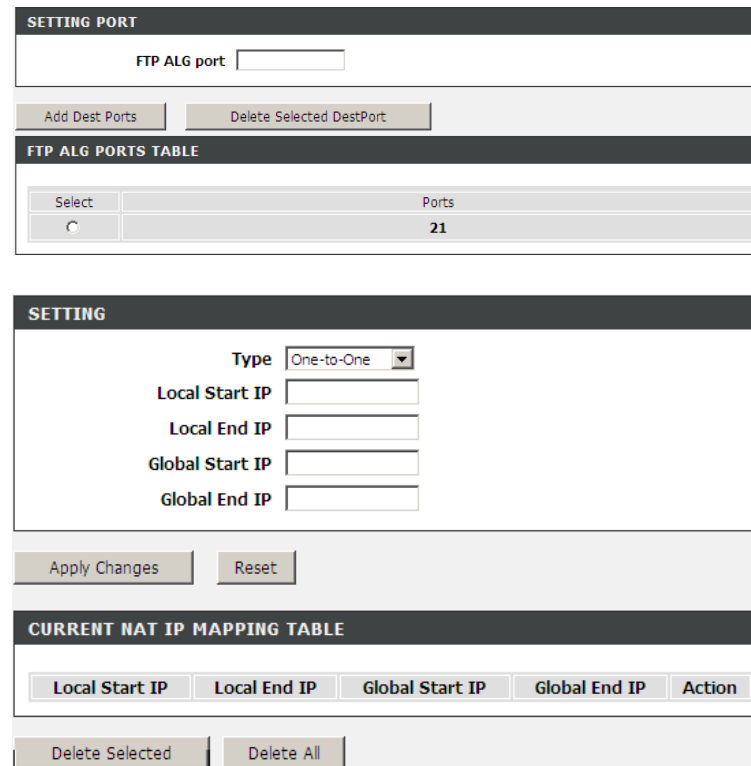
FTP ALG Configuration

Choose **ADVANCED > NAT > FTP ALG Configuration**. The page shown in the figure appears on the right. Under 1483MER or 1483Routed mode, if NAPT (Network Address Port Translation) is enabled, the **Local IP Address** is configured as 192.168.1.3 and the **Remote IP Address** is configured as 202.32.0.2, the PC with the LAN IP 192.168.1.3 will use 202.32.0.2 when it is connected to the Internet via the router without NAPT control.

NAT IP Mapping

NAT is short for Network Address Translation. The Network Address Translation Settings window allows you to share one WAN IP address for multiple computers on your LAN.

Choose **ADVANCED > NAT > NAT IP Mapping**. The page shown in the figure appears on the right. Entries in this table allow you to configure one IP pool for specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.



MAINTENANCE

System

Choose **MAINTENANCE > System**. The page shown in the figure appears on the right. In this page, you can reset your router, backup settings, and update the settings of the router.

COMMIT/REBOOT

Click the button below to reboot the router or reset it to factory default settings.

BACKUP SETTINGS

Back up DSL Router configurations. You may save your router configurations to a file on your PC.
Note: Please always save configuration file first before viewing it.

UPDATE SETTINGS

Update DSL Router settings. You may update your router settings using your saved files.

Settings File Name :

Firmware Update

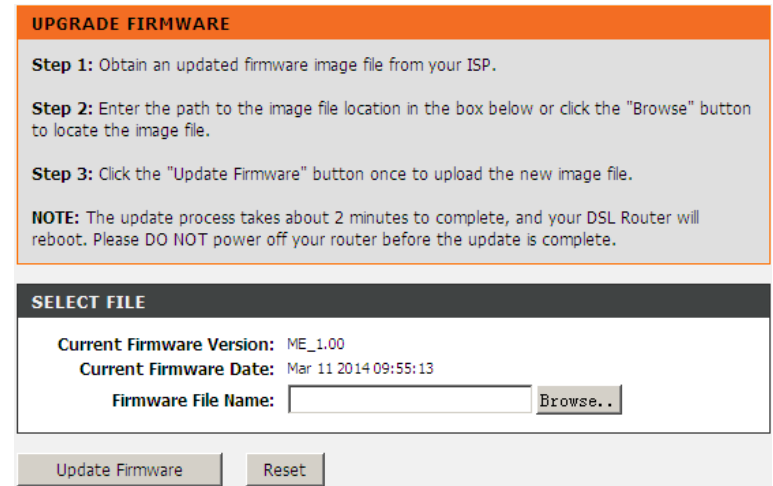
Choose **MAINTENANCE > Firmware Update**. The page shown in the figure appears on the right. In this page, you can upgrade the firmware of your router.

To update your router, do as follow:

- Step 1** Obtain an updated firmware image file from your ISP.
- Step 2** Enter the path of the image file located in the box or click the **Browse** button to locate the image file.
- Step 3** Click the **Update Firmware** button once the new image file is uploaded.

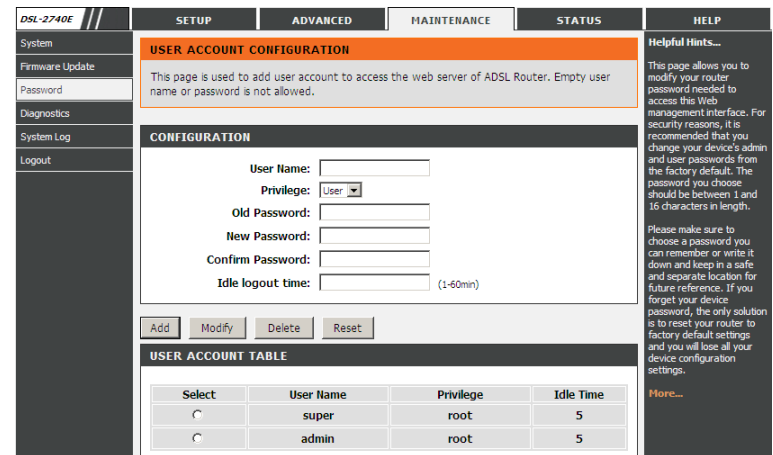
CAUTION:

The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please **DO NOT** power off your router before the update is complete.



Password

Choose **MAINTENANCE > Password**. The page shown in the figure appears on the right. In this page, you can change the username, password, and idle logout time.



Diagnostics

Choose **MAINTENANCE > Diagnostics**. The Diagnostics section is used to diagnose the basic running and connection status of the router, including the diagnostics of the **Ping, Ping6, Traceroute, ADSL, and Diag Test**.

System Log

Choose **MAINTENANCE > System Log**. The page shown in the figure appears on the right. This page is used to display the system event log table. By checking **Error** or **Notice** (or both) will set the log flag. By clicking **>>|**, it will display the newest log information below.

Logout

Choose **MAINTENANCE > Logout**. The page is shown as the figure appears on the right. In this page, you can log out of the configuration page.

Troubleshooting

This chapter provides solutions to problems that might occur during the installation and operation of the DSL-2740U. 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-2740U 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.

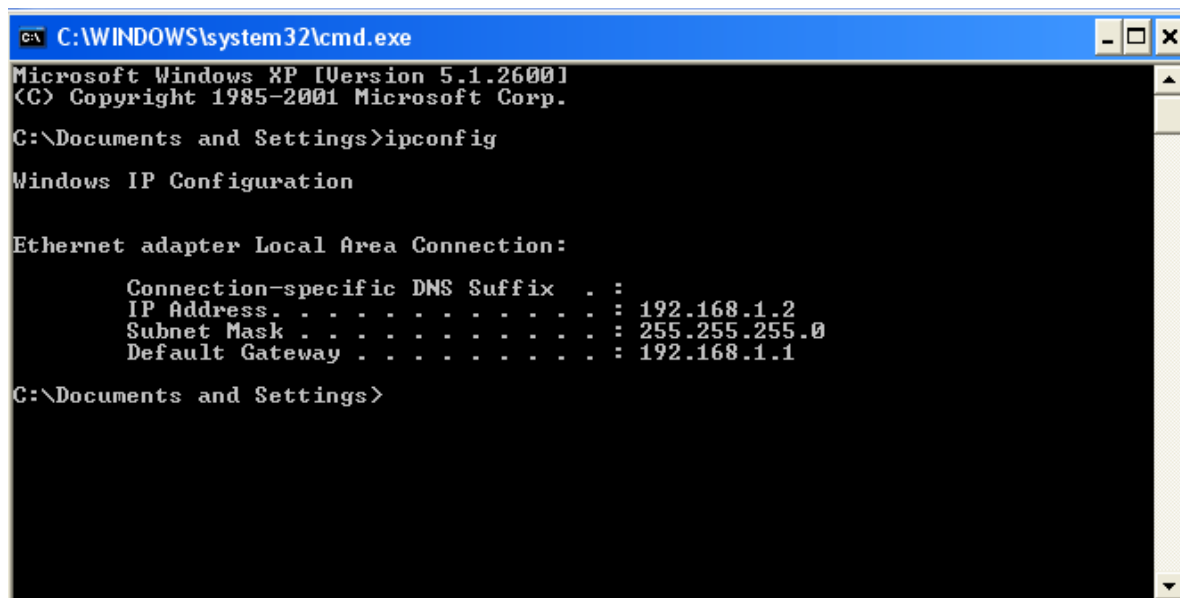
Click on **Start > Run**. In the run box type **cmd** and click on the **OK** button.

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.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . : 
    IP Address . . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Documents and 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

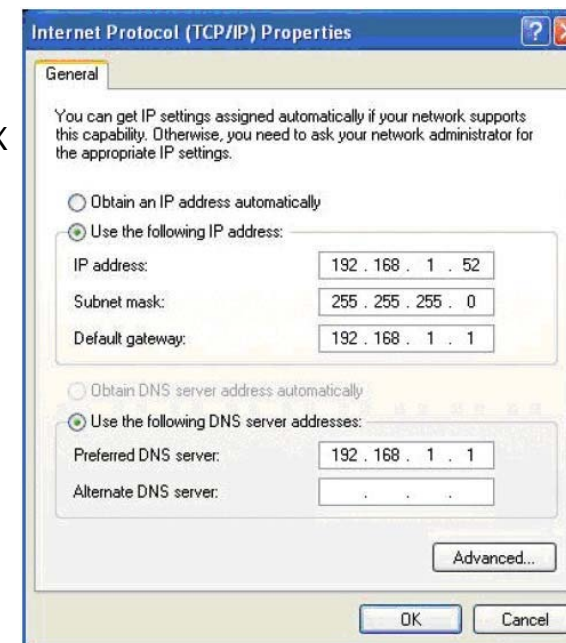
Click on the **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

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