USER MANUAL

DSL-2730U

VERSION 1.0

DSL-2730U

User Manual

D-Link

BROADBAND

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Table of Contents

1 Safety Precautions 1
2 Introduction 1
2.1 LEDs and Interfaces 2
2.2 System Requirements 4
2.3 Features 4
2.4 Standards Compatibility and Compliance 5
3 Hardware Installation.......... 5
3.1 Choosing the Best Location for Wireless Operation 5
3.2 Connecting the Router.......... 6
4 About the Web Configuration 7
4.1 Preparation Before Login 7
4.2 Logging In to the Router 8
4.2.1First-Time Login.......... 8
4.3 Setup 9
4.3.1Wizard 9
4.3.2Internet Setup.......... 18
4.3.3Wireless Connection.......... 24
4.3.4Local Network.......... 29
4.3.5Time and Date 31
4.3.6Logout 32
4.4 Advanced.......... 33
4.4.1Wireless Settings.......... 33
4.4.2Port Forwarding 41
4.4.3Port Triggering 43
4.4.4DMZ.......... 45
4.4.5Parental Control.......... 45
4.4.6Filtering Options 49
4.4.7DNS.......... 53
4.4.8Dynamic DNS 54
4.4.9Multicast 55
4.4.10 Network Tools.......... 56
4.4.11 Routing.......... 67
4.4.12 RIP 70
4.4.13 MultiNat 70
4.4.14 Schedules 71
4.4.15 Logout 72
4.5 Maintenance 73
4.5.1System 73
4.5.2Firmware Update.......... 74
4.5.3Access Controls 74
4.5.4Diagnostics.......... 77
4.5.5System Log 78
4.5.6Logout 78
4.6 Status 79
4.6.1Device Info 79
4.6.2Wireless Clients.......... 80
4.6.3DHCP Clients 80
4.6.4Logs 81
4.6.5Statistics 82
4.6.6Route info.......... 83
4.6.7Logout 83
5 FAQs 84

1 Safety Precautions

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

- Use volume labels to mark the type of power.
- Use the power adapter packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid 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 place where a heat source exists or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

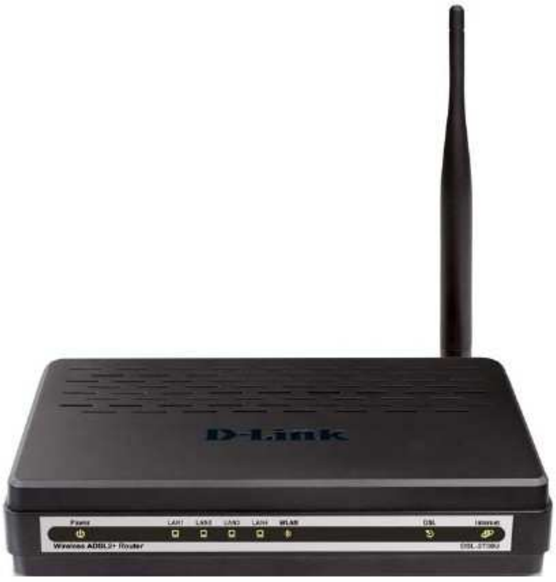
2 Introduction

The DSL-2730U is a highly integrated ADSL2/2+ Integrated Access Device. It provides DSL uplink, Ethernet LAN and wireless LAN services. The wireless LAN is complied with the IEEE802.11b/g /n standards. It is usually prefered to provide high access performance applications for the individual users, the SOHO, the small enterprise and so on.

2.1 LEDs and Interfaces

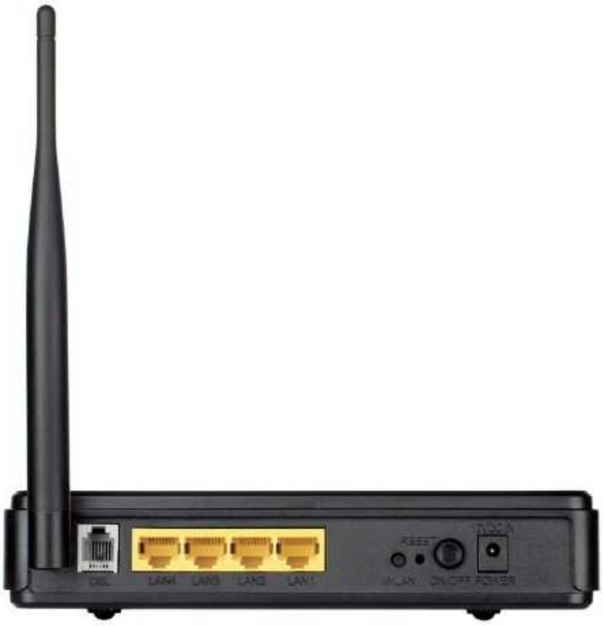
Front Panel

LED	Color	Status	Description
Power	Green	Off	The power is off.
		On	The power is on and the initialization is normal.
	Red	On	The device is initiating.
		Blinks	The firmware is upgrading.
LAN 1/2/3/4	Green	Off	No LAN link.
		Blinks	Data is being transmitted through the LAN interface.
		On	The connection of LAN interface is normal.
WLAN	Green	Blinks	Data is transmitted through the WLAN interface.
		On	The connection of WLAN interface is normal.
		Off	The WLAN connection is not established.
DSL	Green	Off	Initial self-test is failed.
		Blinks	The device is detecting itself.
		On	Initial self-test of the unit has passed.
Internet	Green	Off	The device is under the Bridge mode, DSL connection is not present, or the power is off.
		On	IP is connected and no traffic is detected.
	Red	On	The device is attempted to become IP connected, but failed.
WPS(on theside panel)	Green	Blinks	WPS negotiation is enabled, waiting for the clients.
		Off	Device is ready for new WPS to setup.



Rear Panel

Interface/Button	Description
DSL	RJ-11 interface that connects to the telephone set through the telephone cable.
LAN4/3/2/1	Ethernet RJ-45 interfaces that connect to the Ethernet interfaces of computers or Ethernet devices.
WLAN	Button to enable or disable WLAN.
RESET	Reset to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for one second, and then release.
ON/OFF	Power on or off.
POWER	Interface that connects to the power adapter. The power adapter output is: 12 V DC, A.
WPS (on the side panel)	WPS button to setup connection to client.



2.2 System Requirements

Recommended system requirements are as follows:

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

2.3 Features

The device supports the following features:

- User-friendly GUI for web configuration
- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 8 permanent virtual circuits (PVC)
- Support for up to 8 PPPoE sessions
- Support RIP v1 & RIP v2
- WLAN with high-speed data transfer rates of up to 130 Mbps, compatible with IEEE 802.11b/g/n, 2.4GHz compliant equipment
- Optimized Linux 2.6 Operating System
- IP routing and bridging
- Asynchronous transfer mode (ATM) and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- File server for network attached storage (NAS) devices
- Print server
- Web filtering
- Management and control

-Web-based management (WBM)
-Command line interface (CLI)
-TR-069 WAN management protocol

- Remote update
- System statistics and monitoring

2.4 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g

IEEE 802.11n

3 Hardware Installation

3.1 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.

3.2 Connecting the Router

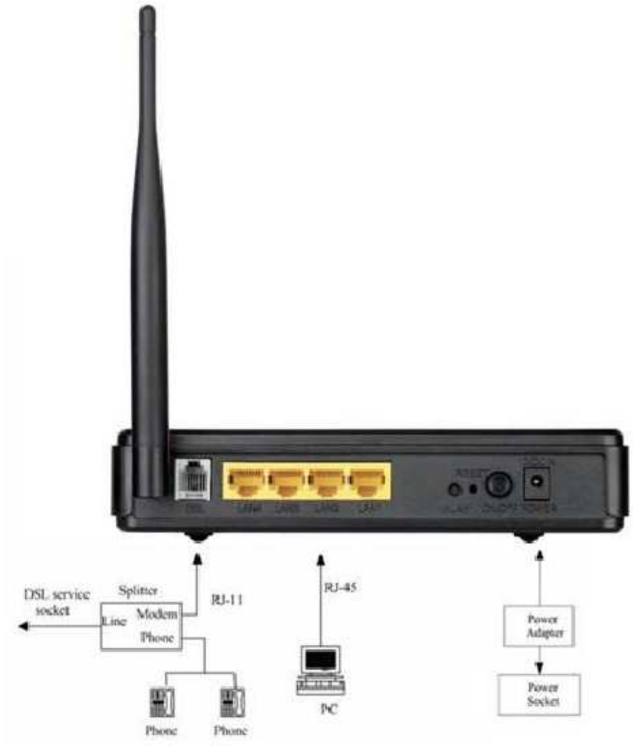
(1) Connect the DSL port of the router and the Modem port of the splitter with a telephone cable; connect the phone to the phone port of the splitter through a cable; and connect the incoming line to the Line port of the splitter.

The spliiter has three ports:

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

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

(3)Plug the power adapter to the wall outlet and then connect the other end of it to the Power port of the router.



4 About the Web Configuration

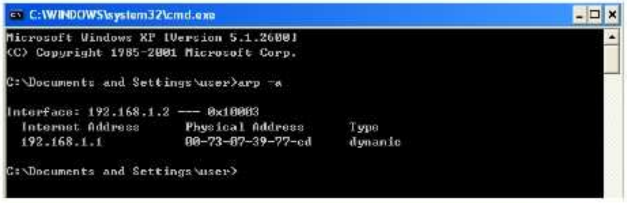
The first time you setup the Router. It is recommended that you configure the WAN connection using a single computer, to ensure that both the computer and the Router are not connected to the LAN. Once the WAN connection operates properly, you may continue to make changes to Router configuration, including IP settings and DHCP setup. This chapter is concerned with using your computer to configure the WAN connection. The following chapter describes the various menus used to configure and monitor the Router, including how to change IP settings and DHCP server setup.

4.1 Preparation Before Login

Before accessing the Routerre the communication between PC and Router is normal. Check the communication as follows.

Configure the IP address of the PC as 192.168.1.X (2~254), net mask as 255.255.255.0, gateway address as 192.168.1.1 (for customized version, configure them according to the actual version).

Enter arp -a in the DOS window to check whether the PC can read the MAC address of the Router.



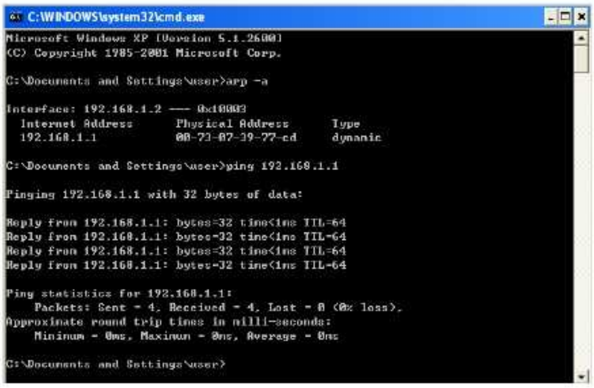
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>arp -a

Interface: 192.168.1.2 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.1           00-73-07-39-77-cd     dynamic

C:\Documents and Settings\user>
```

Ping the MAINTENANCE IP address (192.168.1.1 by default) of the Router. If the PC can read the MAC address of the Router and can ping through the MAINTENANCE IP address of the Router, that means the communication of the PC and the Router is normal.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>arp -a

Interface: 192.168.1.2 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.1           00-73-07-39-77-cd     dynamic

C:\Documents and Settings\user>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\user>
```

Note:

When you manage the Router through Web, you must keep the Router power on. Otherwise, the Router may be damaged.

4.2 Logging In to the Router

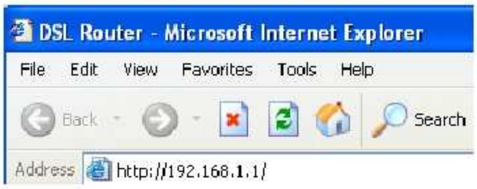
The following description is a detail “How-To” user guide and is prepared for first time users.

4.2.1 First-Time Login

When you log in to the DSL Router for the first time, the login wizard appears.

Step 1 Open a Web browser on your computer.

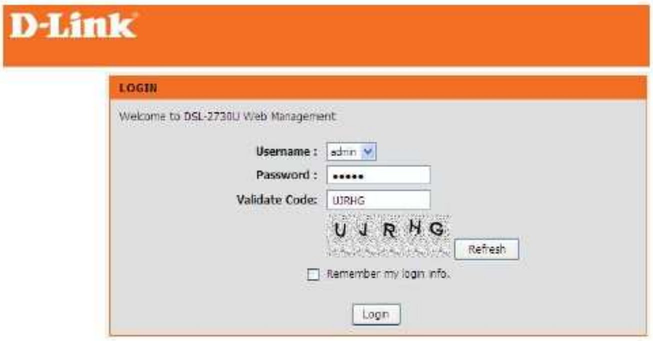
Step 2 Enter http://192.168.1.1 (DSL router default IP address) in the address bar. The login page appears.



http://192.168.1.1/

Step 3 Enter a user name and the password. The default username and password of the super user are admin and admin. The username and password of the common user are user and user. You need not enter the username and password again if you select the option Remember my password. It is recommended to change these default values after logging in to the DSL router for the first time.

Step 4 Click Login to log in.



Welcome to DSL-2730U Web Management

Username : admin

Password : •••••

Validate Code: UJRHG

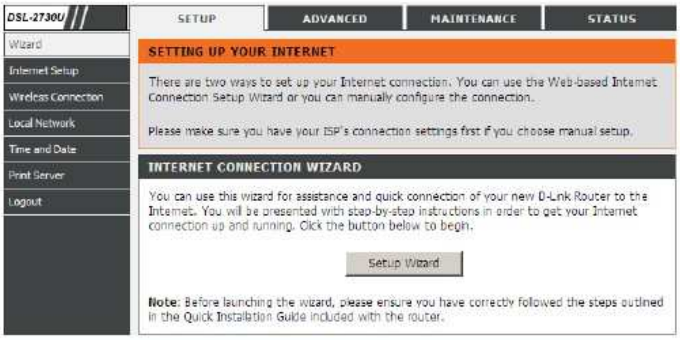
4.3 Setup

4.3.1 Wizard

Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe these various configuration parameters.

When subscribing to a broadband service, you should be aware of the method, by which you are connected to the Internet. Your physical WAN device can be Ethernet, DSL, or both. Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or the protocol, such as PPPoA or PPPoE, that you use to communicate over the Internet.

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



SETTING UP YOUR INTERNET

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.

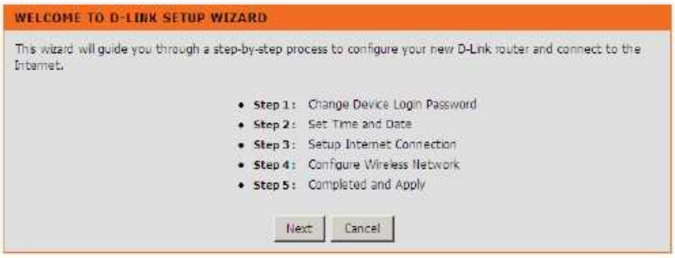
Please make sure you have your ISP's connection settings first if you choose manual setup.

INTERNET CONNECTION WIZARD

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.

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

Click Setup Wizard. The page shown in the right figure appears.



WELCOME TO D-LINK SETUP WIZARD

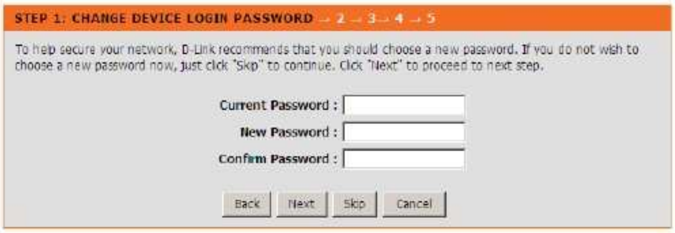
This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

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

There are four steps to configure the device. Click Next to continue.
Change the password for logging in to the device.
The default password is admin. To secure your network, modify the password timely.

Note:
Confirm password must be the same as the new password.

To ignore the step, click Skip.



STEP 1: CHANGE DEVICE LOGIN PASSWORD → 2 → 3 → 4 → 5

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.

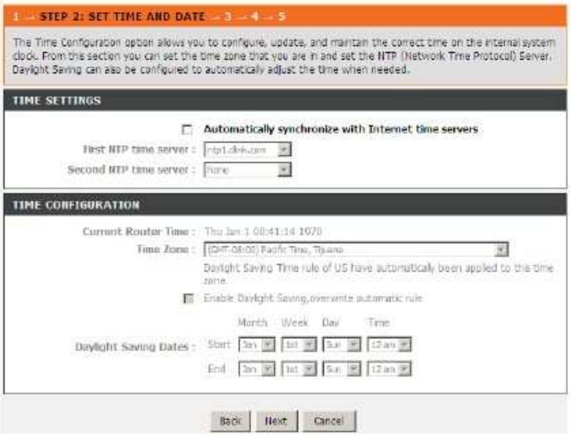
Current Password :

New Password :

Confirm Password :

Set the time and date.

First NTP time server: Select the domain of the time server to which system time will be synchronized.



1 → STEP 2: SET TIME AND DATE → 3 → 4 → 5

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.

TIME SETTINGS

□ Automatically synchronize with Internet time servers

First NTP time server : ntp1.dlink.com

Second NTP time server : None

TIME CONFIGURATION

Current Router Time : Thu Jan 1 00:41:14 1970

Time Zone : (GMT-08:00) Pacific Time, Tijuana

Daylight Saving Time rule of US have automatically been applied to this time zone.

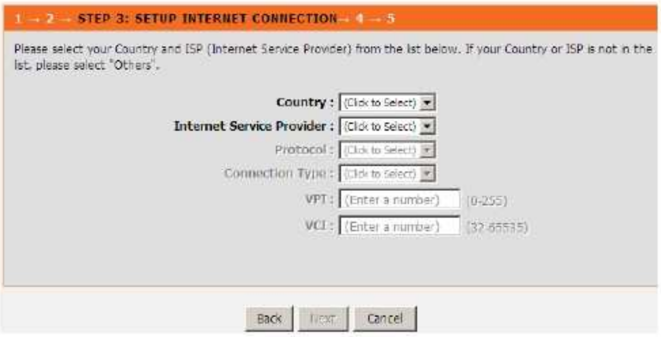
□ Enable Daylight Saving,overwrite automatic rule

Daylight Saving Dates :		Month	Week	Day	Time
	Start	Jan	1st	Sun	12 am
	End	Jan	1st	Sun	12 am

Configure the Internet connection.

Select the country and ISP. Set the VPI and VCI. If you fail to find the country and ISP from the drop-down lists, select Others.

- Protocol: The protocol connection type of the interface. You can select PPPoE, PPPoA, Dynamic IP, Static IP, or Bridge.
- Connection Type: You can select it from the drop-down list according to the uplink equipment. You can select LLC or VC-Mux.
- VPI: The virtual path identifier of the WAN interface (provided by your ISP). The range is 0 to 255.
- VCI: The virtual channel identifier for the WAN interface. The range is 32 to 65535 (1 to 31 are reserved for known protocols).



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

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

Country : (Click to Select)

Internet Service Provider : (Click to Select)

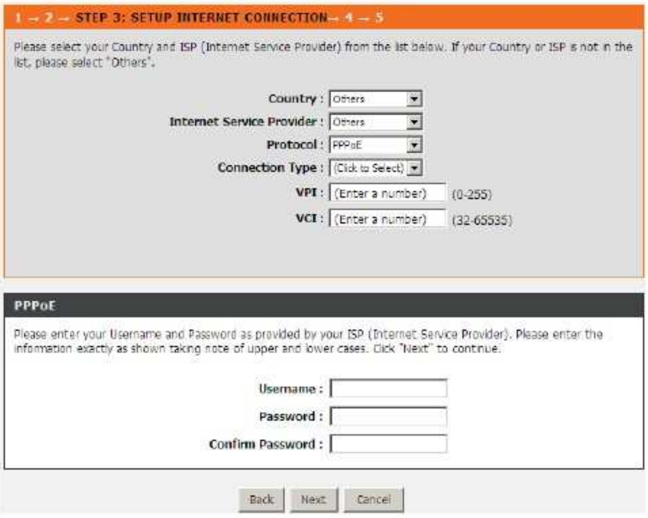
Protocol : (Click to Select)

Connection Type : (Click to Select)

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

VCI : (Enter a number) (32-65535)

If the Protocol is PPPoE or PPPoA, the page shown in either of the two figures appears.



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

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

Country : Others

Internet Service Provider : Others

Protocol : PPPoE

Connection Type : (Click to Select)

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

VCI : (Enter a number) (32-65535)

PPPoE

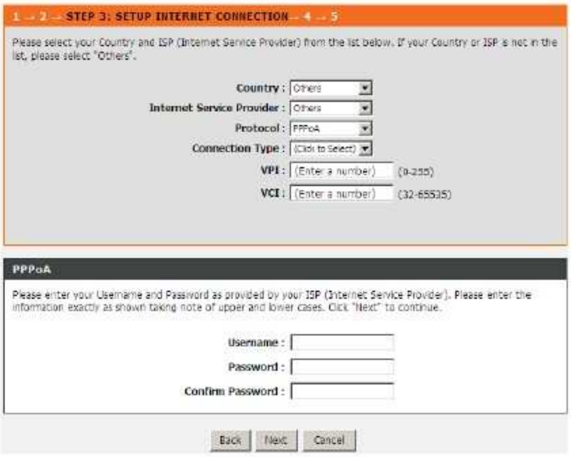
Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.

Username :

Password :

Confirm Password :

Set the user name and password as provided by your ISP.



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

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

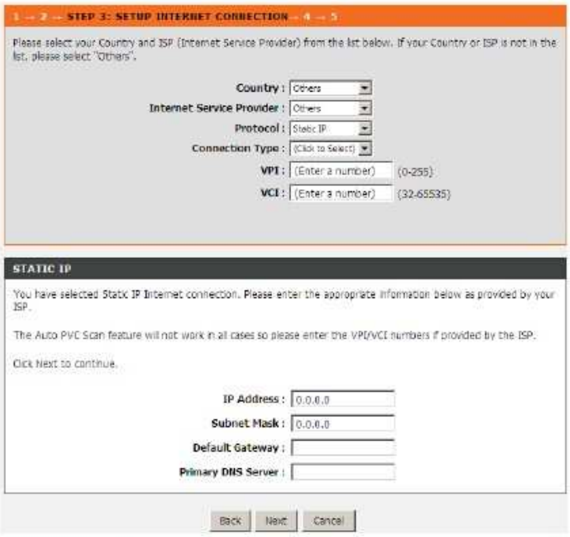
Country : Others
Internet Service Provider : Others
Protocol : PPPoA
Connection Type : (Click to Select)
VPI : (Enter a number) (0-255)
VCI : (Enter a number) (32-65535)

PPPoA

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 :

If the Protocol is Static IP, the page shown in the figure appears.
Enter the IP Address, Subnet Mask, Default Gateway, and Primary DNS Server.



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

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

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

STATIC IP

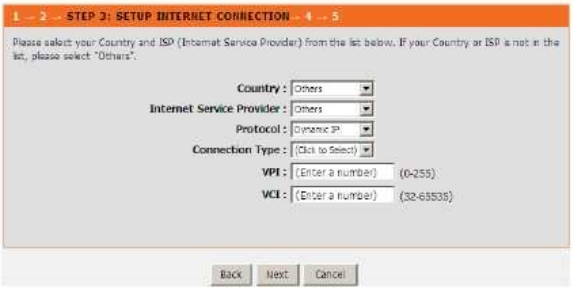
You have selected Static IP Internet connection. Please enter the appropriate information below as provided by your ISP.

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 :

If the Protocol is Dynamic IP or Bridge, the page shown in the figure appears.

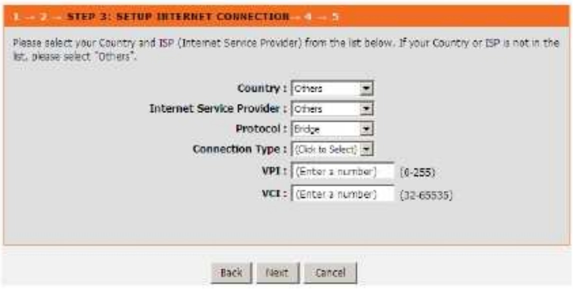


1 → 2 → STEP 3: SETUP INTERNET CONNECTION → 4 → 5

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

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

After proper configuration, click Next.



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

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

Country : Others

Internet Service Provider : Others

Protocol : Bridge

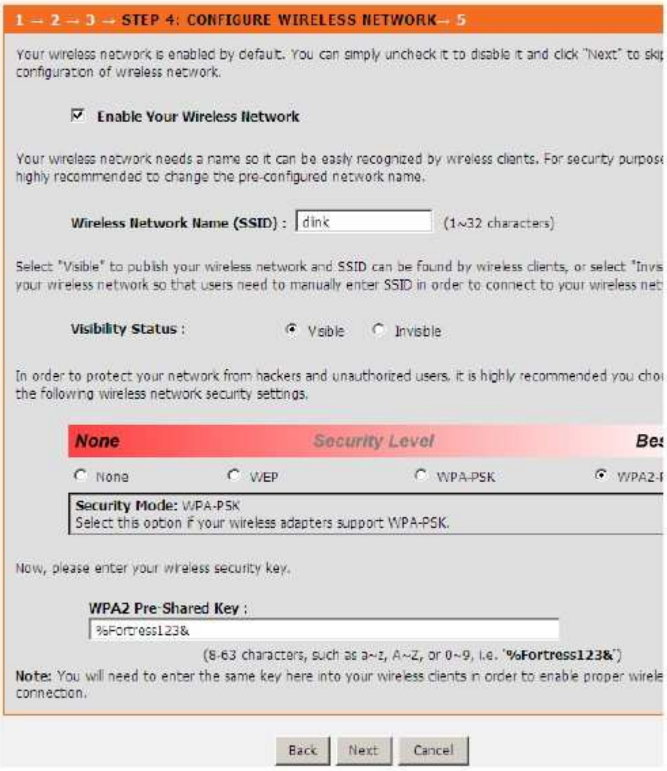
Connection Type : (Click to Select)

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

VCI : (Enter a number) (32-65535)

Configure the wireless network, or keep the default settings. Enter the information and click Next.

- Enable Your Wireless Network: Enable wireless settings on LAN interface.
- Wireless Network Name (SSID): SSID is the name of your wireless network. All wireless-equipped devices share the same SSID to communicate with each other. It must be unique to identify separated wireless network. For security, you should change the default SSID to a special ID.
- Visibility Status: You can select visible or invisible.
- Security Level: 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.
- WPA Pre-Shared Key: Please set it. Then you will need to enter the same key here into your wireless clients in order to enable proper wireless connection.



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

Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to ski 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 purpos highly recommended to change the pre-configured network name.

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

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

Visibility Status : ● Visible ○ Invisible

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

None Security Level Bes

○ None ○ WEP ○ WPA-PSK ● WPA2-

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

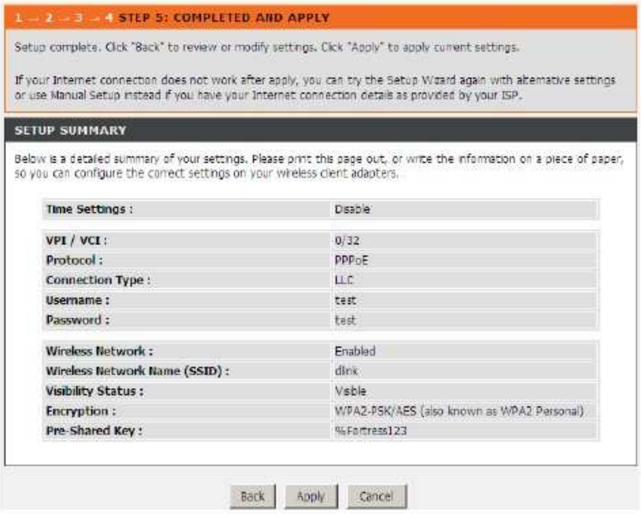
Now, please enter your wireless security key.

WPA2 Pre-Shared Key : %Fortress123&

(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 wirele connection.

The page shown in the right figure appears. In this page, you can view the configuration information. You can check weather the configurations match the information provided by your ISP.



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

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

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

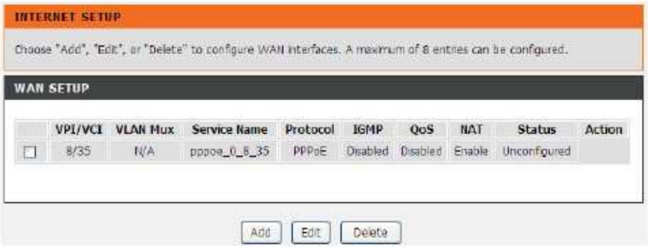
SETUP SUMMARY

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

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

4.3.2 Internet Setup

Choose Setup > Internet Setup. The page as shown in the right figure appears. In this page, you can configure the WAN interface of the device.



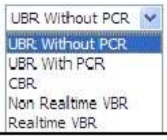
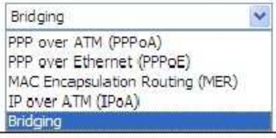
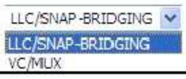
INTERNET SETUP

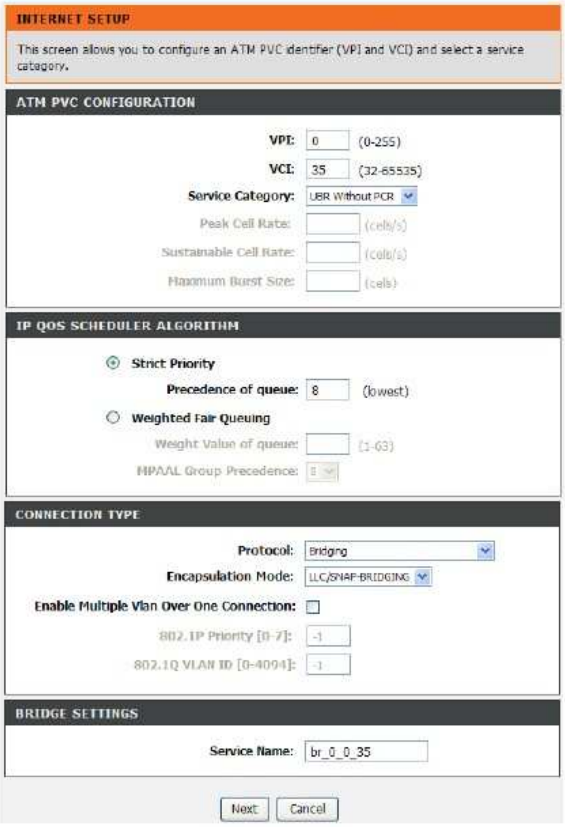
Choose "Add", "Edit", or "Delete" to configure WAN interfaces. A maximum of 8 entries can be configured.

WAN SETUP

	VPI/VCI	VLAN Mux	Service Name	Protocol	IGMP	QoS	NAT	Status	Action
□	8/35	N/A	pppoe_0_8_35	PPPoE	Disabled	Disabled	Enable	Unconfigured	

Click Add in “INTERNET SETUP”. The page shown in the following figure appears.

Field	Description
PVC Settings	● The virtual path between two points in an ATM network and its valid value is from 0 to 255. ● The virtual channel between two points in an ATM network, ranging from 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). You can select from the drop-down list.
Service Category	 UBR Without PCR UBR Without PCR UBR With PCR CBR Non Realtime VBR Realtime VBR
Protocol	You can select from the drop-down list.  Bridging PPP over ATM (PPPoA) PPP over Ethernet (PPPoE) MAC Encapsulation Routing (MER) IP over ATM (IPoA) Bridging
QoS scheduler	You can select one of the item between Strict Priority and Weighted Fair Queuing.
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select from the drop-down list.  LLC/SNAP-BRIDGING LLC/SNAP-BRIDGING VC/MUX



INTERNET SETUP

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

ATM PVC CONFIGURATION

VPI: 0 (0-255)

VCI: 35 (32-65535)

Service Category: UBR Without PCR

Peak Cell Rate: (cells/s)

Sustainable Cell Rate: (cells/s)

Maximum Burst Size: (cells)

IP QOS SCHEDULER ALGORITHM

● Strict Priority

Precedence of queue: 8 (lowest)

○ Weighted Fair Queuing

Weight Value of queue: (1-63)

MPAAL Group Precedence: 8

CONNECTION TYPE

Protocol: Bridging

Encapsulation Mode: LLC/SNAP-BRIDGING

Enable Multiple Vlan Over One Connection: □

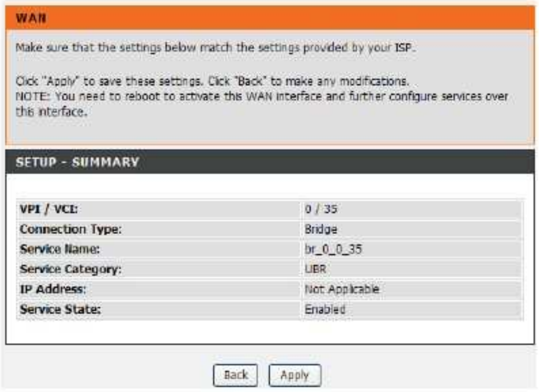
802.1P Priority [0-7]: -1

802.1Q VLAN ID [0-4094]: -1

BRIDGE SETTINGS

Service Name: br_0_0_35

Click Next, the page shown in the following figure appears.



WAN

Make sure that the settings below match the settings provided by your ISP.

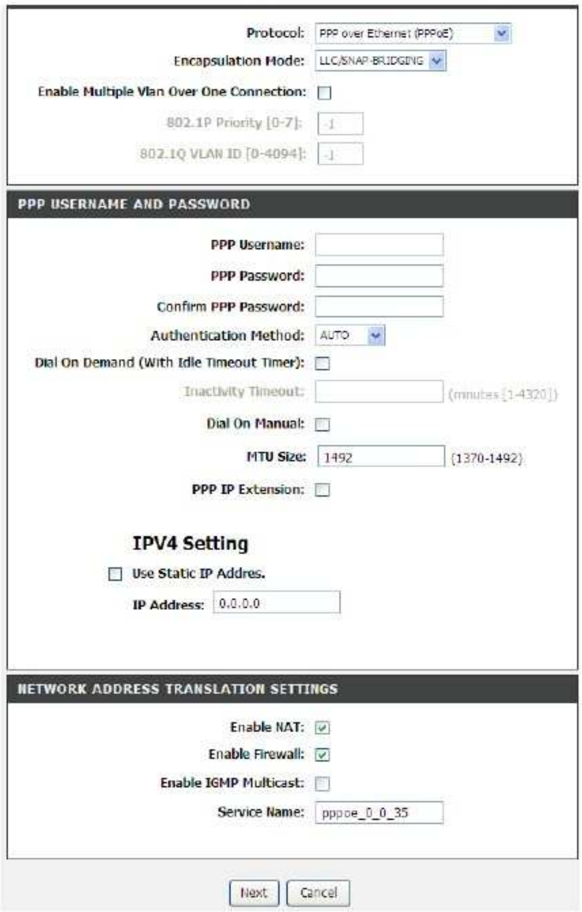
Click "Apply" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

SETUP - SUMMARY

VPI / VCI:	0 / 35
Connection Type:	Bridge
Service Name:	br_0_0_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled

If you select the PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) as the connection protocol, the following page appears.

- PPP Username: The correct user name that your ISP provides to you.
- PPP Password: The correct password that your ISP provides to you.
- Authentication Method: The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- Dial on demand (with idle timeout timer): If this function is enabled, 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 stops the PPPoE connection. Once it detects the flow (like access to a webpage), the router restarts the PPPoE dialup.
  If this function is disabled, the router performs PPPoE dial-up all the time. The PPPoE connnection does not stop, unless the router is powered off and DSLAM or uplink equipment is abnormal.
- MTU Size: Maximum Transmission Unit. Sometimes, you must modify this function to access network successfully.
- PPP IP extension: If this function is enabled, the WAN IP address obtained by the router through built-in dial-up can be directly assigned to the PC being attached to the router (at this time, the router connects to only one PC). From the aspect of the PC user, the PC dials up to obtain an IP addres. But actually, the dial-up is done by the router. If this function is disabled, the router itself obtains the WAN IP address.
- Use Static IP Address: If this function is disabled, the router obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up.
  If this function is enabled, the router uses this IP address as the WAN IP address.
- Enable NAT: Select it to enable the NAT functions of the router. If you do not want to enable NAT and wish the router user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.
- Enable Firewall: Enable or disable IP filtering.
- Enable IGMP Multicast: IGMP proxy. For example, if you wish that the PPPoE mode supports IPTV, enable this function.



Protocol: PPP over Ethernet (PPPoE)
Encapsulation Mode: LLC/SNAP-BRIDGING
Enable Multiple Vlan Over One Connection: □
802.1P Priority [0-7]: -1
802.1Q VLAN ID [0-4094]: -1

PPP USERNAME AND PASSWORD

PPP Username:
PPP Password:
Confirm PPP Password:
Authentication Method: AUTO
Dial On Demand (With Idle Timeout Timer): □
Inactivity Timeout: (minutes [1-4320])
Dial On Manual: □
MTU Size: 1492 (1370-1492)
PPP IP Extension: □

IPV4 Setting

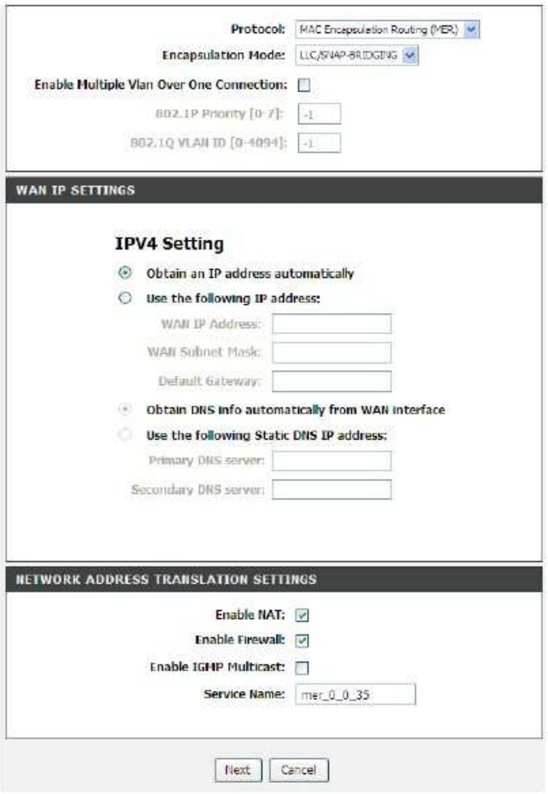
□ Use Static IP Addres.
IP Address: 0.0.0.0

NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT: ☑
Enable Firewall: ☑
Enable IGMP Multicast: □
Service Name: pppoe_0_0_35

If you select the MAC Encapsulation Routing(MER) as the connection protocol, the following page appears.

- Obtain an IP address automatically: The modem obtains a WAN IP address automatically and at this time it enables DHCP client functions. The WAN IP address is obtained from the uplink equipment like BAS and the uplink equipment is required to enable the DHCP server functions.
- Use the following IP address: If you want to manually enter the WAN IP address, select this check box and enter the information in the field.
- WAN IP Address: Enter the IP address of the WAN interface provided by your ISP.
- WAN Subnet Mask: Enter the subnet mask concerned to the IP address of the WAN interface provided by your ISP.
- Default Gateway: Enter the default gateway.
- Obtain DNS info automatically from WAN interface: You can get DNS server information from the selected WAN interface
- Use the following Static DNS IP address: If you want to manually enter the IP address of the DNS server, select this check box and enter the information in the fields.
- Primary DNS server: Enter the IP address of the primary DNS server.
- Secondary DNS server: Enter the IP address of the secondary DNS server provided by your ISP.



Protocol: MAC Encapsulation Routing (MER)
Encapsulation Mode: LLC/SNAP-BRIDGING
Enable Multiple Vlan Over One Connection: □
802.1P Priority [0-7]: -1
802.1Q VLAN ID [0-4094]: -1

WAN IP SETTINGS

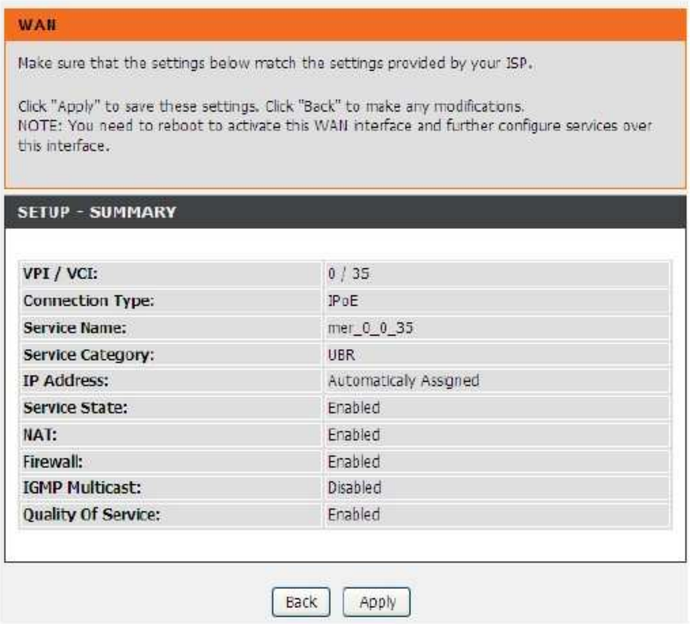
IPV4 Setting

● Obtain an IP address automatically
○ Use the following IP address:
WAN IP Address:
WAN Subnet Mask:
Default Gateway:
● Obtain DNS info automatically from WAN interface
○ Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:

NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT: ☑
Enable Firewall: ☑
Enable IGMP Multicast: □
Service Name: mer_0_0_35

After proper settings, click Next.



WAN

Make sure that the settings below match the settings provided by your ISP.

Click "Apply" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

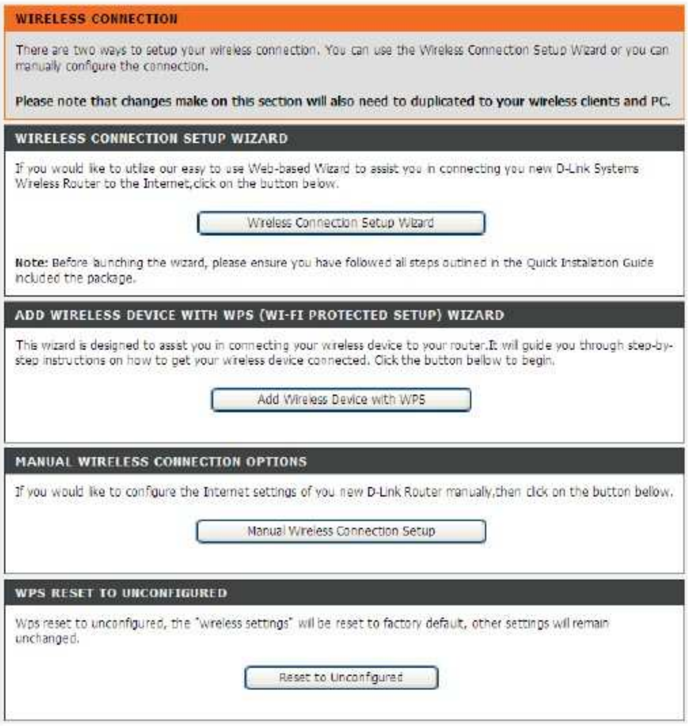
SETUP - SUMMARY

VPI / VCI:	0 / 35
Connection Type:	IPoE
Service Name:	mer_0_0_35
Service Category:	UBR
IP Address:	Automaticaly Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

4.3.3 Wireless Connection

This section includes the wireless connection setup wizard and WPS setup wizard. There are two ways to setup your wireless connection. You can use the Wireless Connection Setup Wizard or you can manually configure the connection.

Choose Setup > Wireless Connection. The Wireless Connection page shown in the following figure appears.



WIRELESS CONNECTION

There are two ways to setup your wireless connection. You can use the Wireless Connection Setup Wizard or you can manually configure the connection.

Please note that changes make on this section will also need to duplicated to your wireless clients and PC.

WIRELESS CONNECTION SETUP WIZARD

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting you new D-Link Systems Wireless Router to the Internet,click on the button below.

Note: Before launching the wizard, please ensure you have followed all steps outlined in the Quick Installation Guide included the package.

ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your router.It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button bellow to begin.

MANUAL WIRELESS CONNECTION OPTIONS

If you would like to configure the Internet settings of you new D-Link Router manually,then click on the button below.

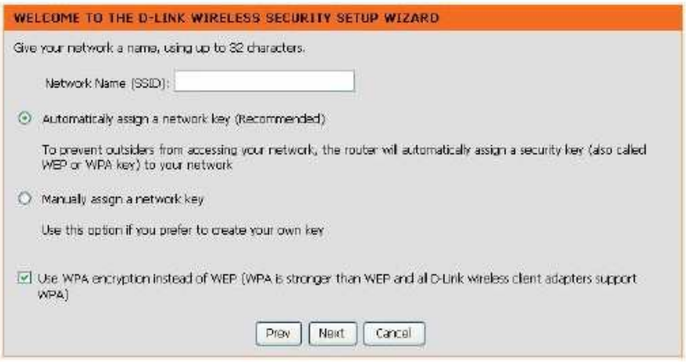
WPS RESET TO UNCONFIGURED

Wps reset to unconfigured, the "wireless settings" will be reset to factory default, other settings will remain unchanged.

Wireless Connection Setup Wizard
Add Wireless Device with WPS
Manual Wireless Connection Setup
Reset to Unconfigured

4.3.3.1 Wireless Wizard

In Wireless Connection page, Click “Wireless Connection Setup Wizard”, the page shown in the following figure appears.


WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Give your network a name, using up to 32 characters.

Network Name (SSID):

● Automatically assign a network key (Recommended)

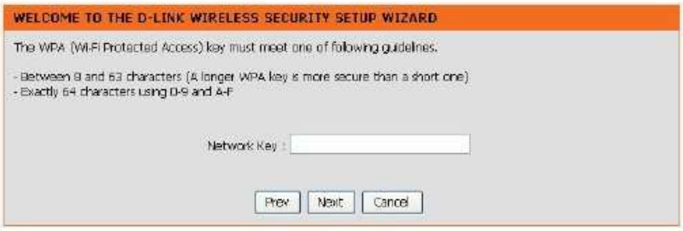
To prevent outsiders from accessing your network, the router will automatically assign a security key (also called WEP or WPA key) to your network

○ Manually assign a network key

Use this option if you prefer to create your own key

☑ Use WPA encryption instead of WEP (WPA is stronger than WEP and all D-Link wireless client adapters support WPA)

If you select “Use WPA encryption instead of WEP” and “Manually assign a network key”, click “Next”, the page shown in the following figure appears.

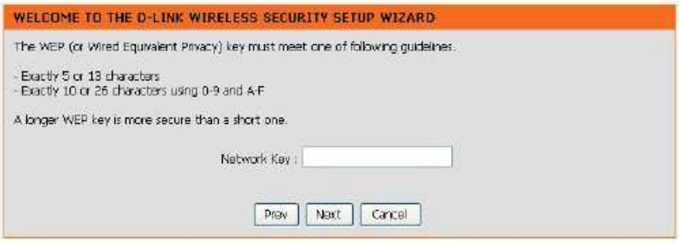

WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

The WPA (Wi-Fi Protected Access) key must meet one of following guidelines.

- Between 8 and 63 characters (A longer WPA key is more secure than a short one)
- Exactly 64 characters using 0-9 and A-F

Network Key :

If you only select “Manually assign a network key”, click “Next”, the page shown in the following figure appears.



WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

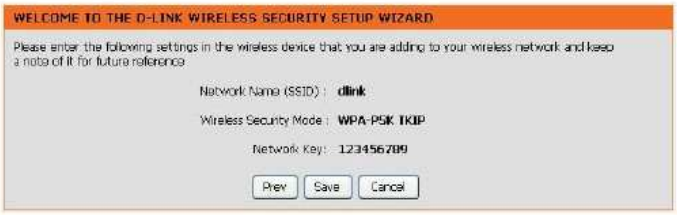
The WEP (or Wired Equivalent Privacy) key must meet one of following guidelines.

- Exactly 5 or 13 characters
- Exactly 10 or 26 characters using 0-9 and A-F

A longer WEP key is more secure than a short one.

Network Key :

After you enter the network key, the page shown in the following figure appears, you can confirm the wireless settings in this page.
Click Save to save the settings.



WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Please enter the following settings in the wireless device that you are adding to your wireless network and keep a note of it for future reference

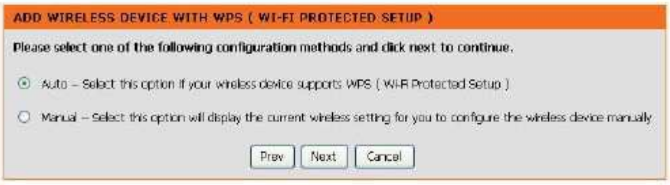
Network Name (SSID) : **dlink**

Wireless Security Mode : **WPA-PSK TKIP**

Network Key: **123456789**

4.3.3.2 Wireless Device Add

In Wireless Connection page, Click Add Wireless Device with WPS, the page shown in the following figure appears.



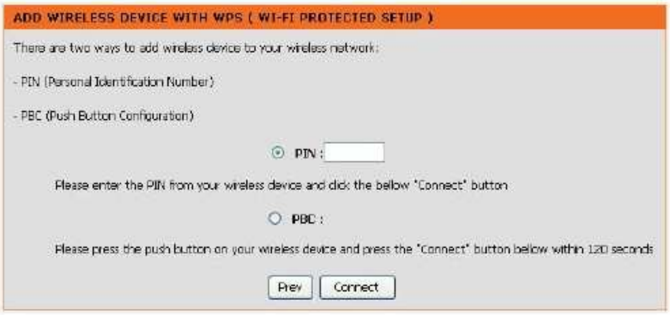
ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP)

Please select one of the following configuration methods and click next to continue.

● Auto – Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

○ Manual – Select this option will display the current wireless setting for you to configure the wireless device manually

Select Auto, click Next, the page shown in the following figure appears.
When PIN is used, users are only allowed to enter no more than eight digits in the field.



ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP)

There are two ways to add wireless device to your wireless network:

- PIN (Personal Identification Number)

- PBC (Push Button Configuration)

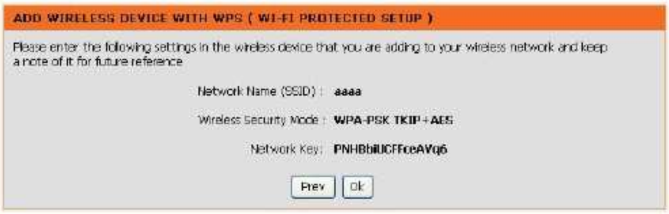
● PIN :

Please enter the PIN from your wireless device and click the bellow "Connect" button

○ PBC :

Please press the push button on your wireless device and press the "Connect" button bellow within 120 seconds

Select Manual, click Next, the page shown in the following figure appears.
It displays the current wireless settings and you can manually enter the settings in the wireless device that's to be added in the wireless network.



ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP)

Please enter the following settings in the wireless device that you are adding to your wireless network and keep a note of it for future reference

Network Name (SSID) : aaaa

Wireless Security Mode : WPA-PSK TKIP+AES

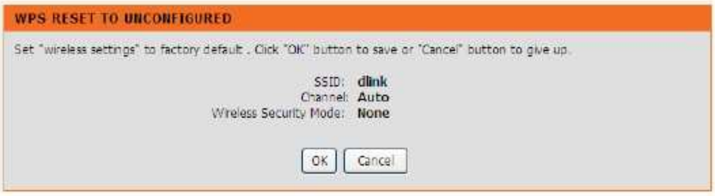
Network Key: PNHBbiUCFFceAVq6

4.3.3.3 Manual Wireless Setup

If you want to configure the Internet settings of you new D-Link Router manually, click Manual Wireless Connection Setup. It will redirect to 4.4.1 Wireless Settings.

4.3.3.4 WPS Reset to Unconfigured

In Wireless Connection page, Click Reset to Unconfigured, the page shown in the following figure appears.
Once the “Reset to Unconfigured” button is clicked, the “wireless settings” will be reset to factory default, other settings will remain unchanged.



WPS RESET TO UNCONFIGURED

Set "wireless settings" to factory default . Click "OK" button to save or "Cancel" button to give up.

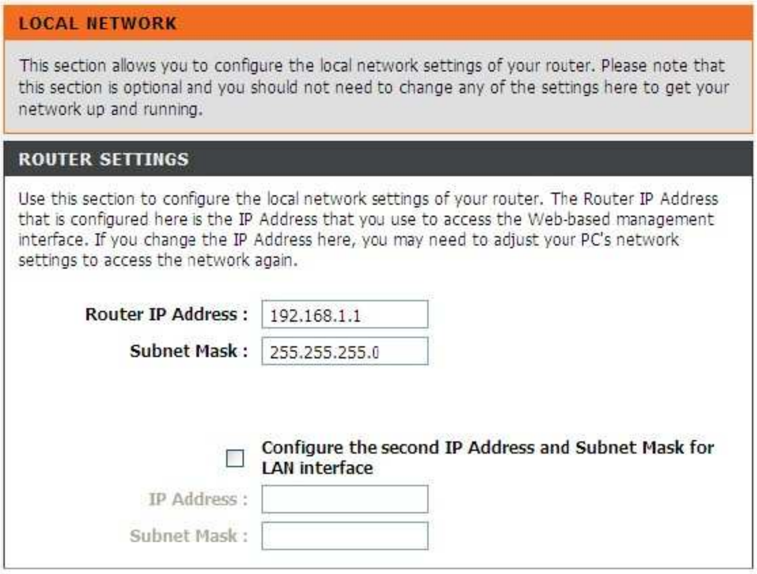
SSID: dlink
Channel: Auto
Wireless Security Mode: None

4.3.4 Local Network

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

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

Choose Setup > Local Network. The Local Network page shown in the following figure appears.



LOCAL NETWORK

This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

ROUTER SETTINGS

Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address : 192.168.1.1

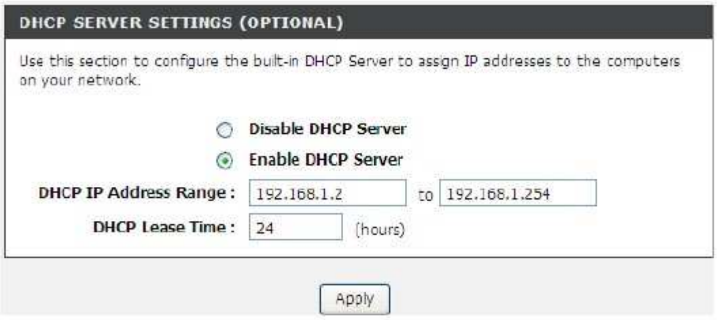
Subnet Mask : 255.255.255.0

□ Configure the second IP Address and Subnet Mask for LAN interface

IP Address :

Subnet Mask :

By default, Enable DHCP Server is selected for the Ethernet LAN interface of the device. DHCP service supplys IP settings to workstations configured to automatically obtain IP settings that are connected to the device through the Ethernet port. When the device is used for DHCP, it becomes the default gateway for DHCP client connected to it. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.
Click Apply to save the settings.

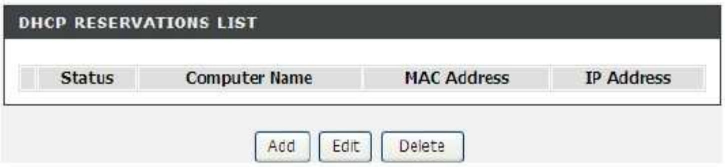

DHCP SERVER SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

○ Disable DHCP Server
● Enable DHCP Server

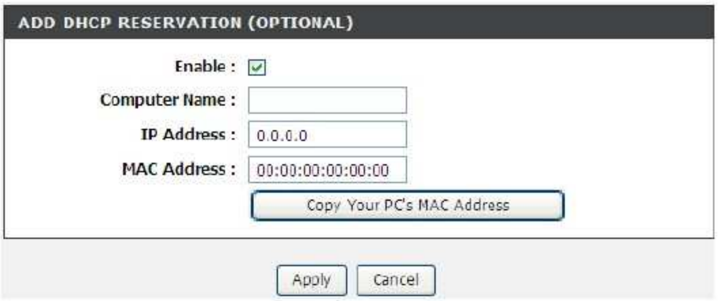
DHCP IP Address Range : 192.168.1.2 to 192.168.1.254
DHCP Lease Time : 24 (hours)

In the Local Network page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.


DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address

Click Add to add static DHCP (optional). The page shown in the following figure appears.
Select Enable to reserve the IP address for the designated PC with the configured MAC address.
The Computer Name helps you to recognize the PC with the MAC address. For example, Father's Laptop.
Click Apply to save the settings.
After the DHCP reservation is saved, the DHCP reservations list displays the configuration.
If the DHCP reservations list table is not empty, you can select one or more items and click Edit or Delete.


ADD DHCP RESERVATION (OPTIONAL)

Enable : ☑
Computer Name :
IP Address : 0.0.0.0
MAC Address : 00:00:00:00:00:00

4.3.5 Time and Date

Choose Setup > Time and Date. The page shown in the following figure appears.

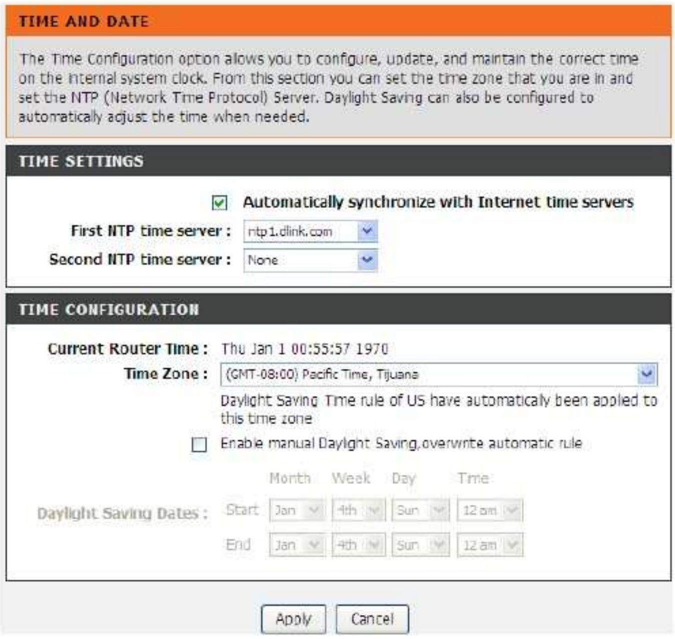
In the Time and Date page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

Select Automatically synchronize with Internet time servers.

Select the specific time server and the time zone from the corresponding drop-down lists.

Select Enable manual Daylight Saving,overwrite automatic rule if necessary. Set the daylight as you want.

Click Apply to save the settings.



TIME AND DATE

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.

TIME SETTINGS

☑ Automatically synchronize with Internet time servers

First NTP time server : ntp1.dlink.com

Second NTP time server : None

TIME CONFIGURATION

Current Router Time : Thu Jan 1 00:55:57 1970

Time Zone : (GMT-08:00) Pacific Time, Tijuana

Daylight Saving Time rule of US have automaticaly been applied to this time zone

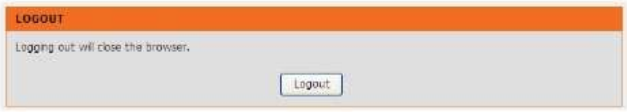
☐ Enable manual Daylight Saving,overwrite automatic rule

Daylight Saving Dates :

	Month	Week	Day	Time
Start	Jan	4th	Sun	12 am
End	Jan	4th	Sun	12 am

4.3.6 Logout

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



LOGOUT

Logging out will close the browser.

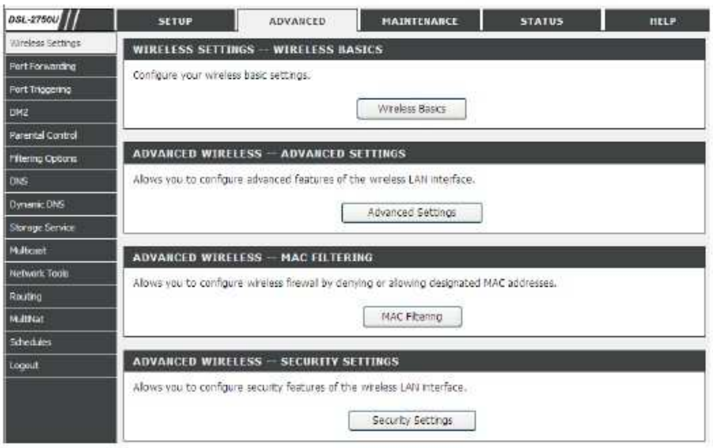
4.4 Advanced

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

4.4.1 Wireless Settings

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

Choose ADVANCED > Wireless Settings. The page shown in the following figure appears.



WIRELESS SETTINGS -- WIRELESS BASICS

Configure your wireless basic settings.

ADVANCED WIRELESS -- ADVANCED SETTINGS

Allows you to configure advanced features of the wireless LAN interface.

ADVANCED WIRELESS -- MAC FILTERING

Allows you to configure wireless firewall by denying or allowing designated MAC addresses.

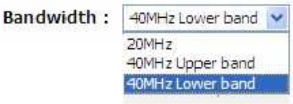
ADVANCED WIRELESS -- SECURITY SETTINGS

Allows you to configure security features of the wireless LAN interface.

4.4.1.1 Wireless Basics

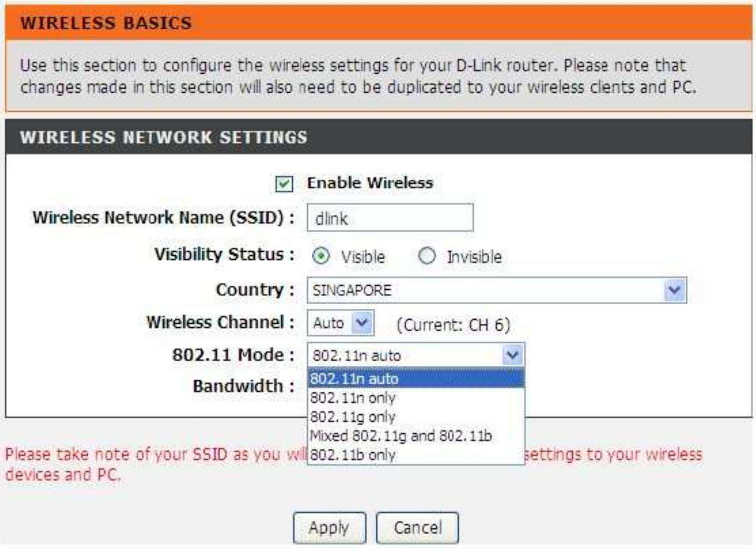
In the Wireless Settings page, click Wireless Basic, the page shown in the following figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.

- Enable Wireless: Select this to turn Wi-Fi on and off.
- Wireless Network Name (SSID): The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.
- Visibility Status: You can select Visible or Invisible.
- Country: Select the country from the drop-down list.
- Wireless Channel: Select the wireless channel from the pull-down menu. It is different for different countries.
- 802.11 Mode: Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are 802.11n auto, 802.11g only, Mixed 802.11g and 802.11b, or 802.11b only.
- Bandwidth: You can select it from the drop-down list:



Bandwidth : 40MHz Lower band

Click Apply to save the settings.



WIRELESS BASICS

Use this section to configure the wireless settings for your D-Link router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

WIRELESS NETWORK SETTINGS

☑ Enable Wireless

Wireless Network Name (SSID) : dlink

Visibility Status : ● Visible ○ Invisible

Country : SINGAPORE

Wireless Channel : Auto (Current: CH 6)

802.11 Mode : 802.11n auto

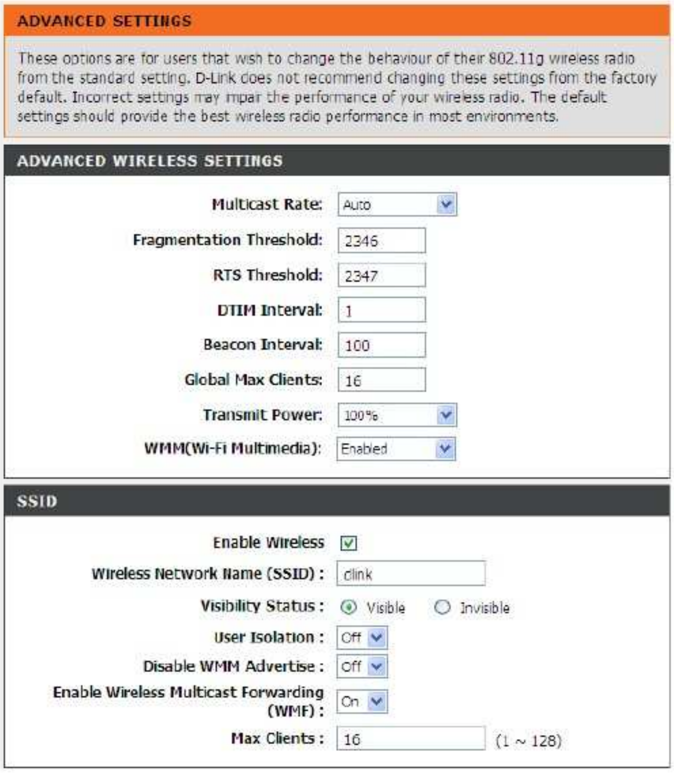
Bandwidth :

Please take note of your SSID as you wil settings to your wireless devices and PC.

4.4.1.2 Advanced Settings

In the Wireless Settings page, click Advanced settings, the page shown in the following figure appears.

- Multicast Rate: Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.
- Fragmentation Threshold: Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reducing networking performance.
- RTS Threshold: This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347 is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- DTIM Interval: (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- Beacon Interval: A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- Global Max Clients: Specifies maximum wireless client stations to be enble to link with AP. Once the clients exceed the max vlaue, all other clients will be refused.



ADVANCED SETTINGS

These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. D-Link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

ADVANCED WIRELESS SETTINGS

Multicast Rate: Auto
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 16
Transmit Power: 100%
WMM(Wi-Fi Multimedia): Enabled

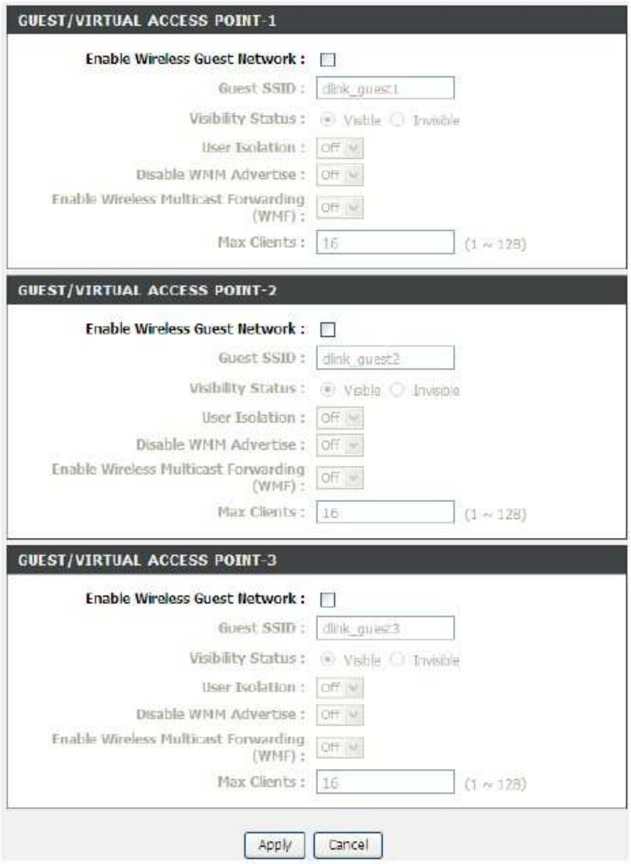
SSID

Enable Wireless ☑
Wireless Network Name (SSID) : clink
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
Disable WMM Advertise : Off
Enable Wireless Multicast Forwarding (WMF) : On
Max Clients : 16 (1 ~ 128)

- Transmit Power: Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
- WMM (Wi-Fi Multimedia): Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes related to wireless do not take effect.
- Enable Wireless: Select this to turn Wi-Fi on and off.
- Wireless Network Name (SSID): The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.
- Visibility Status: You can select Visible or Invisible.
- User Isolation: When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can select On to enable this service.
- Disable WMM Advertise: You can select On or Off from the drop-down list.
- Enable Wireless Multicast Forwarding (WMF): You can select On or Off from the drop-down list.
- Max Clients: Specifies maximum wireless client stations to be enble to link with AP.
- GUEST/VIRTUAL ACCESS POINT: If you want to make Guest/Virtual network function be available, you can set the parameters below.

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

Click Apply to save the settings.



GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network : □
Guest SSID : dlink_guest1
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
Disable WMM Advertise : Off
Enable Wireless Multicast Forwarding (WMF) : Off
Max Clients : 16 (1 ~ 128)

GUEST/VIRTUAL ACCESS POINT-2

Enable Wireless Guest Network : □
Guest SSID : dlink_guest2
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
Disable WMM Advertise : Off
Enable Wireless Multicast Forwarding (WMF) : Off
Max Clients : 16 (1 ~ 128)

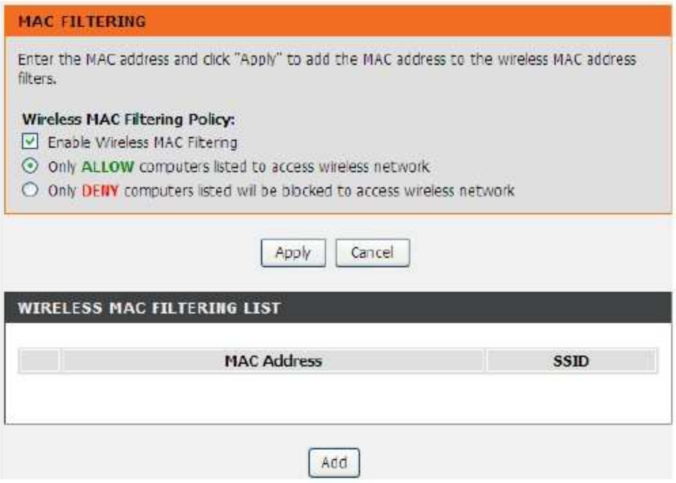
GUEST/VIRTUAL ACCESS POINT-3

Enable Wireless Guest Network : □
Guest SSID : dlink_guest3
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
Disable WMM Advertise : Off
Enable Wireless Multicast Forwarding (WMF) : Off
Max Clients : 16 (1 ~ 128)

4.4.1.3 MAC Filtering

In the Wireless Settings page, click MAC Filtering, the page shown in the following figure appears.

In this page, you can allow or deny users access the wireless router based on their MAC address.



MAC FILTERING

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

Wireless MAC Filtering Policy:

☑ Enable Wireless MAC Filtering

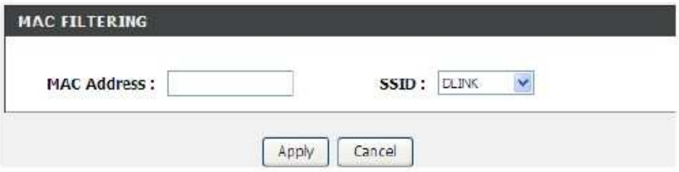
● Only ALLOW computers listed to access wireless network

○ Only DENY computers listed will be blocked to access wireless network

WIRELESS MAC FILTERING LIST

	MAC Address	SSID

Click Add, the page shown in the following figure appears.



MAC FILTERING

MAC Address :

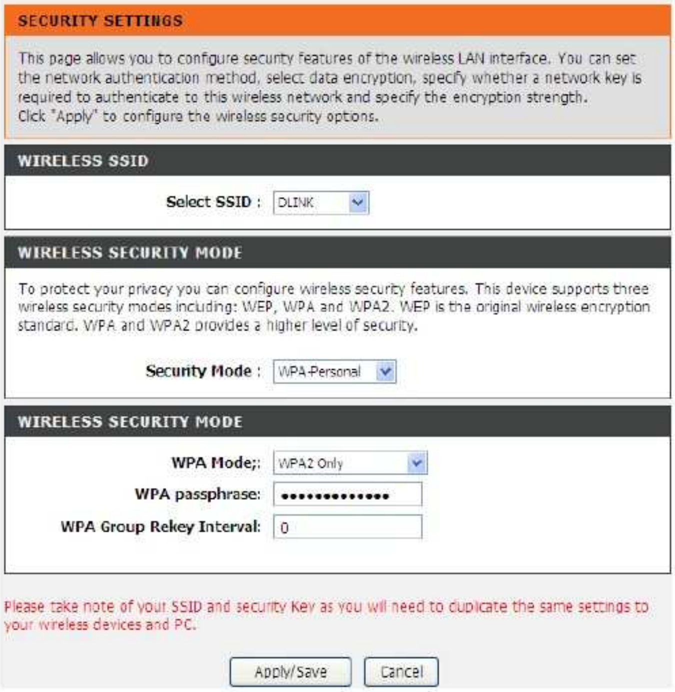
SSID : DLINK

4.4.1.4 Security Settings

In the Wireless Settings page, click Security Settings. The page shown in the following figure appears.

Select the SSID that you want to configure from the drop-down list.

Select the encryption type from the Security Mode drop-down list.You can select None, WEP, WPA-Personal and WPA-Enterprise.



SECURITY SETTINGS

This page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

WIRELESS SSID

Select SSID : DLINK

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : WPA-Personal

WIRELESS SECURITY MODE

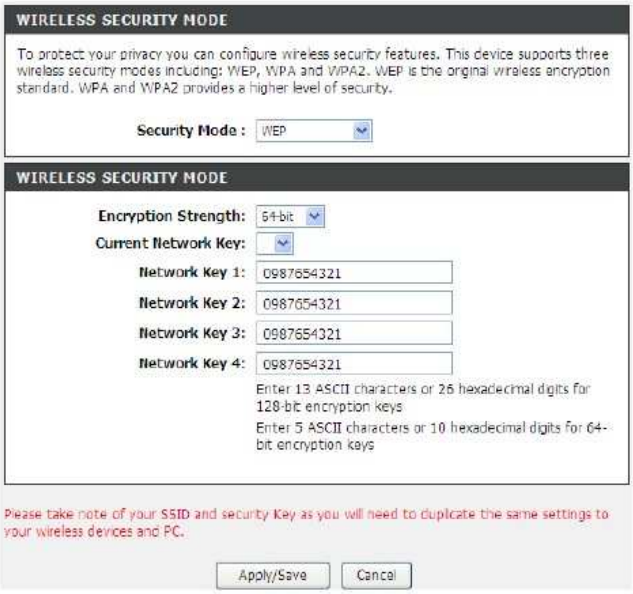
WPA Mode;: WPA2 Only

WPA passphrase: •••••••••••••

WPA Group Rekey Interval: 0

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

If you select WEP, the page shown in the following figure appears.
WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys.
The router offers 64 or 128 bit encryption with four keys available.
Select Encryption Strength from the drop-down menu. (128 bit is stronger than 64 bit)
Enter the key into the Network Key field 1~4. (Key length is outlined at the bottom of the window.)
Click Apply/Save to save the settings.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

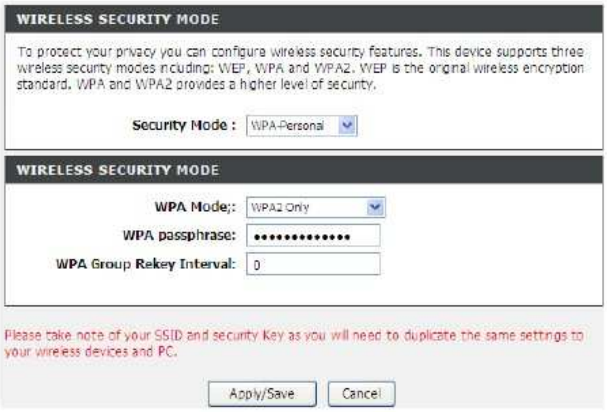
Security Mode : WEP

WIRELESS SECURITY MODE

Encryption Strength: 64-bit
Current Network Key:
Network Key 1: 0987654321
Network Key 2: 0987654321
Network Key 3: 0987654321
Network Key 4: 0987654321
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

If you select WPA-Personal, the page shown in the following figure appears.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : WPA-Personal

WIRELESS SECURITY MODE

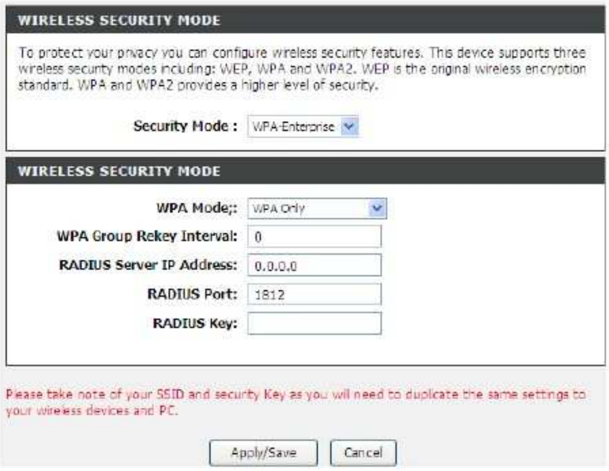
WPA Mode;: WPA2 Only

WPA passphrase: •••••••••••••

WPA Group Rekey Interval: 0

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

If you select WPA- Enterprise, the page shown in the following figure appears. You can only use WPA-enterprise if you have set up RADIUS server. This is the WPA/WPA2 authentication with RADIUS server instead of pre-shared key.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : WPA-Enterprise

WIRELESS SECURITY MODE

WPA Mode;: WPA Only

WPA Group Rekey Interval: 0

RADIUS Server IP Address: 0.0.0.0

RADIUS Port: 1812

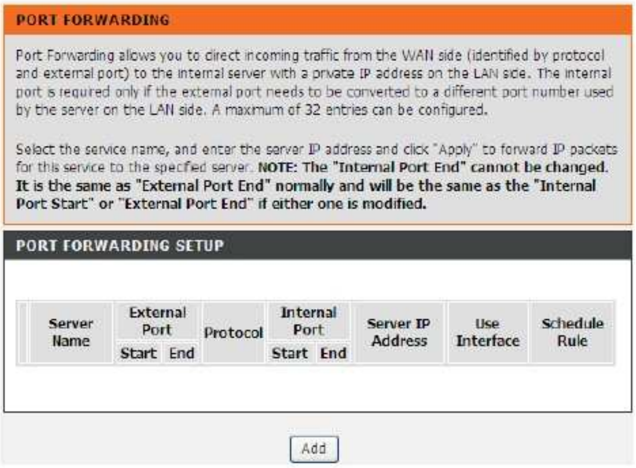
RADIUS Key:

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

4.4.2 Port Forwarding

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

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



PORT FORWARDING

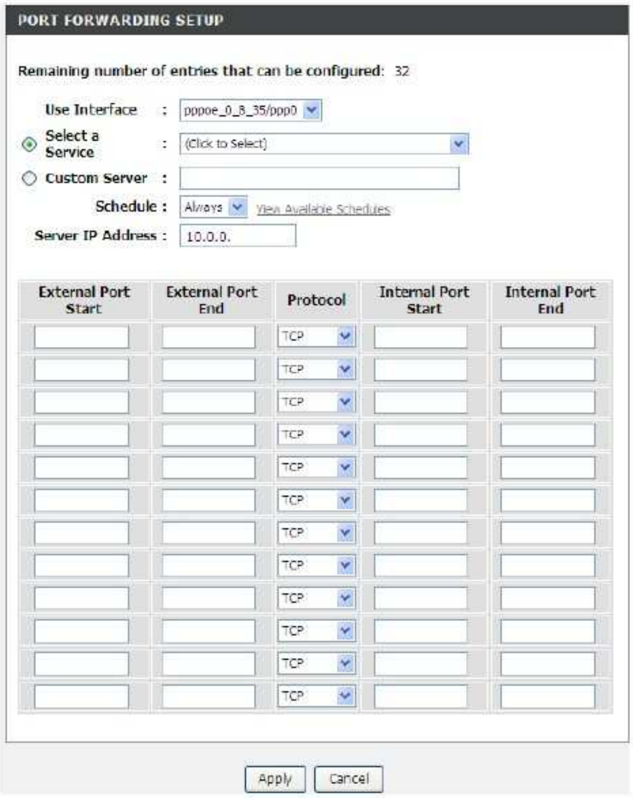
Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**

PORT FORWARDING SETUP

	Server Name	External Port		Protocol	Internal Port		Server IP Address	Use Interface	Schedule Rule
		Start	End		Start	End			

Click Add to add a virtual server.
Select a service for a preset application, or enter a name in the Custom Server field.
Enter an IP address in the Server IP Address field, to appoint the corresponding PC to receive forwarded packets.
The Ports show the ports that you want to open on the device. The TCP/UDP means the protocol type of the opened ports.



PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

Use Interface : pppoe_0_8_35/ppp0

● Select a Service : (Click to Select)

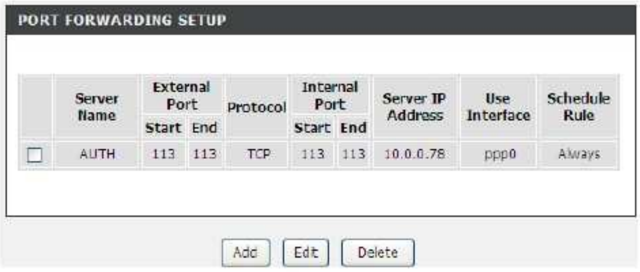
○ Custom Server :

Schedule : Always View Available Schedules

Server IP Address : 10.0.0.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Click Apply to save the settings. The page shown in the following figure appears. A virtual server is added.

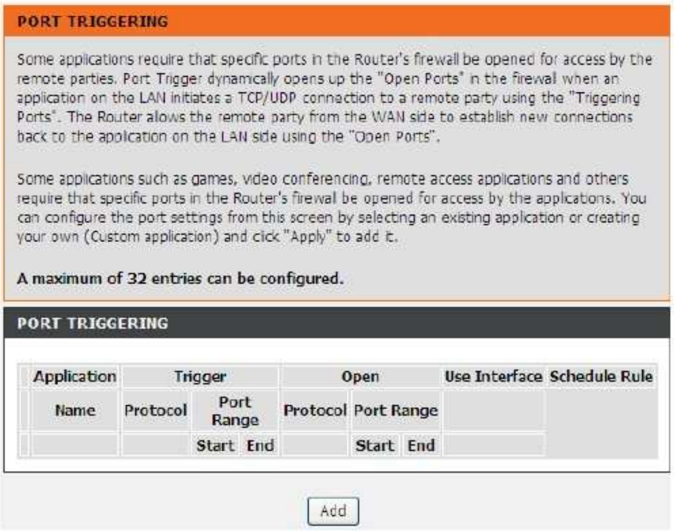


PORT FORWARDING SETUP

	Server Name	External Port		Protocol	Internal Port		Server IP Address	Use Interface	Schedule Rule
		Start	End		Start	End			
□	AUTH	113	113	TCP	113	113	10.0.0.78	ppp0	Always

4.4.3 Port Triggering

Some applications require that specific ports in the firewall of the device are open for the remote parties to access. Application rules dynamically open the firewall ports when an application on the LAN initiates a TCP/UDP connection to a remote party using the trigger ports. The device allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the firewall ports. A maximum of 32 entries can be configured. Choose ADVANCED > Port Triggering. The page shown in the following figure appears.



PORT TRIGGERING

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 "Open Ports" in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the "Triggering Ports". The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the "Open Ports".

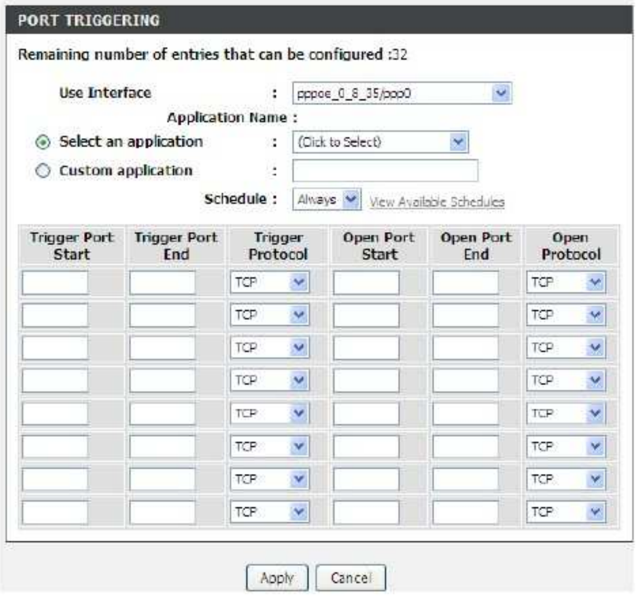
Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Apply" to add it.

A maximum of 32 entries can be configured.

PORT TRIGGERING

Application	Trigger			Open			Use Interface	Schedule Rule
Name	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

Click Add to add a new Port Trigger.
Click the Select an application drop-down menu to choose the application you want to setup for port triggering. When you have chosen an application the default Trigger settings will populate the table below.
If the application you want to setup isn't listed, click the Custom application radio button and type in a name for the trigger in the Custom application field.
Configure the Trigger Port Start, Trigger Port End, Trigger Protocol, Open Port Start, Open Port End and Open Protocol settings for the port trigger you want to configure.
When you have finished click the Apply button.



PORT TRIGGERING

Remaining number of entries that can be configured :32

Use Interface : pppoe_0_8_35/ppp0

Application Name :

● Select an application : (Click to Select)

○ Custom application :

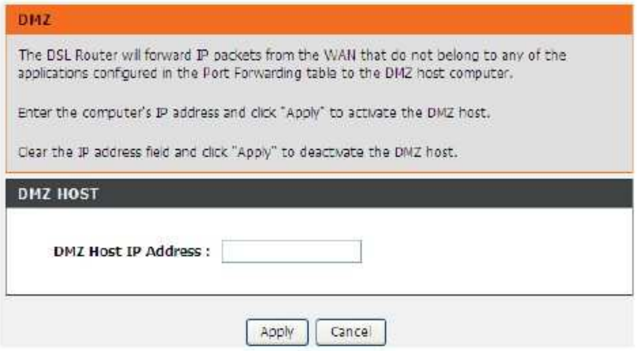
Schedule : Always View Available Schedules

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

4.4.4 DMZ

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. Click Apply to save the settings.



DMZ

The DSL Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

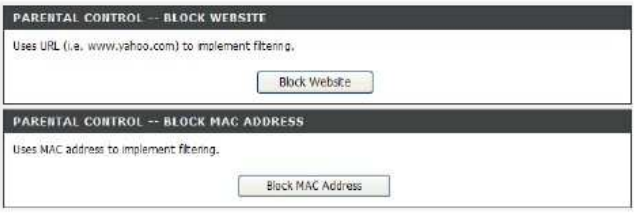
DMZ HOST

DMZ Host IP Address :

4.4.5 Parental Control

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

This page provides two useful tools for restricting the Internet access. Block Websites allows you to quickly create a list of all websites that you wish to stop users from accessing. Block MAC Address allows you to control when clients or PCs connected to the device are allowed to access the Internet.



PARENTAL CONTROL -- BLOCK WEBSITE

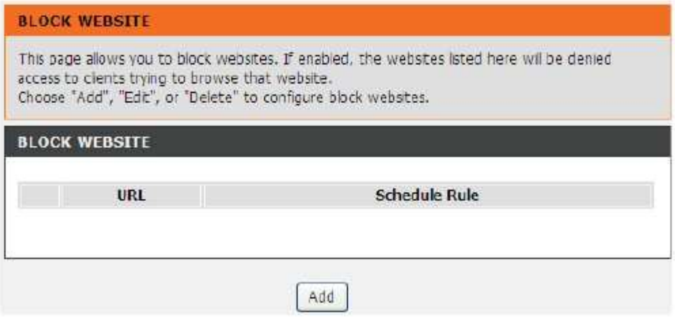
Uses URL (i.e. www.yahoo.com) to implement filtering.

PARENTAL CONTROL -- BLOCK MAC ADDRESS

Uses MAC address to implement filtering.

4.4.5.1 Block Website

In the Parent Control page, click Block Website. The page shown in the following figure appears.



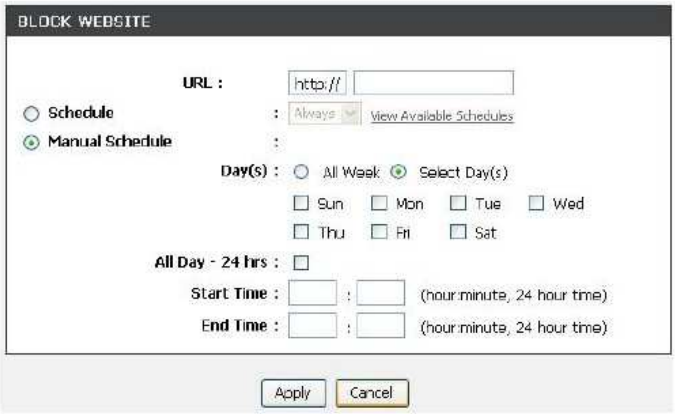
BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.
Choose "Add", "Edit", or "Delete" to configure block websites.

BLOCK WEBSITE

	URL	Schedule Rule

Click Add. The page shown in the following page appears.
Enter the website in the URL field. Select the Schedule from drop-down list, or select Manual Schedule and select the corresponding time and days.



BLOCK WEBSITE

URL : http://

○ Schedule : Always View Available Schedules

● Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

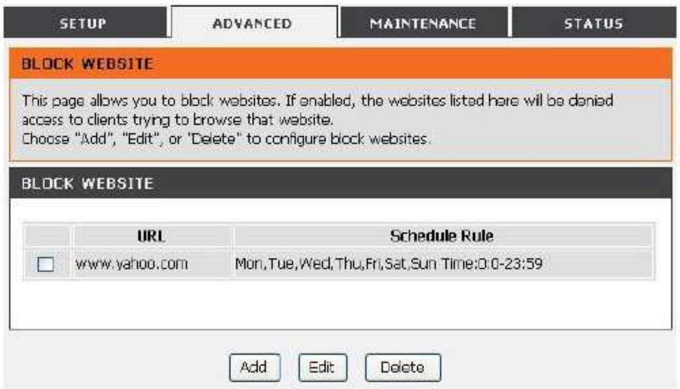
□ Sun □ Mon □ Tue □ Wed
□ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Click Apply to add the website to the BLOCK WEBSITE table.The page shown in the following figure appears.



BLOCK WEBSITE

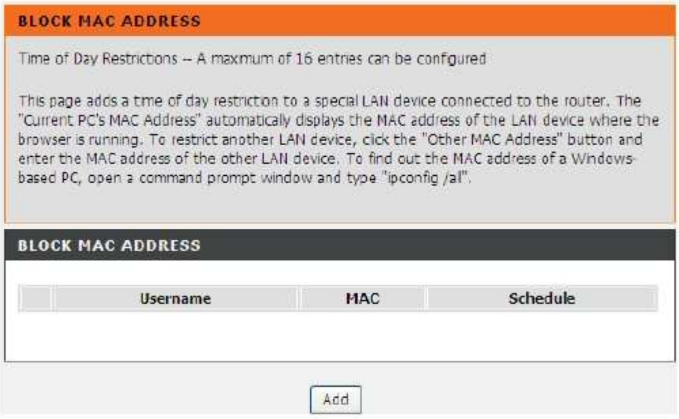
This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.
Choose "Add", "Edit", or "Delete" to configure block websites.

BLOCK WEBSITE

	URL	Schedule Rule
□	www.yahoo.com	Mon,Tue,Wed,Thu,Fri,Sat,Sun Time:0:0-23:59

4.4.5.2 Block MAC Address

In the Parent Control page, click Block MAC Address. The page shown in the following figure appears.



BLOCK MAC ADDRESS

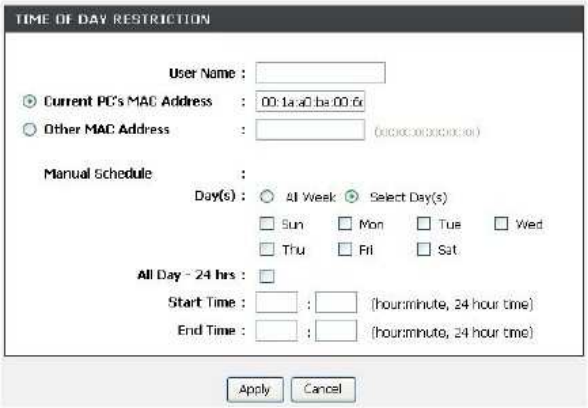
Time of Day Restrictions -- A maxmum of 16 entries can be confgured

This page adds a tme of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".

BLOCK MAC ADDRESS

	Username	MAC	Schedule

Click Add. The page shown in the following figure appears.
Enter the use name and MAC address and select the corresponding time and days.



User Name :

● Current PC's MAC Address : 00:1a:a0:ba:00:6c

○ Other MAC Address : (xx:xx:xx:xx:xx:xx)

Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

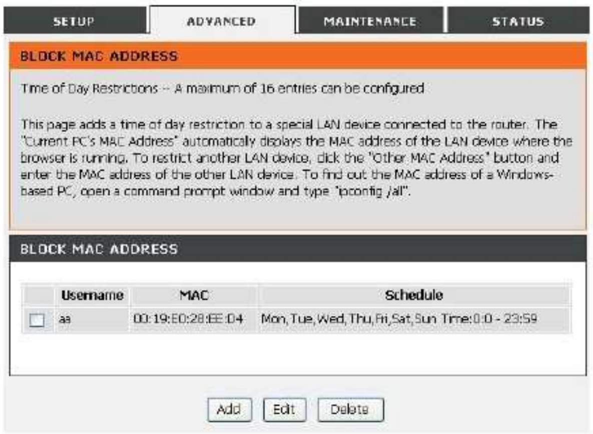
□ Sun □ Mon □ Tue □ Wed
□ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Click Apply to add the MAC address to the BLOCK MAC ADDRESS table. The page shown in the following figure appears.



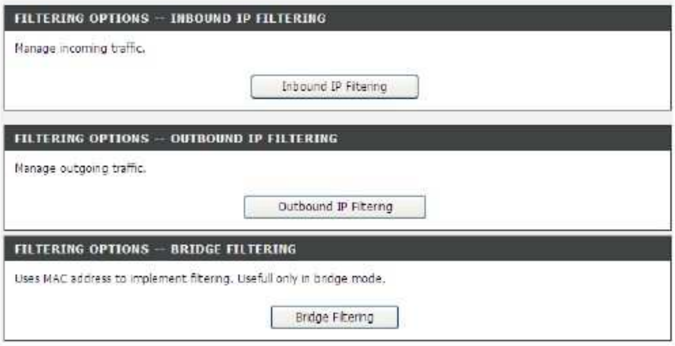
Time of Day Restrictions -- A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automaticaly displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".

	Username	MAC	Schedule
□	aa	00:19:E0:28:EE:04	Mon,Tue,Wed,Thu,Fri,Sat,Sun Time:0:0 - 23:59

4.4.6 Filtering Options

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



FILTERING OPTIONS -- INBOUND IP FILTERING

Manage incoming traffic.

FILTERING OPTIONS -- OUTBOUND IP FILTERING

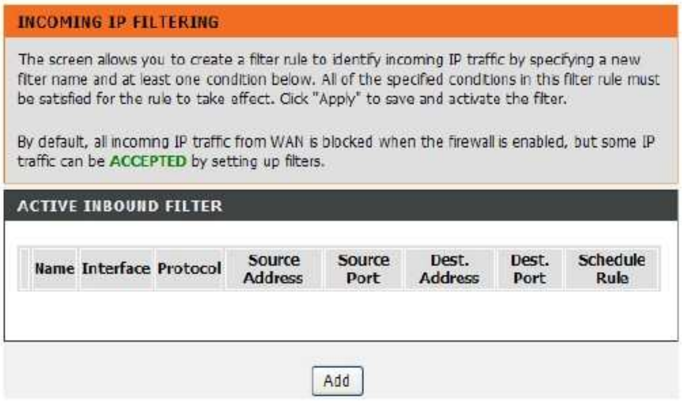
Manage outgoing traffic.

FILTERING OPTIONS -- BRIDGE FILTERING

Uses MAC address to implement filtering. Usefull only in bridge mode.

4.4.6.1 Inbound IP Filtering

In the Filtering Options page, click Inbound IP Filtering. The page shown in the following figure appears.



INCOMING IP FILTERING

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take affect. Click "Apply" to save and activate the filter.

By default, all incoming IP traffic from WAN is blocked when the firewall is enabled, but some IP traffic can be ACCEPTED by setting up filters.

ACTIVE INBOUND FILTER

Name	Interface	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

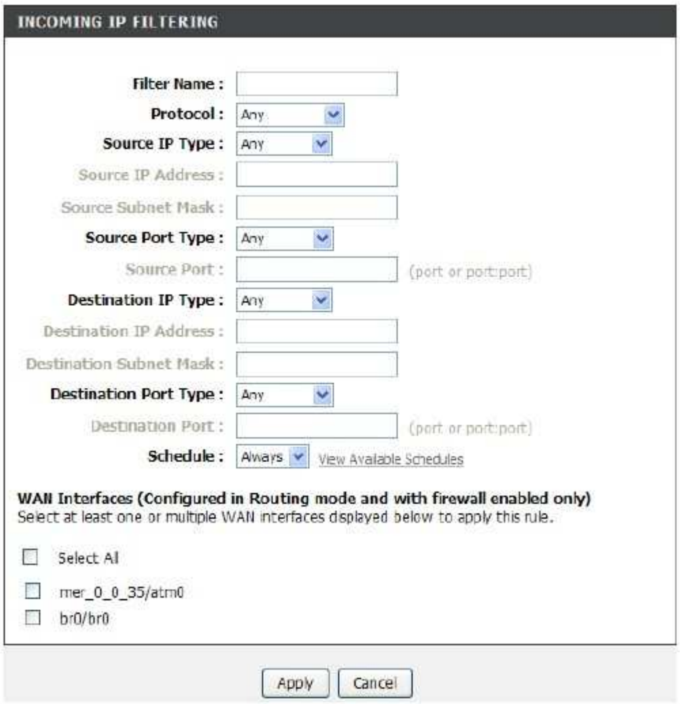
Click Add to add an inbound IP filter. The page shown in the following figure appears.

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

Click Apply to save the settings.

The ACTIVE INBOUND FILTER shows detailed information about each created inbound IP filter.

Note:
The settings only apply when the firewall is enabled.



INCOMING IP FILTERING

Filter Name :

Protocol : Any

Source IP Type : Any

Source IP Address :

Source Subnet Mask :

Source Port Type : Any

Source Port : (port or port:port)

Destination IP Type : Any

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any

Destination Port : (port or port:port)

Schedule : Always View Available Schedules

WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

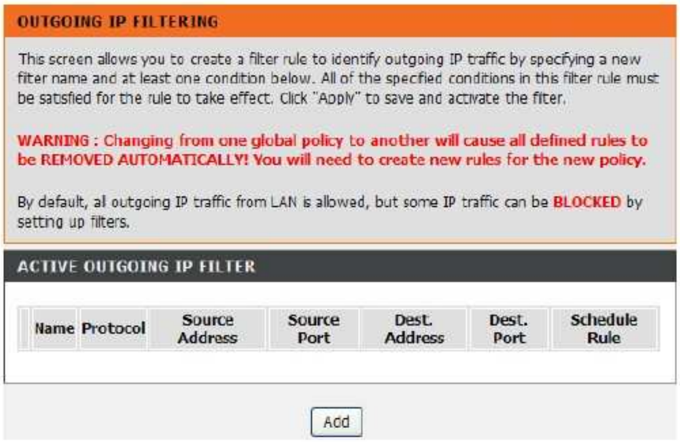
□ Select All

□ mer_0_0_35/atm0
□ br0/br0

4.4.6.2 Outbound IP Filtering

By default, all outgoing IP traffic from the LAN is allowed. The outbound filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one condition.

In the Filtering Options page, click Outbound IP Filtering. The page shown in the following figure appears.



OUTGOING IP FILTERING

This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

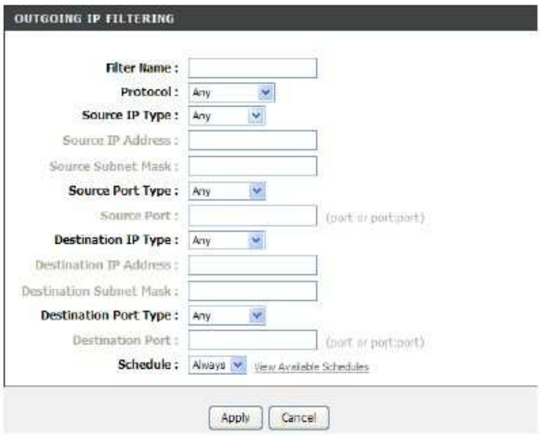
ACTIVE OUTGOING IP FILTER

Name	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

Click Add to add an outbound IP filter. The page shown in the following figure appears.

Enter the Filter Name and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port. Click Apply to save the settings.

The ACTIVE OUTGOING IP FILTER shows detailed information about each created outbound IP filter.

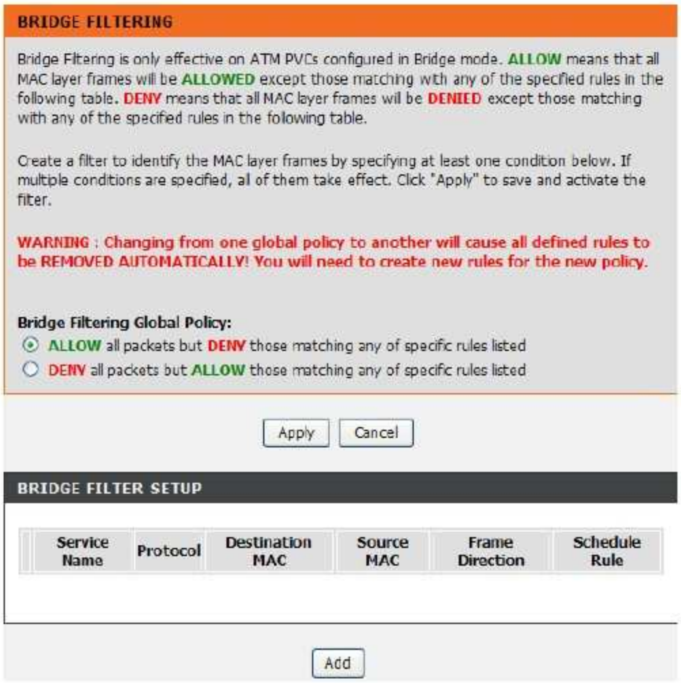


OUTGOING IP FILTERING

Filter Name :	
Protocol :	Any
Source IP Type :	Any
Source IP Address :	
Source Subnet Mask :	
Source Port Type :	Any
Source Port :	(port or port:port)
Destination IP Type :	Any
Destination IP Address :	
Destination Subnet Mask :	
Destination Port Type :	Any
Destination Port :	(port or port:port)
Schedule :	Always View Available Schedules

4.4.6.3 Bridge Filtering

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



BRIDGE FILTERING

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. ALLOW means that all MAC layer frames will be ALLOWED except those matching with any of the specified rules in the following table. DENY means that all MAC layer frames will be DENIED except those matching with any of the specified rules in the following table.

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Bridge Filtering Global Policy:

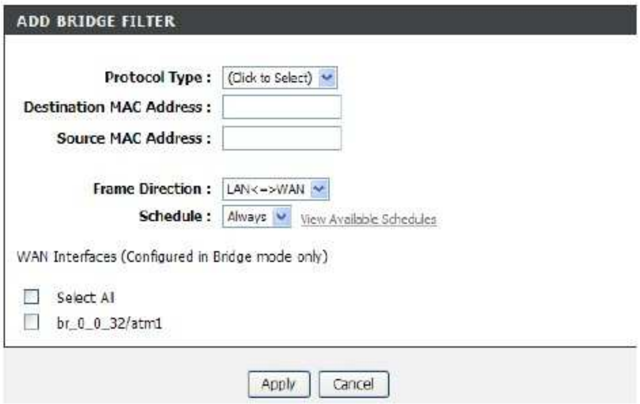
● ALLOW all packets but DENY those matching any of specific rules listed

○ DENY all packets but ALLOW those matching any of specific rules listed

BRIDGE FILTER SETUP

Service Name	Protocol	Destination MAC	Source MAC	Frame Direction	Schedule Rule

Click Add to add a bridge filter. The page shown in the following figure appears.
Click Apply to save the settings.



ADD BRIDGE FILTER

Protocol Type : (Click to Select)

Destination MAC Address :

Source MAC Address :

Frame Direction : LAN<=>WAN

Schedule : Always View Available Schedules

WAN Interfaces (Configured in Bridge mode only)

□ Select Al

□ br_0_0_32/atm1

4.4.7 DNS

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

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

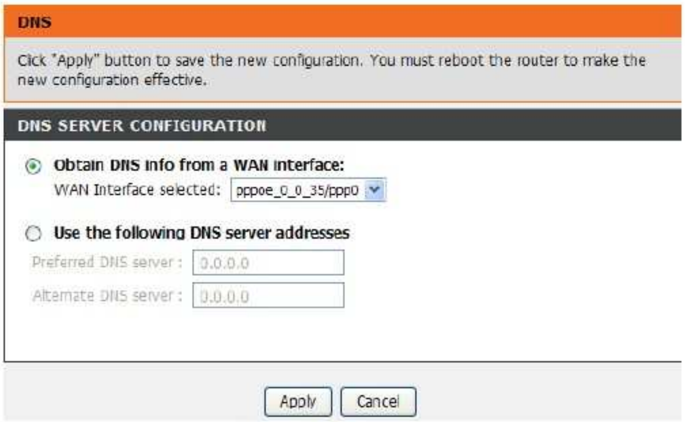
Choose ADVANCED > DNS. The page shown in the folllowin g figure appears.

DNS SERVER CONFIGURATION

If you are using the device for DHCP service on the LAN or if you are using DNS servers on the ISP network, select Obtain DNS Info from a WAN interface.

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

Click Apply to save the settings.



DNS

Click "Apply" button to save the new configuration. You must reboot the router to make the new configuration effective.

DNS SERVER CONFIGURATION

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoe_0_0_35/ppp0

○ Use the following DNS server addresses

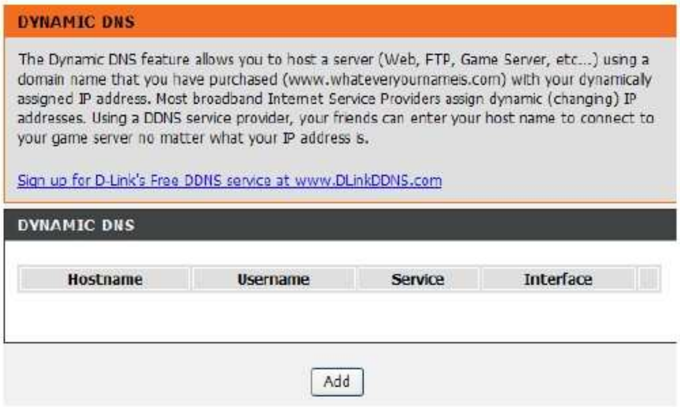
Preferred DNS server : 0.0.0.0

Alternate DNS server : 0.0.0.0

4.4.8 Dynamic DNS

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

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



DYNAMIC DNS

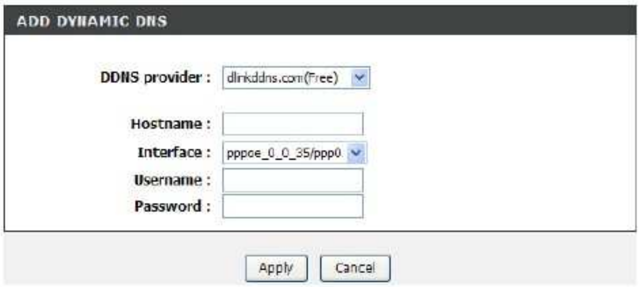
The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamicaly assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com

DYNAMIC DNS

Hostname	Username	Service	Interface

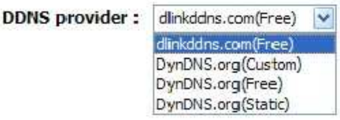
Click Add to add dynamic DNS. The page shown in the following figure appears.



ADD DYNAMIC DNS

DDNS provider :	dlinkddns.com(Free)
Hostname :	
Interface :	pppoe_0_0_35/ppp0
Username :	
Password :	

- DDNS provider: Select one of the DDNS registration organizations from the down-list drop.



DDNS provider : dlinkddns.com(Free)

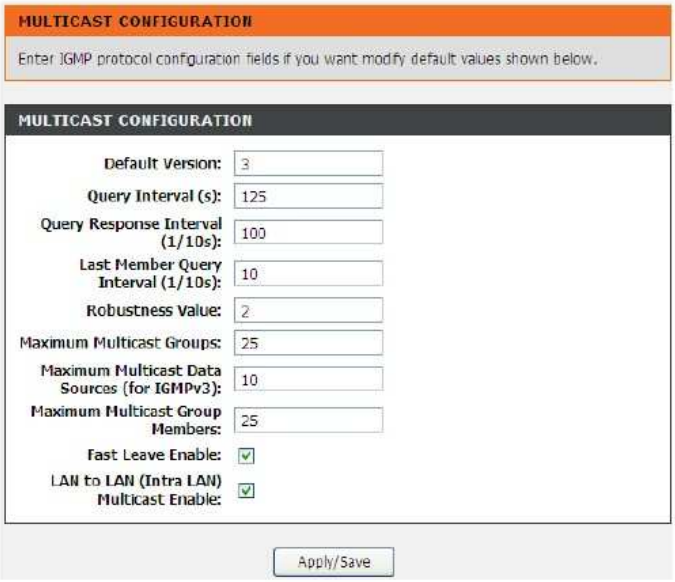
- Host Name: Enter the host name that you registered with your DDNS service provider.
- Interface: Select the interface you want to use.
- Username: Enter the user name for your DDNS account.
- Password: Enter the password for your DDNS account.

Click Apply to save the settings.

4.4.9 Multicast

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

- Default Version:IGMP version
- Query Interval(s):The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet)
- Query Response Interval (1/10s): The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval
- Last Member Query Interval (1/10s): The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.
- Robustness Value: The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets.
- Maximum Multicast Groups:max multicast groups
- Maximum Multicast Data Sources (for IGMPv3): max group data sources that want to receive.
- Maximum Multicast Group Members:Max member in one group
- Fast Leave Enable: Enable or disable fast leave feature.
- LAN to LAN (Intra LAN) Multicast Enable: Enable or disable Lan to Lan msulticast.



MULTICAST CONFIGURATION

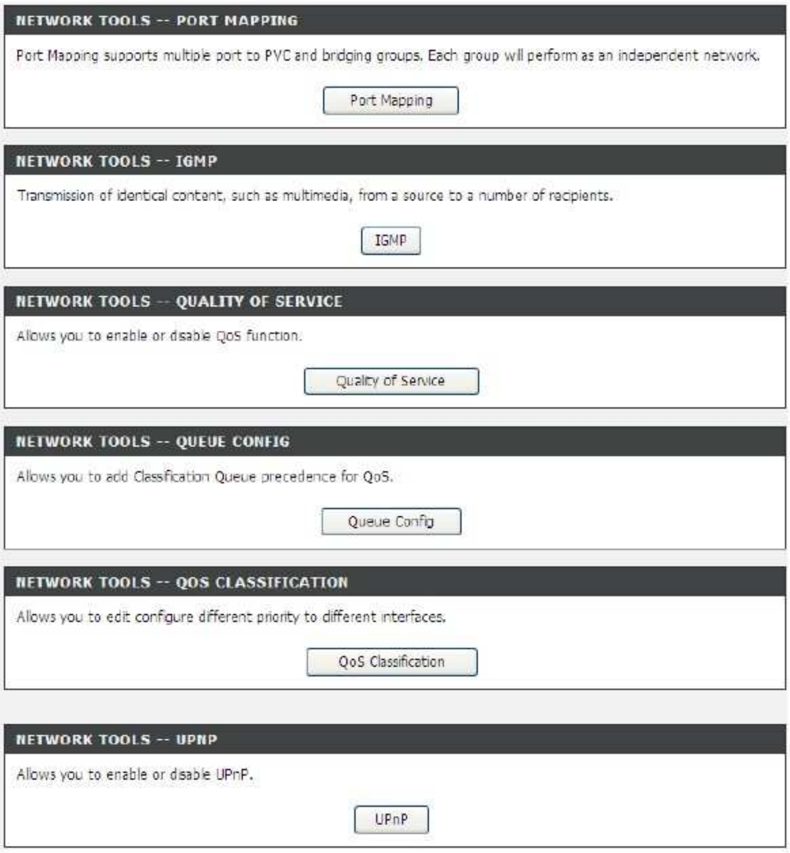
Enter IGMP protocol configuration fields if you want modify default values shown below.

MULTICAST CONFIGURATION

Default Version:	3
Query Interval (s):	125
Query Response Interval (1/10s):	100
Last Member Query Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑

4.4.10 Network Tools

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



NETWORK TOOLS -- PORT MAPPING

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.

NETWORK TOOLS -- IGMP

Transmission of identical content, such as multimedia, from a source to a number of recipients.

NETWORK TOOLS -- QUALITY OF SERVICE

Allows you to enable or disable QoS function.

NETWORK TOOLS -- QUEUE CONFIG

Allows you to add Classification Queue precedence for QoS.

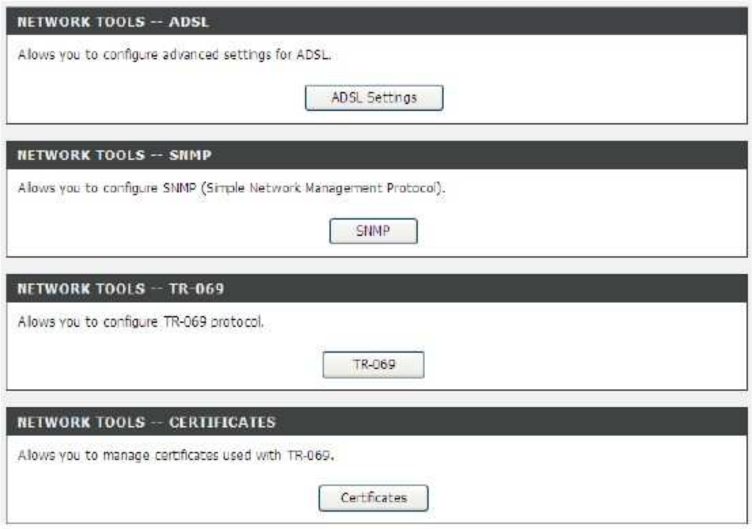
NETWORK TOOLS -- QOS CLASSIFICATION

Allows you to edit configure different priority to different interfaces.

NETWORK TOOLS -- UPNP

Allows you to enable or disable UPnP.

In the NETWORK TOOLS page, you can configure port mapping, IGMP, quality of service, queue, QoS classification, UPnP, ADSL settings, SNMP, TR-069, and certificates through clicking the navigation.



NETWORK TOOLS -- ADSL

Allows you to configure advanced settings for ADSL.

NETWORK TOOLS -- SNMP

Allows you to configure SNMP (Simple Network Management Protocol).

NETWORK TOOLS -- TR-069

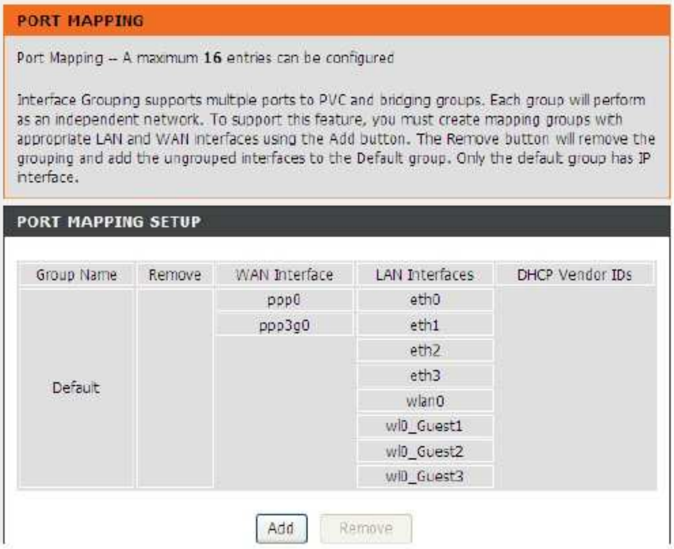
Allows you to configure TR-069 protocol.

NETWORK TOOLS -- CERTIFICATES

Allows you to manage certificates used with TR-069.

4.4.10.1 Port Mapping

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



PORT MAPPING

Port Mapping -- A maximum **16** entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

PORT MAPPING SETUP

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0 ppp3g0	eth0 eth1 eth2 eth3 wlan0 wl0_Guest1 wl0_Guest2 wl0_Guest3	

Click Add to add port mapping. The page shown in the following figure appears.
The procedure for creating a mapping group is as follows:

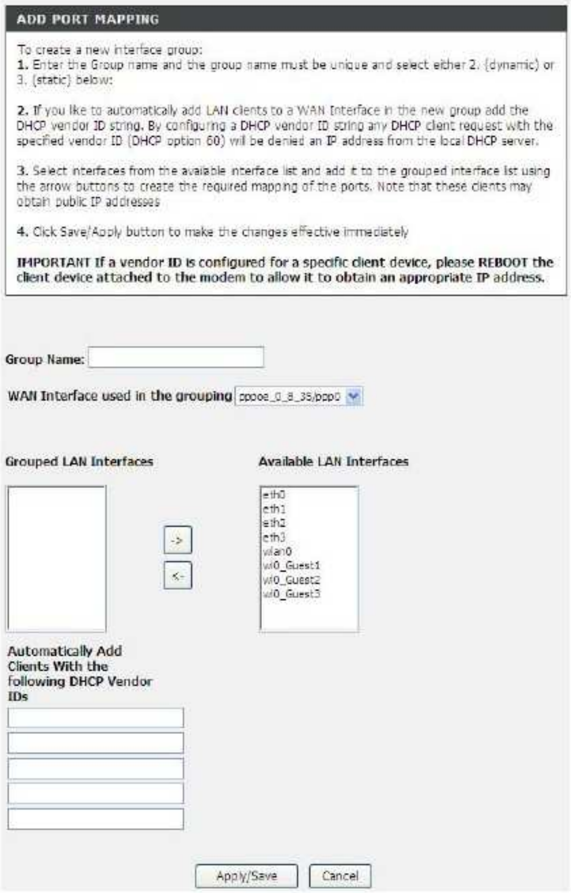
Step 1 Enter the group name.

Step 2 Select the WAN interface for your new group.

Step 3 Select LAN interfaces from the Available Interface list and click the <- arrow button to add them to the grouped interface list, in order to create the required mapping of the ports. The group name must be unique.

Step 4 Enter the option information of DHCP vendor IDs.

Step 5 Click Apply to save the settings.



ADD PORT MAPPING

To create a new interface group:
1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses

4. Click Save/Apply button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

WAN Interface used in the grouping pppoe_0_8_35/ppp0

Grouped LAN Interfaces

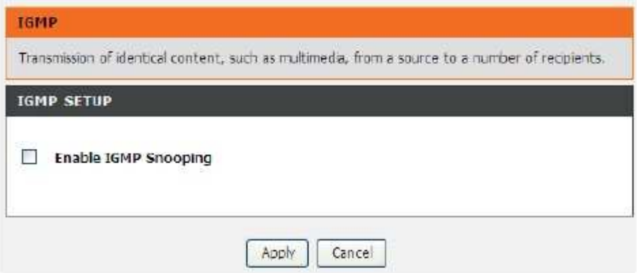
Available LAN Interfaces

eth0
eth1
eth2
eth3
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3

Automatically Add Clients With the following DHCP Vendor IDs

4.4.10.2 IGMP

Choose ADVANCED > Network Tools and click IGMP. The page shown in the following figure appears. When enable IGMP Snooping, the multicast data transmits through the specific LAN port which has received the request report.



IGMP

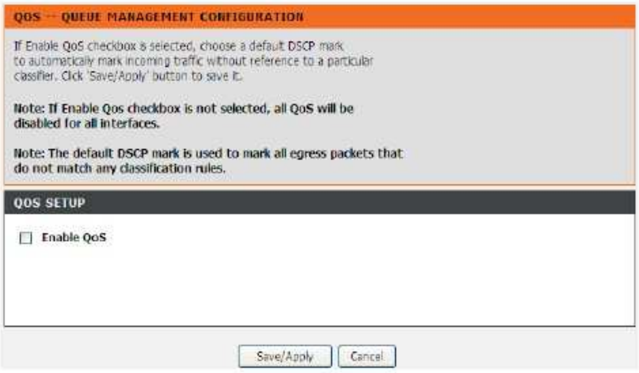
Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP SETUP

□ Enable IGMP Snooping

4.4.10.3 Quality of Service

Choose ADVANCED > Network Tools and click Quality of Service. The page shown in the following figure appears.
In this page, you can enable/disable the QoS. Click Save/Apply to take the setting effect.



QOS -- QUEUE MANAGEMENT CONFIGURATION

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

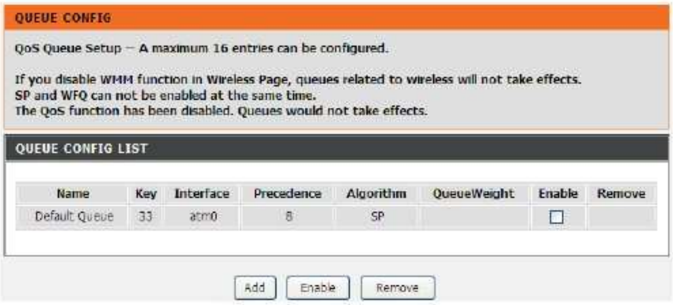
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

QOS SETUP

□ Enable QoS

4.4.10.4 Queue Config

Choose ADVANCED > Network Tools and click Queue Config. The page shown in the following figure appears.



QUEUE CONFIG

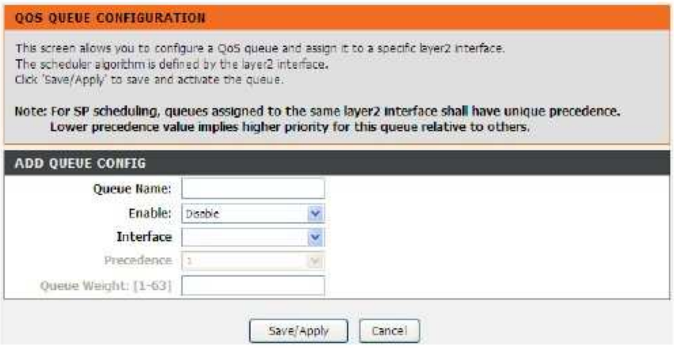
QoS Queue Setup -- A maximum 16 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects.
SP and WFQ can not be enabled at the same time.
The QoS function has been disabled. Queues would not take effects.

QUEUE CONFIG LIST

Name	Key	Interface	Precedence	Algorithm	QueueWeight	Enable	Remove
Default Queue	33	atm0	8	SP		□	

Click Add. The page shown in the following figure appears.
Click Save/Apply to save the settings.



QOS QUEUE CONFIGURATION

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface.
The scheduler algorithm is defined by the layer2 interface.
Click 'Save/Apply' to save and activate the queue.

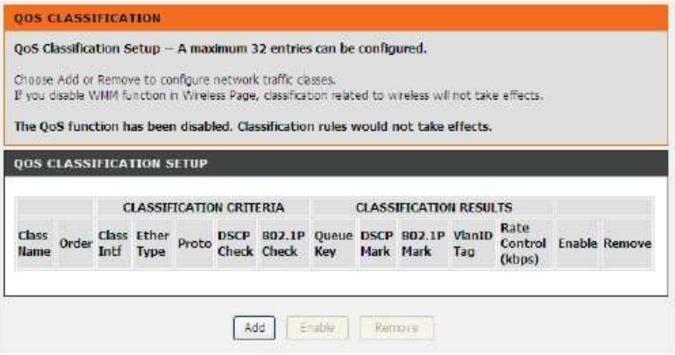
Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence.
Lower precedence value implies higher priority for this queue relative to others.

ADD QUEUE CONFIG

Queue Name:	
Enable:	Disable
Interface	
Precedence	1
Queue Weight: [1-63]	

4.4.10.5 QoS Classification

Choose ADVANCED > Network Tools, and click QoS Classification, the page shown in the following figure appears.This page allows you to config various classification.



QOS CLASSIFICATION

QoS Classification Setup -- A maximum 32 entries can be configured.

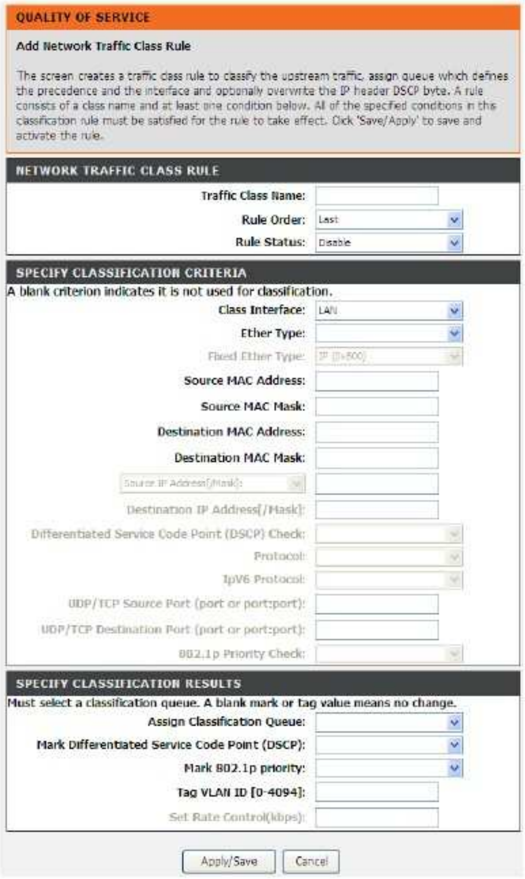
Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

The QoS function has been disabled. Classification rules would not take effects.

QOS CLASSIFICATION SETUP

		CLASSIFICATION CRITERIA					CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	Proto	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove

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



QUALITY OF SERVICE

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

NETWORK TRAFFIC CLASS RULE

Traffic Class Name:

Rule Order: Last

Rule Status: Disable

SPECIFY CLASSIFICATION CRITERIA

A blank criterion indicates it is not used for classification.

Class Interface: LAN

Ether Type:

Fixed Ether Type: IP (0x800)

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Source IP Address[/Mask]:

Destination IP Address[/Mask]:

Differentiated Service Code Point (DSCP) Check:

Protocol:

IpV6 Protocol:

UDP/TCP Source Port (port or port:port):

UDP/TCP Destination Port (port or port:port):

802.1p Priority Check:

SPECIFY CLASSIFICATION RESULTS

Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Tag VLAN ID [0-4094]:

Set Rate Control(kbps):

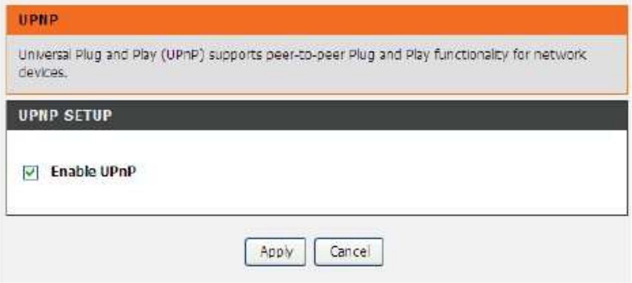
4.4.10.6 UPnP

Choose ADVANCED > Network Tools and click UPnP. The page shown in the following figure appears.

In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Click Apply to save the settings.



UPNP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

UPNP SETUP

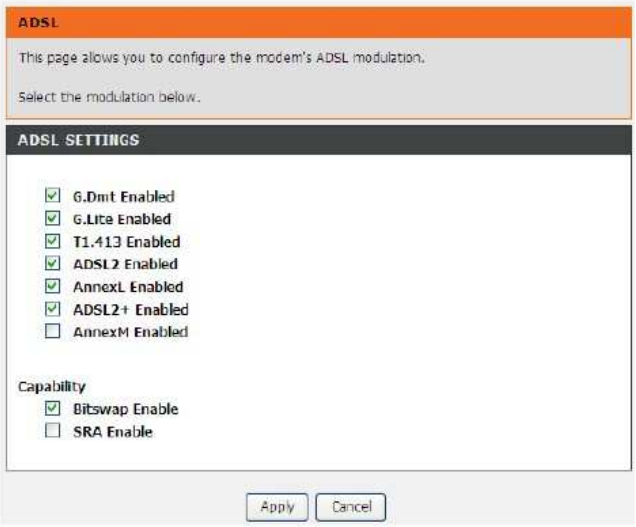
☑ Enable UPnP

4.4.10.7 ADSL

Choose ADVANCED > Network Tools and click ADSL Settings. The page shown in the following figure appears.

In this page, you can select the DSL modulation. Normally, you can keep the factory default setting. The device negotiates the modulation mode with DSLAM.

Click Apply to save the settings.



ADSL

This page allows you to configure the modem's ADSL modulation.

Select the modulation below.

ADSL SETTINGS

☑ G.Dmt Enabled
☑ G.Lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
□ AnnexM Enabled

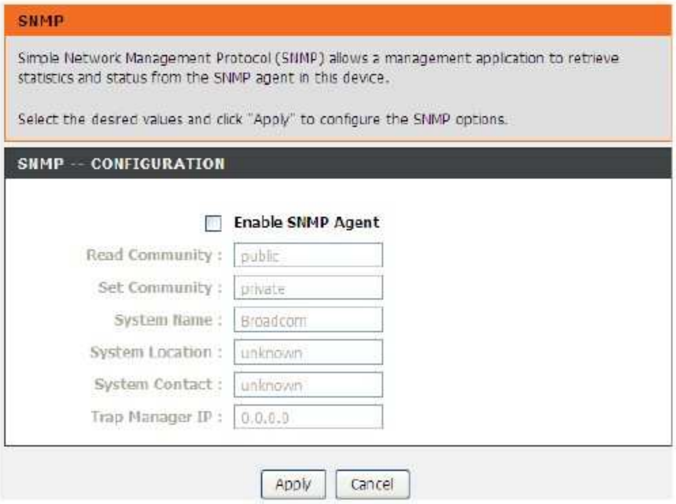
Capability
☑ Bitswap Enable
□ SRA Enable

4.4.10.8 SNMP

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

- Read Community: The network administrator must use this password to read the information of this device.
- Set Community: The network administrator must use this password to configure the information of this device.
- Trap Manager IP: The trap information is sent to this host.

Click Apply to save the settings.



SNMP

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

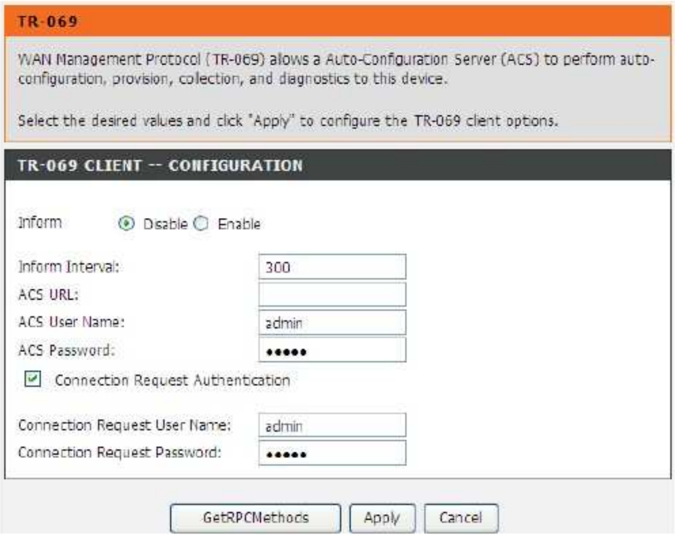
SNMP -- CONFIGURATION

☐ Enable SNMP Agent

Read Community :	public
Set Community :	private
System Name :	Broadcom
System Location :	unknown
System Contact :	unknown
Trap Manager IP :	0.0.0.0

4.4.10.9 TR-069

Choose ADVANCED > Network Tools and click TR-069. The page shown in the following figure appears. In this page, you can configure the TR-069 CPE. WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.
In this page, you may configure the parameters such as the ACS URL, ACS password, and connection request user name.
After finishing setting, click Apply to save and apply the settings.



TR-069

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, colection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

TR-069 CLIENT -- CONFIGURATION

Inform ● Disable ○ Enable

Inform Interval: 300

ACS URL:

ACS User Name: admin

ACS Password: •••••

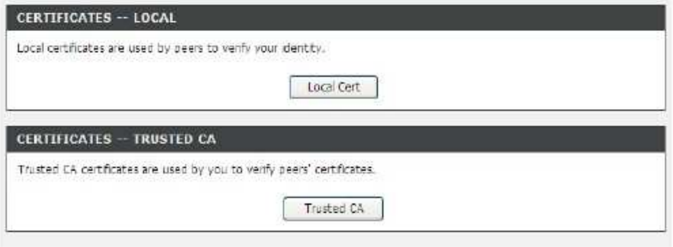
☑ Connection Request Authentication

Connection Request User Name: admin

Connection Request Password: •••••

4.4.10.10 Certificates

Choose ADVANCED > Network Tools and click Certificates. The Certificates page shown in the following figure appears. In this page, you can configure local certificate and trusted certificate.



CERTIFICATES -- LOCAL

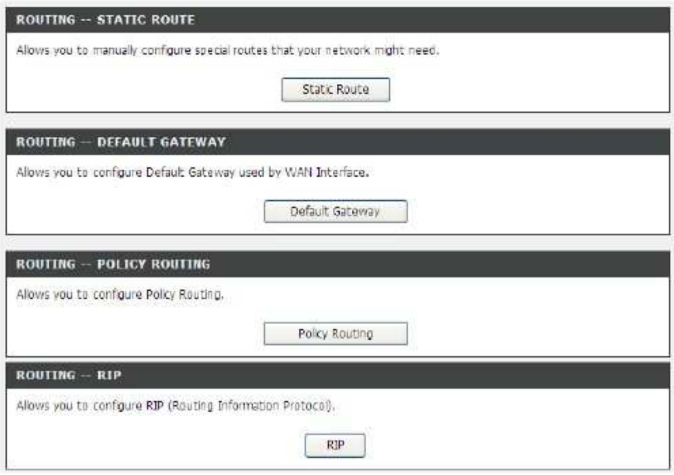
Local certificates are used by peers to verify your identity.

CERTIFICATES -- TRUSTED CA

Trusted CA certificates are used by you to verify peers' certificates.

4.4.11 Routing

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



ROUTING -- STATIC ROUTE

Allows you to manually configure special routes that your network might need.

Static Route

ROUTING -- DEFAULT GATEWAY

Allows you to configure Default Gateway used by WAN Interface.

Default Gateway

ROUTING -- POLICY ROUTING

Allows you to configure Policy Routing.

Policy Routing

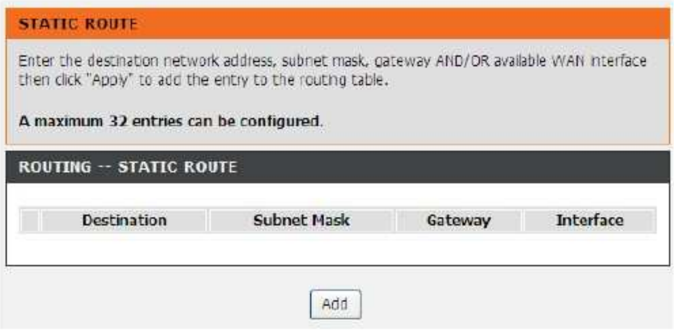
ROUTING -- RIP

Allows you to configure RIP (Routing Information Protocol).

RIP

4.4.11.1 Static Route

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



STATIC ROUTE

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.

A maximum 32 entries can be configured.

ROUTING -- STATIC ROUTE

	Destination	Subnet Mask	Gateway	Interface

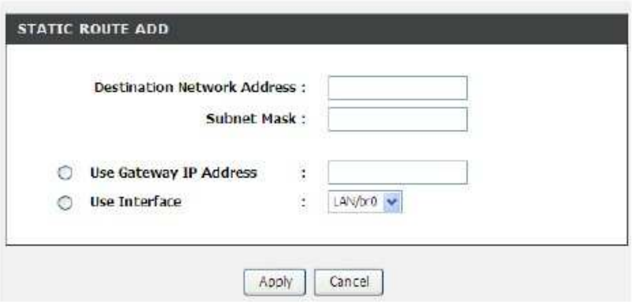
Add

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

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

You can click Use Gateway IP Address or Use Interface.

Click Apply to save the settings.



STATIC ROUTE ADD

Destination Network Address :

Subnet Mask :

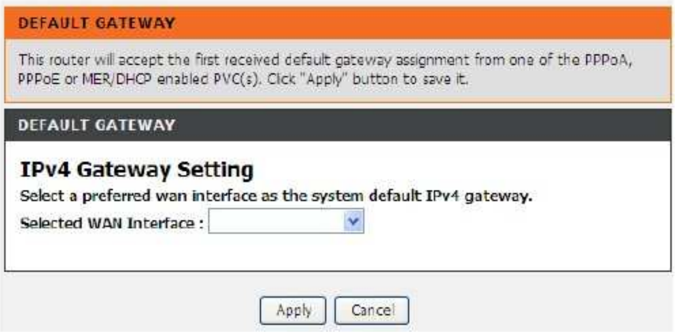
○ Use Gateway IP Address :

○ Use Interface : LAN/br0

4.4.11.2 Default Gateway

Choose ADVANCED > Routing and click Default Gateway. The page shown in the following figure appears.

Select the WAN interface as your default gateway. Click Apply to save the settings.



DEFAULT GATEWAY

This router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). Click "Apply" button to save it.

DEFAULT GATEWAY

IPv4 Gateway Setting

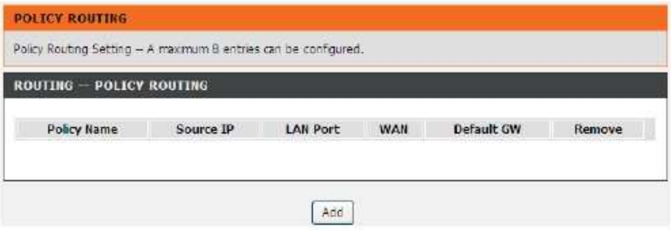
Select a preferred wan interface as the system default IPv4 gateway.

Selected WAN Interface :

4.4.11.3 Policy Routing

Choose ADVANCED > Routing and click policy Routing. The page shown in the following figure appears.

The policy route binds one WAN connection and one LAN interface.



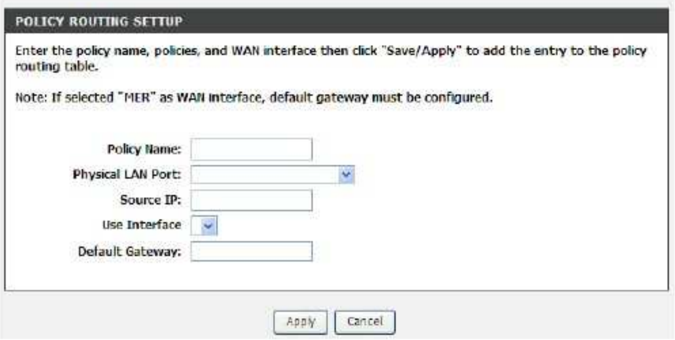
POLICY ROUTING

Policy Routing Setting -- A maximum 8 entries can be configured.

ROUTING -- POLICY ROUTING

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

Click Add, the page shown in the following figure appears.



POLICY ROUTING SETUP

Enter the policy name, policies, and WAN interface then click "Save/Apply" to add the entry to the policy routing table.

Note: If selected "MER" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

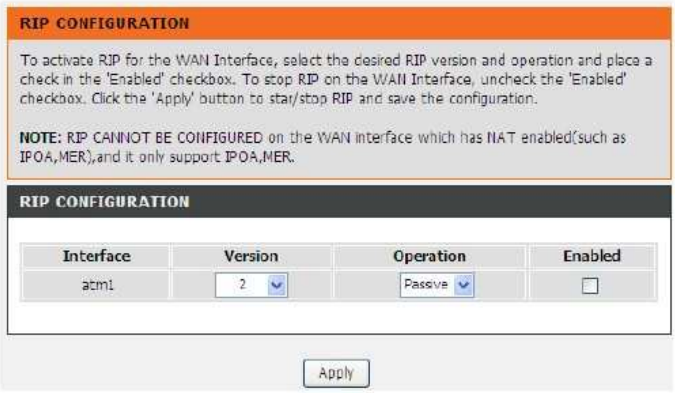
Source IP:

Use Interface

Default Gateway:

4.4.12 RIP

Choose ADVANCED > Routing and click RIP. The page shown in the following figure appears. This page is used to select the interfaces on your device that use RIP and the version of the protocol used.
If you are using this device as a RIP-enabled device to communicate with others using the routing information protocol, enable RIP and click Apply to save the settings.



RIP CONFIGURATION

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply' button to star/stop RIP and save the configuration.

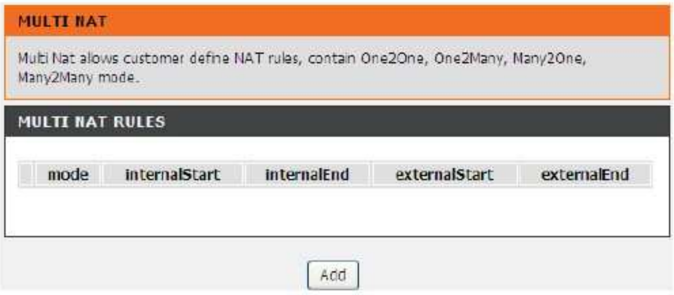
NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled(such as IPOA,MER),and it only support IPOA,MER.

RIP CONFIGURATION

Interface	Version	Operation	Enabled
atm1	2	Passive	□

4.4.13 MultiNat

Network address translation (NAT) is the process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. The packets which source IP address match between “internalStart” and “internalEnd” in the NAT table come to the router, the router changes source IP of this packet by the IP address that set between “externalStart” and “externalEnd”, then transmit the packet into Internet.
Choose ADVANCED > MultiNat. The page shown in the following figure appears.



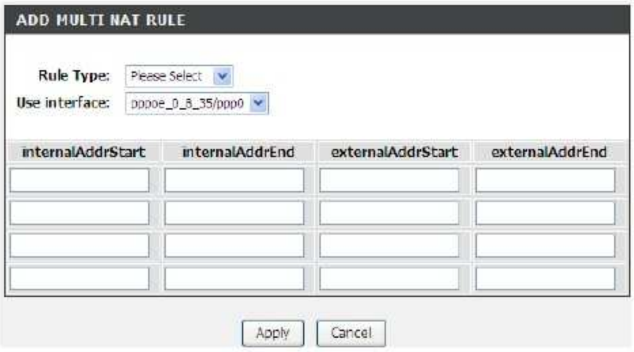
MULTI NAT

Multi Nat allows customer define NAT rules, contain One2One, One2Many, Many2One, Many2Many mode.

MULTI NAT RULES

	mode	internalStart	internalEnd	externalStart	externalEnd

Click Add, the page shown in the following figure appears.
In this page, please select the proper type; select the proper Use interface, and configure the other parameters in this page.
After finishing setting, click Apply to save the settings.



ADD MULTI NAT RULE

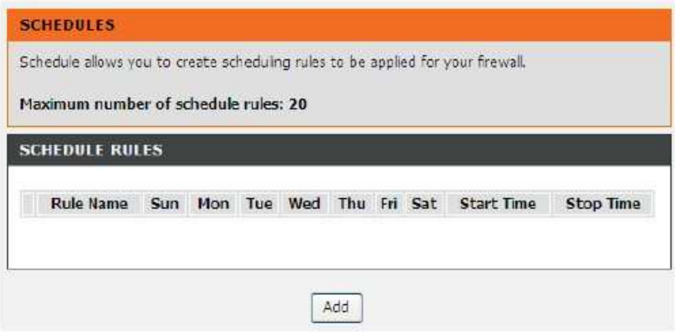
Rule Type: Please Select

Use interface: pppoe_0_8_35/ppp0

internalAddrStart	internalAddrEnd	externalAddrStart	externalAddrEnd

4.4.14 Schedules

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



SCHEDULES

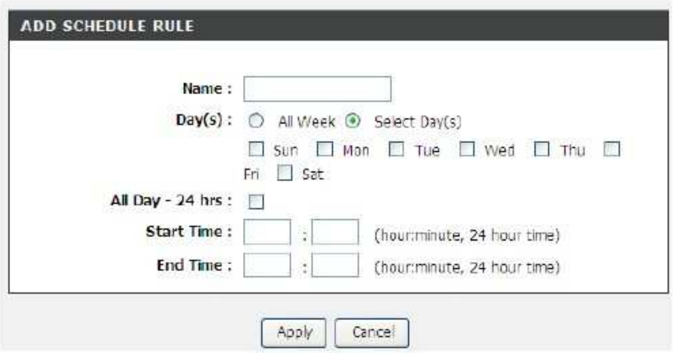
Schedule allows you to create scheduling rules to be applied for your firewall.

Maximum number of schedule rules: 20

SCHEDULE RULES

	Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop Time

Click Add to add schedule rule. The page shown in the following figure appears. Click Apply to save the settings.



ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

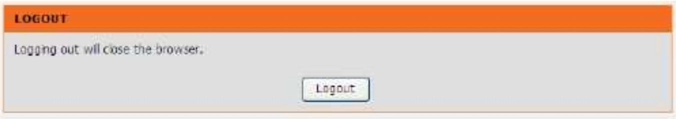
All Day - 24 hrs : □

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

4.4.15 Logout

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



LOGOUT

Logging out will close the browser.

4.5 Maintenance

4.5.1 System

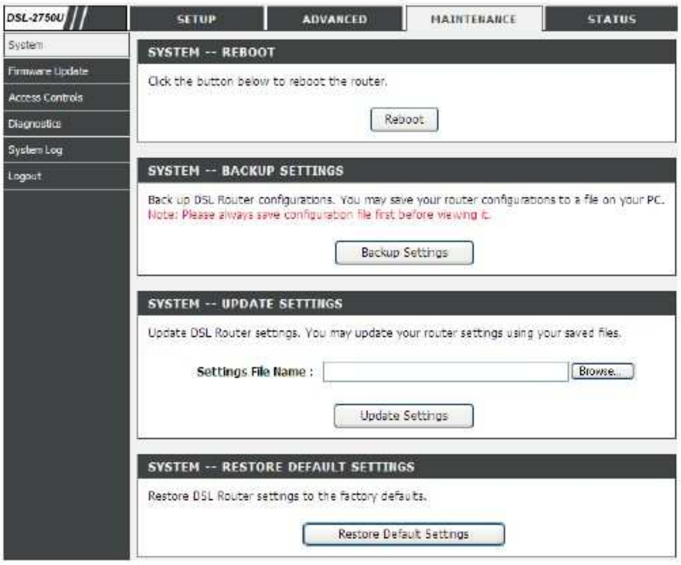
Choose MAINTENANCE > System. The System page shown in the following figure appears.

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

The buttons in this page are described as follows:

- Reboot: Reboot the device.
- Backup Settings: Save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.
- Update settings: Click Browse to select the configuration file of device and click Update Settings to begin restoring the device configuration..
- Restore Default Settings: Reset the device to default settings.

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



SYSTEM -- REBOOT

Click the button below to reboot the router.

SYSTEM -- 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.

SYSTEM -- UPDATE SETTINGS

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

Settings File Name :

SYSTEM -- RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults.

4.5.2 Firmware Update

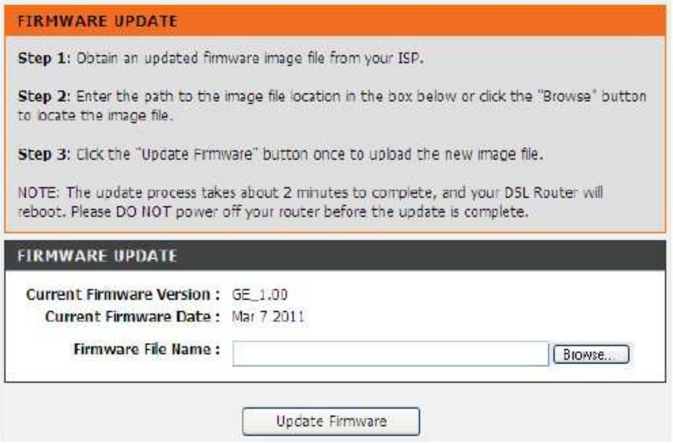
Choose MAINTENANCE > Firmware Update. The page shown in the following figure appears. In this page, you can upgrade the firmware of the device.
The procedure for updating the firmware is as follows:

Step 1 Click Browse…to search the file.

Step 2 Click Update Firmware to update the configuration file.

The device loads the file and reboots automatically.

Notice: Do not turn off your device or press the reset button while this procedure is in progress.



FIRMWARE UPDATE

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.

FIRMWARE UPDATE

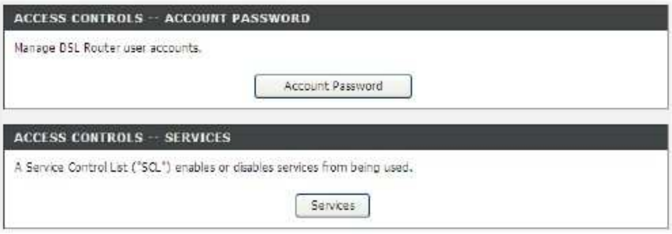
Current Firmware Version : GE_1.00

Current Firmware Date : Mar 7 2011

Firmware File Name :

4.5.3 Access Controls

Choose MAINTENANCE > Access Controls. The Access Controls page shown in the following figure appears. The page contains Account Password, Services.



ACCESS CONTROLS -- ACCOUNT PASSWORD

Manage DSL Router user accounts.

ACCESS CONTROLS -- SERVICES

A Service Control List ("SCL") enables or disables services from being used.

4.5.3.1 Account Password

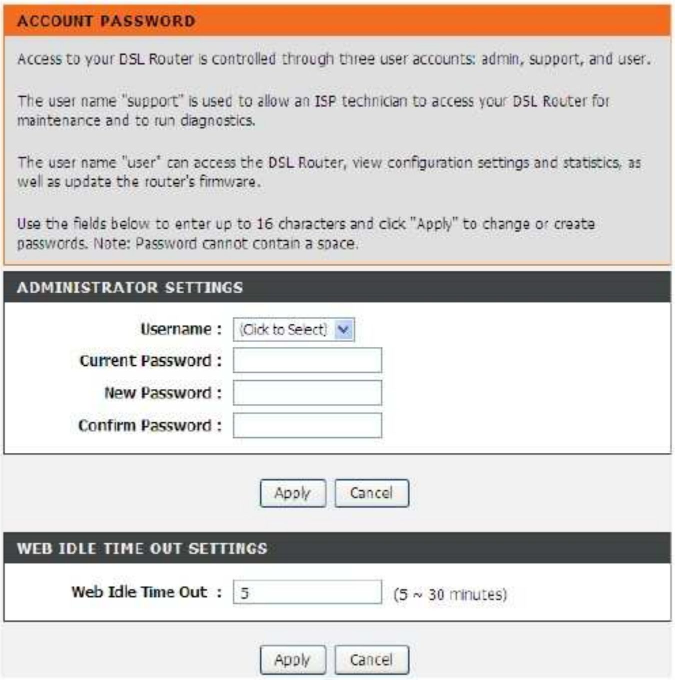
In the Access Controls page, click Account Password. The page shown in the following figure appears. In this page, you can change the password of the user and set time for automatic logout.

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

Select the Username from the drop-down list. You can select admin, support, or user.

Enter the current and new passwords and confirm the new password, to change the password.

Click Apply to apply the settings.



ACCOUNT PASSWORD

Access to your DSL Router is controlled through three user accounts: admin, support, and user.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as update the router's firmware.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

ADMINISTRATOR SETTINGS

Username : (Click to Select)

Current Password :

New Password :

Confirm Password :

WEB IDLE TIME OUT SETTINGS

Web Idle Time Out : 5 (5 ~ 30 minutes)

4.5.3.2 Services

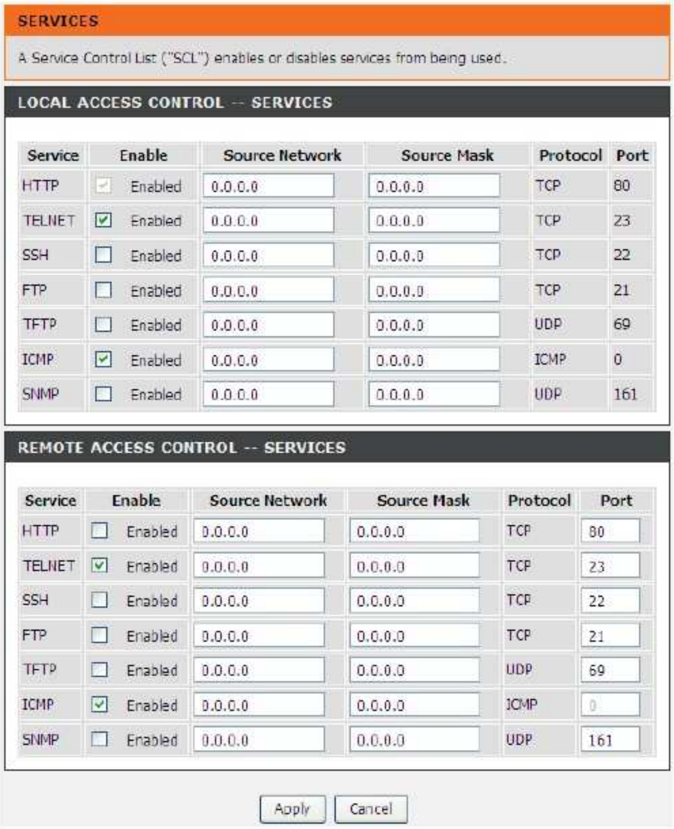
In the Access Controls page, click Services. The page shown in the following figure appears.

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

Select the management services that you want to enable or disable on the LAN or WAN interface.

Click Apply to apply the settings.

Note:
If you disable HTTP service, you cannot access the configuration page of the device any more.



SERVICES

A Service Control List ("SCL") enables or disables services from being used.

LOCAL ACCESS CONTROL -- SERVICES

Service	Enable	Source Network	Source Mask	Protocol	Port
HTTP	✓ Enabled	0.0.0.0	0.0.0.0	TCP	80
TELNET	☑ Enabled	0.0.0.0	0.0.0.0	TCP	23
SSH	□ Enabled	0.0.0.0	0.0.0.0	TCP	22
FTP	□ Enabled	0.0.0.0	0.0.0.0	TCP	21
TFTP	□ Enabled	0.0.0.0	0.0.0.0	UDP	69
ICMP	☑ Enabled	0.0.0.0	0.0.0.0	ICMP	0
SNMP	□ Enabled	0.0.0.0	0.0.0.0	UDP	161

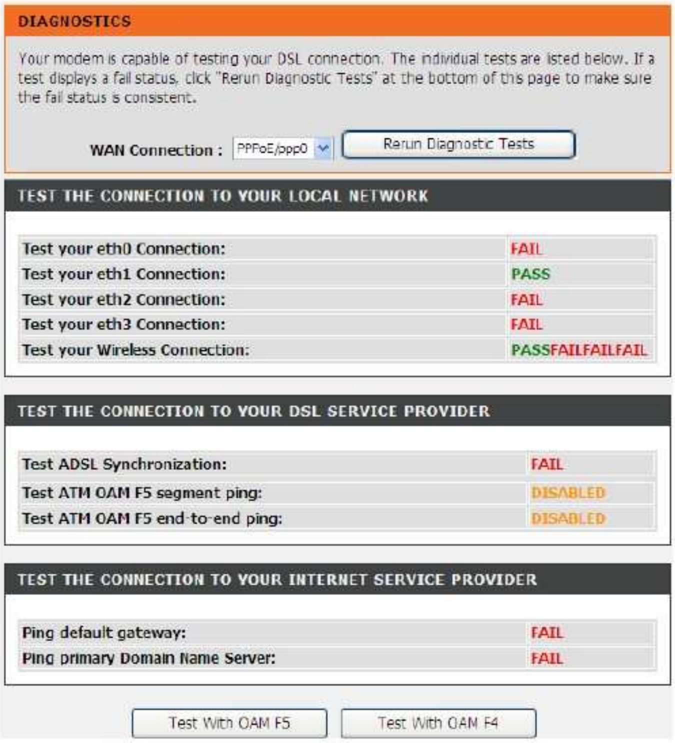
REMOTE ACCESS CONTROL -- SERVICES

Service	Enable	Source Network	Source Mask	Protocol	Port
HTTP	□ Enabled	0.0.0.0	0.0.0.0	TCP	80
TELNET	☑ Enabled	0.0.0.0	0.0.0.0	TCP	23
SSH	□ Enabled	0.0.0.0	0.0.0.0	TCP	22
FTP	□ Enabled	0.0.0.0	0.0.0.0	TCP	21
TFTP	□ Enabled	0.0.0.0	0.0.0.0	UDP	69
ICMP	☑ Enabled	0.0.0.0	0.0.0.0	ICMP	0
SNMP	□ Enabled	0.0.0.0	0.0.0.0	UDP	161

4.5.4 Diagnostics

Choose MAINTENANCE > Diagnostic. The page shown in the following figure appears. In this page, you can test the device.

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider. Click Rerun Diagnostics Test to run diagnostics.



DIAGNOSTICS

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent.

WAN Connection : PPPoE/ppp0

TEST THE CONNECTION TO YOUR LOCAL NETWORK

Test your eth0 Connection:	FAIL
Test your eth1 Connection:	PASS
Test your eth2 Connection:	FAIL
Test your eth3 Connection:	FAIL
Test your Wireless Connection:	PASSFAILFAILFAIL

TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER

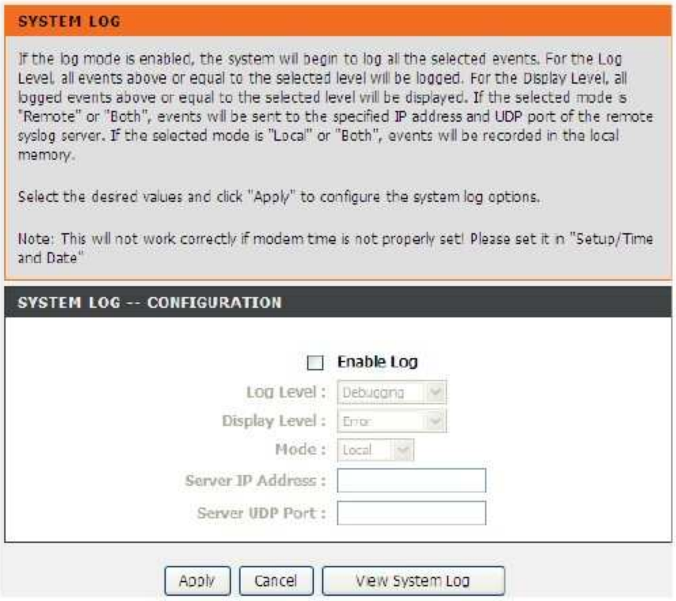
Test ADSL Synchronization:	FAIL
Test ATM OAM F5 segment ping:	DISABLED
Test ATM OAM F5 end-to-end ping:	DISABLED

TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER

Ping default gateway:	FAIL
Ping primary Domain Name Server:	FAIL

4.5.5 System Log

Choose MAINTENANCE > System Log. The System Log page shown in the following figure appears.



SYSTEM LOG

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "Local" or "Both", events will be recorded in the local memory.

Select the desired values and click "Apply" to configure the system log options.

Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"

SYSTEM LOG -- CONFIGURATION

□ Enable Log

Log Level : Debugging

Display Level : Error

Mode : Local

Server IP Address :

Server UDP Port :

This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. Available event severity levels are as follows: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. In this page, you can enable or disable the system log function.

The procedure for logging the events is as follows:

Step 1 Select Enable Log check box.

Step 2 Select the display mode from the Mode drop-down list.

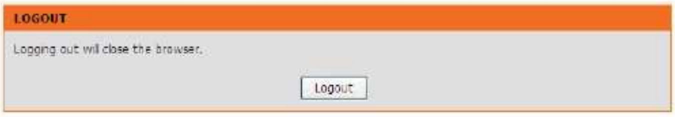
Step 3 Enter the Server IP Address and Server UDP Port if the Mode is set to Both or Remote.

Step 4 Click Apply to apply the settings.

Step 5 Click View System Log to view the detail information of system log.

4.5.6 Logout

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



LOGOUT

Logging out will close the browser.

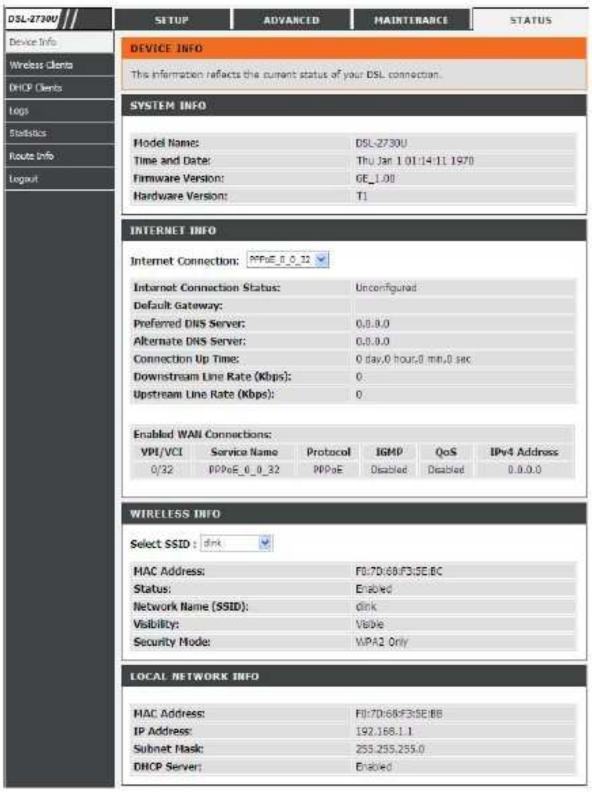
4.6 Status

You can view the system information and monitor performance.

4.6.1 Device Info

Choose STATUS > Device Info. The page shown in the following figure appears.

The page displays the summary of the device status, including the system information, Internet information, wireless information and local network information.



DEVICE INFO

This information reflects the current status of your DSL connection.

SYSTEM INFO

Model Name:	DSL-2730U
Time and Date:	Thu Jan 1 01:14:11 1970
Firmware Version:	GE_1.00
Hardware Version:	T1

INTERNET INFO

Internet Connection: PPPoE_0_0_32

Internet Connection Status:	Unconfigured
Default Gateway:	
Preferred DNS Server:	0.0.0.0
Alternate DNS Server:	0.0.0.0
Connection Up Time:	0 day,0 hour,0 min,0 sec
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0

Enabled WAN Connections:

VPI/VCI	Service Name	Protocol	IGMP	QoS	IPv4 Address
0/32	PPPoE_0_0_32	PPPoE	Disabled	Disabled	0.0.0.0

WIRELESS INFO

Select SSID : dlink

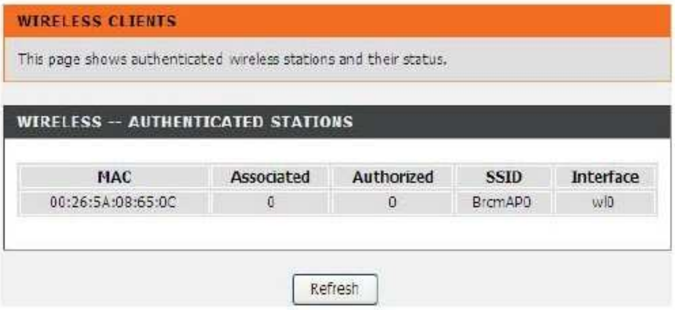
MAC Address:	F0:7D:68:F3:5E:BC
Status:	Enabled
Network Name (SSID):	dlink
Visibility:	Visible
Security Mode:	WPA2 Only

LOCAL NETWORK INFO

MAC Address:	F0:7D:68:F3:5E:BB
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enabled

4.6.2 Wireless Clients

Choose STATUS > Wireless Clients. The page shown in the following figure appears. The page displays authenticated wireless stations and their statuses.



WIRELESS CLIENTS

This page shows authenticated wireless stations and their status.

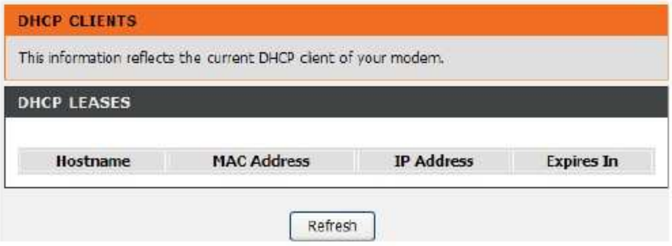
WIRELESS -- AUTHENTICATED STATIONS

MAC	Associated	Authorized	SSID	Interface
00:26:5A:08:65:0C	0	0	BrcmAP0	wl0

4.6.3 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).



DHCP CLIENTS

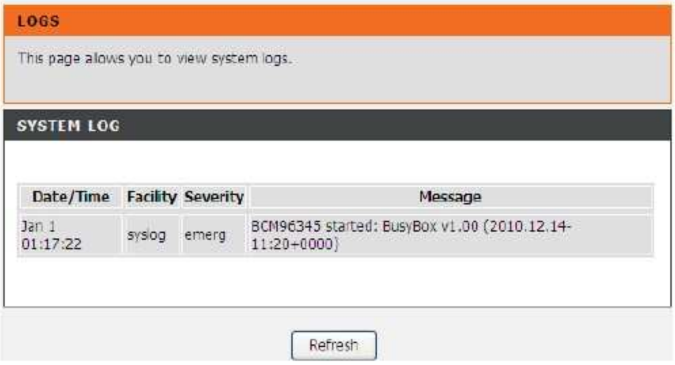
This information reflects the current DHCP client of your modem.

DHCP LEASES

Hostname	MAC Address	IP Address	Expires In

4.6.4 Logs

Choose STATUS > Logs. The page shown in the following figure appears. This page lists the system log. Click Refresh to refresh the system log shown in the table.



LOGS

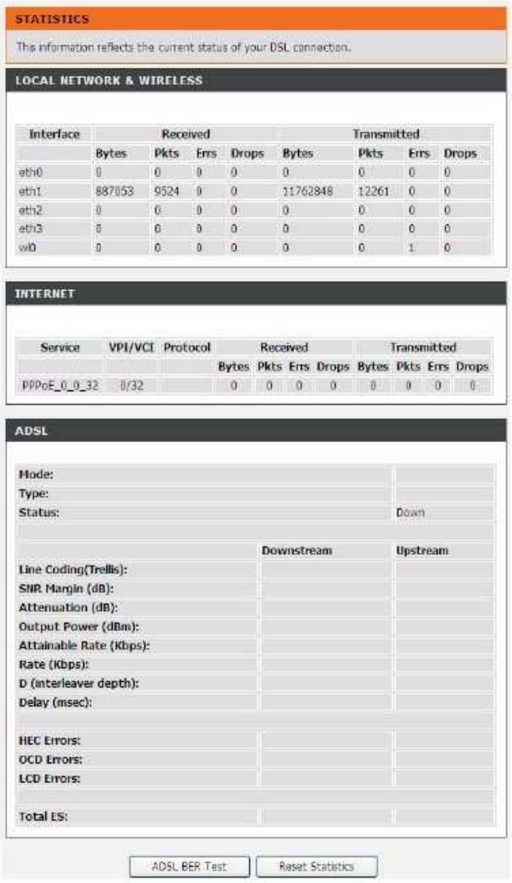
This page allows you to view system logs.

SYSTEM LOG

Date/Time	Facility	Severity	Message
Jan 1 01:17:22	syslog	emerg	BCM96345 started: BusyBox v1.00 (2010.12.14-11:20+0000)

4.6.5 Statistics

Choose STATUS > Statistics. The page shown in the following figure appears. This page displays the statistics of the network and data transfer. This information helps technicians to identify if the device is functioning properly. The information does not affect the function of the device.



STATISTICS

This information reflects the current status of your DSL connection.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	0	0	0	0
eth1	887053	9524	0	0	11762848	12261	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0
wl0	0	0	0	0	0	0	1	0

INTERNET

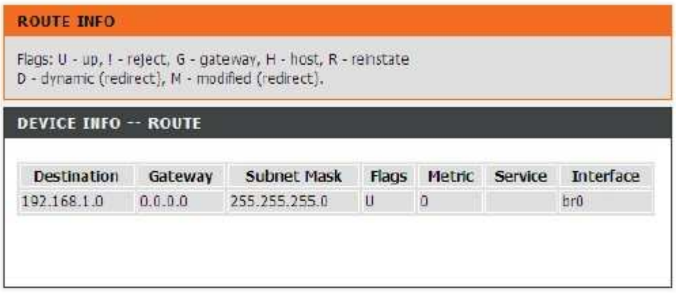
Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
PPPoE_0_0_32	0/32		0	0	0	0	0	0	0	0

ADSL

Mode:		
Type:		
Status:		Down
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (dB):		
Attenuation (dB):		
Output Power (dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
D (interleaver depth):		
Delay (msec):		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total ES:		

4.6.6 Route info

Choose STATUS > Route Info. The page shown in the following figure appears. The table shows a list of destination routes commonly accessed by the network.



ROUTE INFO

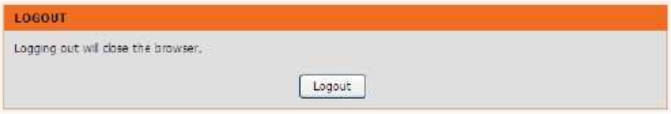
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

DEVICE INFO -- ROUTE

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

4.6.7 Logout

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



LOGOUT

Logging out will close the browser.

5 FAQs

Question	Answer
Why are all the indicators off?	● Check the connection between the power adapter and the power socket. ● Check whether the power switch is turned on.
Why is the LAN indicator not on?	Check the following: ● The connection between the device and the PC, the hub, or the switch. ● The running status of the computer, hub, or switch. ● The cables that connects the device and other devices: – If the device connects to a computer, use the cross over cable. – If the device connects to a hub or a switch, use the straight-through cable.
Why is the DSL indicator not on?	Check the connection between the DSL interface of the device and the socket.
Why does the Internet access fail when the DSL indicator is on?	Ensure that the following information is entered correctly: ● User name and password
Why does the web configuration page of the device fail to be accessed?	Choose start > Run from the desktop. Enter Ping 192.168.1.1 (the default IP address of the device) in the DOS window. If the web configuration page still cannot be accessed, check the following configuration: ● The type of the network cable ● The connection between the device and the computer ● The TCP/IP properties of the network card of the computer
How to restore the default configuration after incorrect configuration?	Keep the device powered on and press the RESET button for 1 second. Then, the device automatically reboots and is restored to the factory default configuration. The default configuration of the device is as follows: ● IP address: 192.168.1.1 ● Subnet mask: 255.255.255.0. ● User name and password of super account: admin/admin ● User name and password of common account: admin/admin

Part 68 Statement

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US:3P7DL01BSL2730BT1 .If requested, this number must be provided to the telephone company.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:3P7DL01BSL2730BT1 . The digits represented by 01 are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Company: D-Link Corporation
Address: 17595 Mt. Herrmann, Fountain Valley, CA 92708 U.S.A
Tel no.: 1.877.943.5465

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Note:The country selection mode is for non-US modes only and is not available to the US mode(s).

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN60950-1:2006+A11: 2009
  Safety of Information Technology Equipment

- EN 300 328 V1.7.1: 2006
- Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
-

  EN 301 489-1 V1.8.1: 2008
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

- EN 301 489-17 V2.1.1: 2009
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

- EN50385 : 2002
- Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE0560(!)

cs Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.