

# **User Manual**

**DSL-G2252**

# Contents

1	Introduction.....	1
1.1	Safety Precautions .....	1
1.2	LEDs and Interfaces .....	2
1.3	System Requirements.....	5
1.4	Features .....	5
2	Hardware Installation.....	7
3	Web Configuration.....	9
3.1	Accessing the Device.....	9
3.2	Setup.....	10
3.2.1	Wizard .....	10
3.2.2	Local Network .....	16
3.2.3	Internet Setup .....	25
3.2.4	Wireless Setup.....	33
3.2.5	Time and Date.....	39
3.3	Advanced.....	41
3.3.1	Advanced Wireless.....	41
3.3.2	Access Control List.....	47
3.3.3	Port Triggering.....	51
3.3.4	Port Forwarding.....	53
3.3.5	DMZ.....	54
3.3.6	Parental Control .....	55
3.3.7	Filtering Options .....	59
3.3.8	DoS Settings.....	63
3.3.9	DNS .....	64
3.3.10	Dynamic DNS .....	66
3.3.11	Network Tools.....	68
3.3.12	Routing.....	81
3.3.13	NAT.....	85
3.4	Maintenance .....	94
3.4.1	System .....	94
3.4.2	Firmware Update.....	95
3.4.3	Password.....	96
3.4.4	Diagnostics.....	98
3.4.5	System Log.....	101

3.4.6	Logout.....	103
3.5	Status.....	103
3.5.1	Device Info.....	103
3.5.2	Wireless Clients .....	106
3.5.3	DHCP Clients.....	106
3.5.4	ADSL Driver.....	106
3.5.5	Statistics.....	107
3.5.6	Route Information.....	108
3.6	Help.....	109

## 1 Introduction

The DSL-G2252 supports multiple line modes. With one 10/100 base-T Ethernet interfaces at the user end, the device provides high-speed ADSL/VDSL broadband connection to the Internet or Intranet for high-end users like net bars and office users. It also provides EWAN and VOIP. It provides high performance access to the Internet with a downstream rate of 24 Mbps and an upstream rate of 1 Mbps. It supports IPv6.

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

### 1.1 Safety Precautions

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

- Use the type of power marked in the volume label.
- Use the power adapter in the product package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines or plugs may cause electric shock or fire accidents. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a heat source or under a high temperature occurs. Keep the device away from direct sunshine.
- Do not put this device close to an overdamp or watery place. Do not spill fluid on this device.
- Do not connect this device to a PC or electronic product unless instructed by our customer engineer or your broadband provider. Wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

## 1.2 LEDs and Interfaces

### Note:

The figures in this document are for reference only.

### Front Panel

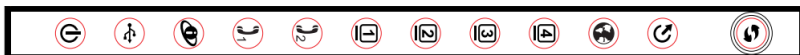










Figure 1 Front panel

The following table describes the LEDs of the device.

LED	Color	Status	Description
 Power	Green	On	The initialization of the system is complete.
	Red	On	The device is powered on.
		Blinking	The firmware is upgrading.
 LAN 1/2/3/4	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.
 USB	Green	Off	The USB interface is not properly connected.
		Blinking	The USB interface is properly connected and data is being transmitted.
		On	The USB interface is properly connected, but no data is being transmitted.

LED	Color	Status	Description
 WLAN	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.
 EWAN	Green	Off	The ethernet wan interface is not connect.
		On	The ethernet wan interface is connected.
 DSL	Green	Off	No signal is being detected.
		Blinking	The device is handshaking with the physical layer of the office end.
		On	A connection is set up with the physical layer of the office end.
 Internet	Green	Off	The device is under the Bridge mode or powered off.
		On	A connection is set up and no traffic is detected.
	Red	On	The authentication of the PPP dial-up is failed or MER is failed to obtain the correct IP address.
 Phone	Green	Off	The Internet phone is not registered.
		Blinking	The Internet phone is using.
		On	The Internet phone registered successful.

## Rear Panel

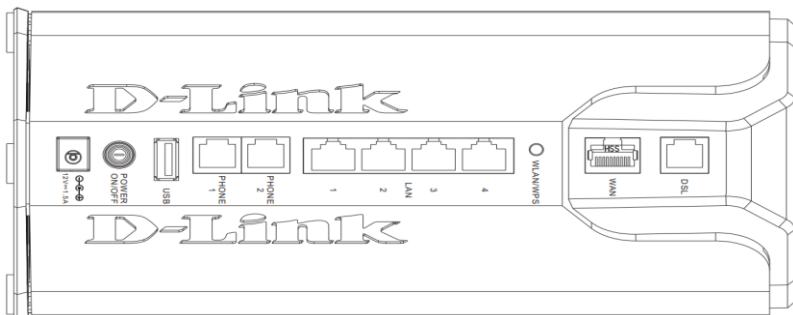


Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
DSL	RJ-11 interface for connecting the host to the telephone jack on the wall or the <b>MODEM</b> interface of the splitter through a telephone line.
EWAN	RJ-45 interface for connecting to internet through a cable line.
WLAN/WPS	Press and hold the button for 3 seconds start WPS negotiation.
LAN4/3/2/1	For a PC or other Ethernet-abled device to join the LAN of G2252 by being connected to this interface with RJ-45 cable.
PHONE2/1	RJ-11 interface for connecting to phone.
USB	USB host connect.
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 beside)	Press and hold the button for 4 seconds to restore the factory defaults.

## 1.3 System Requirements

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

## 1.4 Features

- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- Leased line mode
- 1483B, 1483R, and MER access
- Multiple PVCs (eight at most) and these PVCs can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- 802.1Q and 802.1P protocol
- DHCP server
- NAT and NAPT
- Static route
- Firmware upgrade: Web, TFTP, FTP
- Reset to the factory defaults
- DHCP relay
- Virtual server
- DMZ
- Two-level passwords and user names
- Web user interface
- Telnet CLI
- System status display
- IP filter
- IP QoS



- Remote access control
- Line connection status test
- Remote management (telnet and HTTP)
- Backup and restoration of configuration file
- Ethernet interface supports crossover detection, auto-correction and polarity correction
- UPnP
- IPV6
- DDNS
- USB Printer
- URL Block
- SNMP
- TR069
- ARP Binding
- VDSL
- VOIP
- Ethernet WAN

## 2 Hardware Installation

### 2.1 Choosing the 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.

### 2.2 Connecting the Router

A setup wizard utility is provided on the router webpage to assist with easy configuration. In the event of a problem arising the help screens will suggest the appropriate course of action to resolve the issue.

- (1) If you have a **Fibre-to-the-Home** service, connect the **yellow** Ethernet cable to the **blue** WAN port on the back of the router. Connect the other end of the yellow cable to the LAN port of the fibre device (ONT) otherwise, Skip to Step 4.
- (2) If you have a **DSL** service, connect the splitter/filter to the port marked "OUT" on the power supply. Connect the grey telephone cable to the port marked "IN" on the power supply. Connect the other end of the cable to the telephone wall socket.
- (3) Connect the red telephone cable to the red DSL port at the back of the router and the other end into the red port of the splitter/filter. You can connect a telephone to the green phone port of the splitter/filter.



## 3 Web Configuration

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

---

**Note:**

This user manual is applied for DSL-G2252.

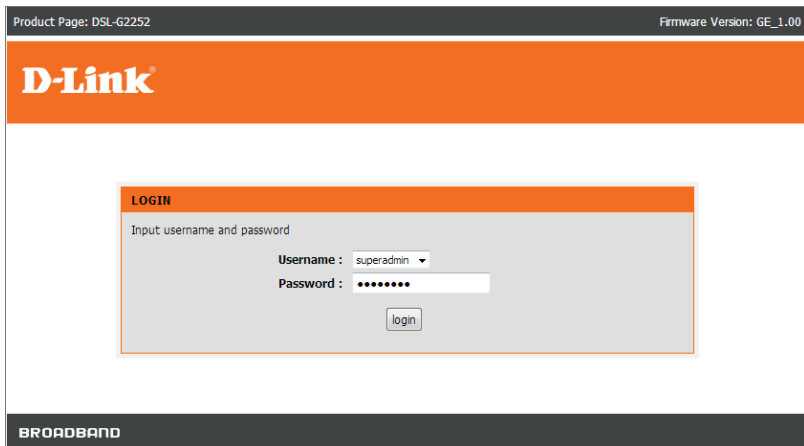
---

### 3.1 Accessing the Device

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

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

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



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

Product Page: DSL-G2252		Firmware Version: GE_1.00			
D-Link®					
DSL-G2252	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
Wizard	<b>SETTING UP YOUR INTERNET</b> There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection. Please make sure you have your ISP's connection settings first if you choose manual setup.				<b>Helpful Hints...</b> First time users are recommended to run the <b>Setup Wizard</b> . Click the <b>Setup Wizard</b> button and you will be guided step by step through the process of setting up your ADSL connection. If you consider yourself an advanced user or have configured a router before, click <b>Setup-&gt;Internet Setup</b> to input all the settings manually. <a href="#">More...</a>
Local Network	<b>INTERNET CONNECTION WIZARD</b> You can use this wizard for assistance and quick connection of your new D-Link Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin. <div style="text-align: center;"> <input type="button" value="Setup Wizard"/> </div> <p><b>Note:</b> Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.</p>				
Internet Setup					
Wireless Setup					
Time and Date					
<b>BROADBAND</b>					

Figure 4 Device information - 1

## 3.2 Setup

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

### 3.2.1 Wizard

**Wizard** enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe configuration parameters. When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet.

Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you that you are connected to the Internet using a static or dynamic IP address, and the protocol you use to communicate over the Internet, such as PPPoA or PPPoE.

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

The screenshot shows the DSL-G2252 web interface. On the left is a navigation menu with options: Wizard, Local Network, Internet Setup, Wireless Setup, and Time and Date. The main content area has tabs for SETUP, ADVANCED, MAINTENANCE, STATUS, and HELP. The SETUP tab is active, showing a section titled "SETTING UP YOUR INTERNET" with instructions on how to set up the Internet connection. Below this is the "INTERNET CONNECTION WIZARD" section, which includes a "Setup Wizard" button and a note about following the Quick Installation Guide. On the right side, there is a "Helpful Hints..." section with additional advice for users.

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

The screenshot shows the "WELCOME TO D-LINK SETUP WIZARD" page. It features a title bar and a main content area. The content area includes a welcome message, a list of six steps for the configuration process, and two buttons: "Next" and "Cancel".

**WELCOME TO D-LINK SETUP WIZARD**

This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

- **Step 1:** Interface Type
- **Step 2:** Change Device Login Password
- **Step 3:** Set Time and Date
- **Step 4:** Setup Internet Connection
- **Step 5:** Configure Wireless Network
- **Step 6:** Completed and Apply

Next Cancel

There are 6 steps to configure the device. Click **Next** to continue.

**Step 1** Select WAN Interface type.

The screenshot shows the "STEP 1: SELECT WAN INTERFACE TYPE" page. It features a title bar with step indicators (1, 2, 3, 4, 5, 6) and a main content area. The content area includes a prompt to select a WAN interface, radio button options for ADSL/VDSL WAN and Ethernet WAN, a note about router restarts, and "Next" and "Cancel" buttons.

**STEP 1: SELECT WAN INTERFACE TYPE** > 2 > 3 > 4 > 5 > 6

Please select which WAN interface to use: ADSL\_VDSL or Ethernet WAN.

**Select Interface Type:**  ADSL\_VDSL WAN  Ethernet WAN

Note: The router will restart if you change from ADSL\_VDSL to ETH or ETH to ADSL\_VDSL. Once done restarting, you can just continue where you left of.

Next Cancel

**Step 2** Change the device login password.

1 > 2 > **STEP 2: CHANGE DEVICE LOGIN PASSWORD** > 3 > 4 > 5 > 6

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.

Current Password :   
 New Password :   
 Confirm Password :

**Step 3** Set the time and date.1 > 2 > **STEP 3: SET TIME AND DATE** > 4 > 5 > 6

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

**SYSTEM TIME**

System time: Mon Jan 2 22:33:3 2012  
 Time Zone: (GMT+03:00) Iraq, Jordan, Kuwait  
 DayLight: LocalTIME  
 Mode: Copy Computer time

**Step 4** Setup the Internet connection.1 > 2 > 3 > **STEP 4: SETUP INTERNET CONNECTION** > 5 > 6

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".

Channel Type : ATM  
 Country : (Click to Select)  
 Internet Service Provider : (Click to Select)  
 Protocol : (Click to Select)  
 Connection Type : (Click to Select)  
 VPI : (Enter a number) (0-255)  
 VCI : (Enter a number) (32-65535)

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

1 > 2 > 3 > **STEP 4: SETUP INTERNET CONNECTION** > 5 > 6

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".

Channel Type : ATM ▾  
Country : Others ▾  
Internet Service Provider : Others ▾  
Protocol : PPPoE ▾  
Connection Type : LLC ▾

VPI : 0 (0-255)  
VCI : (Enter a number) (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 :

Back Next Cancel

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

1 > 2 > 3 > **STEP 4: SETUP INTERNET CONNECTION** > 5 > 6

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".

Channel Type : ATM ▾  
Country : Others ▾  
Internet Service Provider : Others ▾  
Protocol : Dynamic IP ▾  
Connection Type : LLC ▾

VPI : 0 (0-255)  
VCI : (Enter a number) (32-65535)

---

Back Next Cancel



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

1 · 2 · 3 · **STEP 4: SETUP INTERNET CONNECTION** · 5 · 6

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".

Channel Type : ATM ▾  
Country : Others ▾  
Internet Service Provider : Others ▾  
Protocol : Static IP ▾  
Connection Type : LLC ▾  
VPI : 0 (0-255)  
VCI : (Enter a number) (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 : 0.0.0.0  
Subnet Mask : 0.0.0.0  
Default Gateway :  
Primary DNS Server :

Back Next Cancel

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

1 · 2 · 3 · **STEP 4: SETUP INTERNET CONNECTION** · 5 · 6

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".

Channel Type : ATM ▾  
Country : Others ▾  
Internet Service Provider : Others ▾  
Protocol : Bridge ▾  
Connection Type : LLC ▾  
VPI : 0 (0-255)  
VCI : (Enter a number) (32-65535)

---

Back Next Cancel

**Step 5** Configure the wireless network.

1 > 2 > 3 > 4 > **STEP 5: CONFIGURE WIRELESS NETWORK** > 6

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 6** Complete and apply the settings. Click **Apply** to save the settings.

**1 > 2 > 3 > 4 > 5 > STEP 6: 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.

<b>Modem Password :</b>	admin
<b>Time Settings :</b>	Copy from Computer
<b>VPI / VCI :</b>	0/32
<b>Protocol :</b>	Bridge
<b>Connection Type :</b>	LLC
<b>Wireless Network :</b>	Enabled
<b>Wireless Network Name (SSID) :</b>	RTL867x-ADSL
<b>Visibility Status :</b>	Visible
<b>Encryption :</b>	WPA2-PSK/AES (also known as WPA2 Personal)
<b>Pre-Shared Key :</b>	%Fortress123&

**Note:**

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

## 3.2.2 Local Network

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

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

### 3.2.2.1 LAN Interface

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

**LAN SETTING**

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP address, subnet mask, etc..

---

**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

The following table describes the parameters in this page.

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

### 3.2.2.2 LAN IPv6 Interface

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

**LAN IPV6 SETTING**

This page is used to configure ipv6 lan setting. User can set lan RA server work mode and lan DHCPv6 server work mode.

**LAN GLOBAL ADDRESS SETTING**

Global Address:  /

Apply Changes

**RA SETTING**

Enable:

M Flag:

O Flag:

Max Interval:  Secs

Min Interval:  Secs

Prefix Mode:  ▼

ULA Enable:

RA DNS Enable:

Apply Changes

**DHCPV6 SETTING**

DHCPv6 Mode:  ▼

IPv6 Address Suffix Pool:  -   
(ex. :1:1:1:1 or :1)

IPv6 DNS Mode:  ▼

Apply Changes

The following table describes the parameters of this page.

Field	Description
Global Address	Specify the LAN global ipv6 address. It can be

Field	Description
	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.

### 3.2.2.3 DHCP Server

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

**DHCP SERVER SETTING**

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.  
 (1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.  
 (2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.  
 (3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

**DHCP SERVER SETTINGS**

**LAN IP:** 192.168.1.1/255.255.255.0

**DHCP Mode:** DHCP Server ▾

**Interface:**  LAN1  LAN2  LAN3  LAN4  WLAN   
 VAP0  VAP1  VAP2  VAP3

**IP Pool Range:** 192.168.1.5 - 192.168.1.254

**Max Lease Time:** 1440 minutes

**Domain Name:**

**DNS Servers:** 192.168.1.1

The following table describes the parameters of this page.

Field	Description
DHCP Mode	If set to <b>DHCP Server</b> , the router can assign IP addresses, IP default gateway and DNS servers to the host in Windows95, Windows NT and other operation systems that support the DHCP client.
IP Pool Range	It specifies the first and last IP addresses in the IP address pool. The router assigns IP address in the IP pool range to the host.
Max Lease Time	The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.



Field	Description
Domain Name	Enter the domain name if you know. If you leave this blank, the domain name obtained by DHCP from the ISP is used. You must enter host name (system name) on each individual PC. The domain name can be assigned from the router through the DHCP server.
DNS Servers	You can configure the DNS server IP addresses for DNS Relay.

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

**ACTIVE DHCP CLIENT TABLE**

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

**ACTIVE DHCP CLIENT TABLE**

Name	IP Address	MAC Address	Expiry	Type

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

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

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

### DEVICE IP RANGE SET

This page is used to configure the IP address range based on device type.

#### DEVICE IP RANGE SETUP

device name:

start address:

end address:

option60:

#### IP RANGE TABLE:

Select	device name	start address	end address	default gateway	option60
--------	-------------	---------------	-------------	-----------------	----------

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

### DHCP SERVER SETTING

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.

(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.

(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

#### DHCP SERVER SETTINGS

LAN IP: 192.168.1.1/255.255.255.0

DHCP Mode:

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

**DHCP SERVER SETTING**

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.

(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your hosts on the LAN. You can set the DHCP server ip address.

(3)If you choose "None", then the modem will do nothing when the hosts request a IP address.

**DHCP SERVER SETTINGS**

**LAN IP:** 192.168.1.1/255.255.255.0

**DHCP Mode:**  ▼

**Relay Server:**

Set VendorClass IP Range

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

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

### 3.2.2.4 DHCP Reserved

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

**DHCP STATIC IP CONFIGURATION**

This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.

**DHCP STATIC IP CONFIGURATION**

IP Address:

Mac Address:  (ex. 00E086710502)




**DHCP STATIC IP TABLE**




The following table describes the parameters of this page.

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

### 3.2.3 Internet Setup

#### 3.2.3.1 Channel Configuration

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

## CHANNEL CONFIGURATION

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router. Note: When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

## WAN PHYSICAL TYPE

WAN Physical Type:  DSL WAN  Ethernet WAN

## DEFAULT ROUTE SELECTION

Default Route Selection:  Auto  Specified

## CHANNEL CONFIGURATION

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

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

WAN IP Settings: Type:  Fixed IP/IP Unnumbered  DHCP   
 Local IP Address:  Remote IP Address:    
 Netmask:    
 Default Route:  Disable  Enable  Auto   
 Unnumbered


## CURRENT WAN TABLE:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IGMP	DRoute	IPAddr	Remote IP	NetMask	User Name	Status	Edit
<input type="radio"/>	pppoe1	PPPoE	0	35	LLC	On	Off	On	0.0.0.0	0.0.0.0	255.255.255.255		Down	

The following table describes the parameters of this page.

Field	Description
WAN Physical Type	<ul style="list-style-type: none"> <li>● ADSL WAN: ADSL uplink via telephone cable.</li> <li>● Ethernet WAN: Ethernet uplink via Ethernet cable.</li> </ul>
Channel Type	You can select <b>ATM</b> or <b>PTM</b> .
Default Route Selection	You can select <b>Auto</b> or <b>Specified</b> .
VPI	The virtual path between two points in an ATM network, ranging from <b>0</b> to <b>255</b> .
VCI	The virtual channel between two points in an ATM network, ranging from <b>32</b> to <b>65535</b> ( <b>1</b> to <b>31</b> are reserved for known protocols)
Encapsulation	You can choose <b>LLC</b> and <b>VC-Mux</b> .
Channel Mode	You can choose <b>1483 Bridged</b> , <b>1483 MER</b> , <b>PPPoE</b> , <b>PPPoA</b> , <b>1483 Routed</b> or <b>IPoA</b> .
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is enabled.
Enable IGMP	You can enable or disable Internet Group Management Protocol (IGMP) function.
802.1q	You can select <b>Disable</b> or <b>Enable</b> . If enabled, you need to enter the VLAN ID.
VLAN ID	The value ranges from <b>1</b> to <b>4095</b> .
IP Protocol	When any channel mode except 1483 Bridged is selected, select an IP protocol from <b>IPv4/IPv6</b> , <b>IPv4</b> and <b>IPv6</b> .
<b>PPP Settings</b>	
User Name	Enter the correct user name for PPP dial-up, which is provided by your ISP.
Password	Enter the correct password for PPP dial-up, which is provided by your ISP.
Type	You can choose <b>Continuous</b> , <b>Connect on</b>

Field	Description
	<b>Demand</b> or <b>Manual</b> .
Idle Time (min)	If the type is set to <b>Connect on Demand</b> , 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.
<b>WAN IP Settings</b>	
Type	You can choose <b>Fixed IP</b> or <b>DHCP</b> . <ul style="list-style-type: none"> <li>● If select <b>Fixed IP</b>, you should enter the local IP address, remote IP address and subnet mask.</li> <li>● If select <b>DHCP</b>, the router is a DHCP client, the WAN IP address is assigned by the remote DHCP server.</li> </ul>
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Remote IP Address	Enter the IP address of gateway provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Default Route	Routing table entry is not clearly specified in the routing, as to any network prefix forwarding address.
Unnumbered	Select this checkbox to enable IP unnumbered function.

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

**PPP INTERFACE - MODIFY**

This page is used for advanced PPP interface configuration.

**PPP INTERFACE**

**Protocol:** PPPoE

**ATM VCC:** 0/35

**Login Name:**

**Password:**

**Authentication Method:** AUTO

**Connection Type:** Continuous

**Idle Time (s):** 0

**Bridge:**  Bridged Ethernet (Transparent Bridging)  
 Bridged PPPoE (Implies Bridged Ethernet)  
 Disable Bridge

**AC-Name:**

**Service-Name:**

**MTU (1-1500):** 1492

**Static IP:**

**Source Mac address:** 00:05:1D:03:04:06 (ex:00:E0:86:71:05:02)

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 <b>AUTO</b> , <b>CHAP</b> , or <b>PAP</b> .
Connection Type	You can choose <b>Continuous</b> , <b>Connect on Demand</b> , or <b>Manual</b> .
Idle Time (s)	If choose <b>Connect on Demand</b> , 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



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

### 3.2.3.2 ATM Settings

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

**ATM SETTINGS**

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for VPI, VCI, QoS etc ...

**ATM SETTING**

VPI:  VCI:  QoS:

PCR:  CDVT:  SCR:  MBS:

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input checked="" type="radio"/>	0	35	UBR	6144	0	---	---

The following table describes the parameters of this page.

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

### 3.2.3.3 ADSL Settings

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

**ADSL SETTINGS**  
Adsl Settings.

**ADSL SETTINGS**  
**ADSL modulation:**  
 G.Lite  
 G.Dmt  
 T1.413  
 ADSL2  
 ADSL2+  
 VDSL2  
**AnnexL Option:**  
 Enabled  
**AnnexM Option:**  
 Enabled  
**VDSL2 Profile:**  
 8A  
 8B  
 8C  
 8D  
 12A  
 12B  
 17A  
 30A  
**ADSL Capability:**  
 Bitswap Enable  
 SRA Enable

Apply Changes

### 3.2.3.4 PVC Auto Search

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

**AUTO PVC CONFIGURATION**

This page is used to configure pvc auto detect function. Here you can add/delete auto pvc search table.

**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

## 3.2.4 Wireless Setup

### 3.2.4.1 Wireless Basics

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

**WIRELESS BASIC SETTINGS**

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

**WIRELESS NETWORK SETTINGS**

**Disable Wireless LAN Interface**

**Band:** 2.4 GHz (B+G+N) ▾

**Mode:** AP ▾

**SSID:** RTL867x-ADSL

**Channel Number:** Auto ▾ **Current Channel:** 8

**Radio Power (Percent):** 100% ▾

**Associated Clients:**

**WIRELESS OPTIONS**

**Channel Width:** 20/40MHZ ▾

**Control Sideband:** Upper ▾

The following table describes the parameters in this page.

Field	Description
Band	<p>Choose the working mode of the modem. You can choose from the drop-down list.</p> <div style="border: 1px solid black; padding: 2px;"> <p>2.4 GHz (B+G+N) ▾</p> <p>2.4 GHz (B)</p> <p>2.4 GHz (G)</p> <p>2.4 GHz (B+G)</p> <p>2.4 GHz (N)</p> <p>2.4 GHz (G+N)</p> <p>2.4 GHz (B+G+N)</p> </div>
Mode	<p>Choose the network model of the modem, which is varied according to the software. By default, the network model of the modem is <b>AP</b>.</p>
SSID	<p>The service set identification (SSID) is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the modem must have the same SSID. Enter a descriptive name that is used when the wireless client connecting to the modem.</p>

Field	Description
Channel Number	Choose a channel from the drop-down list box. A channel is the radio frequency used by 802.11b/g wireless devices. There are 13 channels (from 1 to 13) available depending on the geographical area. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. Interference and degrading performance occurs when radio signal from different APs overlap.
Radio Power (Percent)	You can choose the transmission power of the radio signal. The default one is <b>100%</b> . It is recommended to choose the default value <b>100%</b> .
Show Active Clients	Click it to view the information of the wireless clients connected to the modem.
Channel Width	Select the appropriate band of <b>20MHZ</b> , <b>20/40MHZ</b> , or <b>40MHZ</b> according to your subscribed broadband service.
Control Sideband	Choose the channel selection mode as <b>Upper</b> or <b>Lower</b> .

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

**ACTIVE WIRELESS CLIENT TABLE**

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client

**ACTIVE WIRELESS CLIENT TABLE**

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---

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

### 3.2.4.2 Wireless Security

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

**WIRELESS SECURITY SETTINGS**

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

**WIRELESS SECURITY SETTINGS**

**SSID TYPE:**  Root  VAP0  VAP1  VAP2  VAP3  
**Encryption:** WPA2 Mixed ▾  
 **Use 802.1x Authentication**  WEP 64bits  WEP 128bits  
**WPA Authentication Mode:**  Enterprise (RADIUS)  Personal (Pre-Shared Key)  
**Pre-Shared Key Format:** Passphrase ▾  
**Pre-Shared Key:**   
**Authentication RADIUS Server:** Port  IP address  Password

Note: When encryption WEP is selected, you must set WEP key value.

The following table describes the parameters of this page:

Field	Description
Encryption	Configure the wireless encryption mode. You can choose <b>None</b> , <b>WEP</b> , <b>WPA (TKIP)</b> , <b>WPA (AES)</b> , <b>WPA2 (AES)</b> , <b>WPA2 (TKIP)</b> or <b>WPA2 Mixed</b> . <ul style="list-style-type: none"> <li>● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network.</li> <li>● Wi-Fi protected access (WPA) is a subset of the IEEE802.11i security specification draft.</li> <li>● WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem</li> </ul>

Field	Description
	through WPA or WPA2. Key differences between WPA and WEP are in user authentication and improved data encryption.
Set WEP Key	It is available when you set the encryption mode to <b>WEP</b> . Click it, the <b>Wireless WEP Key Setup</b> page appears.
WPA Authentication Mode	<ul style="list-style-type: none"><li>● Select <b>Personal (Pre-Shared Key)</b>, enter the pre-shared key in the <b>Pre-Shared Key</b> field.</li><li>● Select <b>Enterprise (RADIUS)</b>, enter the port, IP address, and password of the Radius server.</li></ul> You need to enter the username and password provided by the Radius server when the wireless client connects the modem. If the encryption is set to <b>WEP</b> , the modem uses 802.1 X authentication, which is Radius authentication.

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



## WIRELESS SECURITY SETTINGS

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

## WIRELESS SECURITY SETTINGS

**SSID TYPE:**  Root  VAP0  VAP1  VAP2  VAP3  
**Encryption:** WEP  
**Key Length:** 64-bit  
**Key Format:** ASCII (5 characters)  
**Default Tx Key:** Key 1  
**Encryption Key 1:** \*\*\*\*\*  
**Encryption Key 2:** \*\*\*\*\*  
**Encryption Key 3:** \*\*\*\*\*  
**Encryption Key 4:** \*\*\*\*\*  
 **Use 802.1x Authentication**  WEP 64bits  WEP 128bits  
**WPA Authentication Mode:**  Enterprise (RADIUS)  Personal (Pre-Shared Key)  
**Pre-Shared Key Format:** Passphrase  
**Pre-Shared Key:** \_\_\_\_\_  
**Authentication RADIUS Server:** Port  IP address  Password \_\_\_\_\_

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

The following describes the parameters of this page:

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

Field	Description
	<ul style="list-style-type: none"><li>● If you choose <b>64-bit</b> and <b>ASCII (5 characters)</b>, enter any 5 ASCII characters.</li><li>● If you choose <b>64-bit</b> and <b>Hex (10 characters)</b>, enter any 10 hexadecimal characters.</li><li>● If you choose <b>128-bit</b> and <b>ASCII (13 characters)</b>, enter any 13 ASCII characters.</li><li>● If you choose <b>128-bit</b> and <b>Hex (26 characters)</b>, enter any 26 hexadecimal characters.</li></ul>
Apply Changes	Click it to apply the settings temporarily. If you want to save the settings of this page permanently, click <b>Save</b> in the lower left corner.

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

### 3.2.5 Time and Date

Choose **Setup > Time and Date**. The **System Time Configuration** page appears. In the page, you can configure, update and maintain the correct time on the internal system clock. You can set the time zone that you are in and the Network Time Protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

**SYSTEM TIME CONFIGURATION**

This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

**SYSTEM TIME**

**System Time:** 2012 Year: Jan Month: 3 Day: 2 Hour: 47 min 57 sec

**Time Zone:** (GMT+03:00) Iraq, Jordan, Kuwait

**DayLight:** LocalTIME

**Mode:** Set Time Manually

**START NTP:**

**NTP Start:**

The following table describes the parameters in this page.

Field	Description
System Time	Displays the time currently maintained by the router. If this is incorrect, use the following options to configure the time correctly.
Time Zone	Select your local time zone from the dropdown list.
Daylight	Adjust the clock for daylight savings time.
Mode	To synchronize the time automatically with the Internet or your own computer, you may select <b>Set Time Manually</b> , <b>Copy Computer Time</b> or <b>Set NTP Server Manually</b> .
Get GMT Time	Synchronize to Greenwich Mean Time.

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

**NTP CONFIGURATION:**

State:  Disable  Enable

Server: ntp1.dlink.com

Server2: None

Interval: Every 1 hours

GMT time: Mon Jan 2 23:47:57 2012

The following table describes the parameters in this page.

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

### 3.3 Advanced

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

#### 3.3.1 Advanced Wireless

This function is suggested not to change the defaults, as incorrect settings may reduce the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

##### 3.3.1.1 Advanced Settings

Choose **Advanced > Advanced Wireless > Wireless Advanced**. The page shown in the following figure appears. These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Do not change these settings unless you know the effect of changes on the device.

**WIRELESS ADVANCED SETTINGS**

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

**ADVANCED WIRELESS SETTINGS**

**Authentication Type:**  Open System  Shared Key  Auto

**Fragment Threshold:**  (256-2346)

**RTS Threshold:**  (0-2347)

**Beacon Interval:**  (20-1024 ms)

**DTIM Interval:**  (1-255)

**Data Rate:**

**Preamble Type:**  Long Preamble  Short Preamble

**Broadcast SSID:**  Enabled  Disabled

**Relay Blocking:**  Enabled  Disabled

**Ethernet to Wireless Blocking:**  Enabled  Disabled

**Wifi Multicast to Unicast:**  Enabled  Disabled

**Aggregation:**  Enabled  Disabled

**Short GI:**  Enabled  Disabled

The following table describes the parameters in this page.

Field	Description
Fragment Threshold	Used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.
RTS Threshold (Request to Send Threshold)	Determines the packet size of a transmission through the use of the router to help control traffic flow.
Beacon Interval	A packet of information that is sent from a connected

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

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

### 3.3.1.2 Access Control

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

**WIRELESS ACCESS CONTROL**

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.

**WIRELESS ACCESS CONTROL MODE**

Wireless Access Control Mode:

**WIRELESS ACCESS CONTROL SETTINGS**

MAC Address:  (ex. 00E086710502)

**CURRENT ACCESS CONTROL LIST**

MAC Address	Select

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

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

### 3.3.1.3 WPS

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

**WI-FI PROTECTED SETUP**

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

**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	AES	%Fortress123&

**CLIENT PIN INFO**

**Client PIN Number:**

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

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

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

**Note:**

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



### 3.3.1.4 MBSSID

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

**WIRELESS MULTIPLE BSSID SETUP**  
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 effect.

**WIRELESS MULTIPLE BSSID SETTINGS- VAP0**  
 **Enable VAP0**  
SSID:   
Broadcast SSID:  Enable  Disable  
Relay Blocking:  Enable  Disable  
Authentication Type:  Open System  Shared Key  Auto

**WIRELESS MULTIPLE BSSID SETTINGS- VAP1**  
 **Enable VAP1**  
SSID:   
Broadcast SSID:  Enable  Disable  
Relay Blocking:  Enable  Disable  
Authentication Type:  Open System  Shared Key  Auto

**WIRELESS MULTIPLE BSSID SETTINGS- VAP2**  
 **Enable VAP2**  
SSID:   
Broadcast SSID:  Enable  Disable  
Relay Blocking:  Enable  Disable  
Authentication Type:  Open System  Shared Key  Auto

**WIRELESS MULTIPLE BSSID SETTINGS- VAP3**  
 **Enable VAP3**  
SSID:   
Broadcast SSID:  Enable  Disable  
Relay Blocking:  Enable  Disable  
Authentication Type:  Open System  Shared Key  Auto

The device supports four virtual access points (VAPs). It is a unique name to identify the modem in the wireless LAN. Wireless stations associating to the

modem must have the same name. Enter a descriptive name that is used when the wireless client is connecting to the modem.

### 3.3.2 Access Control List

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

#### 3.3.2.1 Access Control List

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



**Note:**

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

**ACL CONFIGURATION**

You can specify what services are accessible form 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

**ACL CONFIGURATION -- DIRECTION**

**Direction Select:**  LAN  WAN

**LAN ACL SWITCH CONFIGURATION**

**LAN ACL Switch:**  Enable  Disable

**ACL SETTINGS**

**IP Address:**  -  (The IP 0.0.0.0 represent any IP )

**Services Allowed:**  
 Any

**CURRENT ACL TABLE**

Select	Direction	IP Address/Interface	Service	Port	Action
0	WAN	0.0.0.0	ping	--	<input type="button" value="Delete"/>

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

Field	Description
Direction Select	Select the router interface. You can select <b>LAN</b> or <b>WAN</b> . In this example, <b>LAN</b> 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: <b>Web, Telnet, SSH, FTP, TFTP, SNMP</b> and <b>PING</b> . You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the <b>Current ACL Table</b> .
Reset	Click it to refresh this page.

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

## ACL CONFIGURATION -- DIRECTION

Direction Select:  LAN  WAN

## ACL SETTINGS

WAN Setting: WAN Interface: 

Services Allowed:

- web  
 telnet  
 ssh  
 ftp  
 tftp  
 snmp  
 ping

Add

Reset

## CURRENT ACL TABLE

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

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

Field	Description
Direction Select	Select the router interface. You can select <b>LAN</b> or <b>WAN</b> . In this example, <b>WAN</b> is selected.
WAN Setting	You can choose <b>Interface</b> or <b>IP Address</b> .
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: <b>Web, Telnet, SSH, FTP, TFTP, SNMP</b> and <b>PING</b> . You can also choose all the services.

Field	Description
Add	After setting the parameters, click it to add an entry to the <b>Current ACL Table</b> .
Reset	Click it to refresh this page.

### 3.3.2.2 Access Control List IPv6

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

### 3.3.3 Port Triggering

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

**NAT PORTTRIGGER**

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the "Relate Port" in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the "Match Port". The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the "Relate Port".

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

**NAT PORT TRIGGER STATUS**

Nat Port Trigger:  Enable  Disable

Apply Changes

**APPLICATION TYPE**

Usual Application

Name:

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="button" value="v"/>	<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	outgoing <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	outgoing <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	outgoing <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	outgoing <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	outgoing <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	outgoing <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	outgoing <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	UDP <input type="button" value="v"/>	outgoing <input type="button" value="v"/>

Apply Changes

**CURRENT PORTTRIGGER TABLE**

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action
------------	------------------	-----------	------------	---------------	-------------	--------

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

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

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

### 3.3.4 Port Forwarding

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

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



**PORT FORWARDING**

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**

Add

Modify

**CURRENT PORT FORWARDING TABLE**

Select	Service Name	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action
--------	--------------	----------	------------------	------------	----------------	----------	-------	--------

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

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

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

**3.3.5 DMZ**

DMZ is the abbreviation of the Demilitarized Zone. Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a

single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

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

### DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

#### DMZ CONFIGURATION

WAN Interface:

DMZ Host IP Address:

#### CURRENT DMZ TABLE:

Select	WAN Interface	DMZ Ip
--------	---------------	--------

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

Click **Apply** to save the settings.

### 3.3.6 Parental Control

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

clients or PCs connected to the device are allowed to access the Internet.

### 3.3.6.1 URL Block

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



**Note:**

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

**URL BLOCK**

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 in SETUP -- Time and Date.

**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"/>				

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

### 3.3.6.2 Online Time Limit

Choose **Advanced > Parental Control > Online Time Limit**. The **ONLINE TIME LIMIT** page shown in the following figure appears.

**ONLINE TIME LIMIT**

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: you can use IP or MAC to specific PC.  
 Before enable this feature, you must enable that the time of the router is correct. Click [Maintenance->Time](#) to set the time of your router.

**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"/>						

### 3.3.6.3 Schedules

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

**SCHEDULES**

Schedule allows you to create scheduling rules to be applied for URL block.

**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

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

### 3.3.7 Filtering Options

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

#### 3.3.7.1 IP/Port Filter

When you use the Port Triggering or Port Forwarding features to open specific ports to traffic from the Internet, you could be increasing the exposure of your LAN

to cyber attacks from the Internet. In these cases, you can limit that exposure by specifying the IP addresses of Internet hosts that you trust to access your LAN through the ports that you have opened.

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

**IP/PORT FILTERING**

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be 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

**WAN Interface:** pppoe1

**Protocol:** IP

**Direction:** Upstream

**Source IP Address:**

**Dest IP Address:**

**SPort:**  -

**Mask Address:** 255.255.255.255

**Mask Address:** 255.255.255.255

**DPort:**  -

**Enable:**

**CURRENT FILTER TABLE**

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

Direction **Upstream (Downstream)** means packets outgoing (incoming) from (to) router. The Source IP addresses are LAN-side (WAN-side) addresses and the Destination IP addresses are WAN-side (LAN-side) addresses. Select the rule

action, and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask and source/destination port.

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



**Note:**

The settings only apply when the firewall is enabled.

### 3.3.7.2 IPv6/Port Filter

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



**IP/PORT FILTERING**

Entries in this table are used to restrict certain types of ipv6 data packets from your local network to Internet through the Gateway. Use of such filters can be 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:**

Apply Changes

Reset

Help

**CURRENT FILTER TABLE**

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

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

**3.3.7.3 MAC Filter**

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

**MAC FILTERING**

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

---

**DEFAULT POLICY**

**Outgoing Default Policy:**  Deny  Allow

**Incoming Default Policy:**  Deny  Allow

---

**ADD FILTER**

**Direction:**

**Action:**  Deny  Allow

**Source MAC:**  (ex. 00E086710502)

**Destination MAC:**  (ex. 00E086710502)

---

**CURRENT MAC FILTER TABLE**

Select	Direction	Source MAC	Destination MAC

### 3.3.8 DoS Settings

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

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

**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**

- |  |                                  |                |
|--|----------------------------------|----------------|
| <input type="checkbox"/> Whole System Flood: SYN   | <input type="text" value="100"/> | Packets/Second |
| <input type="checkbox"/> Whole System Flood: FIN   | <input type="text" value="100"/> | Packets/Second |
| <input type="checkbox"/> Whole System Flood: UDP   | <input type="text" value="100"/> | Packets/Second |
| <input type="checkbox"/> Whole System Flood: ICMP  | <input type="text" value="100"/> | Packets/Second |
| <input type="checkbox"/> Per-Source IP Flood: SYN  | <input type="text" value="100"/> | Packets/Second |
| <input type="checkbox"/> Per-Source IP Flood: FIN  | <input type="text" value="100"/> | Packets/Second |
| <input type="checkbox"/> Per-Source IP Flood: UDP  | <input type="text" value="100"/> | Packets/Second |
| <input type="checkbox"/> Per-Source IP Flood: ICMP | <input type="text" value="100"/> | Packets/Second |
| <input type="checkbox"/> TCP/UDP PortScan          | <input type="text" value="Low"/> | Sensitivity    |
| <input type="checkbox"/> ICMP Smurf                |                                  |                |
| <input type="checkbox"/> IP Land                   |                                  |                |
| <input type="checkbox"/> IP Spoof                  |                                  |                |
| <input type="checkbox"/> IP TearDrop               |                                  |                |
| <input type="checkbox"/> PingOfDeath               |                                  |                |
| <input type="checkbox"/> TCP Scan                  |                                  |                |
| <input type="checkbox"/> TCP SynWithData           |                                  |                |
| <input type="checkbox"/> UDP Bomb                  |                                  |                |
| <input type="checkbox"/> UDP EchoChargen           |                                  |                |



- |  |                                  |                  |
|--|----------------------------------|------------------|
| <input type="checkbox"/> Enable Source IP Blocking | <input type="text" value="300"/> | Block time (sec) |
|--|----------------------------------|------------------|

**3.3.9 DNS**

Domain Name System (DNS) is an Internet service that translates the URL/domain name into the corresponding IP address. Since URL/Domain Names are

alphabetical, they are easier to remember. But the Internet is based on IP address. For example, the URL/Domain Name www.dlink.com is actually 192.168.0.123.

### 3.3.9.1 DNS

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

**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:

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, and enter the IP addresses of the primary and secondary DNS server.
Apply Changes	Click it to save the settings of this page.
Reset Selected	Click it to start configuring the parameters in this page.

### 3.3.9.2 IPv6 DNS

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

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

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

### 3.3.10 Dynamic DNS

The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host

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

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

**DYNAMIC DNS CONFIGURATION**

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

**DDNS CONFIGURATION**

**DDNS provider:**  ▼

**Hostname:**

**Interface:**  ▼

**Enable:**

---

**DynDns Settings:**

**Username:**

**Password:**

---

**TZO Settings:**

**Email:**

**Key:**

**DYNAMIC DDNS TABLE**

Select	State	Service	Hostname	Username	Interface

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

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

**Note:**

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

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

### 3.3.11 Network Tools

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

#### 3.3.11.1 Port Mapping

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

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

**PORT MAPPING CONFIGURATION**

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

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

**PORT MAPPING CONFIGURATION**

Port Mapping:  Disable  Enable

**WAN****Interface group**

Add &gt;

**LAN**

&lt; Del

Select	Interfaces	Status
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,wlan-vap3,pppoe1	Enabled
Group1 <input type="radio"/>		--
Group2 <input type="radio"/>		--
Group3 <input type="radio"/>		--
Group4 <input type="radio"/>		--

Apply



Follow the steps to manipulate a mapping group.

**Step 1** Select a group from the table.

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

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



**Note:**

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

### 3.3.11.2 IGMP Proxy

IGMP allows support for efficient multicasting -- transmission of identical content, such as multimedia, from a source to a number of recipients. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it.

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

**IGMP PROXY CONFIGURATION**

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

- . Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
- . Enable IGMP on LAN interface (downstream), which connects to its hosts.

**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)

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

Field	Description
Multicast allowed	Enable multicast proxy, only for route mode.
Robust Count	Allows tuning for the expected packet loss on a link. It determines how many times a startup query should be xmitted.
Last Member Query Count	This parameter specifies the times the device sends the query message.
Query Interval	The device sends query messages to check IGMP user periodically. The unit is second.
Query Response Interval	The device waits for the IGMP user's reply. The unit is 100 * millisecond.
Group Leave Delay	The duration for the modem to cease forwarding multicast packets after a corresponding IGMP "Leave Group" message has been successfully offered to the modem.

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

### 3.3.11.3 IP QoS

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

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

**IP QoS**

Entries in this table are used to assign the precedence for each incoming packet based on specified policy.  
 Config Procedure:  
 1: set traffic rule.  
 2: assign the precedence or add marker for different stream.

**IP QoS CONFIGURATION**

IP QoS:  disable  enable

Schedule Mode:  v

Apply Changes

**QoS RULE LIST**

src MAC	dest MAC	src IP	sPort	dest IP	dPort	proto	phy port
---------	----------	--------	-------	---------	-------	-------	----------

**QoS RULE LIST(CONTINUE)**

IPP	TOS	DSCP	TC	802.1p	Prior	IPP Mark	TOS Mark	DSCP Mark	TC Mark	802.1p Mark	sel
-----	-----	------	----	--------	-------	----------	----------	-----------	---------	-------------	-----

Delete
Add Rule

- Step 1** Enable IP QoS and click **Apply Changes** to enable IP QoS function.
- Step 2** Click **Add Rule** to add a new IP QoS rule. The page shown in the following figure appears.

The screenshot shows the 'ADD OR MODIFY QOS RULE' configuration page. At the top, there are two buttons: 'Delete' and 'Add Rule'. Below this is a dark header with the text 'ADD OR MODIFY QOS RULE'. The main area contains the following fields and options:

- Source MAC:
- Destination MAC:
- Source IP:
- Source Mask:
- Destination IP:
- Destination Mask:
- Source Port:
- Destination Port:
- Protocol:  (dropdown)
- Phy Port:  (dropdown)
- IPP/DS Field:  IPP/TOS  DSCP
- IP Precedence Range:  ~  (dropdown)
- Type of Service:  (dropdown)
- DSCP Range:  ~  (Value Range:0~63)
- Traffic Class Range:  ~  (Value Range:0~255)
- 802.1p:  ~  (dropdown)
- Priority:  (dropdown)
- insert or modify QoS mark

At the bottom of the form is an 'Apply Changes' button.

### 3.3.11.4 UPnP

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

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

**UPNP CONFIGURATION**

This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.

**UPNP CONFIGURATION**

UPnP:  Disable  Enable

WAN Interface:

Apply Changes

### 3.3.11.5 SNMP

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

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

**SNMP PROTOCOL CONFIGURATION**

This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap ip address, community name, etc..

**SNMP PROTOCOL CONFIGURATION**

Enable SNMP

**System Description** ADSL SoHo Router

**System Contact**

**System Name** XDSL

**System Location**

**Trap IP Address**

**Community name (read-only)** public

**Community name (read-write)** public

The following table describes the parameters of this page:

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

**3.3.11.6 TR-069**

TR-069 is a WAN management protocol. It is a bidirectional SOAP/HTTP based protocol providing the communication between the ADSL router and an Auto

Configuration Server (ACS) to monitor status and performance and to set configuration parameters from WAN side.

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

**TR-069 CONFIGURATION**

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

**ACS CONFIGURATION**Enable: URL: User Name: Password: Periodic Inform Enable:  Disable  EnablePeriodic Inform Interval:  seconds**CONNECTION REQUEST**User Name: Password: Path: Port: **DEBUG**ACS Certificates CPE:  No  YesShow Message:  Disable  EnableCPE Sends GetRPC:  Disable  EnableSkip MReboot:  Disable  EnableDelay:  Disable  EnableAuto-Execution:  Disable  EnableCT Inform Extension:  Disable  Enable**CERTIFICATE MANAGEMENT**CPE Certificate Password:     CPE Certificate:   CA Certificate:



The following table describes the parameters of this page:

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

Field	Description
CA Certificate	Click it to browse and upload the CA certificate for the router.

### 3.3.11.7 Software Forbidden

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

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

**SOFTWARE FORBIDDEN**

This page is used to config some softwares to be forbidden.By it ,you can deny the ip packets from the specified software.

**CURRENT FORBIDDEN SOFTWARE LIST**

Software	Select

**ADD FORBIDDEN SOFTWARE**

Add Forbidden Software:

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

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

Field	Description
Software	accessing the network.

### 3.3.11.8 ARP Binding

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

**ARP BINDING CONFIGURATION**

This page lists the permanent arp entry table. You can bind ip with corresponding mac to avoid arp spoof.

**ARP BINDING CONFIGURATION**

IP Address:

Mac Address:  (ex. 00E086710502)

**ARP BINDING TABLE**

Select	IP Address	MAC Address

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

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

### 3.3.11.9 Client Limit

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

**CLIENT LIMIT CONFIGURATION**

This page is used to configure the capability of force how many device can access to Internet!

---

**CLIENT LIMIT CONFIGURATION**

Client Limit Capability:  Disable  Enable

[Apply Changes](#)

## 3.3.12 Routing

### 3.3.12.1 Static Route

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

**ROUTING CONFIGURATION**

This page is used to configure the routing information. Here you can add/delete IP routes.

---

**HOST**

Enable

Destination

Subnet Mask

Next Hop

Metric

Interface

[Add Route](#) [Update](#) [Delete Selected](#) [Show Routes](#)

**STATIC ROUTE TABLE**

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf
--------	-------	-------------	-------------	---------	--------	-----

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

Field	Description
-------	-------------

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

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

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
<input type="button" value="Refresh"/> <input type="button" value="Close"/>			

### 3.3.12.2 IPv6 Static Route

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

**IPv6 ROUTING CONFIGURATION**

This page is used to configure the ipv6 routing information. Here you can add/delete IPv6 routes.

**CONFIGURATION**

Destination

Prefix Length

Next Hop

Interface  ▼

Add Route
Delete Selected

**IPv6 STATIC ROUTE TABLE**

Select	Destination	NextHop	Interface

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

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

### 3.3.12.3 RIP

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

Choose **Advanced > Routing > RIP**. The **RIP Configuration** page shown in the following figure appears.

**RIP CONFIGURATION**

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.  
attention: if you want to enable RIP, please make sure remote control is enabled.

**RIP**

Off
  On

**interface** LAN

**Recv Version** RIP1

**Send Version** RIP1

**RIP CONFIG LIST**

Select	interface	Recv Version	Send Version

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

Field	Description
RIP	Select <b>Enable</b> , the router communicates with other RIP-enabled devices.
Apply	Click it to save the settings of this page.
Interface	Choose the router interface that uses RIP.
Receive Version	Choose the interface version that receives RIP messages. You can choose <b>RIP1</b> , <b>RIP2</b> , or <b>Both</b> . <ul style="list-style-type: none"> <li>● Choose <b>RIP1</b> indicates the router receives RIP v1 messages.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>● Choose <b>RIP2</b> indicates the router receives RIP v2 messages.</li> <li>● Choose <b>Both</b> indicates the router receives RIP v1 and RIP v2 messages.</li> </ul>
Send Version	<p>The working mode for sending RIP messages . You can choose <b>RIP1</b> or <b>RIP2</b>.</p> <ul style="list-style-type: none"> <li>● Choose <b>RIP1</b> indicates the router broadcasts RIP1 messages only.</li> <li>● Choose <b>RIP2</b> indicates the router multicasts RIP2 messages only.</li> </ul>
Add	Click it to add the RIP interface to the <b>Rip Config List</b> .
Delete	Select a row in the <b>Rip Config List</b> and click it to delete the row.

### 3.3.13 NAT

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

#### 3.3.13.1 NAT ALG

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



**NAT ALG AND PASS-THROUGH**

Setup NAT ALG and Pass-Through configuration

**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

### 3.3.13.2 NAT Exclude IP

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

**NAT EXCLUDE IP**

In the page ,you can config some source ip address which use the purge route mode when access internet through the specified interface.

**CONFIG**

interface

IP Range  -

**CURRENT NAT EXCLUDE IP TABLE**

WAN Interface	Low IP	High IP	Action

### 3.3.13.3 NAT Forwarding

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

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

Under 1483MER or 1483Routed mode, if NAPT (Network Address Port Translation) is enabled, the **Local IP Address** is configured as 192.168.1.3 and the **Remote IP Address** is configured as 202.32.0.2, the PC with the LAN 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 FORWARDING**

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

**SETTING**

Local IP Address

Remote IP Address

Enable

**CURRENT NAT PORT FORWARDING TABLE**

Local IP Address	Remote IP Address	State	Action

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

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

Field	Description
Reset	Cancel the modification and reconfigure the settings.
Current NAT Port Forwarding Table	Current configuration rule list.

### 3.3.13.4 FTP ALG Configuration

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

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

**FTP ALG CONFIGURATION**

This page is used to configure FTP Server ALG and FTP Client ALG ports .

**SETTING PORT**

FTP ALG port

**FTP ALG PORTS TABLE**

Select	Ports
<input type="radio"/>	21

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

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

### 3.3.13.5 NAT IP Mapping

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

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

**NAT IP MAPPING**

Entries in this table allow you to config one IP pool for specified source ip address from lan,so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT.

**SETTING**

Type

Local Start IP

Local End IP

Global Start IP

Global End IP

**CURRENT NAT IP MAPPING TABLE**

Local Start IP	Local End IP	Global Start IP	Global End IP	Action

### 3.3.14 USB Printer

Choose **Advanced > USB Printer**. The page is shown as the following figure appears.

**USB PRINTER**  
This page is used to configure print server.

**USB PRINTER CONFIGURATION**  
Print Server:  Disable  Enable  
Printer Name:   
Print Server URL:

### 3.3.15 VOIP

#### 3.3.15.1 SIP Server

Choose **Advanced > VOIP > SIP Server**. The page is shown as the following figure appears.

**SIP SERVER**  
This page is used to configure SIP Server.

**SIP SERVER CONFIGURATION**  
**Main SIP Proxy**  
Address:   
Port:   
SIP Domain:   
Reg Expire (sec):   
Enable Session timer:   
Session Expire (sec):   
Outbound Proxy Enable:   
Outbound Proxy Addr:   
Outbound Proxy Port:   
**Backup SIP Proxy**  
Backup SIP Proxy Enable:   
Address:   
Port:   
SIP Domain:   
Reg Expire (sec):   
Enable Session timer:   
Session Expire (sec):   
Outbound Proxy Enable:   
Outbound Proxy Addr:   
Outbound Proxy Port:

### 3.3.15.2 SIP Account

Choose **Advanced > VOIP > SIP Account**. The page is shown as the following figure appears.

**SIP ACCOUNT**

This page is used to configure SIP Account.

**SIP ACCOUNT CONFIGURATION**

**SIP 1 Account**

Enable:

Number:

Login ID:

Password:

**SIP 2 Account**

Enable:

Number:

Login ID:

Password:

**VoIP Interface Select** any ▾

Apply

### 3.3.15.3 VOIP Advanced

Choose **Advanced > VOIP > VOIP Advanced**. The page is shown as the following figure appears.

## VOIP ADVANCED CONFIGURATION

This page is used to configure advanced VOIP.

## VOIP ADVANCED CONFIGURATION

## SIP

SIP Port RTP Port SIP DSCP RTP DSCP DTMF Relay 

## Advanced Setting

Select Country Caller ID Mode Flash Time Setting (ms)  < Flash Time <  
[Space:10, Min:80, Max:2000] Off Hook Alarm(sec) Inter Digit Timer Long(sec) Busy Tone Timer(sec) Hanging Reminder Tone  
Timer(sec) Register Retry Interval(sec) DialPlan  EnableDialPlan FXS Pluse Dial Detection  EnableInterdigit Pause Duration (ms) 

Codec Precedence

codec priority 0: codec priority 1: codec priority 2: codec priority 3: Speaker Voice Gain  (dB) [-32~31] Mute:-32Mic Voice Gain  (dB) [-32~31] Mute:-32

## DSP

Echo Cancellation  EnableVAD  EnableCNG  EnableT.38  EnableSpeaker AGC  EnableMin delay (ms): Jitter Buffer Control Max delay (ms): Optimization factor:

### 3.3.16 FTPD Setting

Choose **Advanced > FTPD Setting**. The page is shown as the following figure appears.

**FTP**

In this page, you can enable or disable the FTP server, and set the FTP port.

**FTP SERVER SETTING**

Interface:

Enable FTP Server

Enable FtpServer for WAN

FTP Server Port

### 3.3.17 FTPD Account

Choose **Advanced > FTPD Account**. The page is shown as the following figure appears.

**FTPD USERACCOUNT CONFIGURATION**

Choose Add, or Remove to configure User Accounts.

**STORAGE USERACCOUNT**

UserName	Remove
superadmin	<input type="radio"/>
admin	<input type="radio"/>

**ADD STORAGE USERACCOUNT**

Username:

Password:

Confirm Password:



## 3.4 Maintenance

### 3.4.1 System

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

**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 :

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

Field	Description
Reset to default	This option restores all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. All settings will be lost. If you want to save your router configuration settings, use the <b>Backup Settings</b> option below.
Save and reboot	This will save all your settings and restart the router.

Field	Description
Back settings	Save your configurations in a file on your computer so that it may be accessed again later if your current settings are changed. Be sure to save the configuration before performing a firmware update.
Update settings	Click <b>Browse</b> to select the configuration file of device and click <b>Update Settings</b> to begin restoring the device configuration.

**Note:**

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

### 3.4.2 Firmware Update

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

UPGRADE FIRMWARE

**Step 1:** Obtain an updated firmware image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Firmware" button once to upload the new image file.

**NOTE:** 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.

SELECT FILE

**Current Firmware Version:** GE\_1.00

**Current Firmware Date:** Mar 5 2018 15:20:26

**Firmware File Name:**  未选择文件.

The procedure for updating the firmware is as follows.

- Step 1** Click **Browse...** to search the file.
- Step 2** Click **Update Firmware** to update the configuration file.
- Step 3** Wait for the router to reboot. This can take another minute or more.



**Note:**

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

### 3.4.3 Password

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

**USER ACCOUNT CONFIGURATION**

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

**CONFIGURATION**

User Name:

Privilege: User ▾

Old Password:

New Password:

Confirm Password:

Idle logout time:  (1-60min)

**USER ACCOUNT TABLE**

Select	User Name	Privilege	Idle Time
<input type="radio"/>	superadmin	root	5
<input type="radio"/>	admin	user	5

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

Field	Description
Privilege	<ul style="list-style-type: none"> <li>● Root: The root account is fixed, having full access to the Web-based management interface.</li> <li>● User: The user account has the privilege to view configuration settings and statistics and update the router's firmware.</li> </ul>

## 3.4.4 Diagnostics

### 3.4.4.1 Ping Diagnostic

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

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

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

### 3.4.4.2 Ping6

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

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

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

### 3.4.4.3 Traceroute

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

**TRACEROUTE DIAGNOSTIC**

This page is used to traceroute diagnostic.

**TRACEROUTE**

Host

NumberOfTries

Timeout  ms

Datasize  Bytes

DSCP

MaxHopCount

Interface

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

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

Traceroute

Click start traceroute.

### 3.4.4.4 ADSL

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

**DIAGNOSTIC ADSL**

This page is used to diagnostic ADSL.

**ADSL TONE DIAGNOSTIC**

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

**ADSL TONE LIST**

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					
5					

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

### 3.4.4.5 Diag Test

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

**DIAGNOSTIC TEST**

The DSL Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.

**SELECT THE INTERNET CONNECTION**

popoe1

### 3.4.5 System Log

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

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



**LOG SETTING**

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 the ">>|", it will display the newest log information below.

**SETTING**

Error:                       Notice:

**REMOTE SETTING**

Remote Log Enable:

**EVENT LOG TABLE**

Old              New

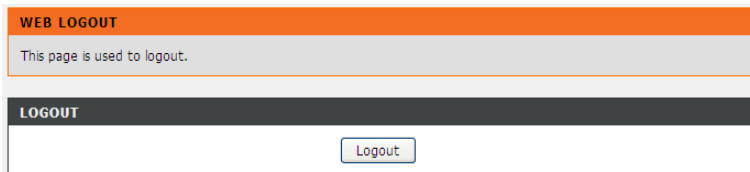
Time	Index	Type	Log Information
Page: 1/1			

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

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

### 3.4.6 Logout

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



## 3.5 Status

You can view the system information and monitor performance

### 3.5.1 Device Info

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

**ADSL ROUTER STATUS**

This page shows the current status and some basic settings of the device.

**SYSTEM**

Alias Name	DSL-G2252
Firmware Version	GE_1.00
Uptime	2 21:39:54
Date/Time	Wed Jan 4 0:39:54 2012
Built Date	Mar 5 2018 15:20:26
Serial Number	00051D030405

**DSL**

Operational Status	ADSL2+ AnnexA
Upstream Speed	997 kbps
Downstream Speed	22920 kbps

**LAN CONFIGURATION**

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	00:05:1D:03:04:05

**WIRELESS INFO**

Status:	Enabled
MAC Address:	00:05:1D:03:04:05
Network Name (SSID):	RTL867x-ADSL
Current Channel:	8
Encryption:	WPA2 Mixed

Figure 5 Device information - 1

DNS STATUS							
DNS Mode	Auto						
DNS Servers							
IPv6 DNS Mode	Auto						
IPv6 DNS Servers							

WAN CONFIGURATION							
Interface	VPI/VCI	Encap	Droute	Protocol	IP Address	Gateway	Status
pppoe1	0/35	LLC	On	PPPoE	0.0.0.0	0.0.0.0	Down 0 0:0:0 / 0 0:0:0 <input type="button" value="connect"/>

WAN IPV6 CONFIGURATION								
Interface	VPI/VCI	Encap	Protocol	IPv6 Address	Prefix	Gateway	Droute	Status
pppoe1	0/35	LLC	PPPoE					Down

ETHERNET WAN CONFIGURATION						
Interface	Droute	Protocol	IP Address	Gateway	Status	

ETHERNET WAN IPV6 CONFIGURATION						
Interface	Protocol	IPv6 Address	Prefix	Gateway	Droute	Status

Figure 6 Device information - 2

### 3.5.2 Wireless Clients

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

ACTIVE WIRELESS CLIENT TABLE					
This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client					
ACTIVE WIRELESS CLIENT TABLE					
MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---
<input type="button" value="Refresh"/>					

### 3.5.3 DHCP Clients

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

ACTIVE DHCP CLIENT TABLE				
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.				
ACTIVE DHCP CLIENT TABLE				
Name	IP Address	MAC Address	Expiry	Type
<input type="button" value="Refresh"/>				

### 3.5.4 ADSL Driver

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

**ADSL CONFIGURATION**

This page shows the setting of the ADSL Router.

**ADSL**

Adsl Line Status	SHOWTIME.
Adsl Mode	G992.5
Channel Mode	Interleave
Up Stream	997 kbps
Down Stream	22920 kbps
Attenuation Down Stream	4
Attenuation Up Stream	3
SNR Margin Down Stream	8.9
SNR Margin Up Stream	9.0
Vendor ID	RETK
Firmware Version	v134fc17
CRC Errors	5003
Up Stream BER	0e-7
Down Stream BER	0e-7
Up Output Power	12
Down Output Power	14
ES	2689
SES	49
UAS	86560

Retrain

Refresh

### 3.5.5 Statistics

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

**STATISTICS**

This page shows the packet statistics for transmission and reception regarding to network interface.

**STATISTICS**

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
e1	34301	0	0	32953	0	0
pppoe1	0	0	0	41578	0	0
w1	4511189	0	0	65681	0	140937
w2	0	0	0	0	0	0
w3	0	0	0	0	0	0
w4	0	0	0	0	0	0
w5	0	0	0	0	0	0

### 3.5.6 Route Information

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

**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

### 3.5.7 VOIP Status

Choose **Status > VOIP Status**. The page shown in the following page appears. This table shows the status of VOIP on your network.

VOIP STATUS		
This shows VOIP status.		
STATUS		
SIP Number		
Register Status	Disabled	Disabled

## 3.6 Help

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



## HELP MENU

- [Setup](#)
- [Advanced](#)
- [Maintenance](#)
- [Status](#)

## SETUP HELP

- [Local Network](#)
- [Internet Setup](#)
- [Wireless Setup](#)
- [Time and Date](#)

## ADVANCED HELP

- [Advanced Wireless](#)
- [Access Control List](#)
- [Port Triggering](#)
- [Port Forwarding](#)
- [DMZ](#)
- [Parental Control](#)
- [Filtering Options](#)
- [DOS settings](#)
- [DNS](#)
- [Dynamic DNS](#)
- [Network Tools](#)
- [Routing](#)
- [NAT](#)
- [USB Printer](#)
- [VOIP](#)
- [FTP Setting](#)
- [FTP Account](#)

## MAINTENANCE HELP

- [System](#)
- [Firmware Update](#)
- [Password](#)
- [Diagnostics](#)
- [System Log](#)
- [Logout](#)

## STATUS HELP

- [Device Info](#)
- [Wireless Clients](#)
- [DHCP Clients](#)
- [ADSL Driver](#)
- [Statistics](#)
- [Route Info](#)
- [VOIP status](#)