DSL-G225

User Manual

Contents

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.
- Don't mount this device on the wall.

2 Introduction

The DSL-G225 is a highly integrated VDSL2 Access Device. It provides ADSL/VDSL connectivity as well as 3G/LTE, EWAN and Wireless LAN services. The wireless LAN complies with the IEEE802.11b/g/n standards and supports 2T2R. It is usually prefered to provide high access performance for the individual users, SOHO, the small enterprises.

2.1 Packing List

- 1 x DSL-G225
- 2 x 5 dBi External Deteachable Antennas
- 1 x Splitter/Filtter
- 1 x Power Adapter
- 2 x Telephone Cables (RJ-11, 1.5m)
- 1 x Ethernet Cable (RJ-45, 1.5m)
- 1 x Quick Installation Guide

2.2 LEDs and Interfaces

Note:

The figures in this document are for reference only.

Front Panel

Figure 1 Front panel

The LED indicators are as follows from left to right: Power, Internet, WLAN, USB, LAN4/3/2/1, WAN and DSL. The WPS indicator is on the side panel.
The following table describes the LEDs of the device.

LED	Color	Status	Description
Power	Green	On	The system startup is complete.
	Red	On	The device is powered on.
		Blinking	The firmware is upgrading.
Internet	Green	Off	The device is under the Bridge mode or powered off.
		Blinking	The device has Internet access
		On	A connection is set up and no traffic is detected.
	Red	On	The authentication of the PPP dial-up failed
	Amber	On	3G internet Connected
WLAN	Green	Blinking	The WLAN function is enabled and data is being transmitted on the WLAN.
		On	The WLAN function is enabled, but no data is being transmitted on the WLAN.
		Off	The WLAN function is disabled.
USB	Green	On	The USB connection is set up or USB flash disk is enabled.
		Blinking	A connection is set up and data is being transmitted.
		Off	No signal is detected.
LAN 4/3/2/1	Green	Off	The Ethernet interface is not properly connected.
		Blinking	The Ethernet interface is properly connected and data is being transmitted.
		On	The Ethernet interface is properly connected, but no data is being transmitted.
WAN	Green	Blinking	The WAN interface is properly connected and data is being transmitted.
		On	The WAN interface is properly connected, but no data is being transmitted.
		Blinking	The WAN interface is properly connected and data is being transmitted.
DSL	Green	Off	No signal is being detected.

LED	Color	Status	Description
		Blinking	The device is handshaking with the physical layer of the office end.
		On	A connection is set up with the physical layer of the office end.

Rear Panel

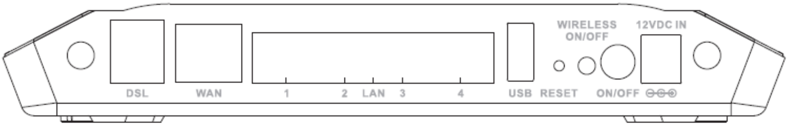


Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
DSL	RJ-11 interface for connecting to the ADSL interface or a splitter through the telephone cable.
LAN4/3/2/1	RJ-45 interface for connecting to the Ethernet interface of PC or other Ethernet devices through the Ethernet cable.
WAN	RJ-45 interface for connecting to the Ethernet interface of WAN
USB	USB port for connecting the 3G network card or other USB storage devices.
WIRELESS ON/OFF	Switch to enable or disable the WLAN function.
RESET	Reset to the factory defaults. To restore factory defaults, keep the device powered on, and then insert a needle into the hole. Press it and hold for one second, and then release.
ON/OFF	Power switch to power on or power off the device.
POWER	Interface for connecting to the power adapter.
WPS (on the side panel)	WPS button for starting WPS negotiation.

2.3 System Requirements

Recommended system requirements are as follow:

- A 10 baseT/100BaseT Ethernet card is installed on your PC
- Operating system: Windows 98SE, Windows 2000, Windows ME, Windows XP, Windows Vista, Windows 7, Windows 8, 8.1 and Windows 10
- Internet Explorer V5.0 or higher, Netscape V4.0 or higher, or Firefox 1.5 or higher

2.4 Features

The device supports the following features:

- User-friendly GUI for web configuration
- 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
- WLAN with high-speed data transfer rates of up to 300 Mbps, compatible with IEEE 802.11b/g/n, 2.4GHz compliant equipment
- 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)
- Print server
- Web filtering
- 3G/4G LTE WAN connection
- USB mass-storage, SAMBA
- System statistics and monitoring

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

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

(1) If you have a **Fibre-to-the-Home** service, connect the **yellow** Ethernet cable to the **blue** WAN port on the back of the router. Connect the other end of the yellow cable to the LAN port of the fibre device (ONT) otherwise, Skip to Step 4.

(2) If you have a **DSL** service, connect the splitter/filter to the port marked “OUT” on the power supply. Connect the grey telephone cable to the port marked “IN” on the power supply. Connect the other end of the cable to the telephone wall socket.

(3) Connect the red telephone cable to the red DSL port at the back of the router and the other end into the red port of the splitter/filter. You can connect a telephone to the green phone port of the splitter/filter.

(4) Connect the power connector of the power supply to the power socket at the back of the router. Plug the power supply into the wall outlet. Switch the wall outlet and the router on.

(5) You can connect a device to your router using either Ethernet cable (recommend) or Wi-Fi.

Ethernet cable:

Connect the yellow RJ-45 Ethernet cable to any yellow LAN port at the back of the router and the other end into your PC/Laptop LAN port.

Wi-Fi:

Use the default SSID and password (printed on the bottom of the router) to connect your Wi-Fi enabled device to the router.

(6) **DSL and FTTH**

Launch an Internet browser (Google Chrome, Firefox, Internet Explorer, Safari, etc.) on your connected device.

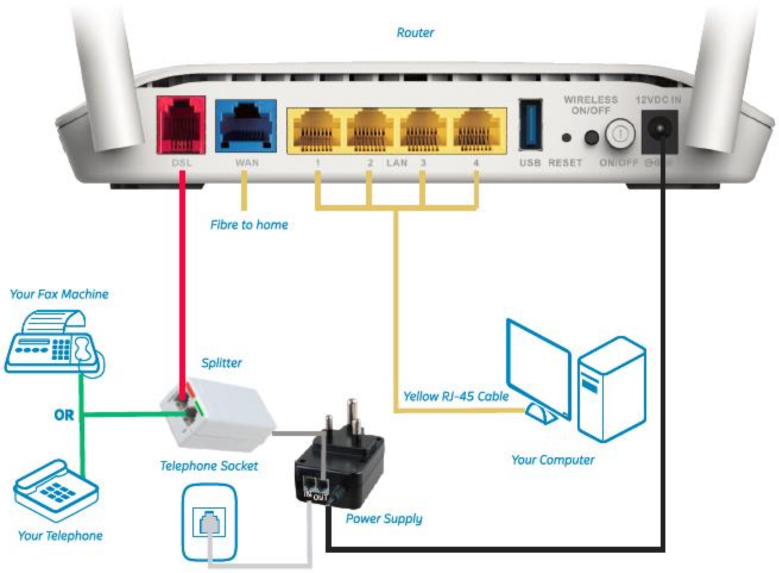
In the URL web address field, enter **10.0.0.2**

When prompted, enter admin for the **user name** and admin as the **password**

The installation wizard will start automatically. Please follow the steps of the wizard to finish the configuration of the router.

(7) To connect your LTE/3G USB dongle (optional) for failover mode, simply connect the dongle to the USB port at the back of your router.

(8) To add additional USB storage (optional), simply insert the device into the USB port at the back of the router



4 About the Web Configurator

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

4.1 Access the Router

Configuring IP Address of the Network Card

Configure TCP/IP properties of your network card to **Obtain an IP address automatically from modem**, or set the IP address of the computer with the same network mask of the modem.

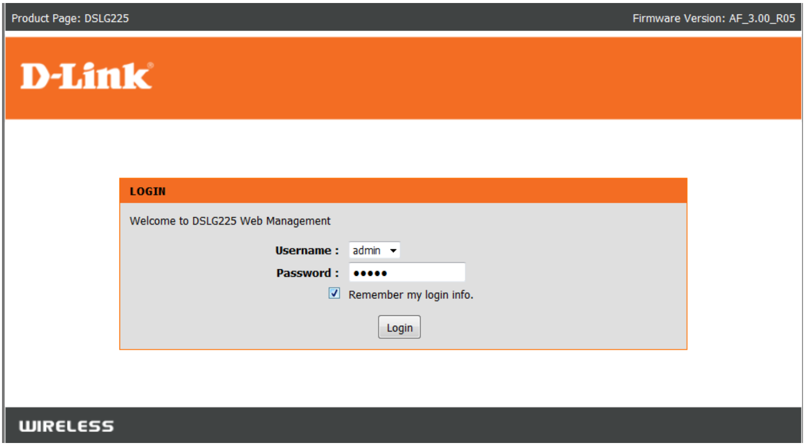
For example, if the IP address of Router is 10.0.0.2/255.255.255.0, you can set the IP address of the computer to **10.0.0.x/255.255.255.0**. The range for x is from 3 to 254.

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

Step 1 Open the Internet Explorer (IE) browser and enter http://10.0.0.2.

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

- The password is **admin**.



Product Page: DSLG225

Firmware Version: AF_3.00_R05

LOGIN

Welcome to DSLG225 Web Management

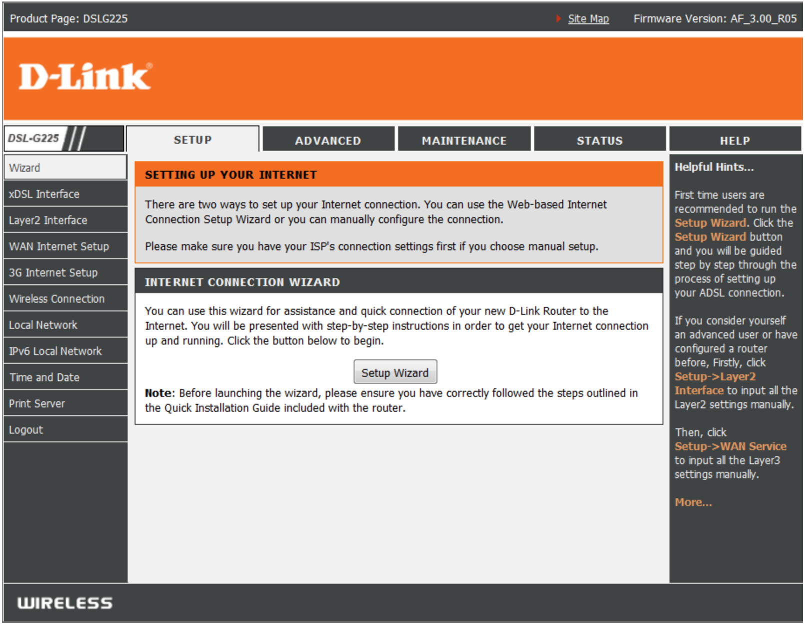
Username : admin

Password : ●●●●●

☑ Remember my login info.

Figure 3

If you log in as the super user successfully, the page shown as the following 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.

Helpful Hints...

First time users are recommended to run the Setup Wizard. Click the Setup Wizard button and you will be guided step by step through the process of setting up your ADSL connection.

If you consider yourself an advanced user or have configured a router before, Firstly, click Setup->Layer2 Interface to input all the Layer2 settings manually.

Then, click Setup->WAN Service to input all the Layer3 settings manually.

More...

Figure 4

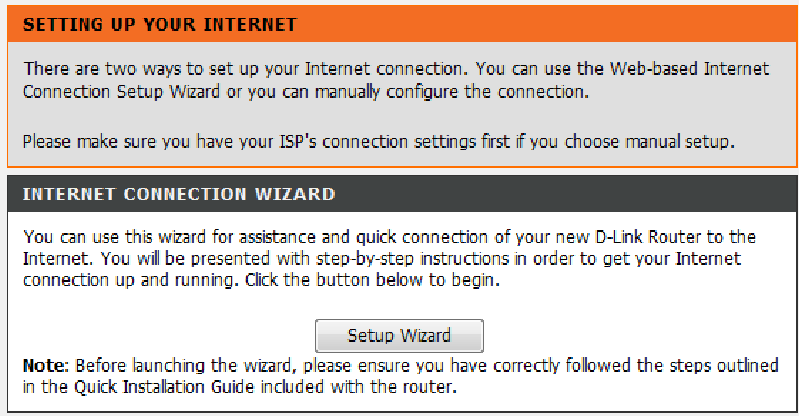
4.2 Setup

4.2.1 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. The connection type of your physical WAN device can be Ethernet, ADSL/VDSL, or both. Technical information about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or the protocol, such as PPPoA or PPPoE, that you use to communicate over the Internet.

Choose **Setup** > **Wizard**. The page is shown as the following 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.

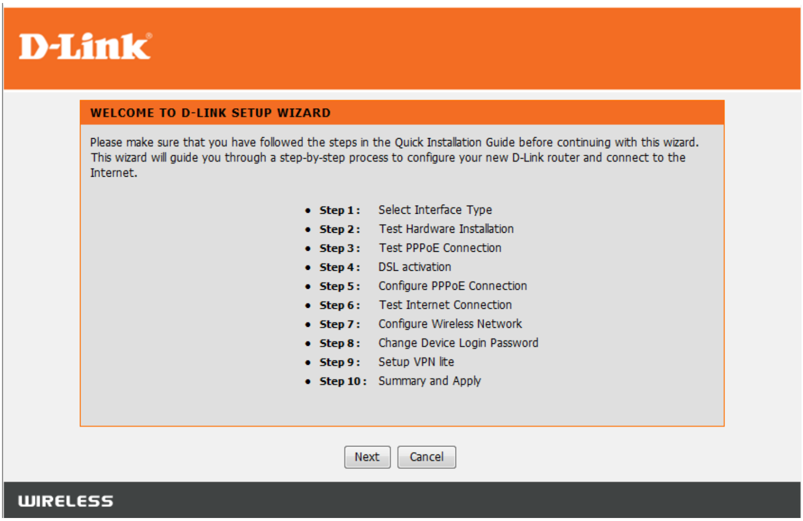
INTERNET CONNECTION WIZARD

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.

Figure 5

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



WELCOME TO D-LINK SETUP WIZARD

Please make sure that you have followed the steps in the Quick Installation Guide before continuing with this wizard. This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

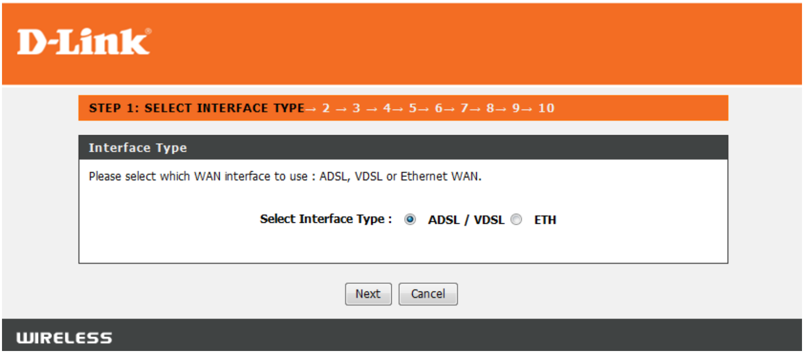
- **Step 1 :** Select Interface Type
- **Step 2 :** Test Hardware Installation
- **Step 3 :** Test PPPoE Connection
- **Step 4 :** DSL activation
- **Step 5 :** Configure PPPoE Connection
- **Step 6 :** Test Internet Connection
- **Step 7 :** Configure Wireless Network
- **Step 8 :** Change Device Login Password
- **Step 9 :** Setup VPN lite
- **Step 10 :** Summary and Apply

Figure 6

There are 10 steps to configure the device. Click **Next** to continue.

Step 1 Select Interface Type.

Please select which WAN interface to use : ADSL/VDSL or ETH WAN. Your ISP should inform you whether you are connected to the Internet using.

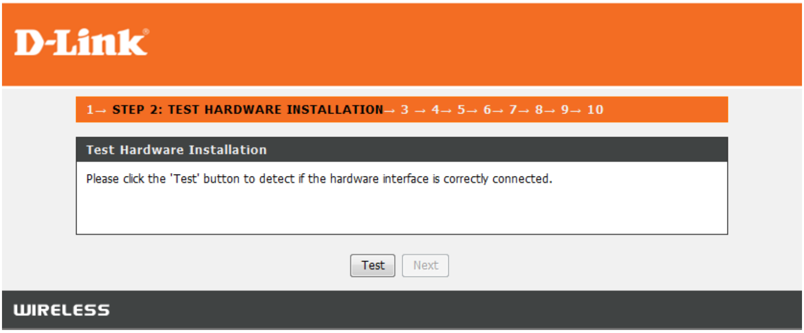


Please select which WAN interface to use : ADSL, VDSL or Ethernet WAN.

Select Interface Type : ● ADSL / VDSL ○ ETH

Figure 7

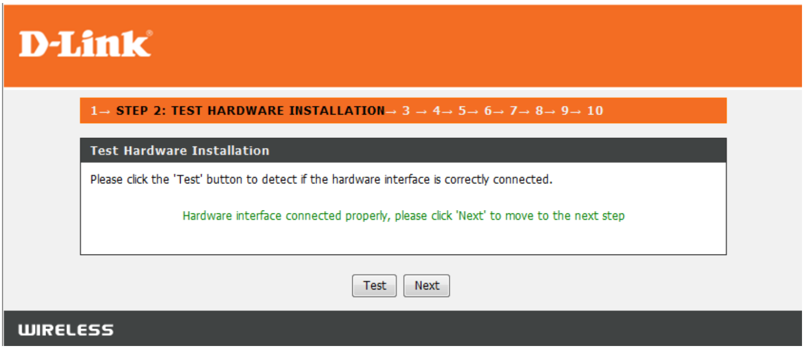
Step 2 Test Hardware Installation


D-Link
1→ STEP 2: TEST HARDWARE INSTALLATION→ 3 → 4→ 5→ 6→ 7→ 8→ 9→ 10
Test Hardware Installation
Test
Next
WIRELESS

Please click the 'Test' button to detect if the hardware interface is correctly connected.

Figure 8

If you select interface type “ADSL/VDSL” as your connection and the xDSL line is connected to the DSL port you will see the following message when you click on Test.



1→ STEP 2: TEST HARDWARE INSTALLATION→ 3 → 4→ 5→ 6→ 7→ 8→ 9→ 10

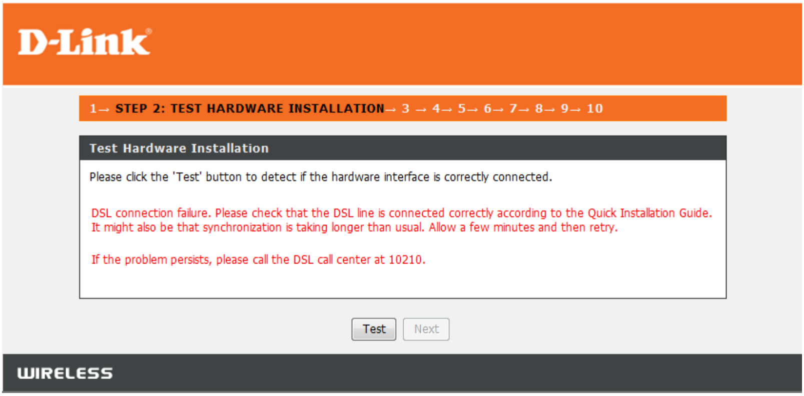
Test Hardware Installation

Please click the 'Test' button to detect if the hardware interface is correctly connected.

Hardware interface connected properly, please click 'Next' to move to the next step

Figure 9

If the line is not connected, you will see the follow message then you should connect the line to the DSL port.



1→ STEP 2: TEST HARDWARE INSTALLATION→ 3 → 4→ 5→ 6→ 7→ 8→ 9→ 10

Test Hardware Installation

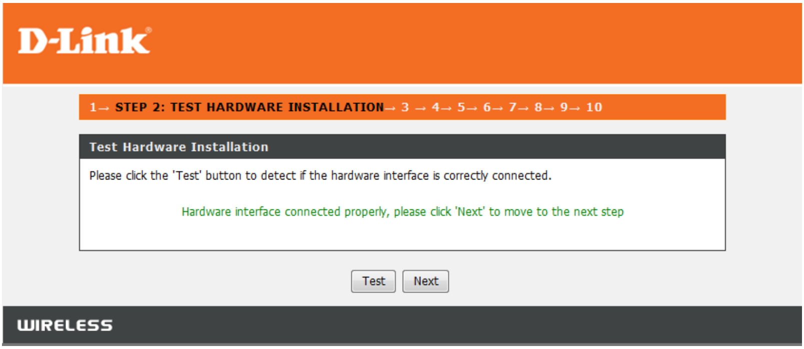
Please click the 'Test' button to detect if the hardware interface is correctly connected.

DSL connection failure. Please check that the DSL line is connected correctly according to the Quick Installation Guide. It might also be that synchronization is taking longer than usual. Allow a few minutes and then retry.

If the problem persists, please call the DSL call center at 10210.

Figure 10

If you select interface type “ETH” as your connection and the Ethernet cable is connected to the WAN port you will see the following message when you click on Test


D-Link
1→ STEP 2: TEST HARDWARE INSTALLATION→ 3 → 4→ 5→ 6→ 7→ 8→ 9→ 10
Test
Next
WIRELESS

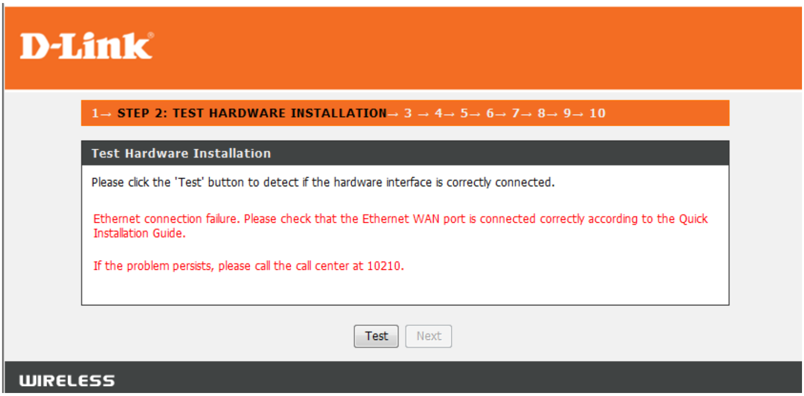
Test Hardware Installation

Please click the 'Test' button to detect if the hardware interface is correctly connected.

Hardware interface connected properly, please click 'Next' to move to the next step

Figure 11

If the line is not connected, you will see the follow message then you should connect the line to the ETH port.


D-Link
1→ STEP 2: TEST HARDWARE INSTALLATION→ 3 → 4→ 5→ 6→ 7→ 8→ 9→ 10
Test
Next
WIRELESS

Test Hardware Installation

Please click the 'Test' button to detect if the hardware interface is correctly connected.

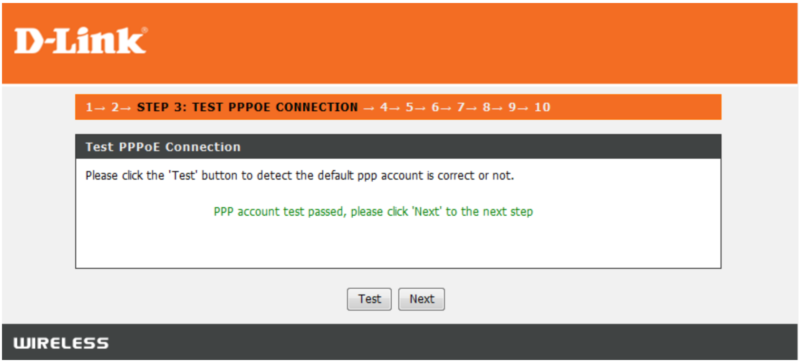
Ethernet connection failure. Please check that the Ethernet WAN port is connected correctly according to the Quick Installation Guide.

If the problem persists, please call the call center at 10210.

Figure 12

Step 3 Test PPPoE Connection.

When you click **Test**, if the default ppp account is correct, you will see the follow message then you can click **Next**.



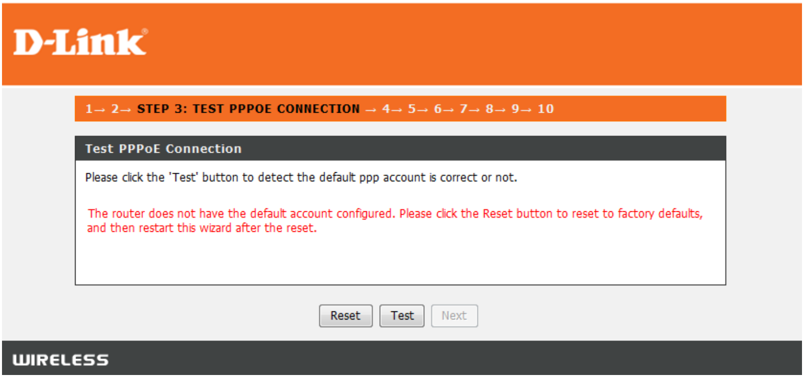
Test PPPoE Connection

Please click the 'Test' button to detect the default ppp account is correct or not.

PPP account test passed, please click 'Next' to the next step

Figure 13

If the default ppp account is not correct, you should click **Reset** to reset default config.



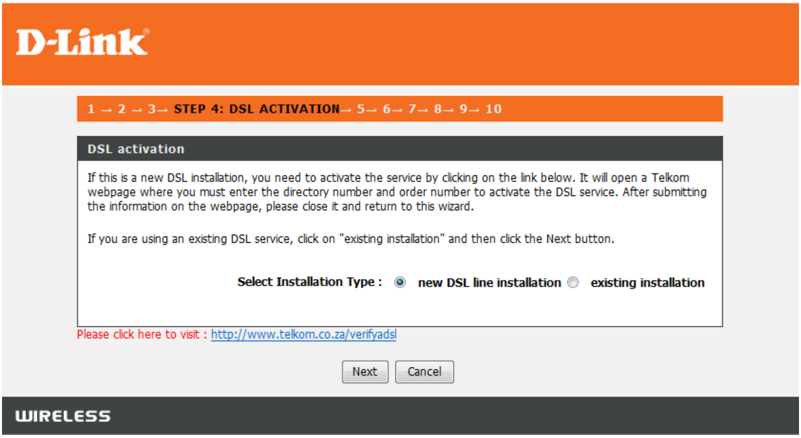
Test PPPoE Connection

Please click the 'Test' button to detect the default ppp account is correct or not.

The router does not have the default account configured. Please click the Reset button to reset to factory defaults, and then restart this wizard after the reset.

Figure 14

Step 4 DSL activation



1 → 2 → 3→ STEP 4: DSL ACTIVATION→ 5→ 6→ 7→ 8→ 9→ 10

DSL activation

If this is a new DSL installation, you need to activate the service by clicking on the link below. It will open a Telkom webpage where you must enter the directory number and order number to activate the DSL service. After submitting the information on the webpage, please close it and return to this wizard.

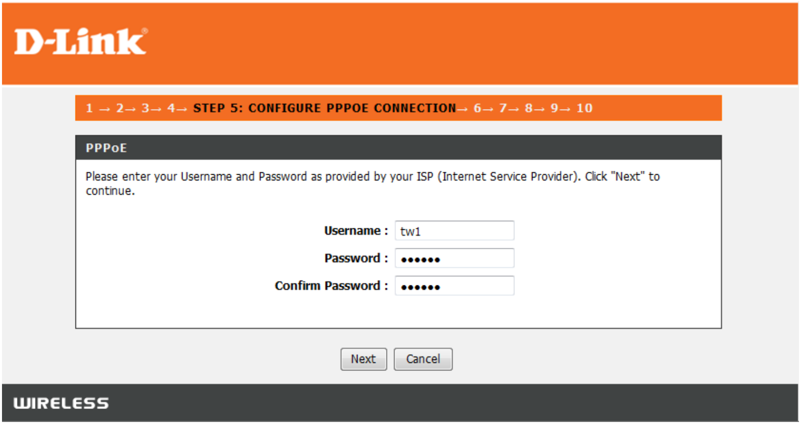
If you are using an existing DSL service, click on "existing installation" and then click the Next button.

Select Installation Type : ● new DSL line installation ○ existing installation

Please click here to visit : http://www.telkom.co.za/verifyadsl

Step 5 Test Internet Connection

In this page, enter the user name and password provided by your ISP, and then click **Next.**



1 → 2→ 3→ 4→ STEP 5: CONFIGURE PPPOE CONNECTION→ 6→ 7→ 8→ 9→ 10

PPPoE

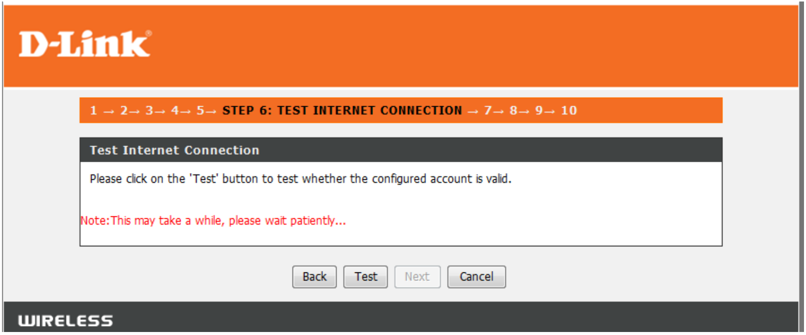
Please enter your Username and Password as provided by your ISP (Internet Service Provider). Click "Next" to continue.

Username : tw1

Password : ••••••

Confirm Password : ••••••

Step 6 Test Internet Connection



D-Link
1 → 2→ 3→ 4→ 5→ STEP 6: TEST INTERNET CONNECTION → 7→ 8→ 9→ 10

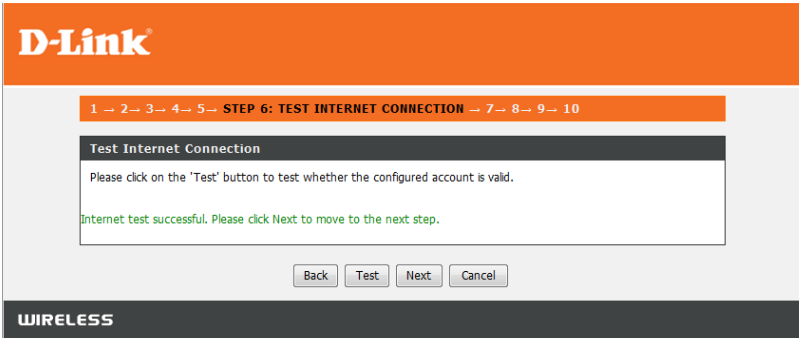
Test Internet Connection

Please click on the 'Test' button to test whether the configured account is valid.

Note:This may take a while, please wait patiently...

Back
Test
Next
Cancel
WIRELESS

When you click **Test**, if the configured account is valid, you will see the follow message.



D-Link
1 → 2→ 3→ 4→ 5→ STEP 6: TEST INTERNET CONNECTION → 7→ 8→ 9→ 10

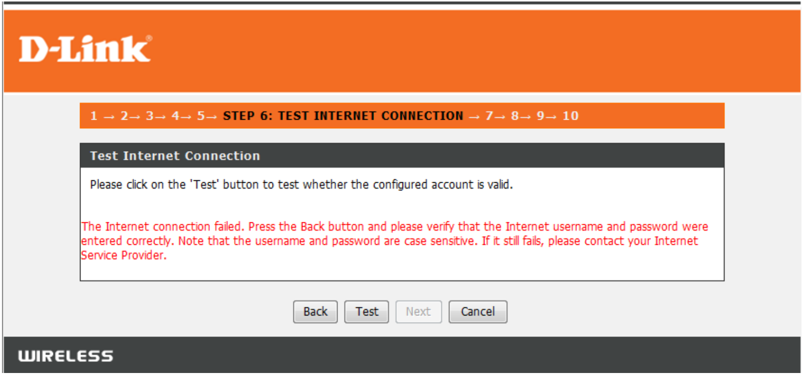
Test Internet Connection

Please click on the 'Test' button to test whether the configured account is valid.

Internet test successful. Please click Next to move to the next step.

Back
Test
Next
Cancel
WIRELESS

If the configured account is unvalid, you will see the follow message then you need click **Back** to enter the valid username and password.


D-Link
1 → 2→ 3→ 4→ 5→ STEP 6: TEST INTERNET CONNECTION → 7→ 8→ 9→ 10

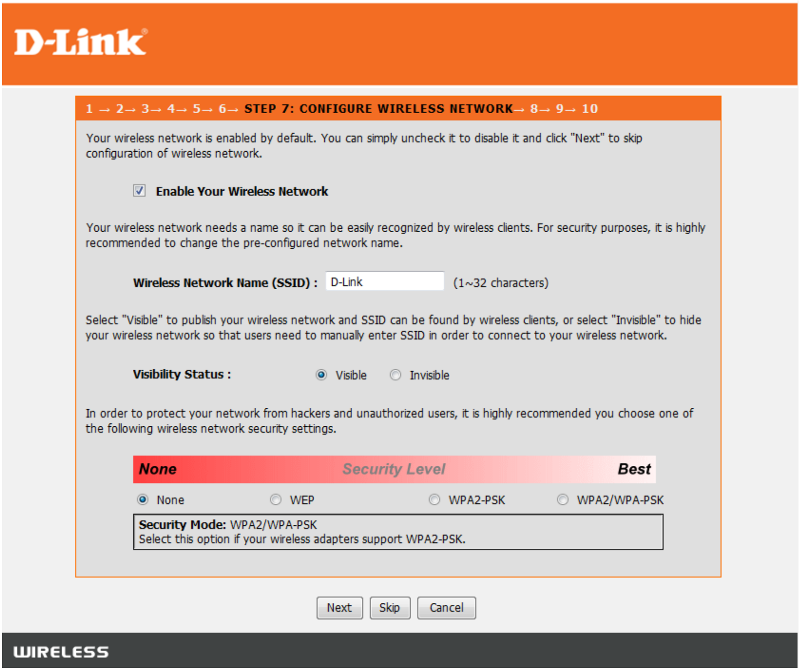
Test Internet Connection

Please click on the 'Test' button to test whether the configured account is valid.

The Internet connection failed. Press the Back button and please verify that the Internet username and password were entered correctly. Note that the username and password are case sensitive. If it still fails, please contact your Internet Service Provider.

Step 7 Configure Wireless Network

In this step you configure the Wireless Network. You can click on “Next” once you have modified the settings or click on “Skip” if you want to configure the Wireless Network on a later stage.



1 → 2→ 3→ 4→ 5→ 6→ STEP 7: CONFIGURE WIRELESS NETWORK→ 8→ 9→ 10

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

☑ **Enable Your Wireless Network**

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

Wireless Network Name (SSID) : D-Link (1~32 characters)

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

Visibility Status : ● Visible ○ Invisible

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

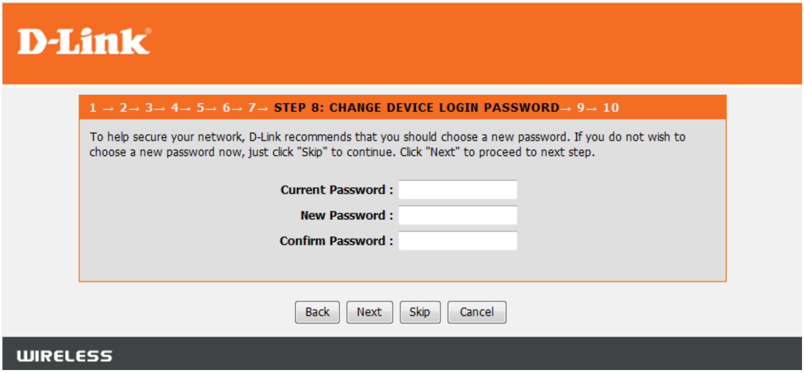
● None ○ WEP ○ WPA2-PSK ○ WPA2/WPA-PSK

Security Mode: WPA2/WPA-PSK
Select this option if your wireless adapters support WPA2-PSK.

Figure 15

Step 8 Change Device Login Password

The default admin account password is “admin”. To better secure your network we recommend changing the device login password. You can skip this step if you do not wish to change the default credentials of this device.



1 → 2→ 3→ 4→ 5→ 6→ 7→ STEP 8: CHANGE DEVICE LOGIN PASSWORD→ 9→ 10

To help secure your network, D-Link recommends that you should choose a new password. If you do not wish to choose a new password now, just click "Skip" to continue. Click "Next" to proceed to next step.

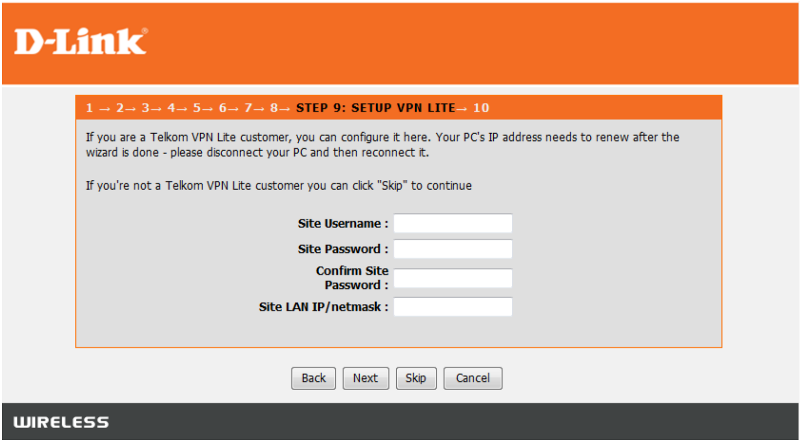
Current Password :

New Password :

Confirm Password :

Step 9 Setup VPN lite

If you have a VPN Lite account this section allows you to setup your account. Please enter your Username, Password and LAN IP/Netmask provided by your ISP. Example of IP/Netmask 10.0.16.0/24.



1 → 2→ 3→ 4→ 5→ 6→ 7→ 8→ STEP 9: SETUP VPN LITE→ 10

If you are a Telkom VPN Lite customer, you can configure it here. Your PC's IP address needs to renew after the wizard is done - please disconnect your PC and then reconnect it.

If you're not a Telkom VPN Lite customer you can click "Skip" to continue

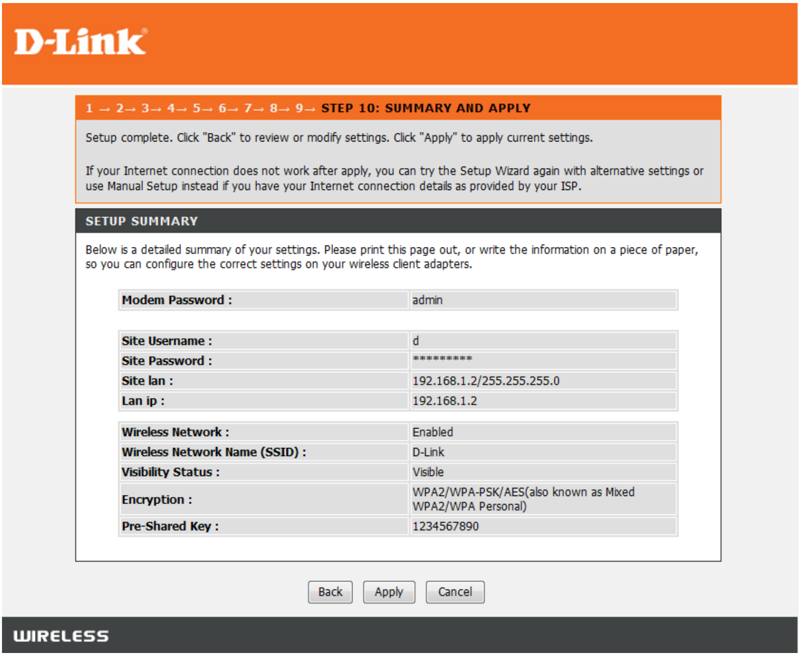
Site Username :

Site Password :

Confirm Site Password :

Site LAN IP/netmask :

Step 10 Summary and Apply



1 → 2→ 3→ 4→ 5→ 6→ 7→ 8→ 9→ STEP 10: SUMMARY 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

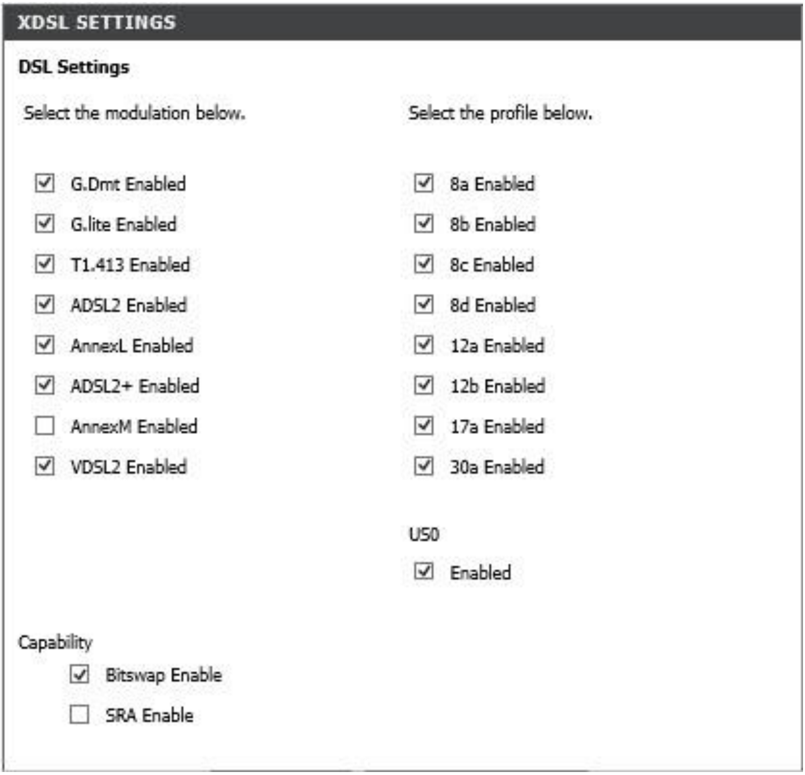
Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Modem Password :	admin
Site Username :	d
Site Password :	**********
Site lan :	192.168.1.2/255.255.255.0
Lan ip :	192.168.1.2
Wireless Network :	Enabled
Wireless Network Name (SSID) :	D-Link
Visibility Status :	Visible
Encryption :	WPA2/WPA-PSK/AES(also known as Mixed WPA2/WPA Personal)
Pre-Shared Key :	1234567890

Figure 16

4.2.2 xDSL Interface

The page is shown as the following figure appears.



XDSL SETTINGS

DSL Settings

Select the modulation below.

- ☑ G.Dmt Enabled
- ☑ G.lite Enabled
- ☑ T1.413 Enabled
- ☑ ADSL2 Enabled
- ☑ AnnexL Enabled
- ☑ ADSL2+ Enabled
- □ AnnexM Enabled
- ☑ VDSL2 Enabled

Select the profile below.

- ☑ 8a Enabled
- ☑ 8b Enabled
- ☑ 8c Enabled
- ☑ 8d Enabled
- ☑ 12a Enabled
- ☑ 12b Enabled
- ☑ 17a Enabled
- ☑ 30a Enabled

US0

- ☑ Enabled

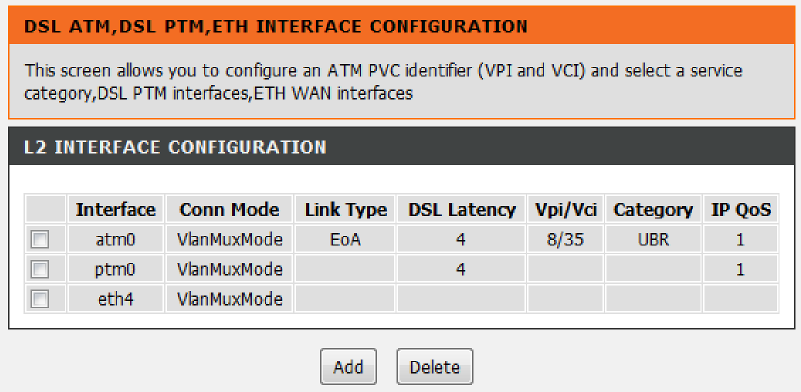
Capability

- ☑ Bitswap Enable
- □ SRA Enable

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.

4.2.3 Layer 2 Interface

Choose **Setup** > **Layer 2 Interface**. The page is shown as the following figure appears. In this page, you can configure the Layer 2 interface of the device.



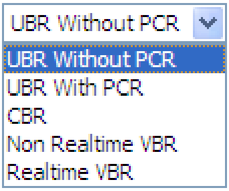
DSL ATM,DSL PTM,ETH INTERFACE CONFIGURATION

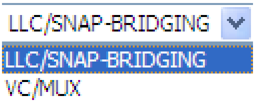
This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category,DSL PTM interfaces,ETH WAN interfaces

L2 INTERFACE CONFIGURATION

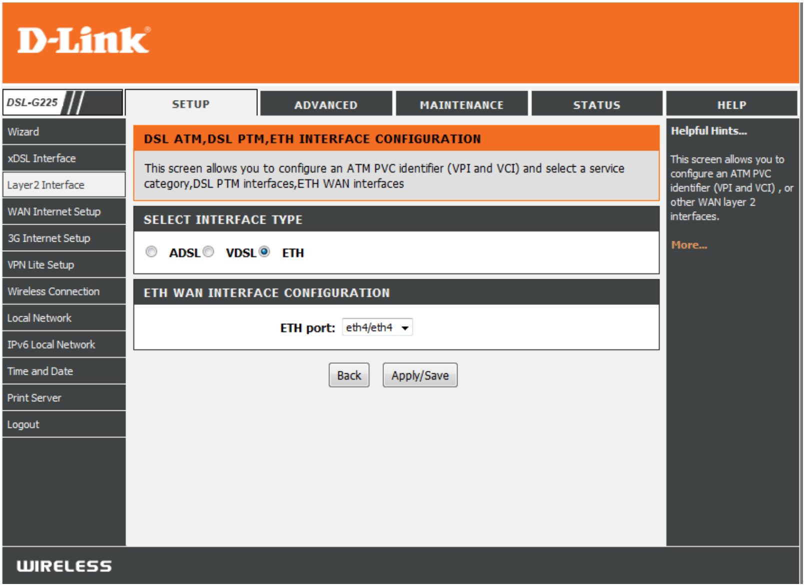
	Interface	Conn Mode	Link Type	DSL Latency	Vpi/Vci	Category	IP QoS
□	atm0	VlanMuxMode	EoA	4	8/35	UBR	1
□	ptm0	VlanMuxMode		4			1
□	eth4	VlanMuxMode					

Figure 17

Field	Description
PTM Layer2 Settings	● The virtual path between two points in an PTM
ETH Layer2 Settings	● The virtual path between two points in an ETH
ADSL 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).
Service Category	You can select from the drop-down list.  UBR Without PCR UBR Without PCR UBR With PCR CBR Non Realtime VBR Realtime VBR
QoS scheduler	You can select one of the items between **Strict Priority** and **Weighted Fair Queuing**.
Encapsulation	Select the method of encapsulation provided by your

Field	Description
Mode	ISP. You can select from the drop-down list.  LLC/SNAP-BRIDGING LLC/SNAP-BRIDGING VC/MUX

ETH Layer2 Settings



DSL ATM,DSL PTM,ETH INTERFACE CONFIGURATION

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category,DSL PTM interfaces,ETH WAN interfaces

SELECT INTERFACE TYPE

○ ADSL ○ VDSL ● ETH

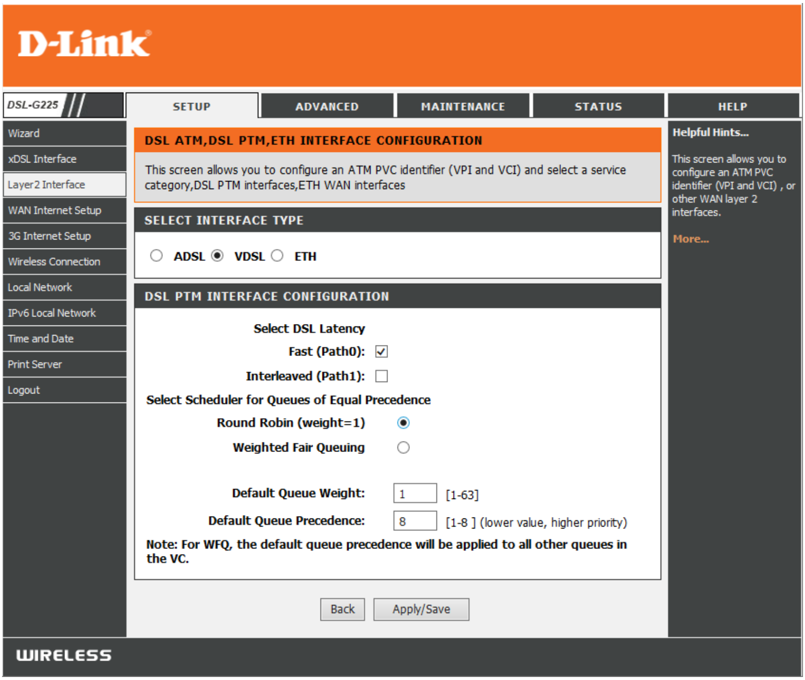
ETH WAN INTERFACE CONFIGURATION

ETH port: eth4/eth4

Helpful Hints...

This screen allows you to configure an ATM PVC identifier (VPI and VCI) , or other WAN layer 2 interfaces.

PTM Layer2 Settings



DSL ATM,DSL PTM,ETH INTERFACE CONFIGURATION

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category,DSL PTM interfaces,ETH WAN interfaces

SELECT INTERFACE TYPE

○ ADSL ● VDSL ○ ETH

DSL PTM INTERFACE CONFIGURATION

Select DSL Latency

Fast (Path0): ☑

Interleaved (Path1): □

Select Scheduler for Queues of Equal Precedence

Round Robin (weight=1) ●

Weighted Fair Queuing ○

Default Queue Weight: 1 [1-63]

Default Queue Precedence: 8 [1-8] (lower value, higher priority)

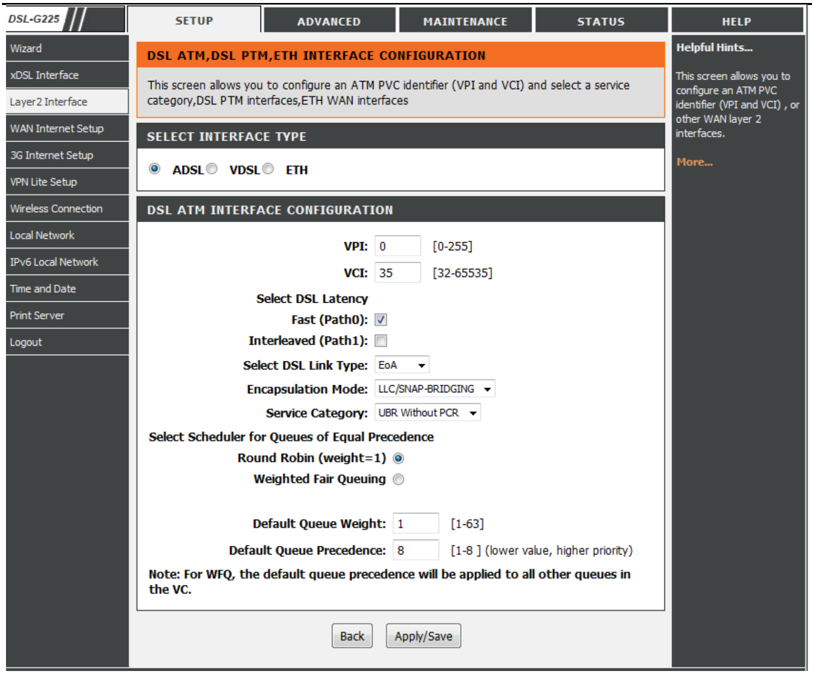
Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

Helpful Hints...

This screen allows you to configure an ATM PVC identifier (VPI and VCI) , or other WAN layer 2 interfaces.

More...

ADSL PVC Settings



DSL ATM,DSL PTM,ETH INTERFACE CONFIGURATION

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category,DSL PTM interfaces,ETH WAN interfaces

SELECT INTERFACE TYPE

● ADSL ○ VDSL ○ ETH

DSL ATM INTERFACE CONFIGURATION

VPI: 0 [0-255]

VCI: 35 [32-65535]

Select DSL Latency

Fast (Path0): ☑

Interleaved (Path1): □

Select DSL Link Type: EoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select Scheduler for Queues of Equal Precedence

Round Robin (weight=1) ●

Weighted Fair Queuing ○

Default Queue Weight: 1 [1-63]

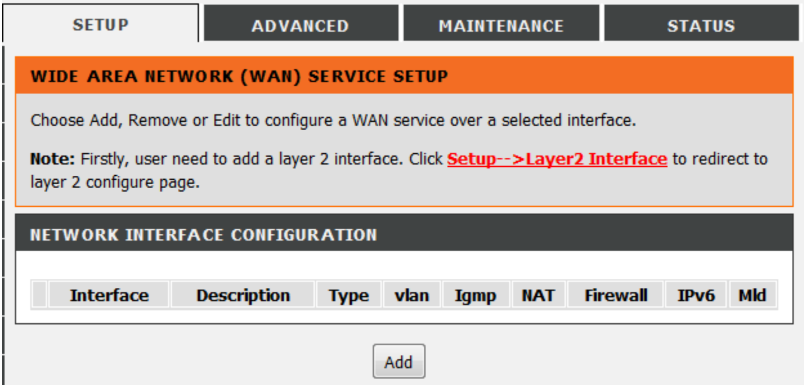
Default Queue Precedence: 8 [1-8] (lower value, higher priority)

Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

This screen allows you to configure an ATM PVC identifier (VPI and VCI) , or other WAN layer 2 interfaces.

4.2.4 WAN Service

Then choose **Setup** > **WAN Service**. The page is shown as the following figure appears. In this page, you can configure the WAN interface of the device.



WIDE AREA NETWORK (WAN) SERVICE SETUP

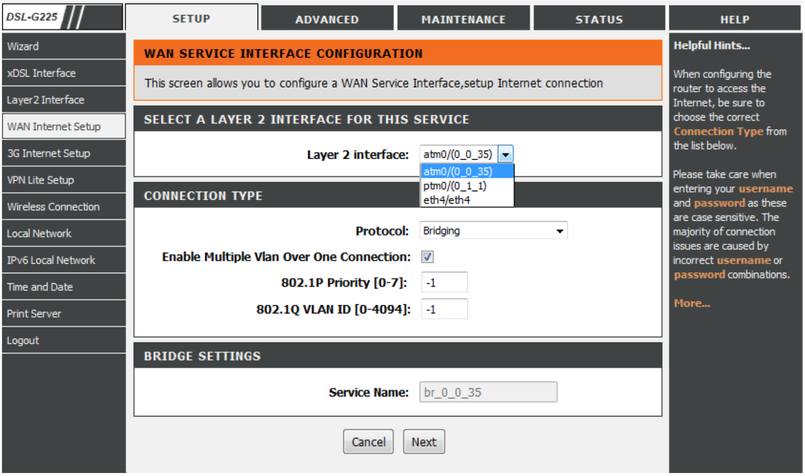
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Note: Firstly, user need to add a layer 2 interface. Click Setup-->Layer2 Interface to redirect to layer 2 configure page.

NETWORK INTERFACE CONFIGURATION

	Interface	Description	Type	vlan	Igmp	NAT	Firewall	IPv6	Mld

Click **Add in “WIDE AREA NETWORK (WAN) SERVICE SETUP”**. The page is shown in the following figure appears.you can select atm(ADSL), ptm(VDSL) or eth(ethernet WAN).



WAN SERVICE INTERFACE CONFIGURATION

This screen allows you to configure a WAN Service Interface,setup Internet connection

SELECT A LAYER 2 INTERFACE FOR THIS SERVICE

Layer 2 interface: atm0/(0_0_35)

atm0/(0_0_35)
ptm0/(0_1_1)
eth4/eth4

CONNECTION TYPE

Protocol: 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

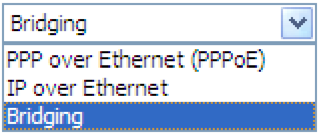
Helpful Hints...

When configuring the router to access the Internet, be sure to choose the correct Connection Type from the list below.

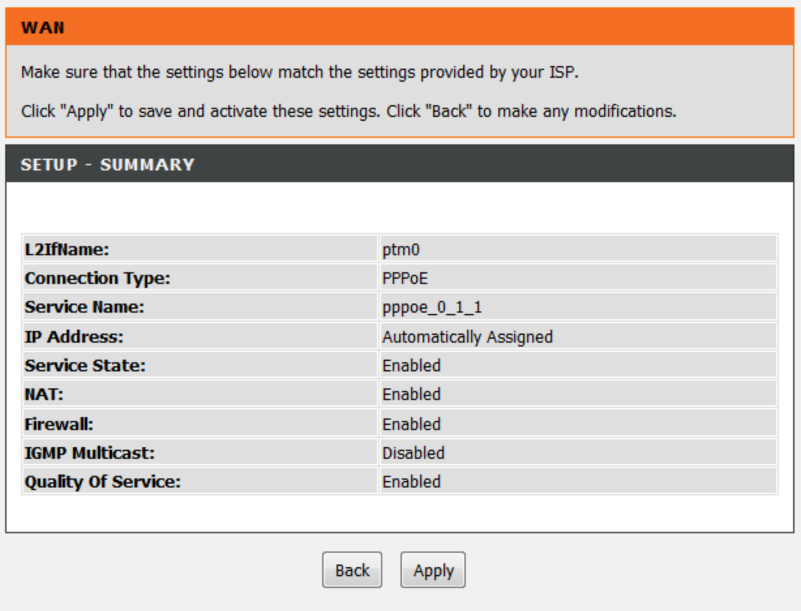
Please take care when entering your username and password as these are case sensitive. The majority of connection issues are caused by incorrect username or password combinations.

More...

Protocol	You can select from the drop-down list.

	 Bridging PPP over Ethernet (PPPoE) IP over Ethernet Bridging

Click **Next**, the page is shown as the following figure appears.



WAN

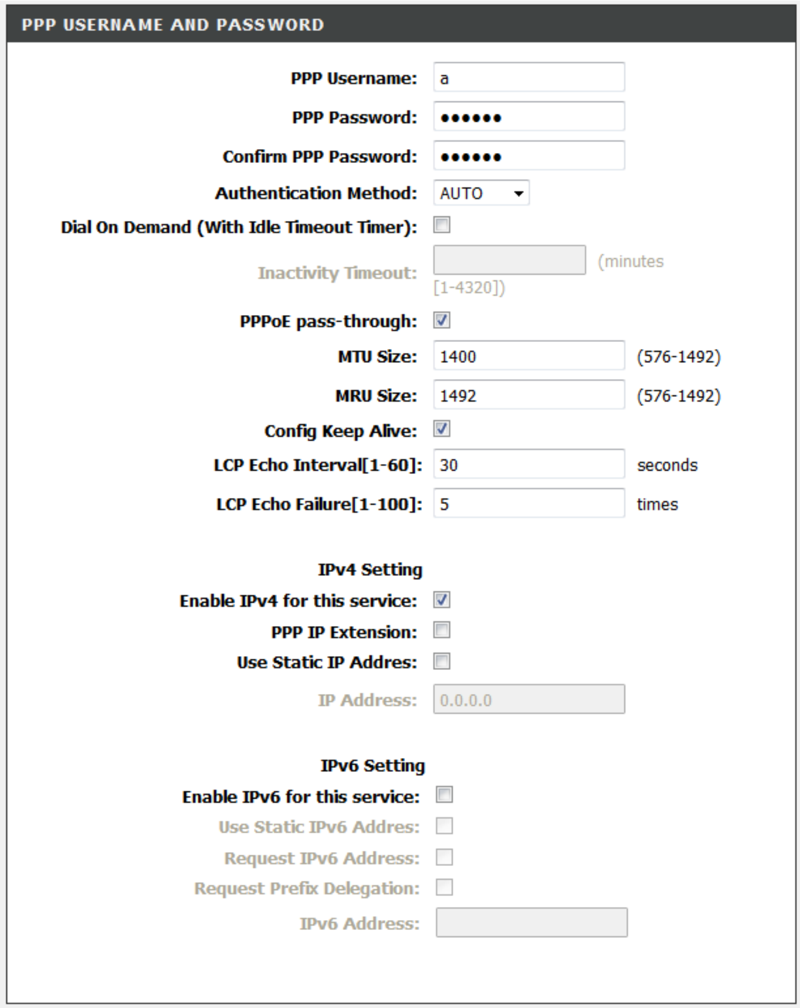
Make sure that the settings below match the settings provided by your ISP.

Click "Apply" to save and activate these settings. Click "Back" to make any modifications.

SETUP - SUMMARY

L2IfName:	ptm0
Connection Type:	PPPoE
Service Name:	pppoe_0_1_1
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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



PPP USERNAME AND PASSWORD

PPP Username:	a
PPP Password:	••••••
Confirm PPP Password:	••••••
Authentication Method:	AUTO
Dial On Demand (With Idle Timeout Timer):	□
Inactivity Timeout:	(minutes [1-4320])
PPPoE pass-through:	☑
MTU Size:	1400 (576-1492)
MRU Size:	1492 (576-1492)
Config Keep Alive:	☑
LCP Echo Interval[1-60]:	30 seconds
LCP Echo Failure[1-100]:	5 times
IPv4 Setting	
Enable IPv4 for this service:	☑
PPP IP Extension:	□
Use Static IP Addres:	□
IP Address:	0.0.0.0
IPv6 Setting	
Enable IPv6 for this service:	□
Use Static IPv6 Addres:	□
Request IPv6 Address:	□
Request Prefix Delegation:	□
IPv6 Address:	

- **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 modem does not detect the flow of the user continuously, the modem automatically stops the PPPoE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoE dialup.

  If this function is disabled, the modem performs PPPoE dial-up all the time. The PPPoE connection does not stop, unless the modem 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.
- **MRU Size:** Maximum Receive Unit. The Maximum Receive Unit(MRU) option must not be negotiated to a size larger than 1492, unless both the PPPoE client and server have indicated the ability to support a larger MRU in the PPPoE Discovery Stage.
- **PPP IP extension:** If this function is enabled, the WAN IP address obtained by the modem through built-in dial-up can be directly assigned to the PC being attached to the modem (at this time, the modem 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 modem.

If this function is disabled, the modem itself obtains the WAN IP address.

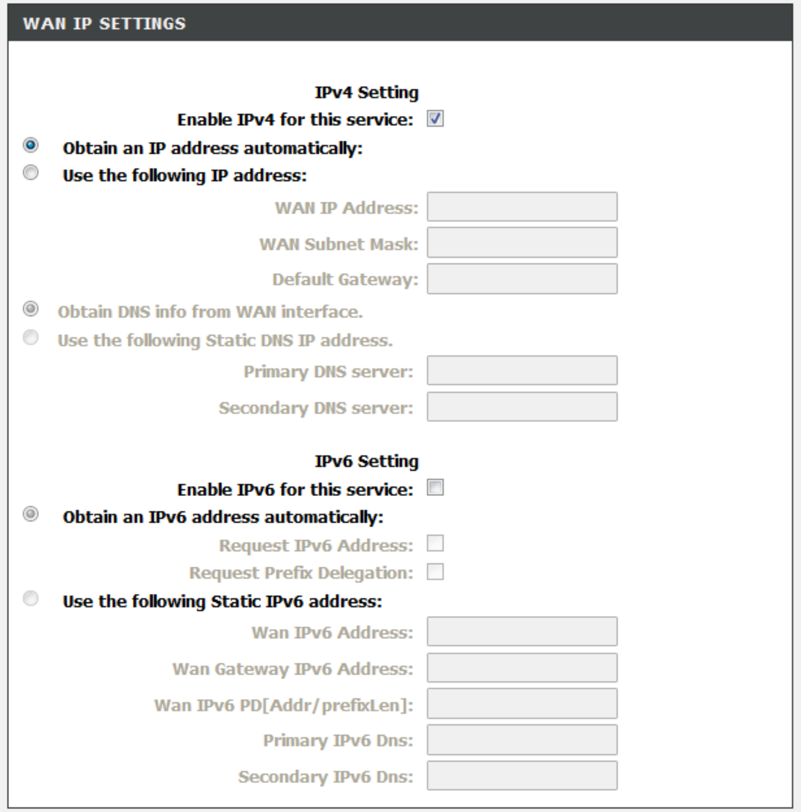
- **Config KeepAlive:** Whether to let the PPPoE dial-up keep alive
- **Use Static IP Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up.

If this function is enabled, the modem uses this IP address as the WAN IP address.

- **Enable IPv6 for this service:** If you want IPv6 to support this service, please select the **Enable IPv6 for this service** check box.
- **Request IPv6 Address:** The modem will obtain a WAN IPv6 address automatically.
- **Request Prefix Delegation**: The modem will request Prefix Delegation for local network.
- **Enable NAT:** Select it to enable the NAT functions of the modem. If you do not want to enable NAT and wish the modem 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.
- **Enable MLD Proxy**: MLD Proxy can be used to support IPv6 multicast data.

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



WAN IP SETTINGS

IPv4 Setting

Enable IPv4 for this service: ☑

● Obtain an IP address automatically:

○ Use the following IP address:

WAN IP Address:

WAN Subnet Mask:

Default Gateway:

● Obtain DNS info from WAN interface.

○ Use the following Static DNS IP address.

Primary DNS server:

Secondary DNS server:

IPv6 Setting

Enable IPv6 for this service: □

● Obtain an IPv6 address automatically:

Request IPv6 Address: □

Request Prefix Delegation: □

○ Use the following Static IPv6 address:

Wan IPv6 Address:

Wan Gateway IPv6 Address:

Wan IPv6 PD[Addr/prefixLen]:

Primary IPv6 Dns:

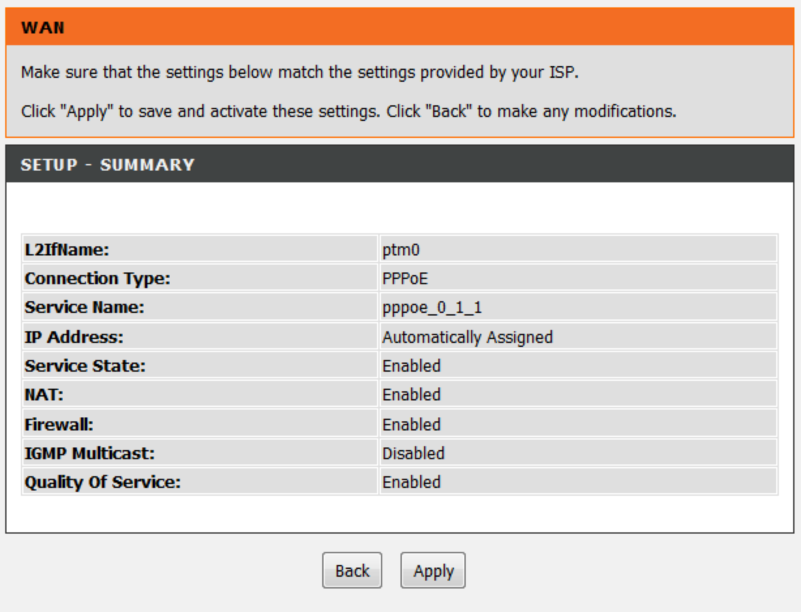
Secondary IPv6 Dns:

- **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.
- **Obtain an IPv6 address automatically:** Notice: If "**Obtain an IPv6 address automatically**" is chosen, DHCPv6 Client will be enabled on this WAN interface.
- **Use the following Static IPv6 address:** If "**Use the following Static IPv6 address**" is chosen, enter information provided to you by your ISP to configure the WAN IPv6 settings.

After proper settings, click **Next.**



WAN

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

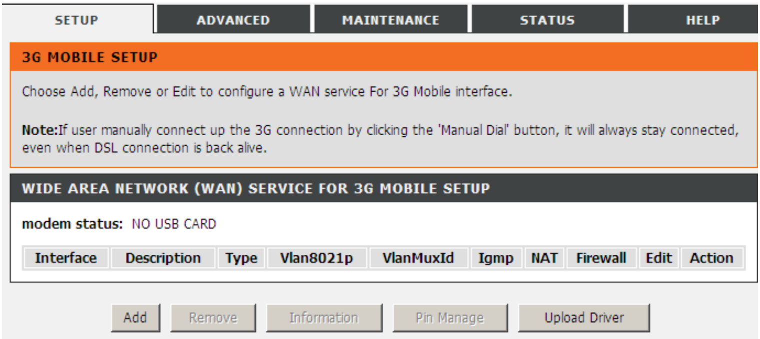
Click "Apply" to save and activate these settings. Click "Back" to make any modifications.

SETUP - SUMMARY

L2IfName:	ptm0
Connection Type:	PPPoE
Service Name:	pppoe_0_1_1
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

4.2.5 3G Internet Setup

Choose **3G Internet Setup** , and the following page appears.



3G MOBILE SETUP

Choose Add, Remove or Edit to configure a WAN service For 3G Mobile interface.

Note: If user manually connect up the 3G connection by clicking the 'Manual Dial' button, it will always stay connected, even when DSL connection is back alive.

WIDE AREA NETWORK (WAN) SERVICE FOR 3G MOBILE SETUP

modem status: NO USB CARD

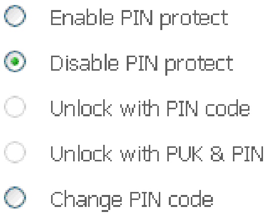
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Edit	Action

This page is used to configure 3G connection. If you want to access the Internet through 3G connection, a 3G network card is required. Connect the 3G network card to the USB interface of the Router.

If the 3G network card is installed, you may click the button on the **Action** column to establish or disconnect the 3G connection.

- **Add**:
- **Remove**:
- **Information**: Click it to display the information of the 3G network card.
- **Upload Driver**: For a un-support USB dongle, click it to upload the new driver for supporting the USB. The driver is a text file.
- **Pin Manage**: Click this button to manage the PIN.

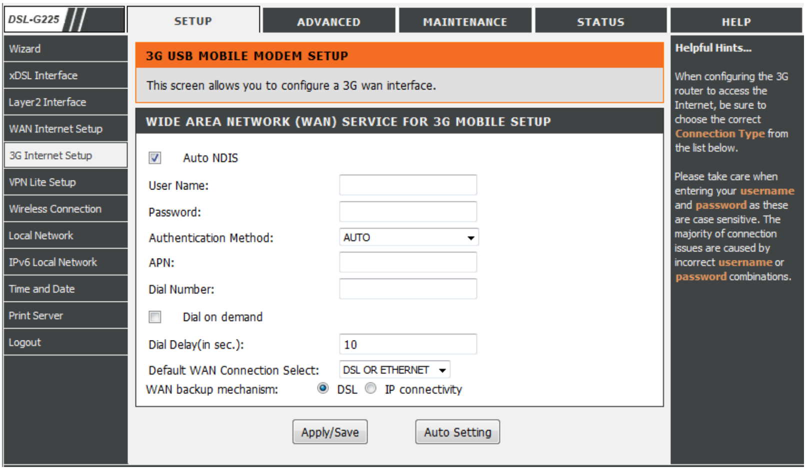
Click **Pin Manage** to show the following modes of PIN manage.



○ Enable PIN protect
● Disable PIN protect
○ Unlock with PIN code
○ Unlock with PUK & PIN
○ Change PIN code

  - **Enable PIN protect**: If you enable it, you need to enter the PIN code when rebooting or inserting the USB.
  - **Disable PIN protect**
  - **Unlock with PIN code**: If you disable it, you need to enter PIN code when using 3G.
  - **Unlock with PUK & PIN**: If you disable it, you need to enter PUK code when failing to enter the PIN code for 3 times.
  - **Change PIN code**: Choose it to change the PIN code.
- **Upload Driver**

Click **Add** in the **3G Mobile Setup** to display the following page.



3G USB MOBILE MODEM SETUP

This screen allows you to configure a 3G wan interface.

WIDE AREA NETWORK (WAN) SERVICE FOR 3G MOBILE SETUP

☑ Auto NDIS

User Name:

Password:

Authentication Method: AUTO

APN:

Dial Number:

□ Dial on demand

Dial Delay(in sec.): 10

Default WAN Connection Select: DSL OR ETHERNET

WAN backup mechanism: ● DSL ○ IP connectivity

Helpful Hints...

When configuring the 3G router to access the Internet, be sure to choose the correct **Connection Type** from the list below.

Please take care when entering your **username** and **password** as these are case sensitive. The majority of connection issues are caused by incorrect **username** or **password** combinations.

In this page, you are allowed to configure the settings of the 3G USB modem.

- **User Name:** Username provided by your 3G ISP.
- **Password:** Password provided by your 3G ISP.
- **Authentication Method:** Select a proper authentication method in the drop- down list. You can select Auto, PAP, CHAP, or MSCHAP.
- **APN:** APN (Access Point Name) is used to identify the service type. Enter the APN provided by your 3G ISP.
- **Dial Number:** Enter the dial number provided by your 3G ISP.
- **Dial on demand**: Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the 3G connection. Once it detects the flow (like access to a webpage), the modem restarts the 3G dialup.
- **Default WAN Connection Select**: You can select DSL or 3G from the drop-down list.
- **WAN back mechanism**: The 3G connection is the backup for the DSL connection.
  - **DSL**: If the DSL is disconnected, the 3G starts to dial.
  - **IP connectivity**: If the system fails to ping the specified IP address, the 3G starts to dial.

After finishing the setting, click the **Apply/Save** button to save the settings.

You may also click the **auto setting** button to automatically configure the 3G connection.

After clicking the **Apply/Save** button to take the settings in to effect.

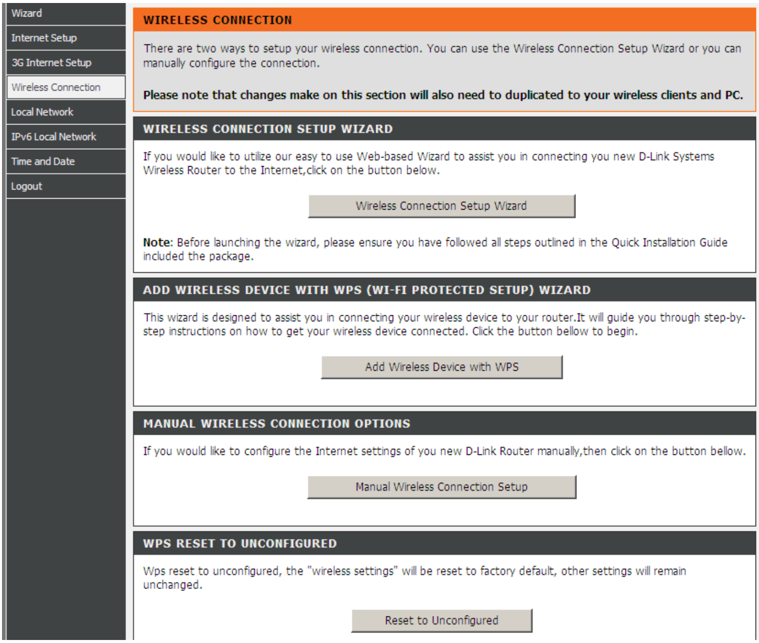
Note:

When there is no DSL WAN connection, insert the 3G network card, and then system will perform dial-up automatically. If the DSL WAN connection and the 3G connection coexist, the DSL WAN connection takes priority over the 3G connection. When the DSL WAN connection starts to perform dial-up, the 3G connection will be disconnected. If the DSL WAN connection has established, you may manually to perform 3G dial-up, and then the DSL WAN connection will be disconnected.

4.2.6 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 is shown as 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

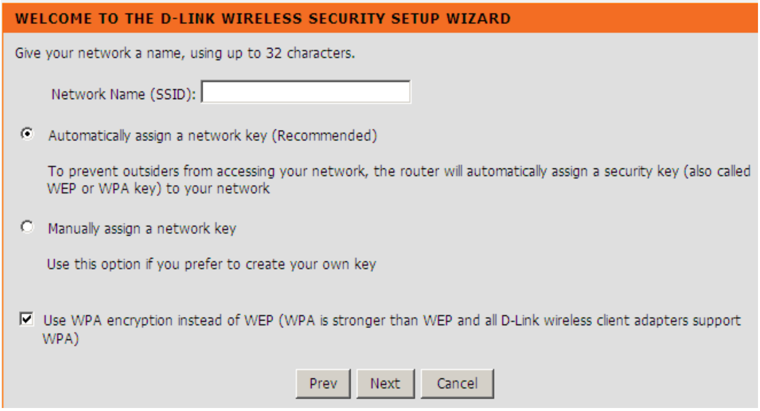
If you would like to configure the Internet settings of you new D-Link Router manually,then click on the button bellow.

WPS RESET TO UNCONFIGURED

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

4.2.6.1 Wireless Wizard

In **Wireless Connection** page, Click “**Wireless Connection Setup Wizard**”, the page is shown as 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)

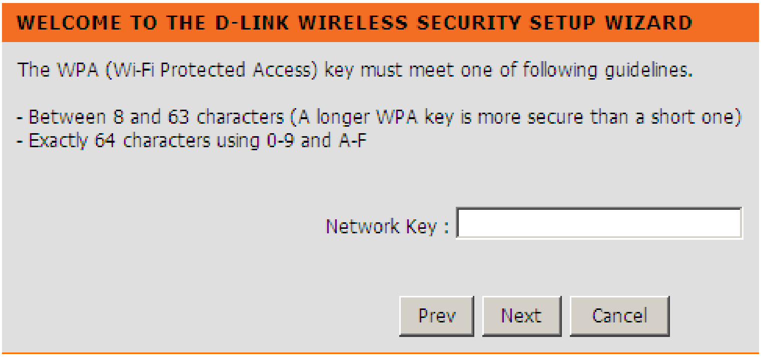
To prevent outsiders from accessing your network, the router will automatically assign a security key (also called WEP or WPA key) to your network

○ 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 choose "**Manually assign a network key**" and "**Use WPA encryption instead of WEP**", click "**Next**", the page is shown as the following figure appears.



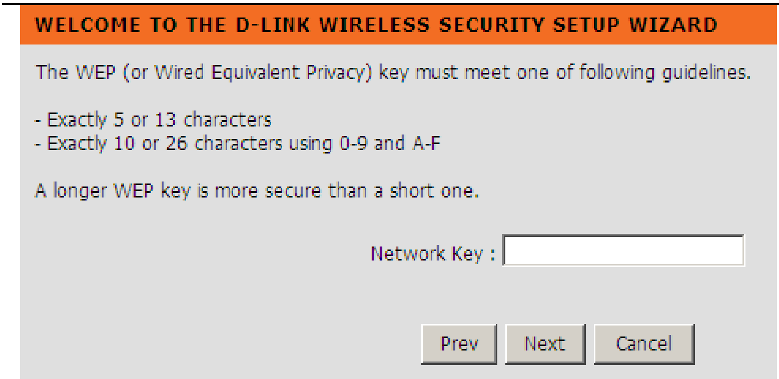
WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

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 is shown as the following figure appears.



WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

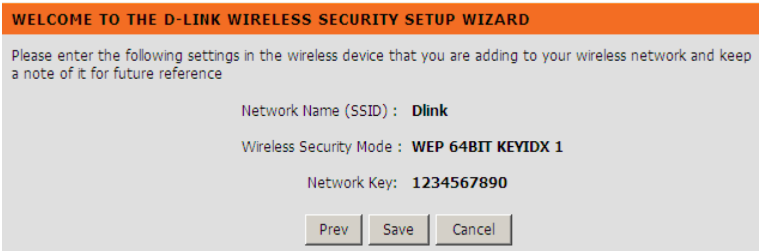
The WEP (or Wired Equivalent Privacy) key must meet one of following guidelines.

- 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 is shown as the following figure appears, you can confirm the wireless settings in this page.



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**

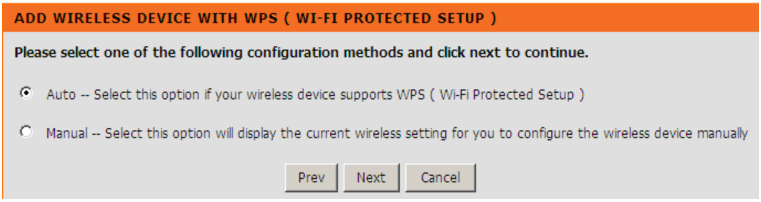
Wireless Security Mode : **WEP 64BIT KEYIDX 1**

Network Key: **1234567890**

Click **Save** to save the settings.

4.2.6.2 Adding Wireless Device

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



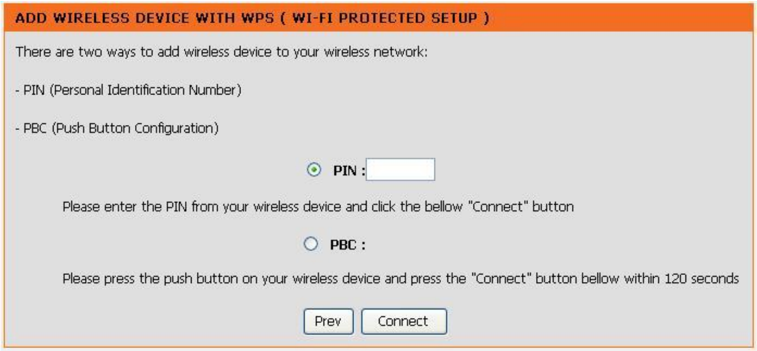
ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP)

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

Choose **Auto**, and then click **Next**, the page is shown as the following figure appears.



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)

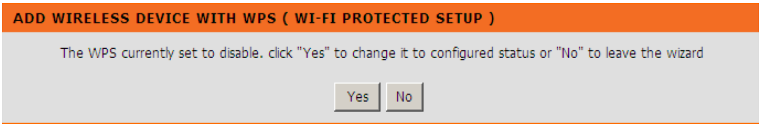
- PBC (Push Button Configuration)

● 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

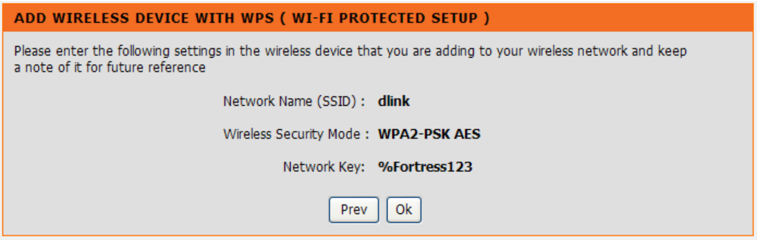


ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP)

The WPS currently set to disable. click "Yes" to change it to configured status or "No" to leave the wizard

When **PIN** is used, users are only allowed to enter no more than eight digits in the field.

Select **Manual**, click **Next**, the page is shown as 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) : dlink

Wireless Security Mode : WPA2-PSK AES

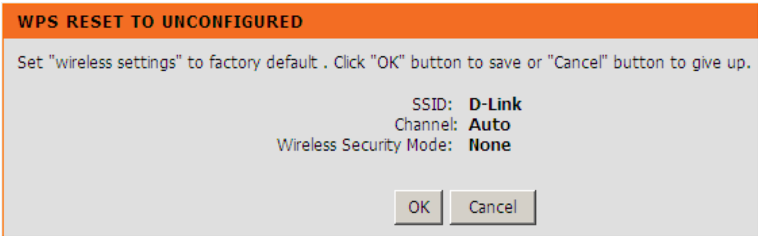
Network Key: %Fortress123

4.2.6.3 Manual Wireless Setup

If you want to configure the Internet settings of you new D-Link Router manually, click **Manual Wireless Connection Setup**. For the setup of this item, you can refer to **4.3.1 Wireless Settings.**

4.2.6.4 Resetting Wireless WPS

In **Wireless Connection** page, Click **Reset to Unconfigured,** the page is shown as the following figure appears.



WPS RESET TO UNCONFIGURED

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

SSID: **D-Link**
Channel: **Auto**
Wireless Security Mode: **None**

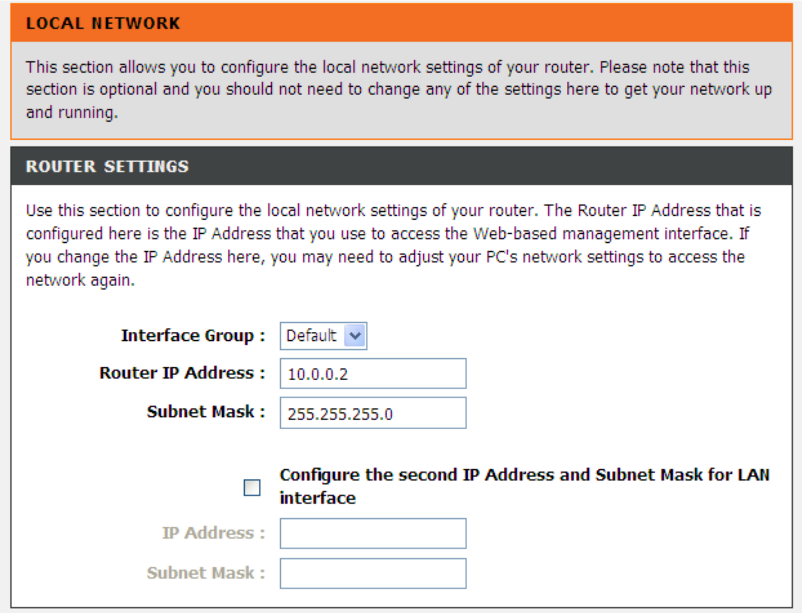
Once the "**Reset to Unconfigured**" button is clicked, the "wireless settings" will be reset to factory default, other settings will remain unchanged.

4.2.7 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 10.0.0.2. 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 is shown as 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.

Interface Group : Default

Router IP Address : 10.0.0.2

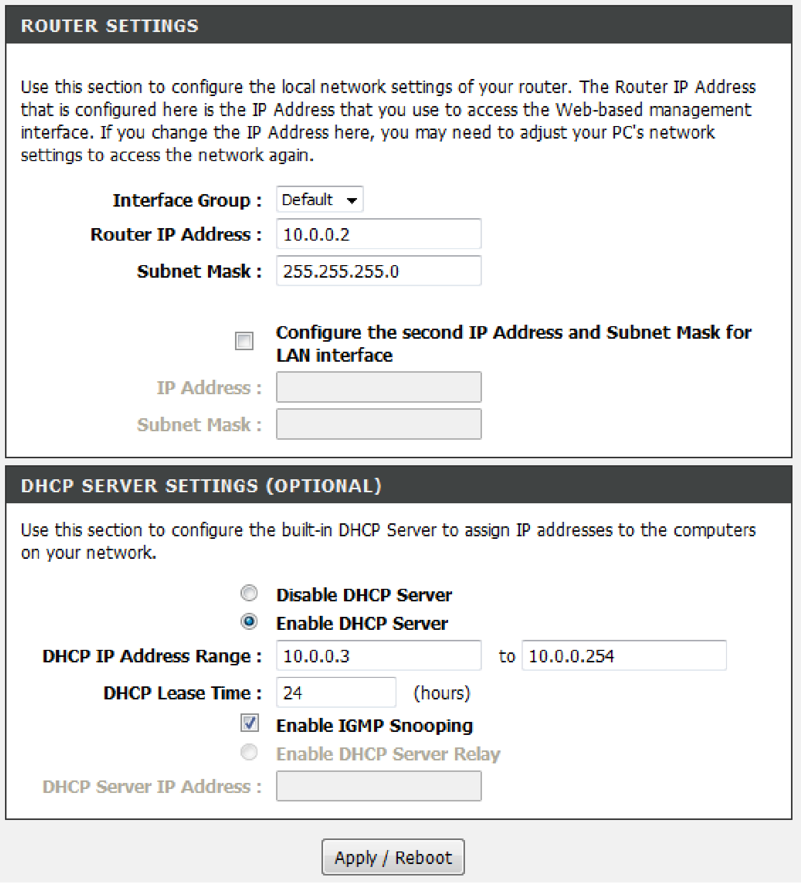
Subnet Mask : 255.255.255.0

□ 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 supplies 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.



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.

Interface Group :	Default
Router IP Address :	10.0.0.2
Subnet Mask :	255.255.255.0

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

IP Address :	
Subnet Mask :	

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 :	10.0.0.3 to 10.0.0.254
DHCP Lease Time :	24 (hours)

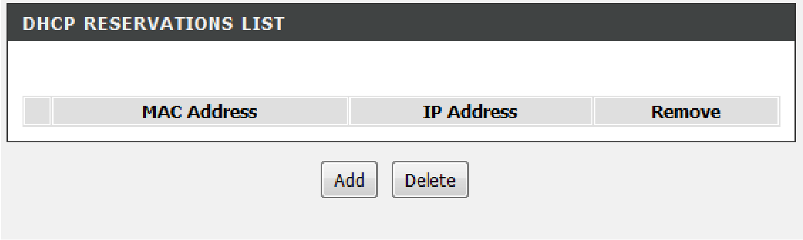
☑ Enable IGMP Snooping

○ Enable DHCP Server Relay

DHCP Server IP Address :

Click **Apply** to save the settings.

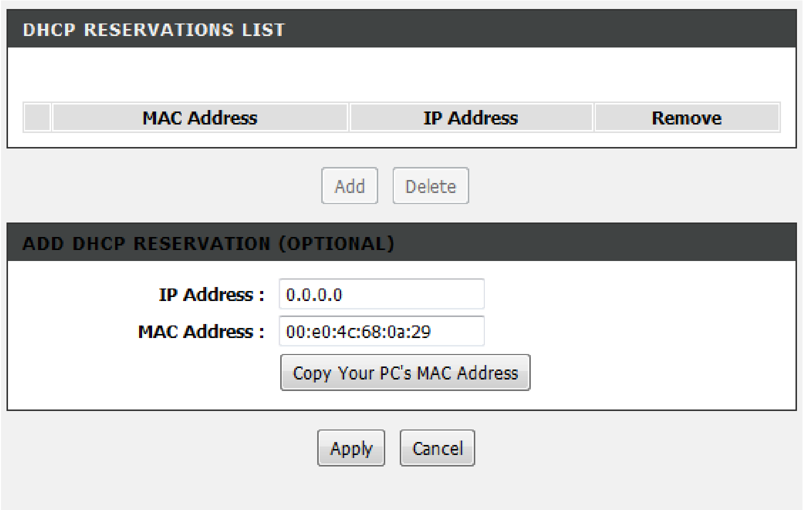
In the **Local Network** page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.



DHCP RESERVATIONS LIST

	MAC Address	IP Address	Remove

Click **Add** to add static DHCP (optional). The page is shown as the following figure appears.



DHCP RESERVATIONS LIST

	MAC Address	IP Address	Remove

ADD DHCP RESERVATION (OPTIONAL)

IP Address : 0.0.0.0

MAC Address : 00:e0:4c:68:0a:29

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.

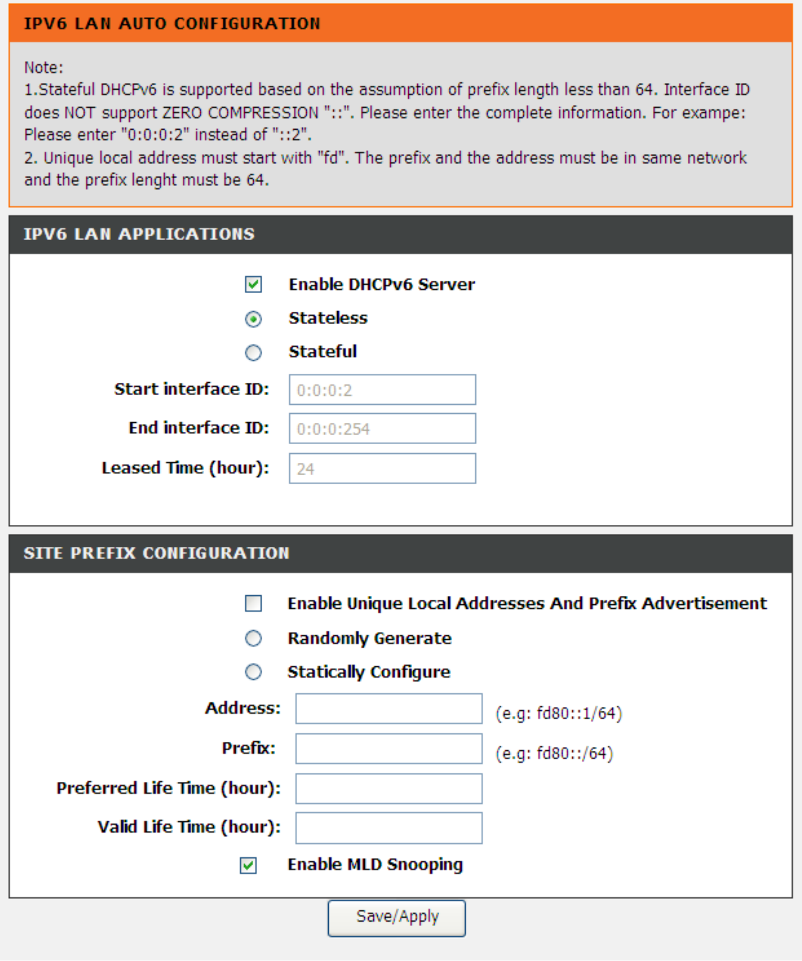
Click **Apply** to save the settings.

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**.

4.2.8 IPv6 Local Network

Choose **Setup** > **IPv6 Local Network**. **The IPv6 Local Network** page is shown as the following figure appears.



IPV6 LAN AUTO CONFIGURATION

Note:
1.Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For exampe: Please enter "0:0:0:2" instead of "::2".
2. Unique local address must start with "fd". The prefix and the address must be in same network and the prefix lenght must be 64.

IPV6 LAN APPLICATIONS

☑ Enable DHCPv6 Server

● Stateless

○ Stateful

Start interface ID: 0:0:0:2

End interface ID: 0:0:0:254

Leased Time (hour): 24

SITE PREFIX CONFIGURATION

□ Enable Unique Local Addresses And Prefix Advertisement

○ Randomly Generate

○ Statically Configure

Address: (e.g: fd80::1/64)

Prefix: (e.g: fd80::/64)

Preferred Life Time (hour):

Valid Life Time (hour):

☑ Enable MLD Snooping

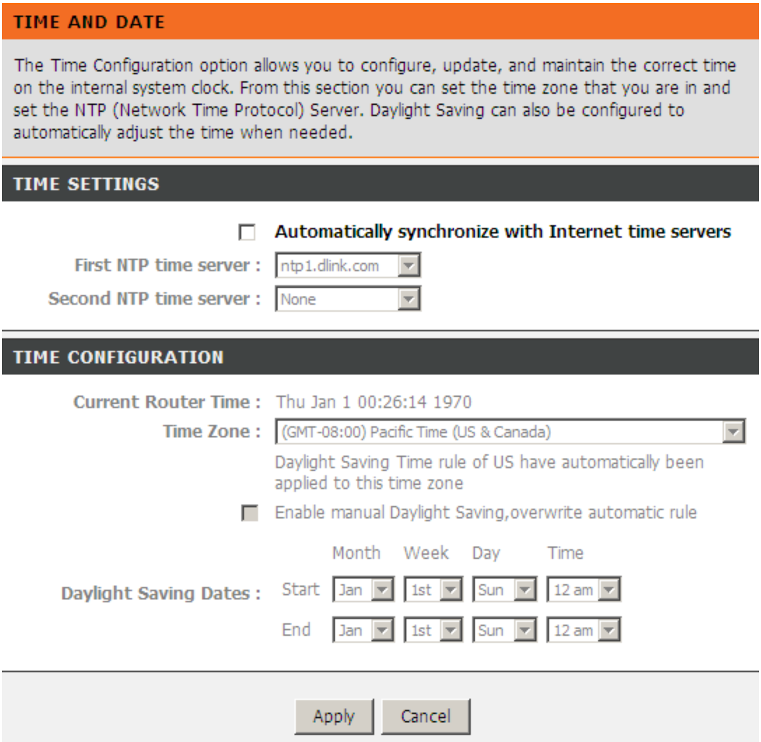
In this page, you can set an IP address for the DSL IPv6 router, enable the DHCPv6 server, enable RADVD and enable the MLD snooping function.

- **Enable DHCPv6 Server:** WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6) originally developed by the KAME project. The implementation mainly complies with the following standards: RFC3315, RFC3319, RFC3633, RFC3646, RFC4075, RFC 4272 etc.
- **Enable RADVD:** The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.
- **Enable MLD Snooping**: Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

After finishing setting, click the **Save/Apply** button to apply the settings.

4.2.9 Time and Date

Choose **Setup** > **Time and Date**. The page is shown as the following figure appears.



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 00:26:14 1970

Time Zone : (GMT-08:00) Pacific Time (US & Canada)

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

☐ Enable manual Daylight Saving,overwrite automatic rule

Daylight Saving Dates :

	Month	Week	Day	Time
Start	Jan	1st	Sun	12 am
End	Jan	1st	Sun	12 am

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**.

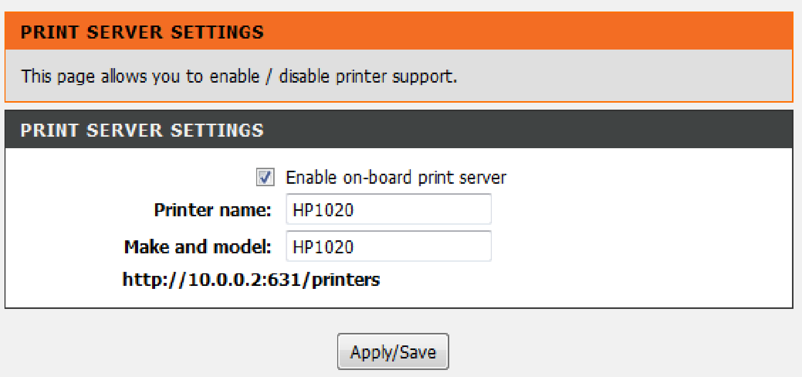
Select the specific time server and the time zone from the corresponding drop-down lists.

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

Click **Apply** to save the settings.

4.2.10 Print Server

Choose **Setup** > **Print Server**. The page is shown as the following figure appears.



PRINT SERVER SETTINGS

This page allows you to enable / disable printer support.

PRINT SERVER SETTINGS

☑ Enable on-board print server

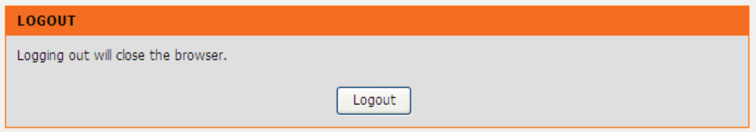
Printer name: HP1020

Make and model: HP1020

http://10.0.0.2:631/printers

4.2.11 Logout

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



LOGOUT

Logging out will close the browser.

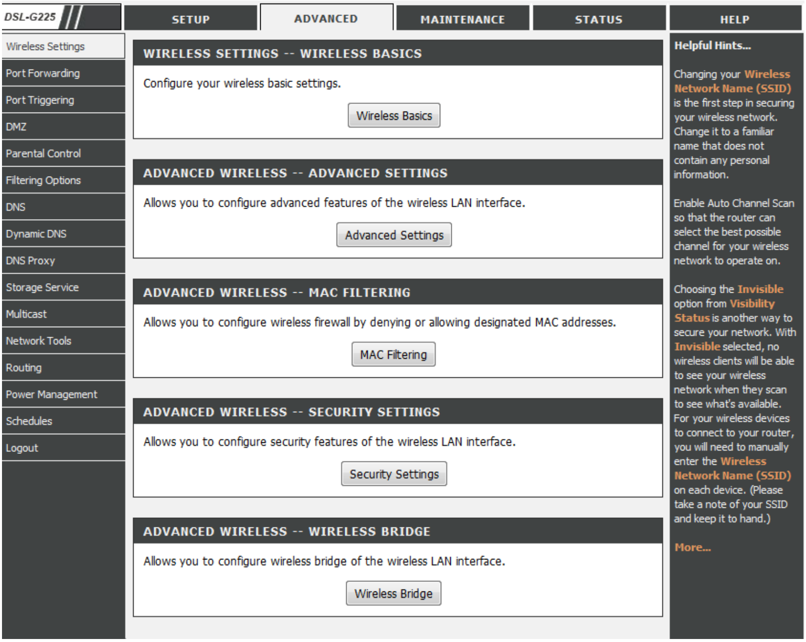
4.3 Advanced

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.

4.3.1 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 is shown as the following figure appears.



WIRELESS SETTINGS -- WIRELESS BASICS

Configure your wireless basic settings.

Wireless Basics

ADVANCED WIRELESS -- ADVANCED SETTINGS

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

Advanced Settings

ADVANCED WIRELESS -- MAC FILTERING

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

MAC Filtering

ADVANCED WIRELESS -- SECURITY SETTINGS

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

Security Settings

ADVANCED WIRELESS -- WIRELESS BRIDGE

Allows you to configure wireless bridge of the wireless LAN interface.

Wireless Bridge

Helpful Hints...

Changing your **Wireless Network Name (SSID)** is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.

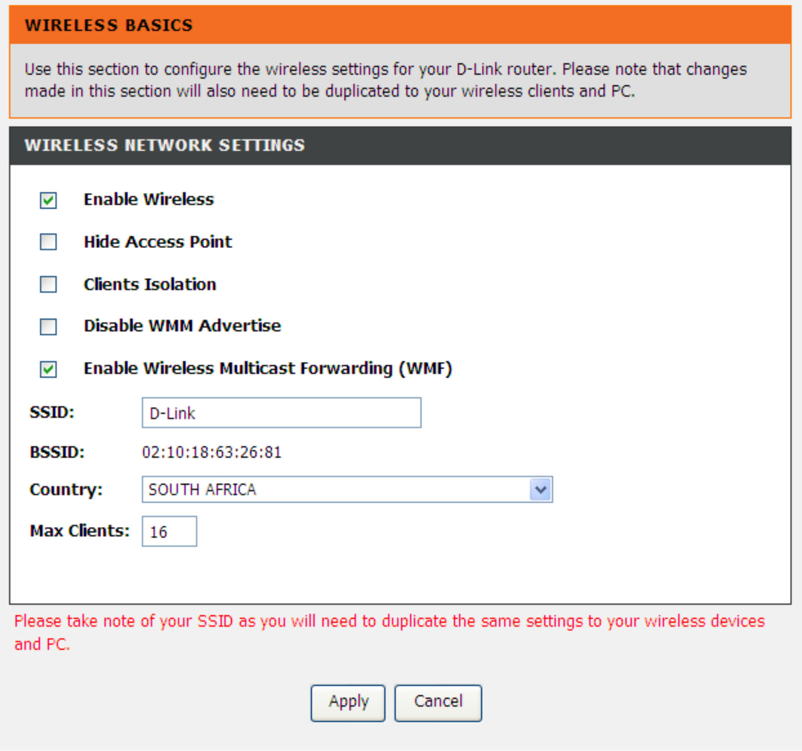
Enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on.

Choosing the **Invisible** option from **Visibility Status** is another way to secure your network. With **Invisible** selected, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your router, you will need to manually enter the **Wireless Network Name (SSID)** on each device. (Please take a note of your SSID and keep it to hand.)

More...

4.3.1.1 Wireless Basics

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



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

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

☑ Enable Wireless Multicast Forwarding (WMF)

SSID:	D-Link
BSSID:	02:10:18:63:26:81
Country:	SOUTH AFRICA
Max Clients:	16

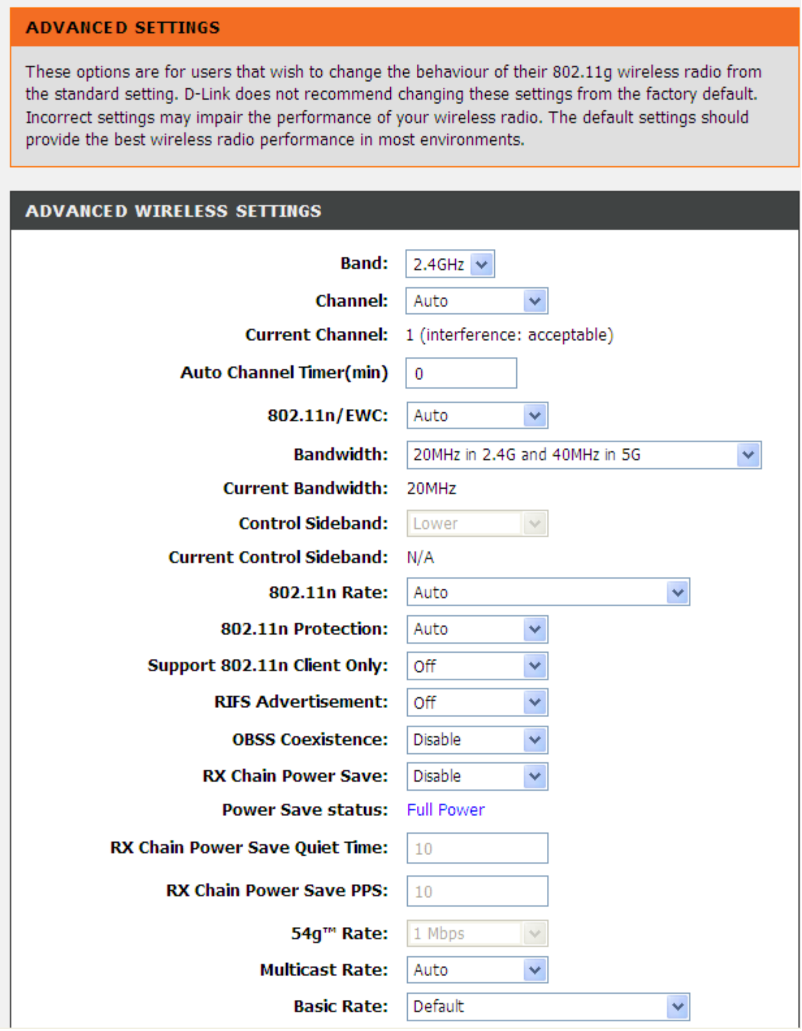
Please take note of your SSID as you will need to duplicate the same settings to your wireless devices and PC.

- **Enable Wireless**: Select the check box to turn the Wi-Fi on.
- **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.

Click **Apply** to save the settings.

4.3.1.2 Advanced Settings

Select **Advance Settings.** For a better view, the page is divided into two parts shown as the following figures appear.



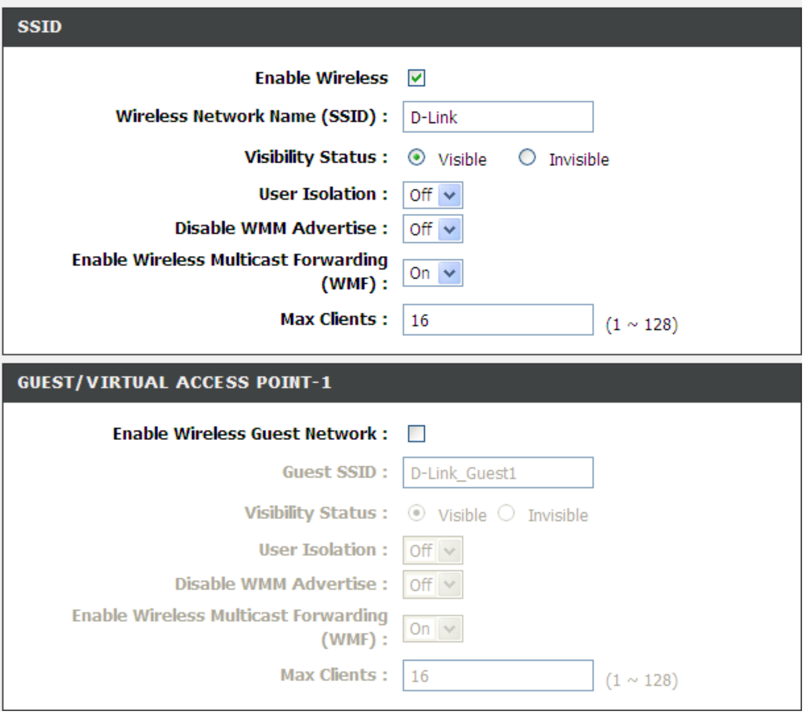
ADVANCED SETTINGS

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

Band:	2.4GHz
Channel:	Auto
Current Channel:	1 (interference: acceptable)
Auto Channel Timer(min)	0
802.11n/EWC:	Auto
Bandwidth:	20MHz in 2.4G and 40MHz in 5G
Current Bandwidth:	20MHz
Control Sideband:	Lower
Current Control Sideband:	N/A
802.11n Rate:	Auto
802.11n Protection:	Auto
Support 802.11n Client Only:	Off
RIFS Advertisement:	Off
OBSS Coexistence:	Disable
RX Chain Power Save:	Disable
Power Save status:	Full Power
RX Chain Power Save Quiet Time:	10
RX Chain Power Save PPS:	10
54g™ Rate:	1 Mbps
Multicast Rate:	Auto
Basic Rate:	Default

Figure 18 Advanced wireless setting-1



SSID

Enable Wireless ☑

Wireless Network Name (SSID) : D-Link

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

Disable WMM Advertise : Off

Enable Wireless Multicast Forwarding (WMF) : On

Max Clients : 16 (1 ~ 128)

GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network : □

Guest SSID : D-Link_Guest1

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

Disable WMM Advertise : Off

Enable Wireless Multicast Forwarding (WMF) : On

Max Clients : 16 (1 ~ 128)

Figure 19 Advanced wireless setting-2

- **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**.

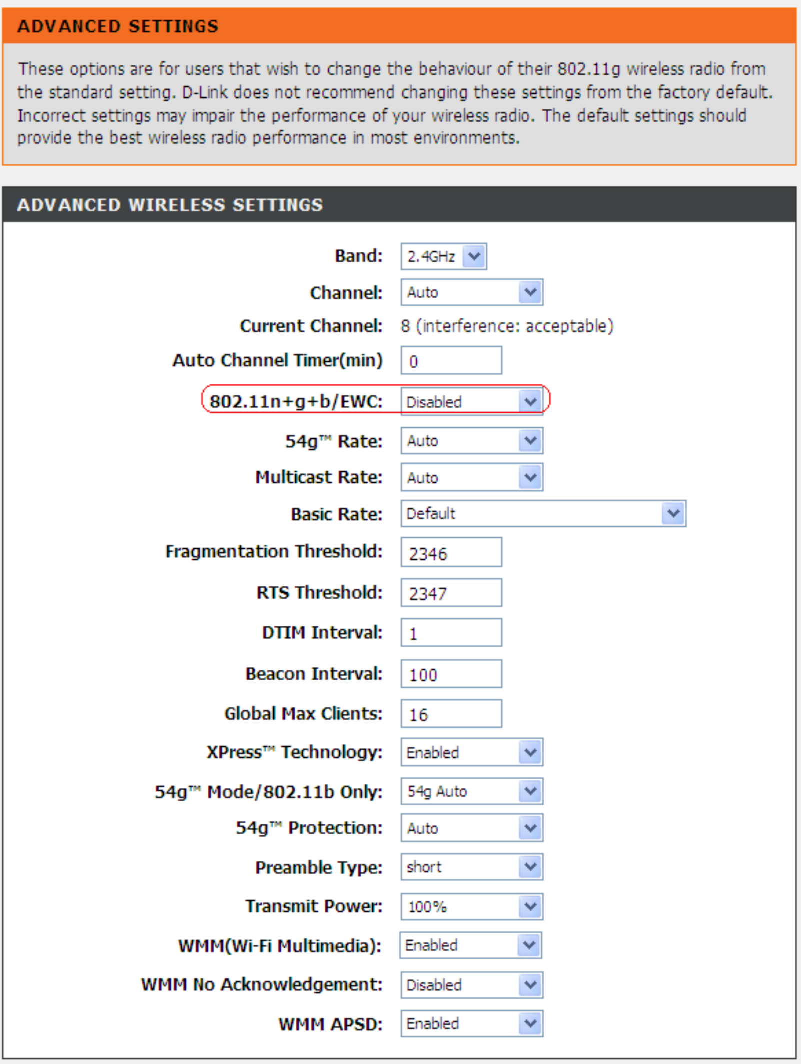
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** 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:**
- **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 relate to wireless do not take effects.
- **Enable Wireless**: Select this check box to turn Wi-Fi on.
- **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:** After enabling this option, the transmission performance multimedia of the voice and video data can be improved.
- **Enable Wireless Multicast Forwarding (WMF):** After enabling this option, the transmission quality of video service such as IPTV can be improved.
- **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.
- **GUEST/VIRTUAL ACCESS POINT-1/-2:** 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.

- **802.11b/g mode**



ADVANCED SETTINGS

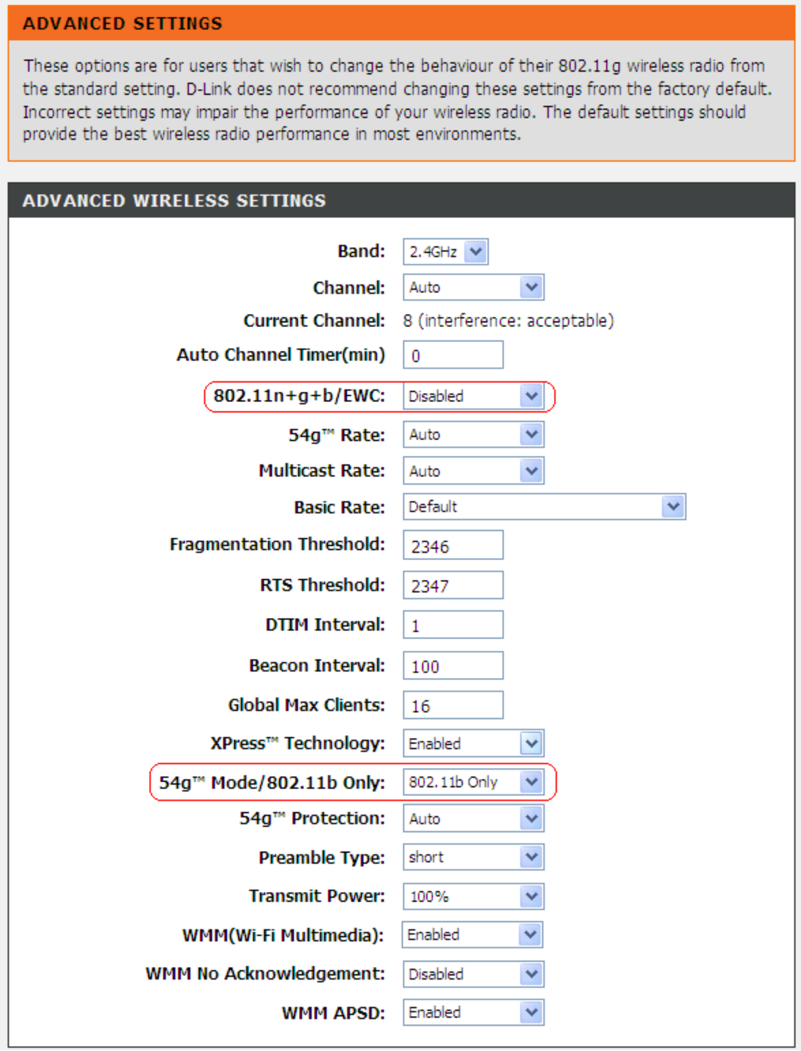
These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. D-Link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide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

ADVANCED WIRELESS SETTINGS

Band:	2.4GHz
Channel:	Auto
Current Channel:	8 (interference: acceptable)
Auto Channel Timer(min)	0
802.11n+g+b/EWC:	Disabled
54g™ Rate:	Auto
Multicast Rate:	Auto
Basic Rate:	Default
Fragmentation Threshold:	2346
RTS Threshold:	2347
DTIM Interval:	1
Beacon Interval:	100
Global Max Clients:	16
XPress™ Technology:	Enabled
54g™ Mode/802.11b Only:	54g Auto
54g™ Protection:	Auto
Preamble Type:	short
Transmit Power:	100%
WMM(Wi-Fi Multimedia):	Enabled
WMM No Acknowledgement:	Disabled
WMM APSD:	Enabled

Figure 20

- 802.11b mode



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.

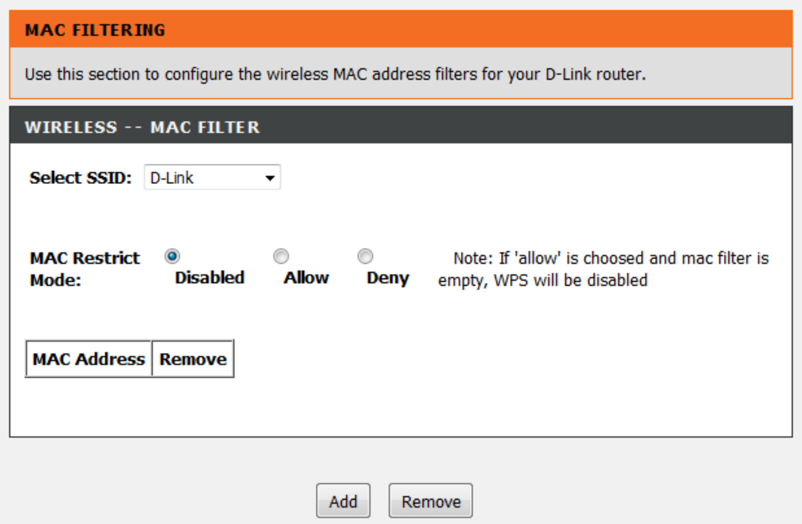
ADVANCED WIRELESS SETTINGS

Band:	2.4GHz
Channel:	Auto
Current Channel:	8 (interference: acceptable)
Auto Channel Timer(min)	0
802.11n+g+b/EWC:	Disabled
54g™ Rate:	Auto
Multicast Rate:	Auto
Basic Rate:	Default
Fragmentation Threshold:	2346
RTS Threshold:	2347
DTIM Interval:	1
Beacon Interval:	100
Global Max Clients:	16
XPress™ Technology:	Enabled
54g™ Mode/802.11b Only:	802.11b Only
54g™ Protection:	Auto
Preamble Type:	short
Transmit Power:	100%
WMM(Wi-Fi Multimedia):	Enabled
WMM No Acknowledgement:	Disabled
WMM APSD:	Enabled

4.3.1.3 MAC Filtering

In the **Wireless Settings** page, click **MAC Filtering**, the page is shown as the following figure appears.

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



MAC FILTERING

Use this section to configure the wireless MAC address filters for your D-Link router.

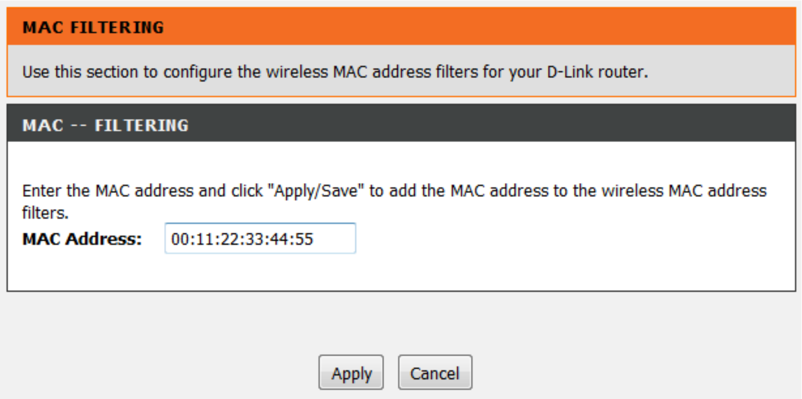
WIRELESS -- MAC FILTER

Select SSID: D-Link

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address	Remove

Click **Add**, the page is shown as the following figure appears.



MAC FILTERING

Use this section to configure the wireless MAC address filters for your D-Link router.

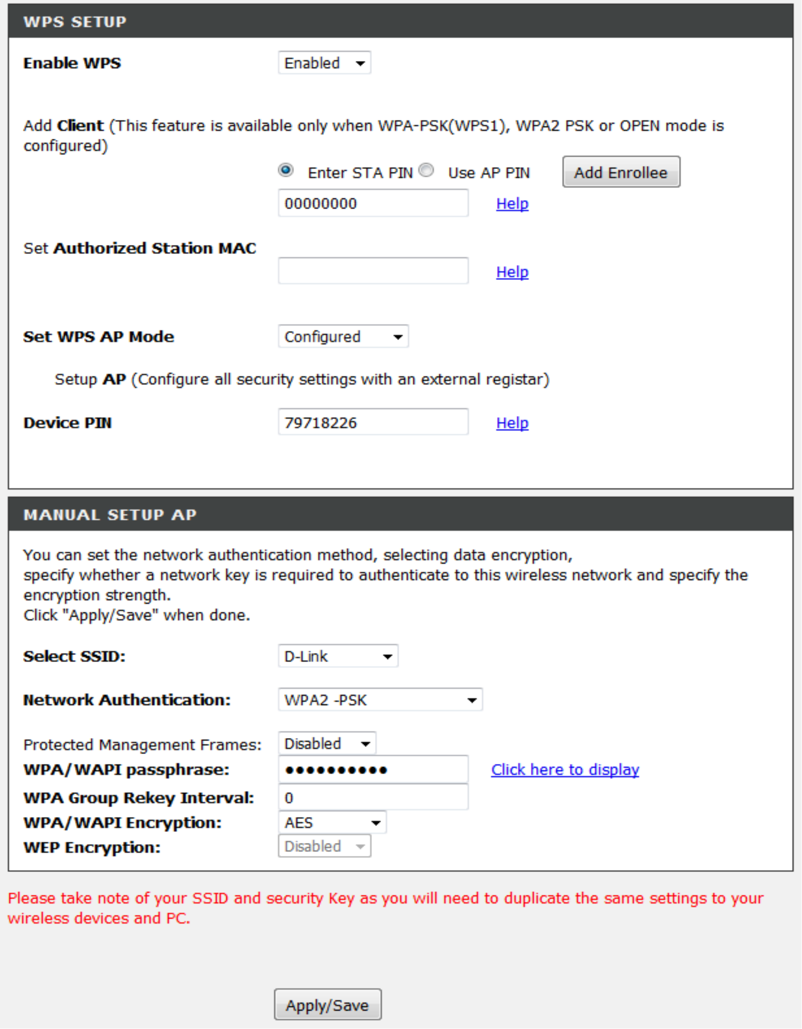
MAC -- FILTERING

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

MAC Address: 00:11:22:33:44:55

4.3.1.4 Security Settings

In the **Wireless Settings** page, click **Security Settings.** The page is shown as the following figure appears. This page allows you to select a security mode and to enable or disable WEP encryption. Note that depending on the network authentication that is selected, the page will change accordingly so additional fields can be configured for the specific security mode.



WPS SETUP

Enable WPS: Enabled

Add **Client** (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

● Enter STA PIN ○ Use AP PIN

00000000

Set **Authorized Station MAC**

Set WPS AP Mode: Configured

Setup **AP** (Configure all security settings with an external registar)

Device PIN: 79718226

MANUAL SETUP AP

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID: D-Link

Network Authentication: WPA2 -PSK

Protected Management Frames: Disabled

WPA/WAPI passphrase: ●●●●●●●●●●●

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: AES

WEP Encryption: Disabled

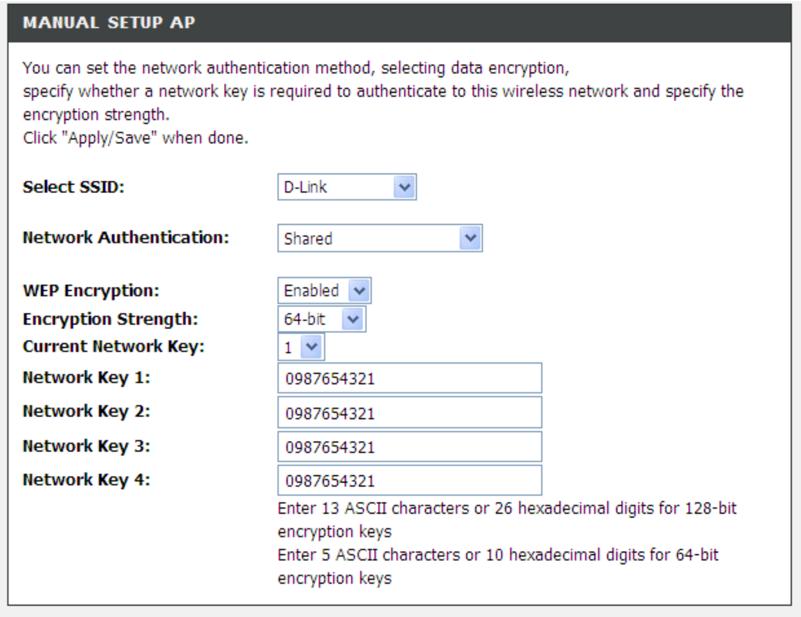
Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

- **Enable WPS**: Enable or disable the WPS function.
- **Select SSID:** Select the SSID that you want to configure from the drop-down list.
- **Network Authentication:** Select the encryption type from the **Security**

Mode

- **WEP Encryption:** Enable or disable WEP encryption.

Shared Key:



MANUAL SETUP AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:	D-Link
Network Authentication:	Shared
WEP Encryption:	Enabled
Encryption Strength:	64-bit
Current Network Key:	1
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

Shared Key (WEP) 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.

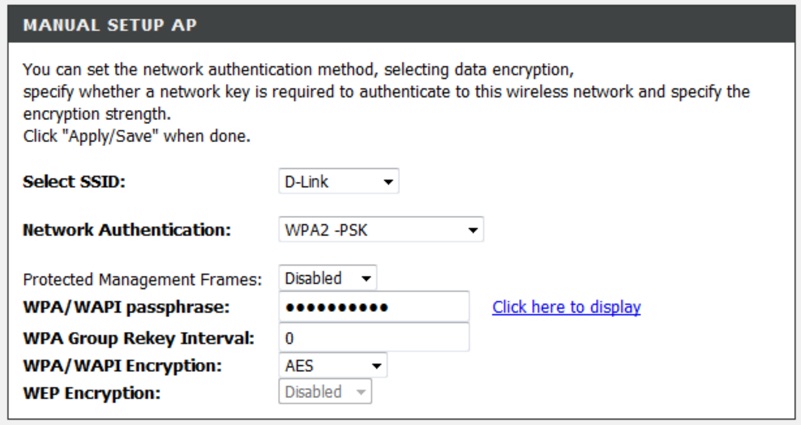
The router offers 64 or 128 bit encryption with four keys available.

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 the **Apply/Save** button to apply settings.

WPA2 only configuration is similar to WEP. The key length is between 8 to 63 ASCII characters or 64 hexadecimal digits.



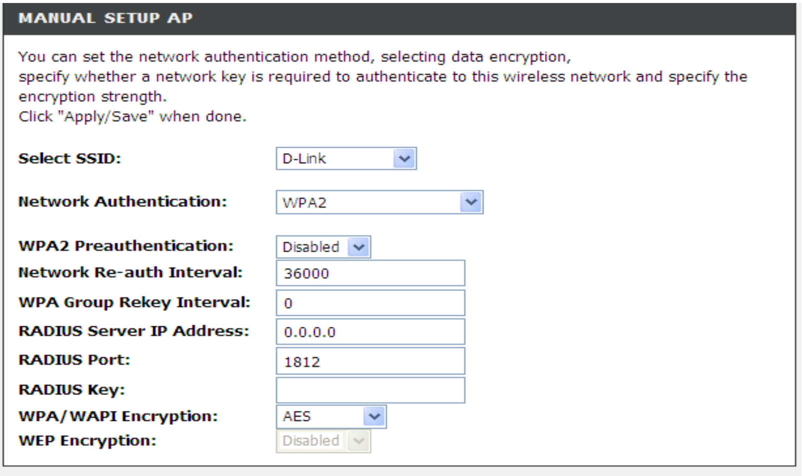
MANUAL SETUP AP

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:	D-Link
Network Authentication:	WPA2 -PSK
Protected Management Frames:	Disabled
WPA/WAPI passphrase:	●●●●●●●●●●●
WPA Group Rekey Interval:	0
WPA/WAPI Encryption:	AES
WEP Encryption:	Disabled

Radius:

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,



MANUAL SETUP AP

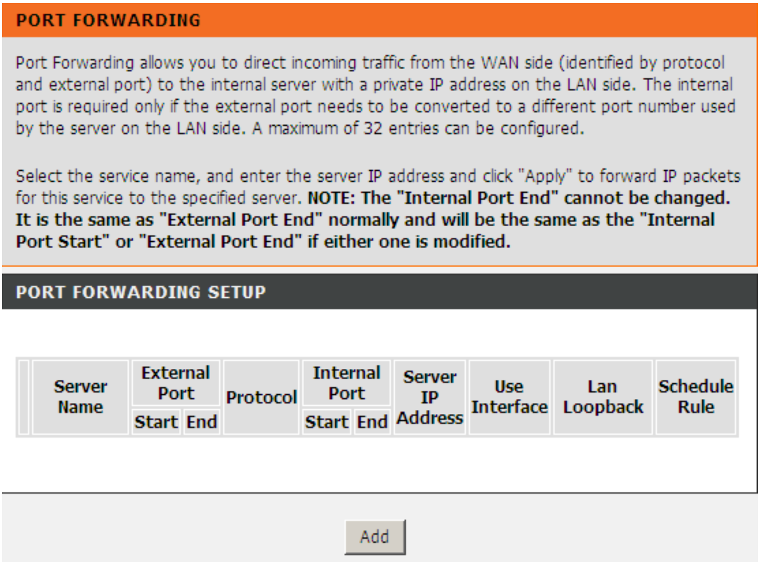
You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:	D-Link
Network Authentication:	WPA2
WPA2 Preauthentication:	Disabled
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	0
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	AES
WEP Encryption:	Disabled

4.3.2 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 is shown as the following figure appears.



PORT FORWARDING

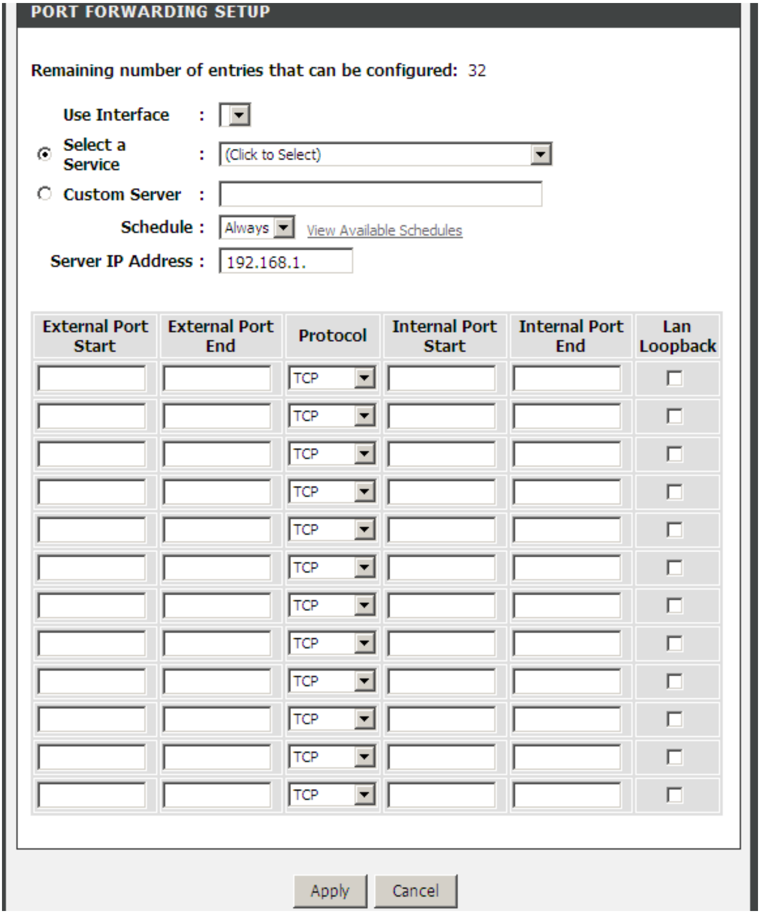
Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server 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	Lan Loopback	Schedule Rule
		Start	End		Start	End				

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



PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

Use Interface :

● Select a Service : (Click to Select)

○ Custom Server :

Schedule : Always

View Available Schedules

Server IP Address : 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Lan Loopback
		TCP			□
		TCP			□
		TCP			□
		TCP			□
		TCP			□
		TCP			□
		TCP			□
		TCP			□
		TCP			□
		TCP			□
		TCP			□
		TCP			□

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.

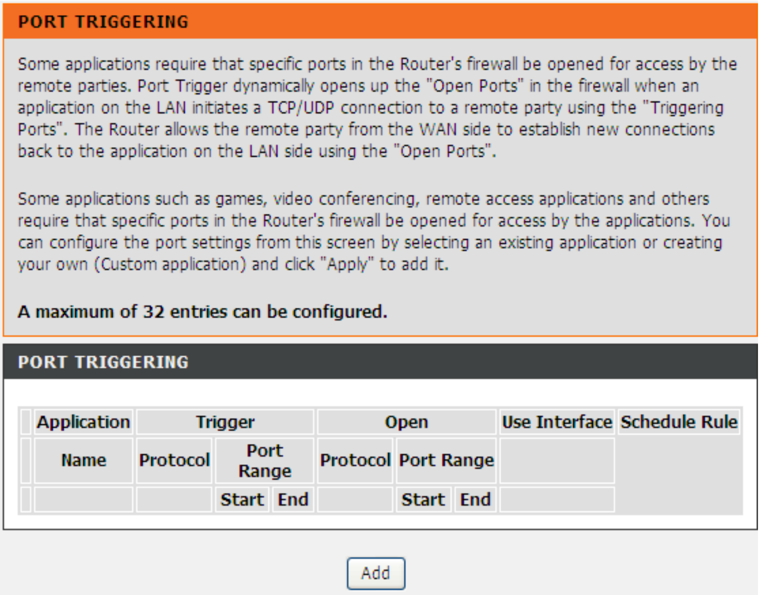
The Ports show the ports that you want to open on the device. The **TCP/UDP** means the protocol type of the opened ports.

Click **Apply** to save the settings.

4.3.3 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 is shown as 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".

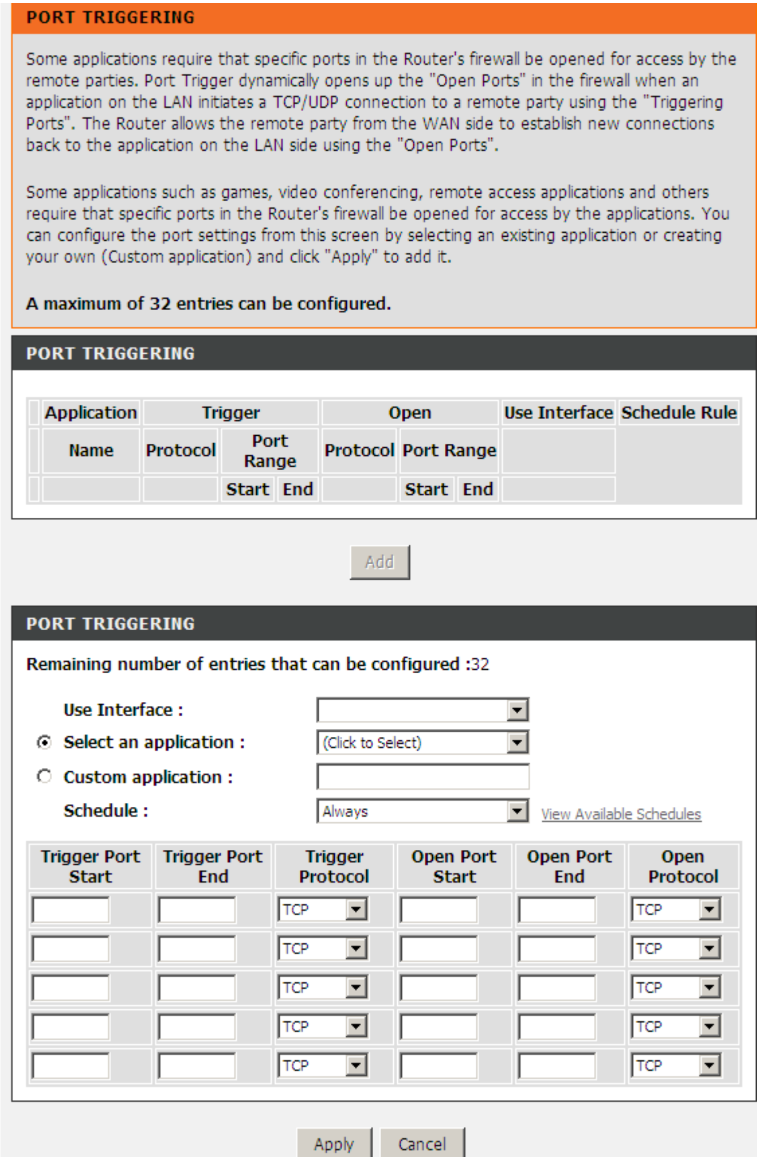
Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom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



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		

PORT TRIGGERING

Remaining number of entries that can be configured :32

Use Interface :	▾
● **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 ▾

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.

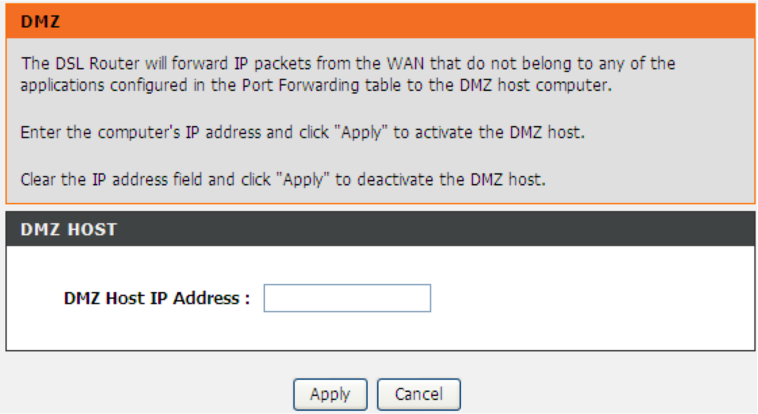
If the application you want to setup isn’t listed, click the **Custom application** radio button and type in a name for the trigger in the Custom application field. Configure the **Trigger Port Start**, **Trigger Port End**, **Trigger Protocol**, **Open Port Start**, **Open Port End** and **Open Protocol** settings for the port trigger you want to configure.

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

4.3.4 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 is shown as the following figure appears.



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.

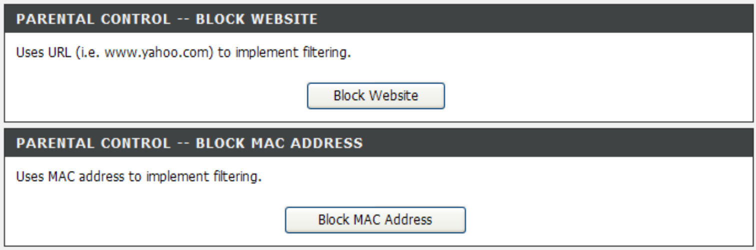
DMZ HOST

DMZ Host IP Address :

Click **Apply** to save the settings.

4.3.5 Parental Control

Choose **ADVANCED** > **Parental Control**. The **Parent Control** page is shown as the following figure appears.



PARENTAL CONTROL -- BLOCK WEBSITE

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

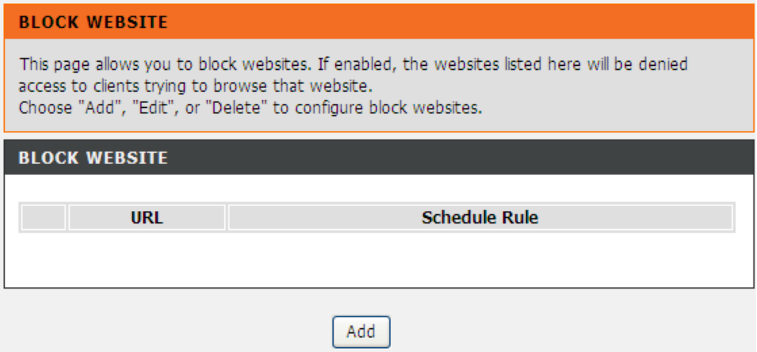
PARENTAL CONTROL -- BLOCK MAC ADDRESS

Uses MAC address to implement filtering.

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.

4.3.5.1 Block Website

The router can only block http sites and not secure sites, the router can’t block https sites. In the **Parent Control** page, click **Block Website**. The page is shown as the following figure appears.



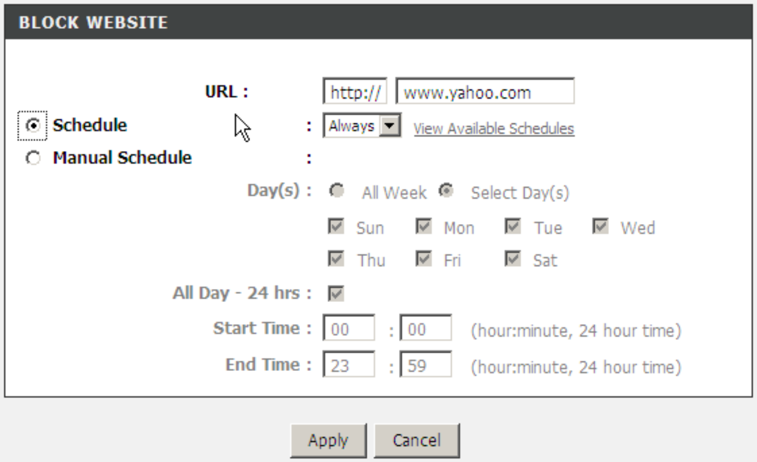
BLOCK WEBSITE

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.

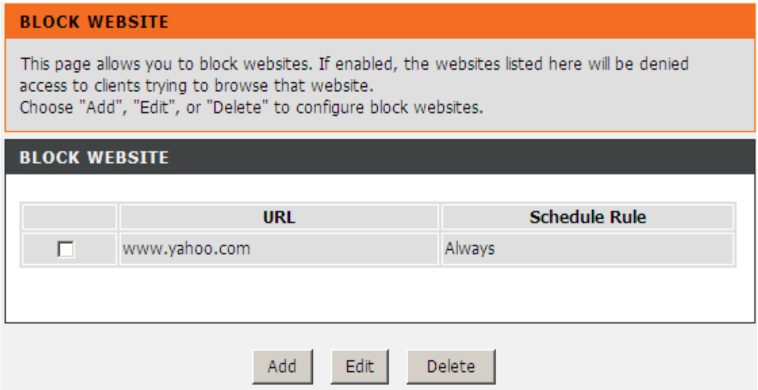


BLOCK WEBSITE

URL :	http:// www.yahoo.com	
● 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 :	00 : 00	(hour:minute, 24 hour time)
End Time :	23 : 59	(hour:minute, 24 hour time)

Enter the website to be blocked in the **URL** field. Select the **Schedule** from drop-down list, or select **Manual Schedule** and select the corresponding time and days.

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



BLOCK WEBSITE

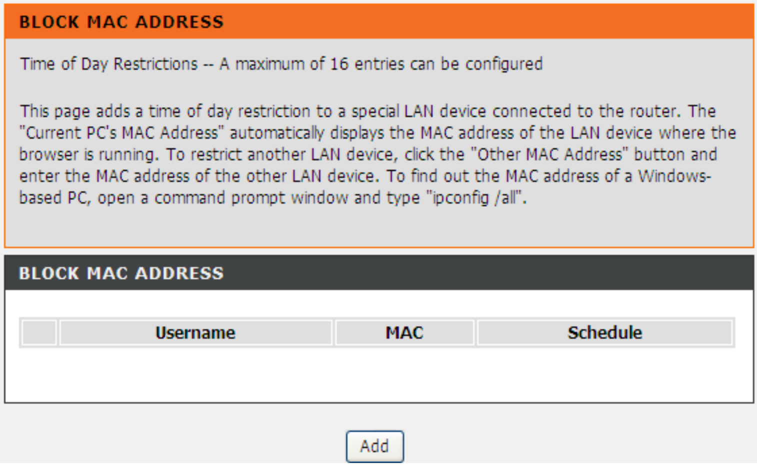
This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.
Choose "Add", "Edit", or "Delete" to configure block websites.

BLOCK WEBSITE

	URL	Schedule Rule
□	www.yahoo.com	Always

4.3.5.2 Block MAC Address

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



BLOCK MAC ADDRESS

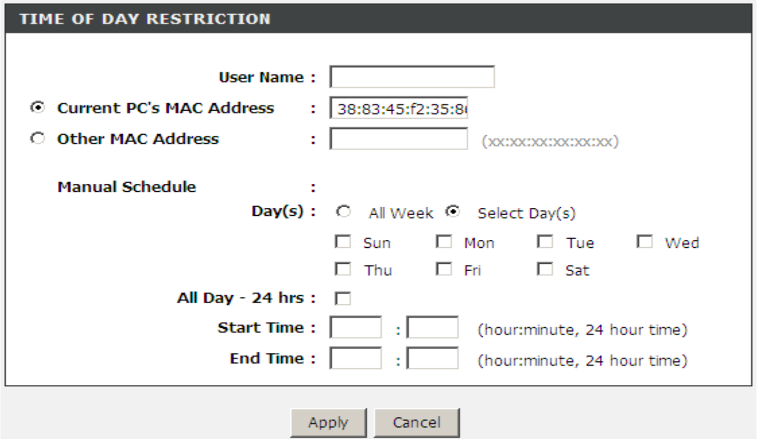
Time of Day Restrictions -- A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" 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 is shown as the following figure appears.



TIME OF DAY RESTRICTION

User Name :

● Current PC's MAC Address : 38:83:45:f2:35:8

○ 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)

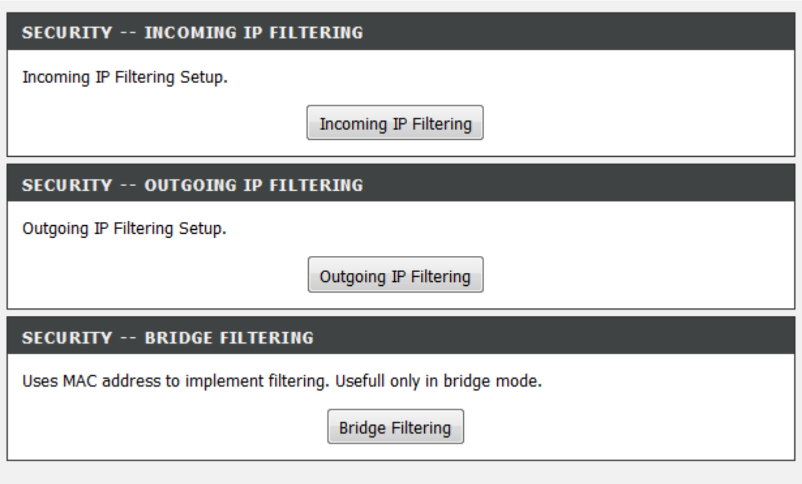
End Time : : (hour:minute, 24 hour time)

Enter the use name and MAC address and select the corresponding time and days.

Click **Apply** to add the MAC address to the **BLOCK MAC ADDRESS** table.

4.3.6 Filtering Options

Choose **ADVANCED** > **Filtering Options**. The **Filtering Options** page is shown as the following figure appears.



SECURITY -- INCOMING IP FILTERING

Incoming IP Filtering Setup.

SECURITY -- OUTGOING IP FILTERING

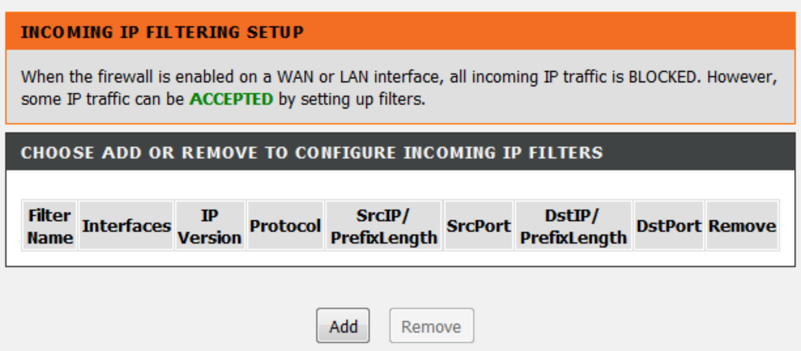
Outgoing IP Filtering Setup.

SECURITY -- BRIDGE FILTERING

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

4.3.6.1 Incoming IP Filtering

In the **Incoming IP Filtering** page, you can configure all the iptables rules, include creat rule chains.

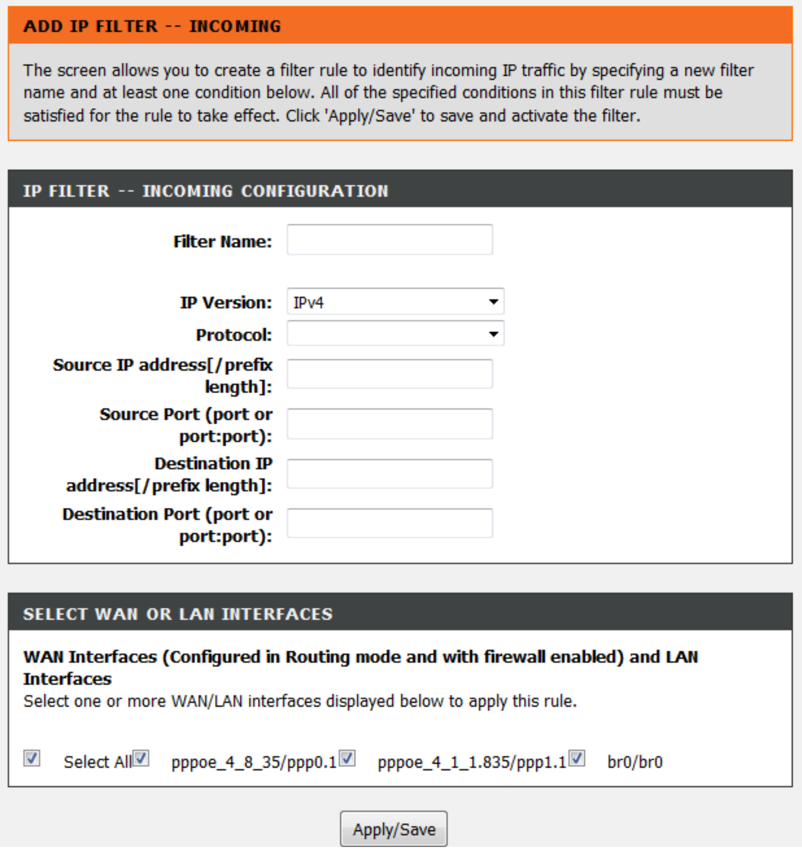


INCOMING IP FILTERING SETUP

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be ACCEPTED by setting up filters.

CHOOSE ADD OR REMOVE TO CONFIGURE INCOMING IP FILTERS

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove



ADD IP FILTER -- INCOMING

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 effect. Click 'Apply/Save' to save and activate the filter.

IP FILTER -- INCOMING CONFIGURATION

Filter Name:	
IP Version:	IPv4
Protocol:	
Source IP address[/prefix length]:	
Source Port (port or port:port):	
Destination IP address[/prefix length]:	
Destination Port (port or port:port):	

SELECT WAN OR LAN INTERFACES

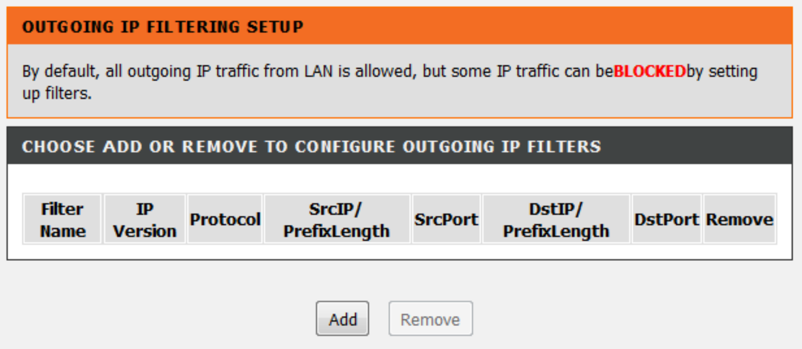
WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces

Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑ Select All ☑ pppoe_4_8_35/ppp0.1 ☑ pppoe_4_1_1.835/ppp1.1 ☑ br0/br0

4.3.6.2 Outgoing IP Filtering

In the **Outgoing IP Filtering** page, you can configure all the iptables rules, include creat rule chains.

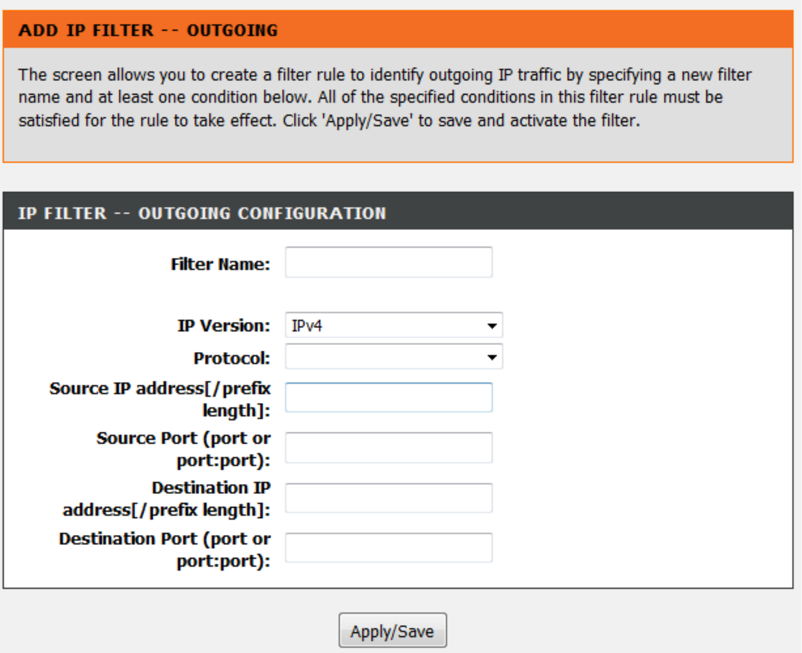


OUTGOING IP FILTERING SETUP

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

CHOOSE ADD OR REMOVE TO CONFIGURE OUTGOING IP FILTERS

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove



ADD IP FILTER -- OUTGOING

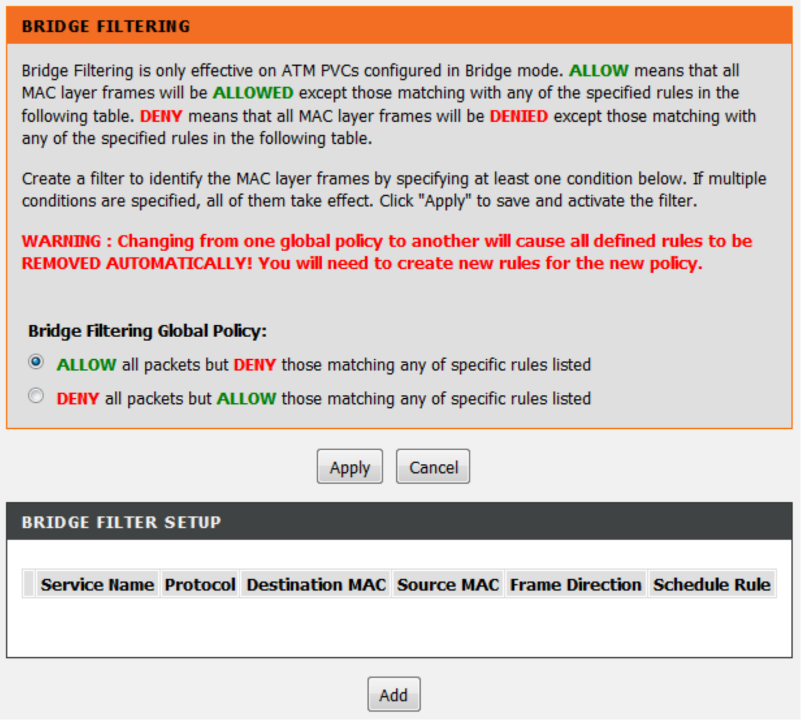
The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

IP FILTER -- OUTGOING CONFIGURATION

Filter Name:	
IP Version:	IPv4
Protocol:	
Source IP address[/prefix length]:	
Source Port (port or port:port):	
Destination IP address[/prefix length]:	
Destination Port (port or port:port):	

4.3.6.3 Bridge Filtering

In the **Filtering Options** page, click **Bridge Filtering**. The page is shown as 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:

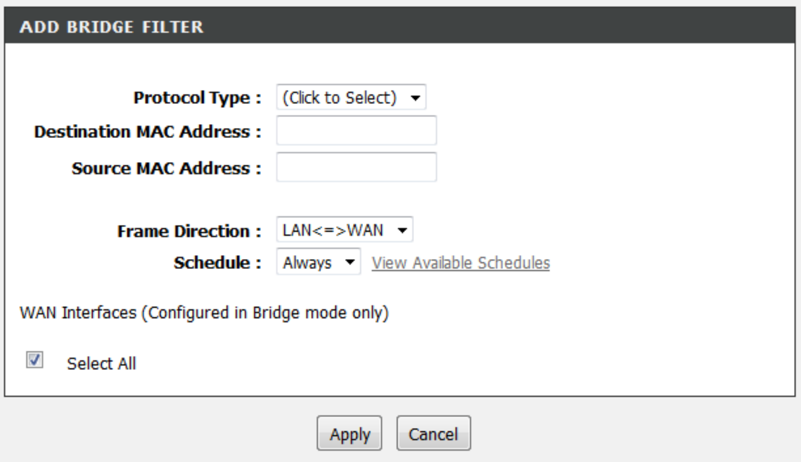
● ALLOW all packets but DENY those matching any of specific rules listed

○ 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 is shown as the following figure appears.



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 All

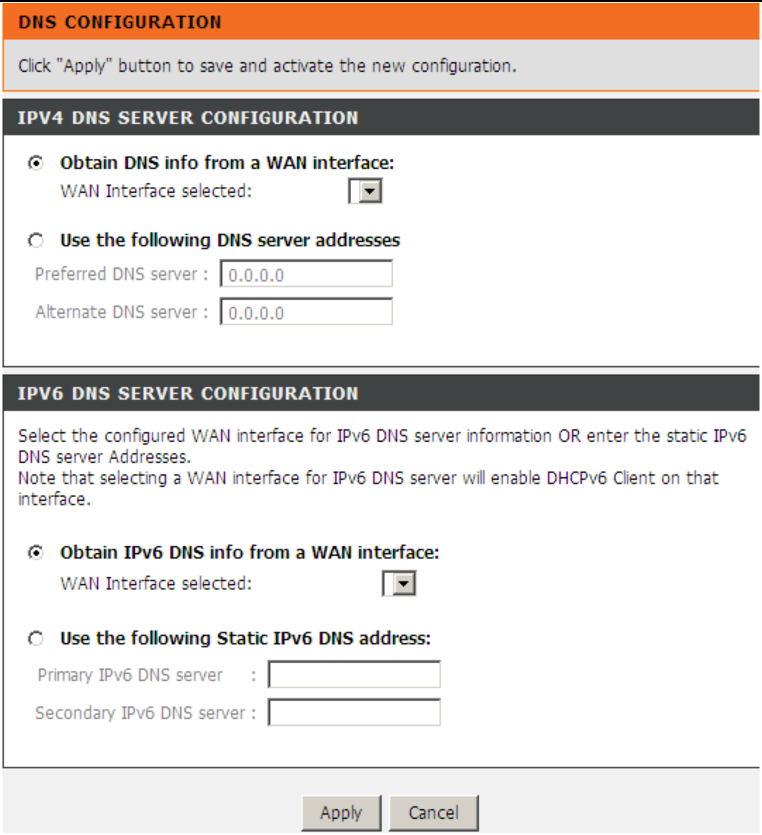
Click **Apply** to save the settings.

4.3.7 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 is shown as the following figure appears.



DNS CONFIGURATION

Click "Apply" button to save and activate the new configuration.

IPV4 DNS SERVER CONFIGURATION

● Obtain DNS info from a WAN interface:

WAN Interface selected:

○ Use the following DNS server addresses

Preferred DNS server : 0.0.0.0

Alternate DNS server : 0.0.0.0

IPV6 DNS SERVER CONFIGURATION

Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

● Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected:

○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server :

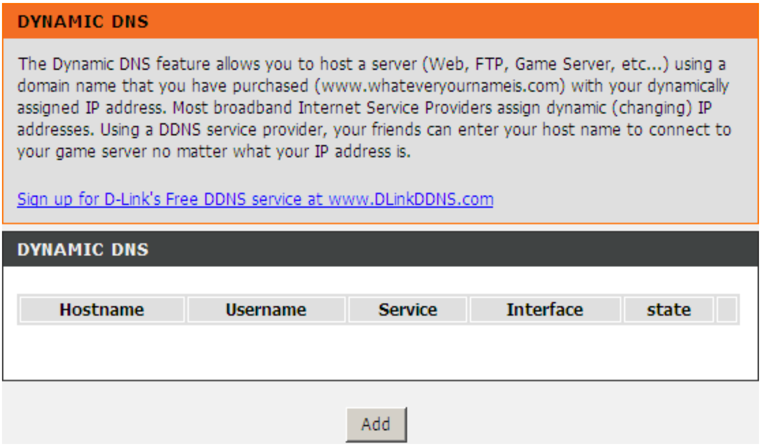
Secondary IPv6 DNS server :

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, select **Use the following DNS server addresses** and enter these IP addresses in the available entry fields of the **preferred DNS server** and the **alternate DNS server**. Click **Apply** to save the settings.

4.3.8 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 is shown as the following page appears.



DYNAMIC DNS

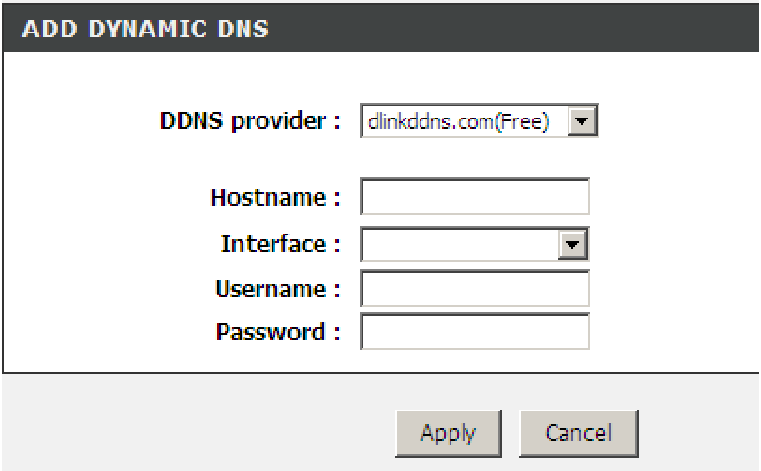
The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service 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	state	

Click **Add** to add dynamic DNS. The page is shown as the following figure appears.



ADD DYNAMIC DNS

DDNS provider : dlinkddns.com(Free)

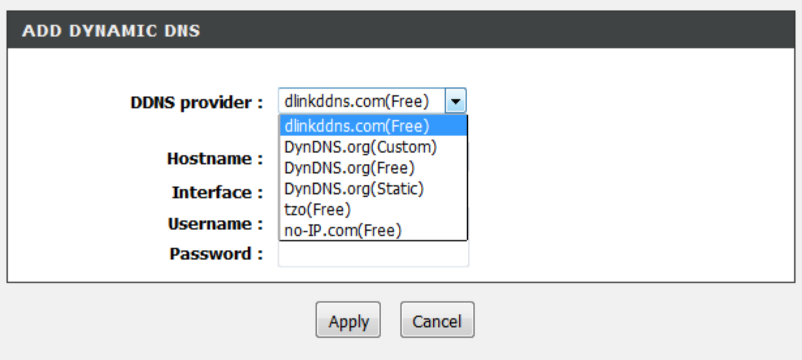
Hostname :

Interface :

Username :

Password :

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



ADD DYNAMIC DNS

DDNS provider : dlinkddns.com(Free)

Hostname :

Interface :

Username :

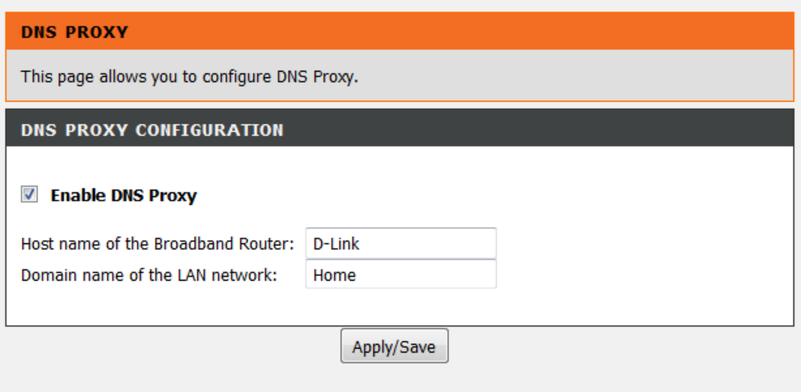
Password :

- **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.

4.3.9 Dns Proxy

Choose **ADVANCED** >**Dns Proxy**. The **Dns Proxy** page is shown as the following figure appears.



DNS PROXY

This page allows you to configure DNS Proxy.

DNS PROXY CONFIGURATION

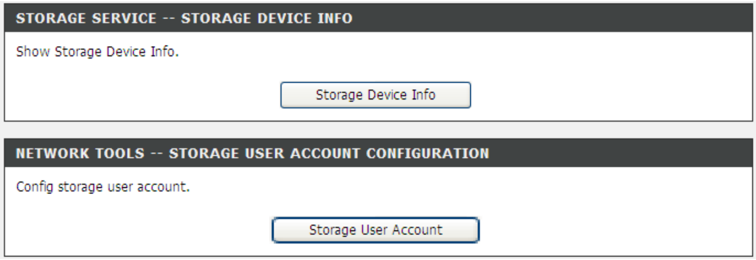
☑ Enable DNS Proxy

Host name of the Broadband Router: D-Link

Domain name of the LAN network: Home

4.3.10 Storage Service

Choose **ADVANCED** > **Storage Service**. The **Storage Service** page is shown as the following figure appears.



STORAGE SERVICE -- STORAGE DEVICE INFO

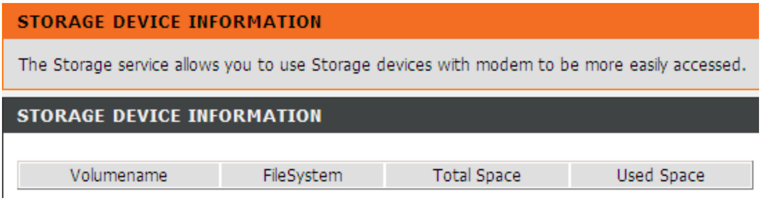
Show Storage Device Info.

NETWORK TOOLS -- STORAGE USER ACCOUNT CONFIGURATION

Config storage user account.

4.3.10.1 Storage Device Info

In the **Storage Service** page, click **Storage Device Info**. The page is shown as the following figure appears.



STORAGE DEVICE INFORMATION

The Storage service allows you to use Storage devices with modem to be more easily accessed.

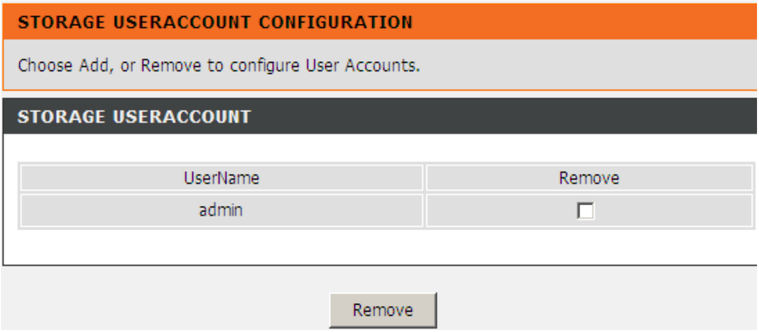
STORAGE DEVICE INFORMATION

Volumename	FileSystem	Total Space	Used Space

When you insert USB storage, this page will show the information of USB storage, such as file system, total space and used space.

4.3.10.2 User Accounts

In the **Storage Service** page, click **Storage User Account**. The page is shown as the following figure appears.



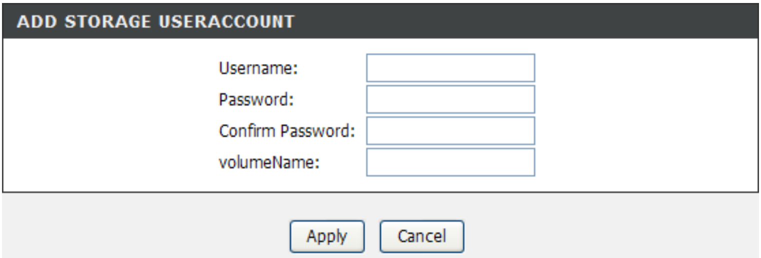
STORAGE USERACCOUNT CONFIGURATION

Choose Add, or Remove to configure User Accounts.

STORAGE USERACCOUNT

UserName	Remove
admin	□

Click **Add** to add a user. The page is shown as the following figure appears.



ADD STORAGE USERACCOUNT

Username:

Password:

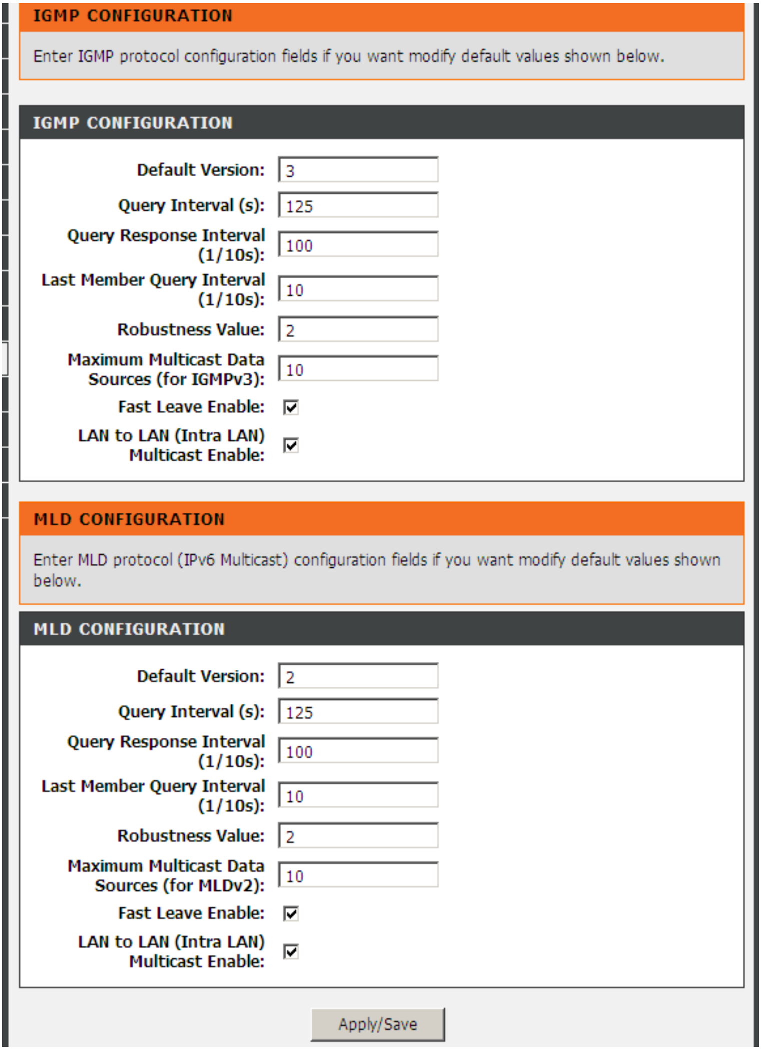
Confirm Password:

volumeName:

- **Username**: set valid user that access CPE’s samba server
- **Password**: user’s password
- **Confirm Password**: user’s password
- **volumeName**: the directory you want to share

4.3.11 Multicast

Choose **ADVANCED** > **Multicast**. The page is shown as the following figure appears.



IGMP CONFIGURATION

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

IGMP 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 Data Sources (for IGMPv3):	10
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑

MLD CONFIGURATION

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

MLD CONFIGURATION

Default Version:	2
Query Interval (s):	125
Query Response Interval (1/10s):	100
Last Member Query Interval (1/10s):	10
Robustness Value:	2
Maximum Multicast Data Sources (for MLDv2):	10
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑

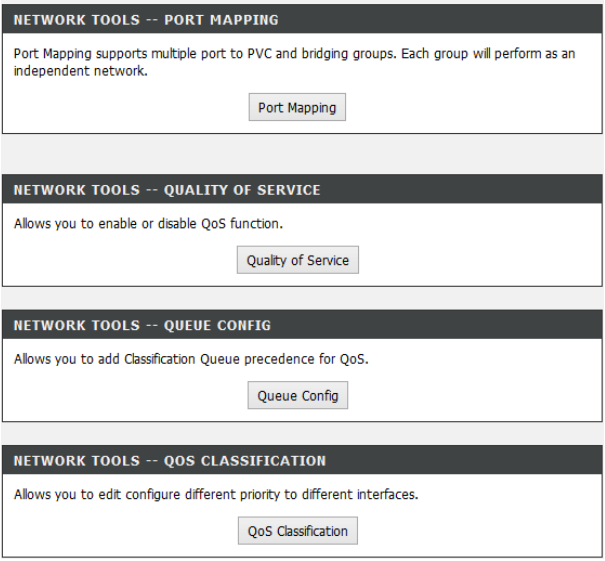
- **Default Version**: IGMP version

- **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 Data Sources (for IGMPv3)**: max group data sources that want to receive.
- **Fast Leave Enable**: Enable or disable fast leave feature.
- **LAN to LAN (Intra LAN) Multicast Enable**: Enable or disable Lan to Lan multicast.

For the field description of **MLD CONFIGURATION**, you can refer to the field description of **IGMP CONFIGURATION**.

4.3.12 Network Tools

Choose **ADVANCED** > **Network Tools**. The page is shown as the following figures appear.



NETWORK TOOLS -- PORT MAPPING

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

NETWORK TOOLS -- QUALITY OF SERVICE

Allows you to enable or disable QoS function.

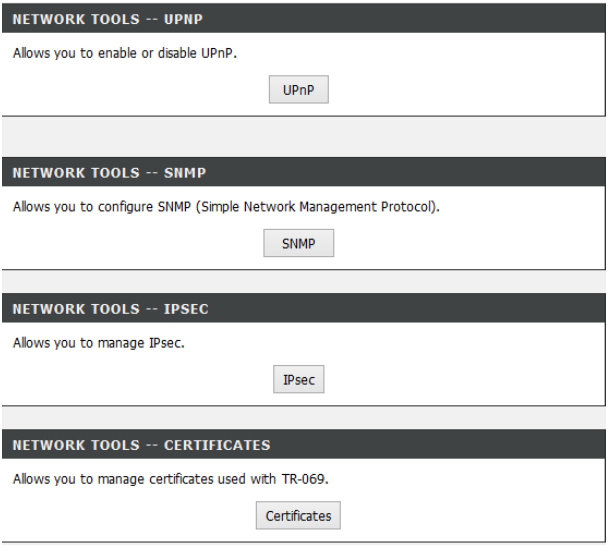
NETWORK TOOLS -- QUEUE CONFIG

Allows you to add Classification Queue precedence for QoS.

NETWORK TOOLS -- QOS CLASSIFICATION

Allows you to edit configure different priority to different interfaces.

Figure 21 Network tools-1



NETWORK TOOLS -- UPNP

Allows you to enable or disable UPnP.

NETWORK TOOLS -- SNMP

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

NETWORK TOOLS -- IPSEC

Allows you to manage IPsec.

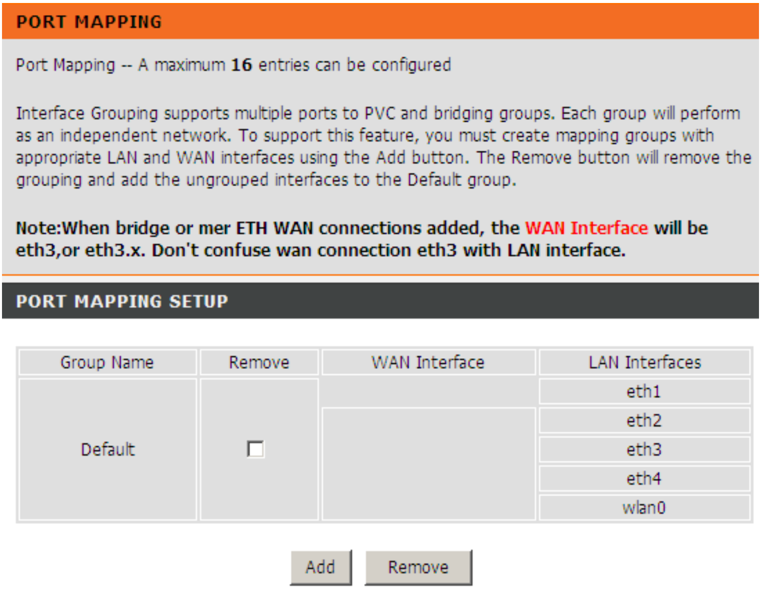
NETWORK TOOLS -- CERTIFICATES

Allows you to manage certificates used with TR-069.

Figure 22 Network tools-2

4.3.12.1 Port Mapping

Choose **ADVANCED** > **Network Tools** and click **Port Mapping**. The page is shown as 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

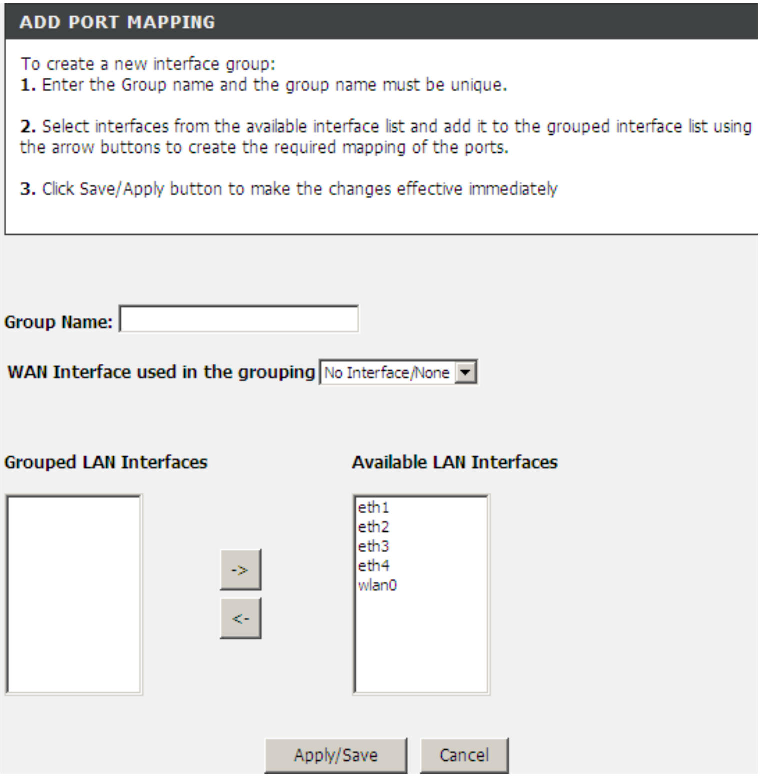
Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped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

Note:When bridge or mer ETH WAN connections added, the WAN Interface will be eth3,or eth3.x. Don't confuse wan connection eth3 with LAN interface.

PORT MAPPING SETUP

Group Name	Remove	WAN Interface	LAN Interfaces
Default	□		eth1
			eth2
			eth3
			eth4
			wlan0

Click **Add** to add a port mapping. The page is shown as the following figure appears.


ADD PORT MAPPING

To create a new interface group:
1. Enter the Group name and the group name must be unique.

2. 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.

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

Group Name:

WAN Interface used in the grouping: No Interface/None

The procedures for creating a mapping group are as follows:

Step 11 Enter the group name.

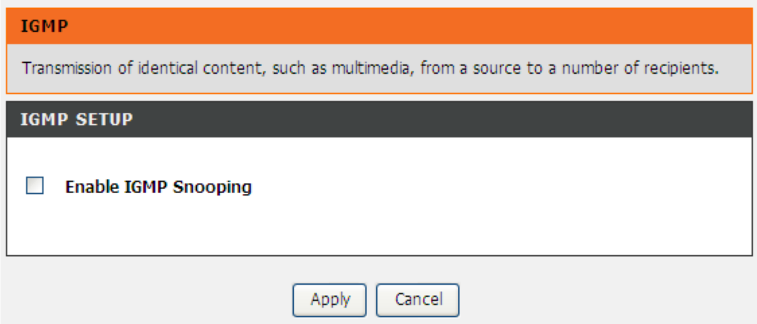
Step 12 Select the WAN interface for your new group.

Step 13 Select LAN interfaces from the **Available LAN Interfaces** list and click the **<-** arrow button to add them to the **Grouped LAN Interfaces** list. In order to create the required mapping of the ports, the group name must be unique.

Step 14 Click **Apply/Save** to save the settings.

4.3.12.2 IGMP

Choose **ADVANCED** > **Network Tools** and click **IGMP**. The page is shown as the following figure appears. Select the check box of **Enable IGMP Snooping**, the multicast data is transmitted through the specific LAN port which has received the request report.



IGMP

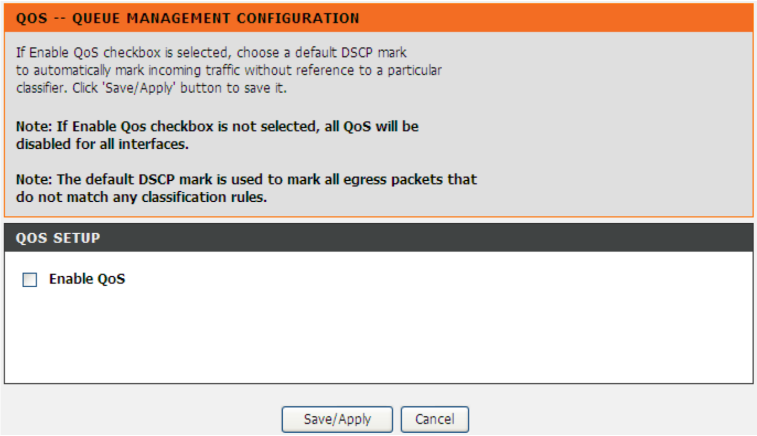
Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP SETUP

□ Enable IGMP Snooping

4.3.12.3 Quality of Service

Choose **ADVANCED** > **Network Tools** and click **Quality of Service.** The page is shown as the following figure appears.



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.

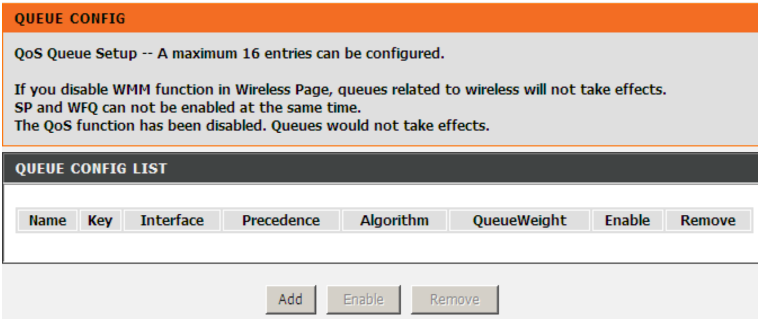
QOS SETUP

□ Enable QoS

In this page, you can enable/disable the QoS. Click **Save/Apply** to take the setting in to effect.

4.3.12.4 Queue Configuration

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



QUEUE CONFIG

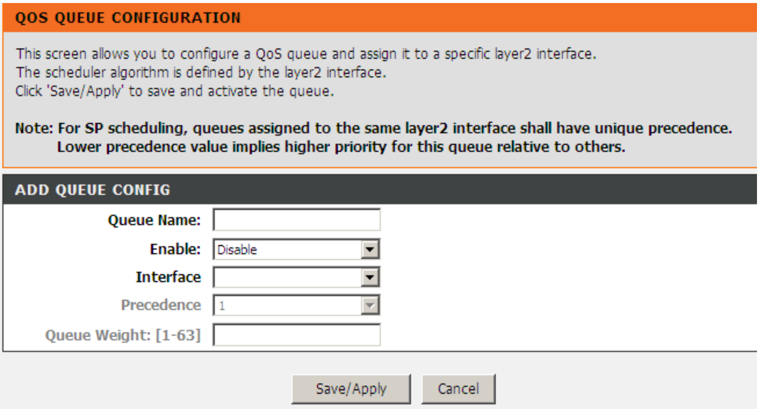
QoS Queue Setup -- A maximum 16 entries can be configured.

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

Click **Add**. The page is shown as the following figure appears.



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.

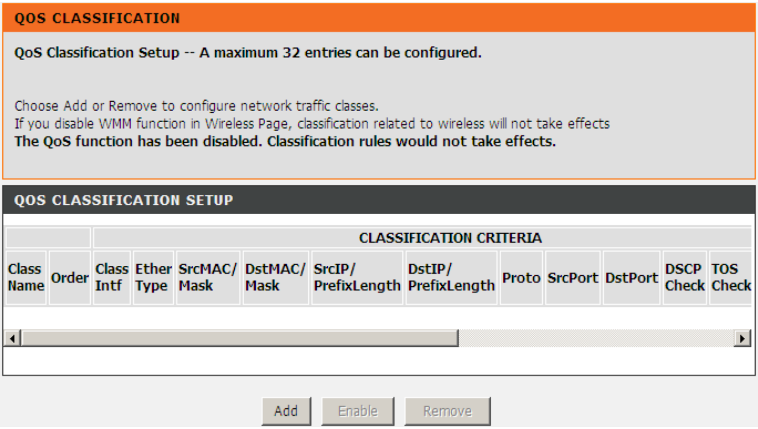
ADD QUEUE CONFIG

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

Click **Save**/**Apply** to save the settings.

4.3.12.5 QoS Classification

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



QOS CLASSIFICATION

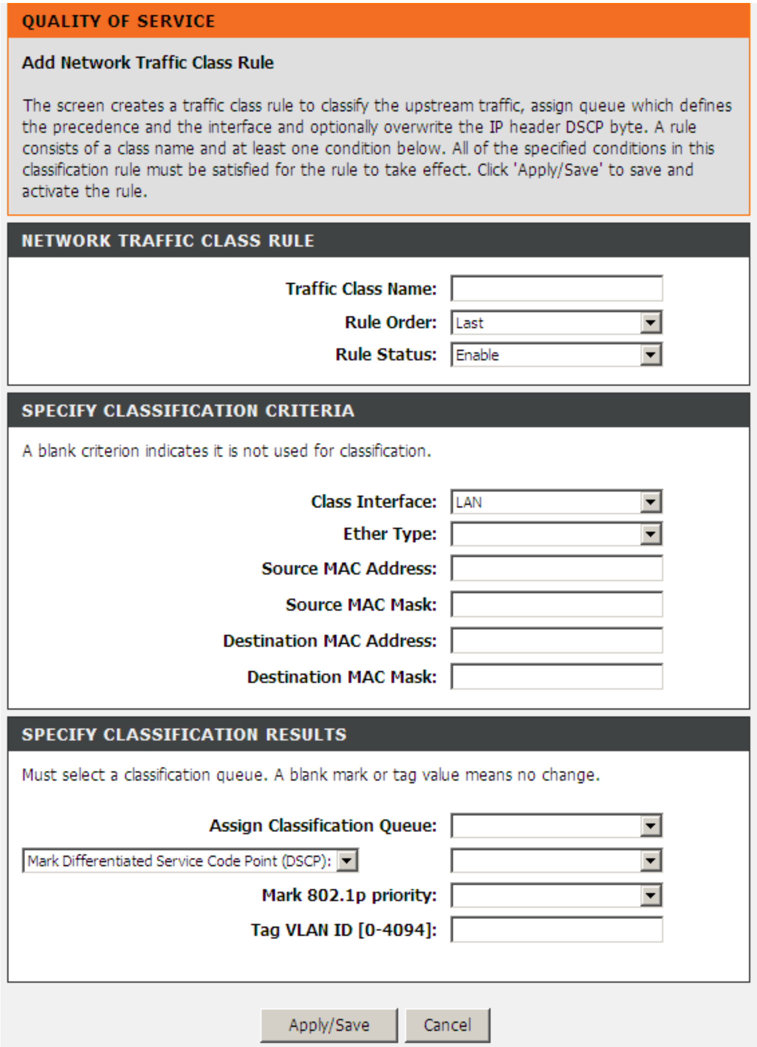
QoS Classification Setup -- A maximum 32 entries can be configured.

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											
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	TOS Check

Click **Add**，and the page is shown as 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 'Apply/Save' to save and activate the rule.

NETWORK TRAFFIC CLASS RULE

Traffic Class Name:	
Rule Order:	Last
Rule Status:	Enable

SPECIFY CLASSIFICATION CRITERIA

A blank criterion indicates it is not used for classification.

Class Interface:	LAN
Ether Type:	
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

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]:	

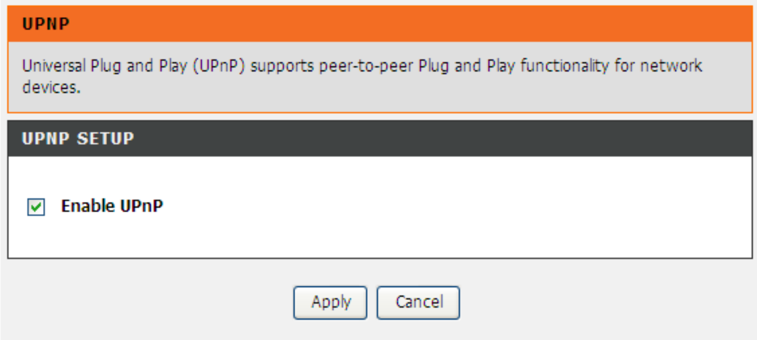
- Rule Status: select **Enable** from the drop-down list.
- Class interface: select the interface.
- Ether Type: select the ethernet type from the drop-down list.

- Assign Classification Queue: select the queue which is configured in **Queue Config.**

Click **Apply/save** to enable the rule.

4.3.12.6 UPnP

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



UPNP

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

UPNP SETUP

☑ Enable UPnP

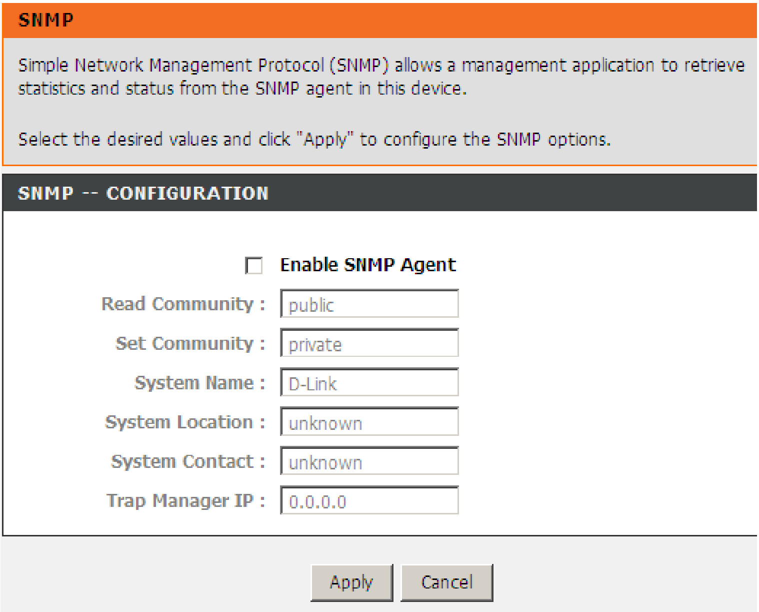
In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

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.

4.3.12.7 SNMP

Choose **ADVANCED** > **Network Tools** and click **SNMP**. The page is shown as the following figure appears.



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

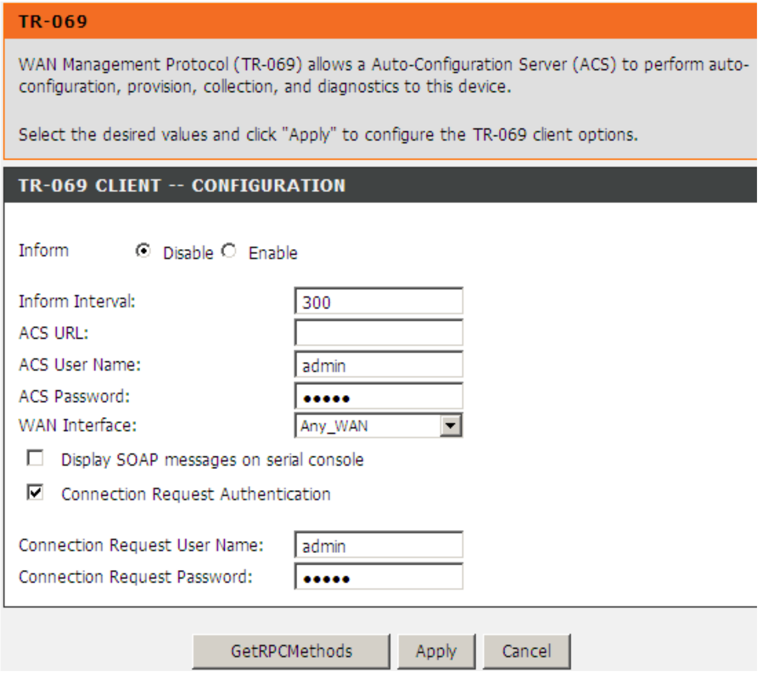
□ Enable SNMP Agent

Read Community :	public
Set Community :	private
System Name :	D-Link
System Location :	unknown
System Contact :	unknown
Trap Manager IP :	0.0.0.0

SNMP configuration allows a management application to retrieve statistics and status from the SNMP agent in this device.

4.3.12.8 TR-069

Choose **ADVANCED** > **Network Tools** and click **TR-069**. The page is shown as the following figure appears. In this page, you can configure the TR-069 CPE.



TR-069

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, 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:	●●●●●
WAN Interface:	Any_WAN

□ Display SOAP messages on serial console

☑ Connection Request Authentication

Connection Request User Name:	admin
Connection Request Password:	●●●●●

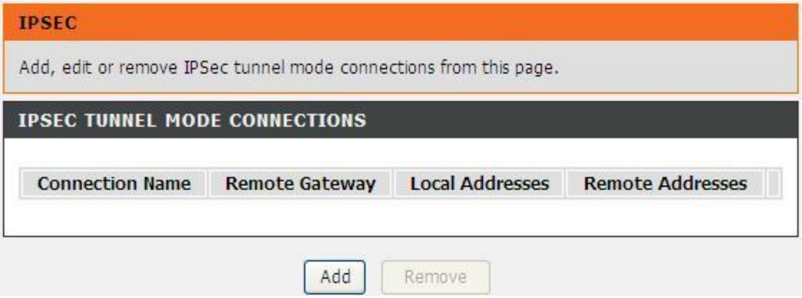
WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

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.

4.3.12.9 IPSEC

Choose **ADVANCED** > **Network Tools** and click **IPsec**. The page is shown as the following figure appears.



IPSEC

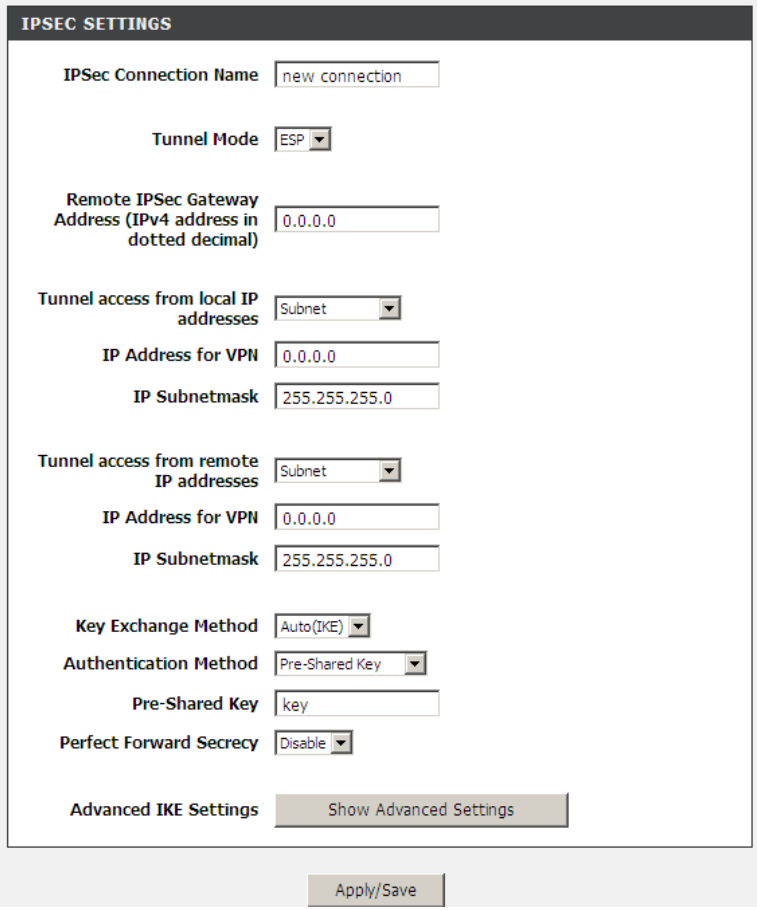
Add, edit or remove IPSec tunnel mode connections from this page.

IPSEC TUNNEL MODE CONNECTIONS

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	

In this page, you can add or remove the IPSec tunnel connections.

Click the **Add** button to display the following page.



IPSEC SETTINGS

IPSec Connection Name	new connection
Tunnel Mode	ESP
Remote IPSec Gateway Address (IPv4 address in dotted decimal)	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Show Advanced Settings

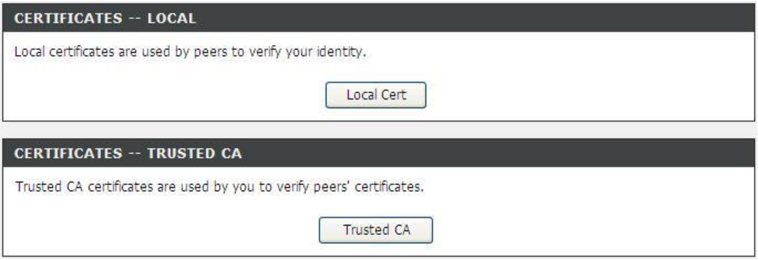
In this page, set the parameters such as the IPSec connection name, tunnel mode, and remote IPSec gateway address.

If you need to configure the advanced settings of this IPSec tunnel connection, please click **Show Advanced Settings** to display other parameters.

After finishing the settings, click **Apply/Save** to save and apply the settings.

4.3.12.10 Certificates

Choose **ADVANCED** > **Network Tools** > **Certificates**. The **Certificates** page is shown as the following figure appears.



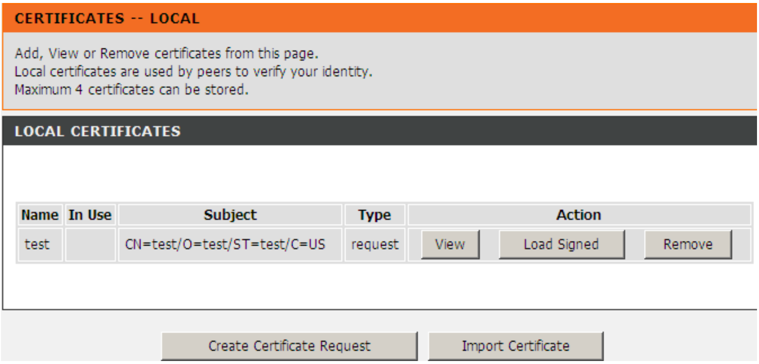
CERTIFICATES -- LOCAL

Local certificates are used by peers to verify your identity.

CERTIFICATES -- TRUSTED CA

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

Click **Local Cert** to import local certificates that are used by peers to verity your identity.



CERTIFICATES -- LOCAL

Add, View or Remove certificates from this page.
Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

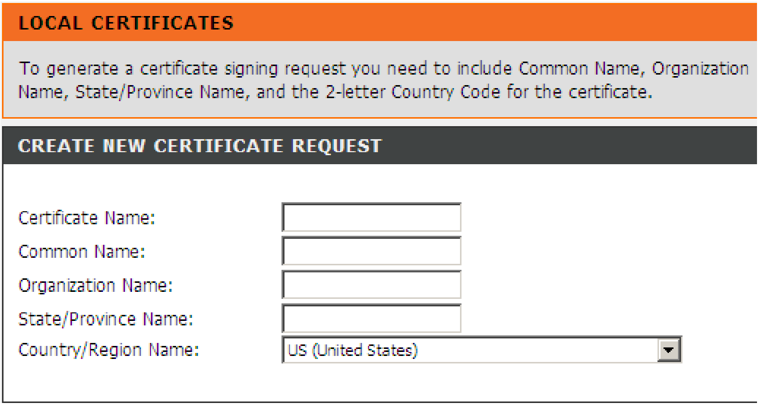
LOCAL CERTIFICATES

Name	In Use	Subject	Type	Action		
test		CN=test/O=test/ST=test/C=US	request	View	Load Signed	Remove

In this page, you can acquire the local certificate by creating a certificate request or importing a certificate. You may also create or remove a certificate.

- **Creating a New Certificate Request**

Click the **Create Certificate Request** button to display the following page.



LOCAL CERTIFICATES

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

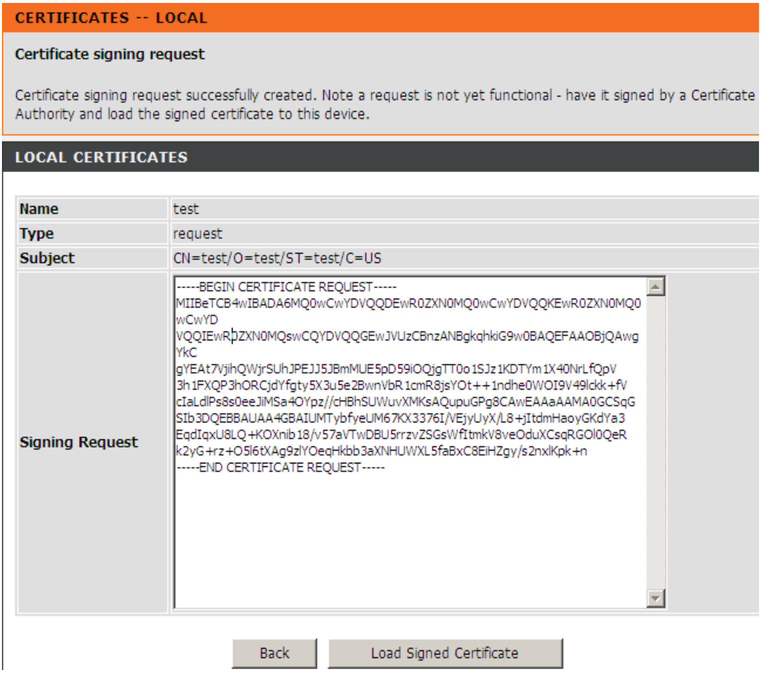
CREATE NEW CERTIFICATE REQUEST

Certificate Name:	
Common Name:	
Organization Name:	
State/Province Name:	
Country/Region Name:	US (United States)

In this page, please set the following parameters.

- **Certificate name:** Set the certificate name.
- **Common Name:** The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol symbol "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as "*****" or "**?"**, and do not use an IP address.
- **Organization Name:** The name of the organization which the entity belongs to (such as the name of a company).
- **State/Province Name:** This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province.
- **Country/Region Name:** This is the two-letter ISO abbreviation for your country (for example, US for the United States).

After finishing setting, click the **Apply** button to apply the settings and the page is shown as the following figure appears.



CERTIFICATES -- LOCAL

Certificate signing request

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

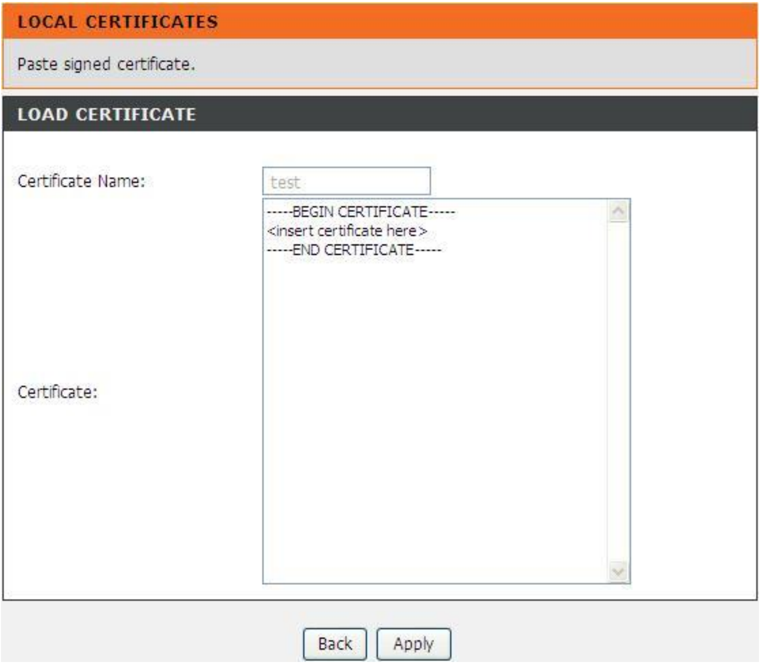
LOCAL CERTIFICATES

Name	test
Type	request
Subject	CN=test/O=test/ST=test/C=US

Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBeTCB4wIBADA6MQ0wCwYDVQQDEwR0ZXN0MQ0wCwYDVQQKEwR0ZXN0MQ0
wCwYD
VQQIEwR0ZXN0MQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwg
YkC
gYEAt7VjihQWjrSUhJPEJJ5JBmMUE5pD59iOQjgTT0o1SJz1KDTYm1X40NrLfQpV
3h1FXQP3hORCjdYfgty5X3u5e2BwnVbR1cmR8jsYOt++1ndhe0WOI9V49lckk+fV
cIaLdlPs8s0eeJiMSa4OYpz//cHBhSUWuvXMKsAQupuGPg8CAwEAAaAAMA0GCSqG
SIb3DQEBBAUAA4GBAIUMTybfyeUM67KX3376I/VEjyUyX/L8+jItdmHaoyGKdYa3
EqdIqxU8LQ+KOXnib18/v57aVTwDBU5rrzvZSGsWfItmkV8veOduXCsqRGOl0QeR
k2yG+rz+O5l6tXAg9zlYOeqHkbb3aXNHUWXL5faBxC8EiHZgy/s2nxlKpk+n
-----END CERTIFICATE REQUEST-----
```

The certificate request needs to be submitted to a certificate authority which will sign the request. Then the signed certificate needs to be loaded to the DSL router. Click **Load Signed Certificate** in this page, and the following page appears.



LOCAL CERTIFICATES

Paste signed certificate.

LOAD CERTIFICATE

Certificate Name: test

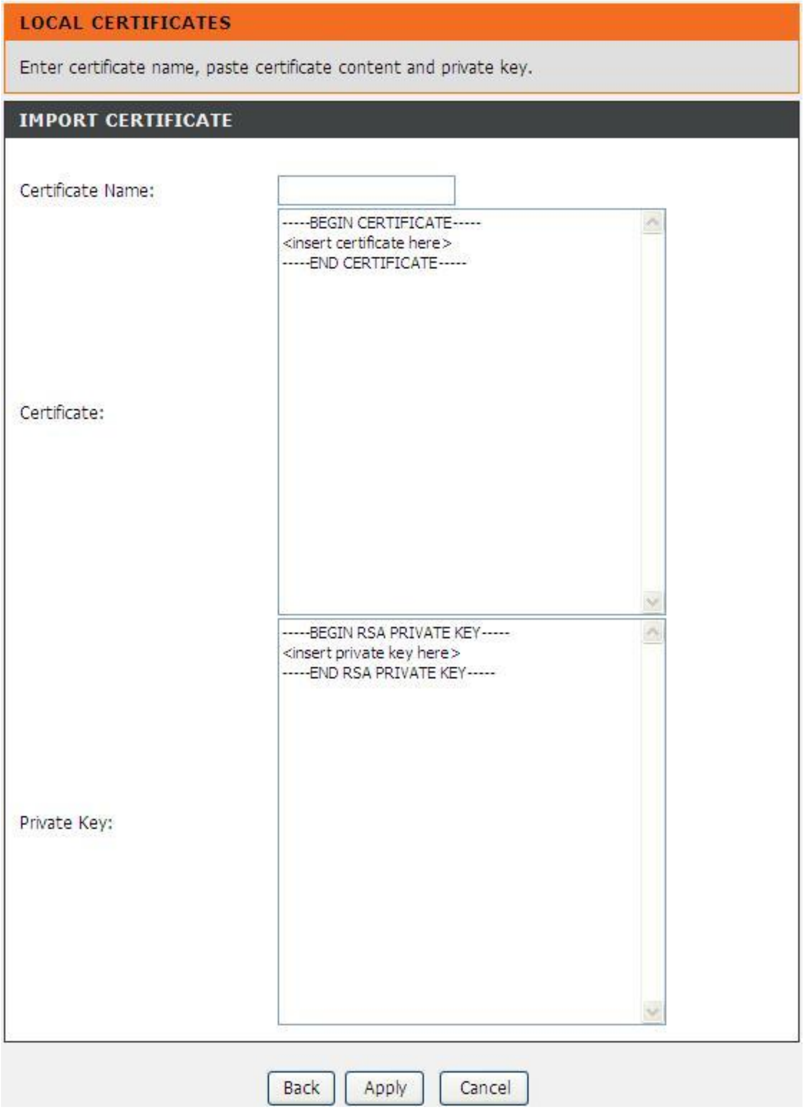
Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

In this page, paste the signed certificate, and then click the **Apply** button. A new certificate is created.

- **Importing an Existing Local Certificate**

To import an existing certificate, click the **Import Certificate** button to display the following page.



LOCAL CERTIFICATES

Enter certificate name, paste certificate content and private key.

IMPORT CERTIFICATE

Certificate Name:

Certificate:

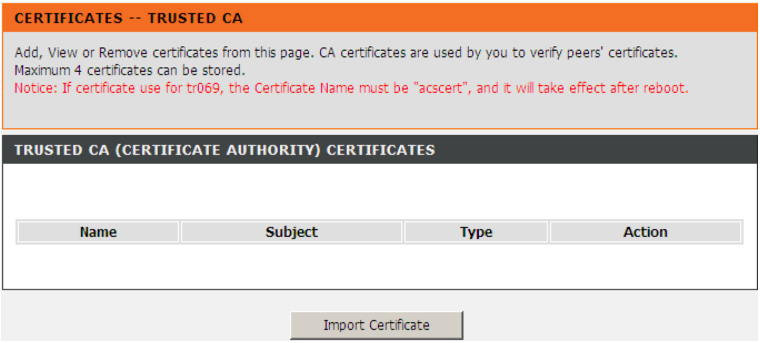
```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

In this page, paste the certificate and the private key. Finally, click the **Apply** button to import the certificate.

Choose **ADVANCED** > **Network Tools** > **Certificates**, and click **Trusted CA** button in this page to import a certificate, the page is shown as the following figure appears.



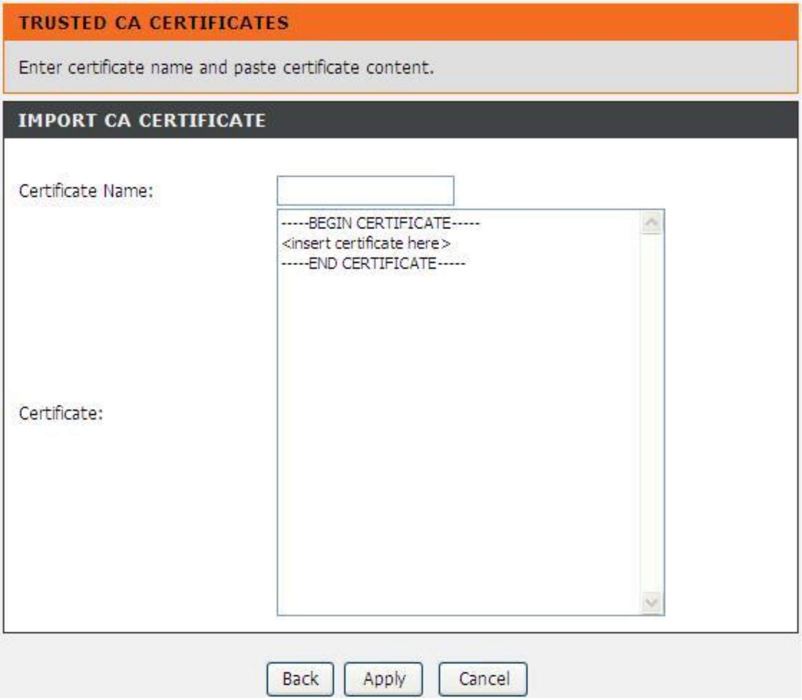
CERTIFICATES -- TRUSTED CA

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.
Notice: If certificate use for tr069, the Certificate Name must be "acscert", and it will take effect after reboot.

TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Type	Action

Click the **Import Certificate** button to display the following page.



TRUSTED CA CERTIFICATES

Enter certificate name and paste certificate content.

IMPORT CA CERTIFICATE

Certificate Name:

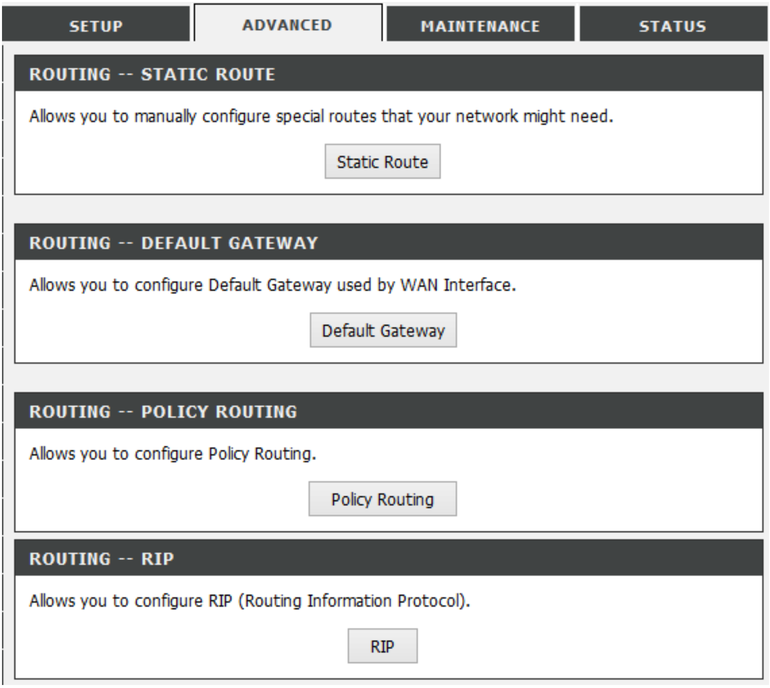
Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Click the **Apply** button to import the certificate.

4.3.13 Routing

Choose **ADVANCED** > **Routing**. The page is shown as the following page appears.



ROUTING -- STATIC ROUTE

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

ROUTING -- DEFAULT GATEWAY

Allows you to configure Default Gateway used by WAN Interface.

ROUTING -- POLICY ROUTING

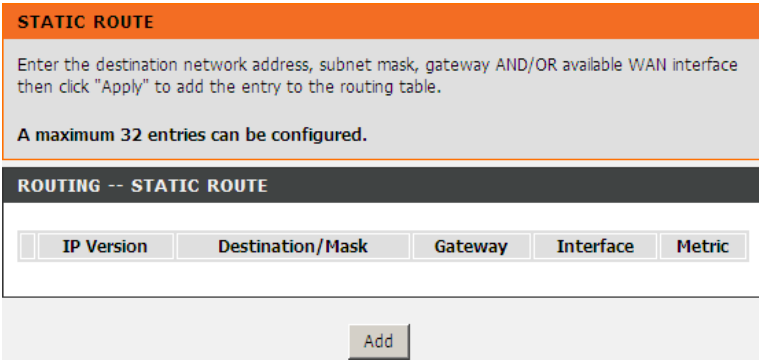
Allows you to configure Policy Routing.

ROUTING -- RIP

Allows you to configure RIP (Routing Information Protocol).

4.3.13.1 Static Route

Choose **ADVANCED** > **Routing** and click **Static Route**. The page is shown as 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

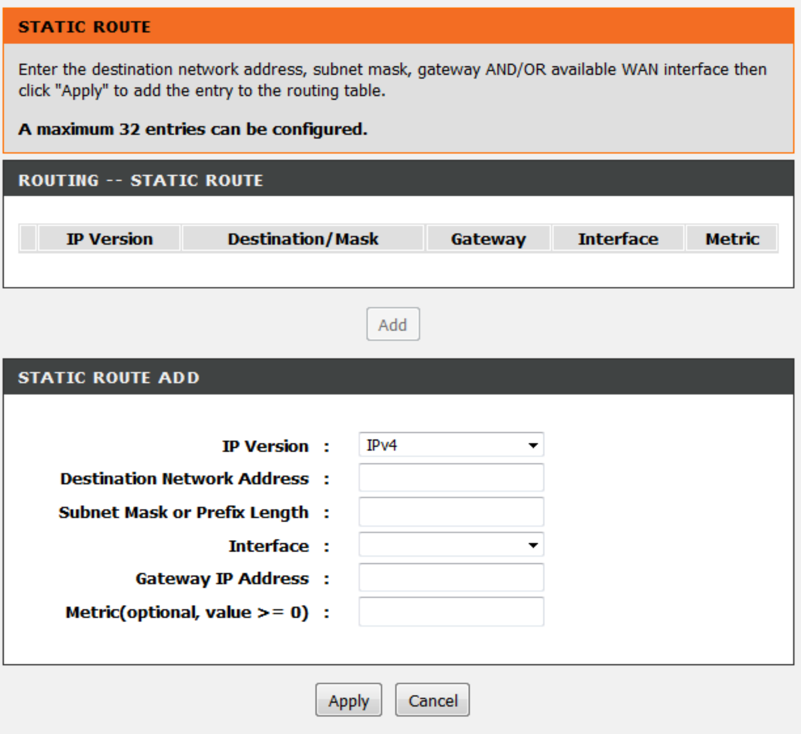
Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.

A maximum 32 entries can be configured.

ROUTING -- STATIC ROUTE

	IP Version	Destination/Mask	Gateway	Interface	Metric

Click **Add** to add a static route. The page is shown as the following figure appears.



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

	IP Version	Destination/Mask	Gateway	Interface	Metric

STATIC ROUTE ADD

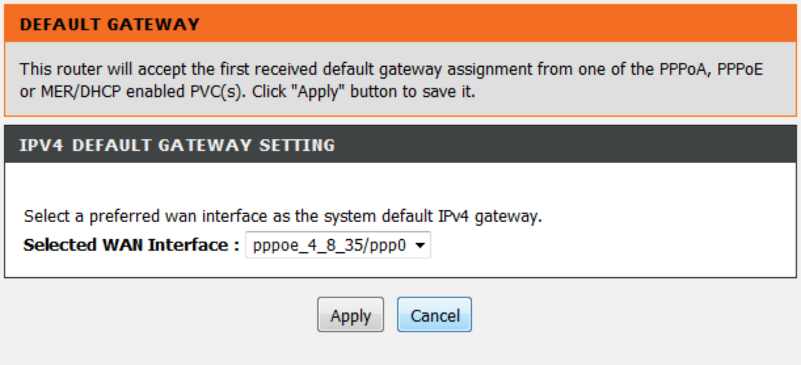
IP Version :	IPv4
Destination Network Address :	
Subnet Mask or Prefix Length :	
Interface :	
Gateway IP Address :	
Metric(optional, value >= 0) :	

- **IP Version:** Select the IP version to be **IPv4** or **IPv6**.
- **Destination Network Address**: The destination IP address of the router.
- **Subnet Mask or Prefix Length**: The subnet mask of the destination IP address or Prefix Length.
- **Interface:** Select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

Click **Apply** to save the settings.

4.3.13.2 Default Gateway

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



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.

IPV4 DEFAULT GATEWAY SETTING

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

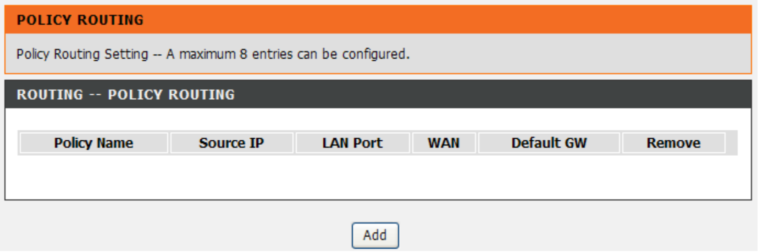
Selected WAN Interface : pppoe_4_8_35/ppp0

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

4.3.13.3 Policy Routing

Choose **ADVANCED** > **Routing** and click **policy Routing**. The page is shown as the following figure appears.

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



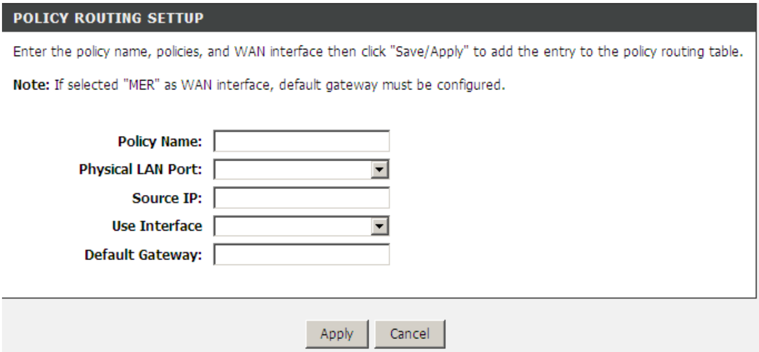
POLICY ROUTING

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 is shown as the following figure appears.



POLICY ROUTING SETTUP

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:

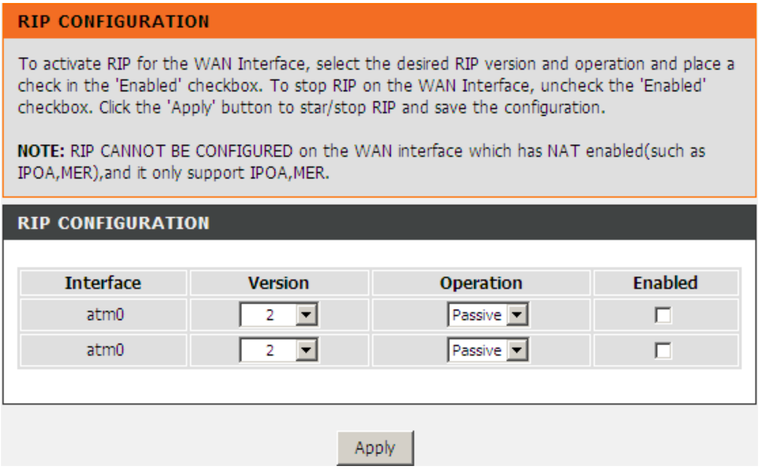
Use Interface

Default Gateway:

In this page, enter the policy name, source IP and default gateway, and select the physical LAN port and the use interface.

4.3.13.4 RIP

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



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.

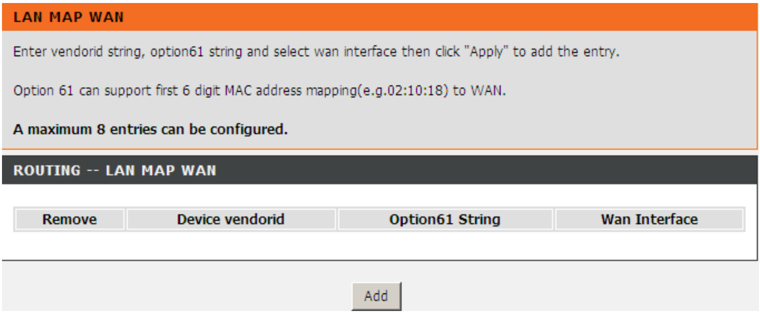
RIP CONFIGURATION

Interface	Version	Operation	Enabled
atm0	2	Passive	□
atm0	2	Passive	□

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.

4.3.13.5 Lan Map Wan

Choose **ADVANCED** > **Routing** and click **Lan Map Wan**. The page is shown as the following figure appears.



LAN MAP WAN

Enter vendorid string, option61 string and select wan interface then click "Apply" to add the entry.

Option 61 can support first 6 digit MAC address mapping(e.g.02:10:18) to WAN.

A maximum 8 entries can be configured.

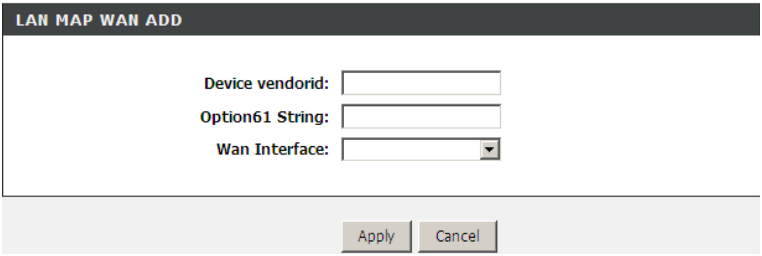
ROUTING -- LAN MAP WAN

Remove	Device vendorid	Option61 String	Wan Interface

This function can support to get Vendor Class ID (option 60) or can support get first 6 digit MAC address from client device and map it with WAN interface.

We deployed such concept by connecting IP phone on it and let device learn from DHCP request (Option 60 or Option 61), then map it to the correct PVC. Such IP phone can map to the voice PVC (1/33 as our vendor ID mapping configuration) and register at the SIP server.In other words, the traffic of the specific IP phone can only pass through the mapped WAN interface and can not flow to or from other WAN interface.

Click **Add** to add schedule rule. The page is shown as the following figure appears.



LAN MAP WAN ADD

Device vendorid:

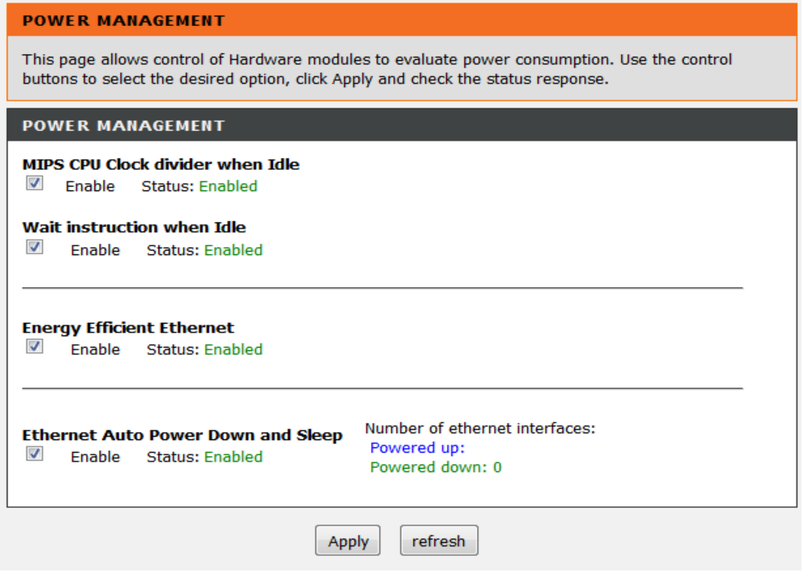
Option61 String:

Wan Interface:

- **Device vendorid:** DHCP Option 60 ID, such as MSFT 5.0.
- **Option61 String:** DHCP Option 61 ID, it can support MAC address mapping (only first 6 digits) to WAN, such as 02:10:18.
- **Wan Interface:** Select the Wan Interface from the drop-down list.

4.3.14 Power Managemnet

Choose **ADVANCED** > **Power Management**. The page is shown as the following figure appears.



POWER MANAGEMENT

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

POWER MANAGEMENT

MIPS CPU Clock divider when Idle

☑ Enable Status: Enabled

Wait instruction when Idle

☑ Enable Status: Enabled

Energy Efficient Ethernet

☑ Enable Status: Enabled

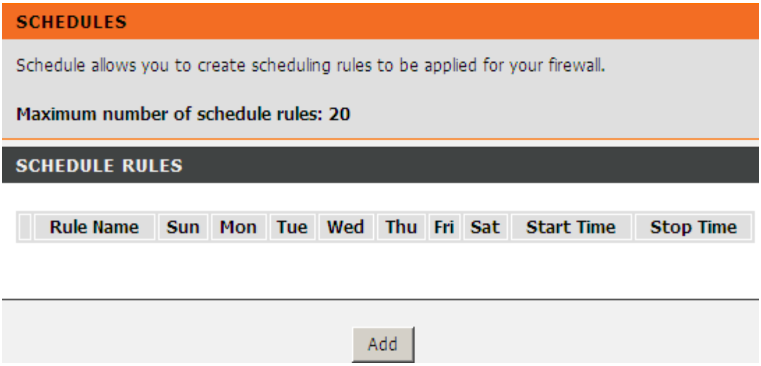
Ethernet Auto Power Down and Sleep

☑ Enable Status: Enabled

Number of ethernet interfaces:
Powered up:
Powered down: 0

4.3.15 Schedules

Choose **ADVANCED** > **Schedules**. The page is shown as the following figure appears.



SCHEDULES

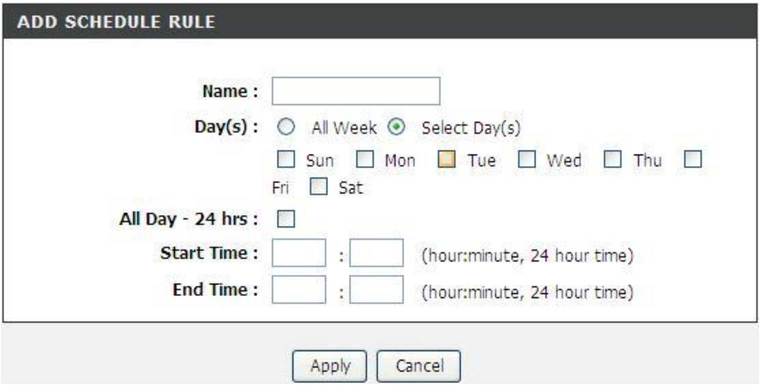
Schedule allows you to create scheduling rules to be applied for your firewall.

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 is shown as the following figure appears.



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)

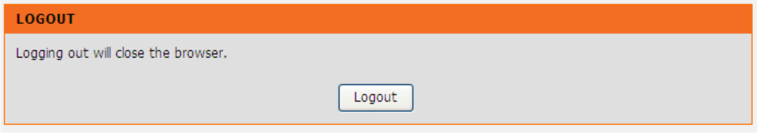
End Time : : (hour:minute, 24 hour time)

You can establish the schedule rules that can be used by other applications (such as Port Forwarding, Port Triggering and so on).

Click **Apply** to save the settings.

4.3.16 Logout

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



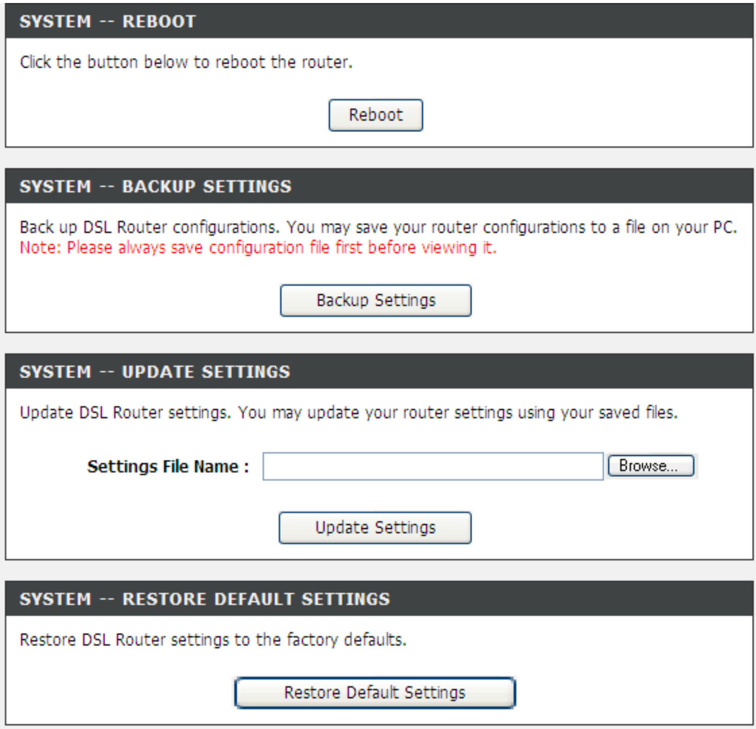
LOGOUT

Logging out will close the browser.

4.4 Maintenance

4.4.1 System

Choose **MAINTENANCE** > **System**. The **System** page is shown as the following figure appears.



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.

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

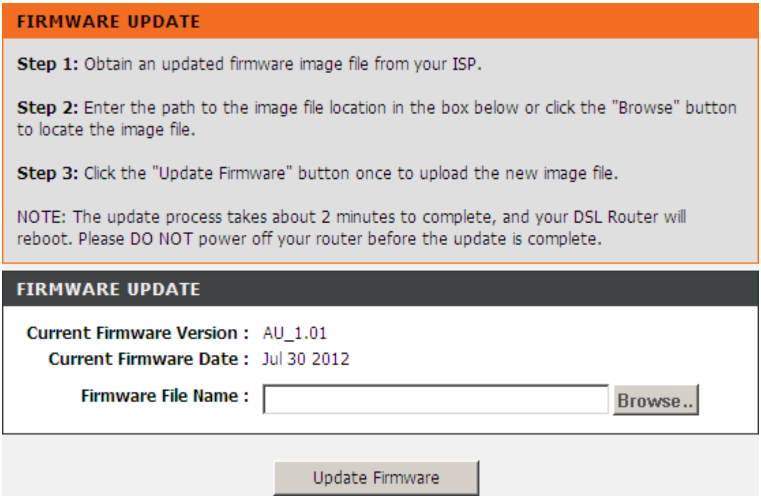
The buttons in this page are described as follows:

- **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.*

4.4.2 Firmware Update

Choose **MAINTENANCE** > **Firmware Update**. The page is shown as the following figure appears. In this page, you can upgrade the firmware of the device.



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 : AU_1.01
Current Firmware Date : Jul 30 2012
Firmware File Name :

The procedures for updating the firmware are as follows:

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

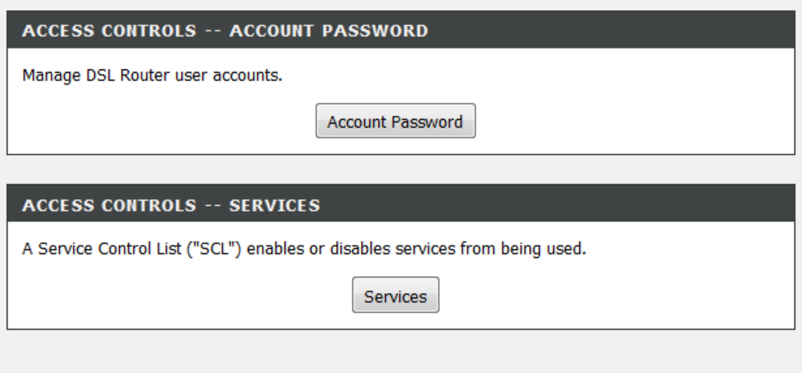
Step 2 Click **Update Firmware** to update the configuration file.

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.*

4.4.3 Access Controls

Choose **MAINTENANCE** > **Access Controls**. The **Access Controls** page is shown as the following figure appears. The page contains **Account Password**, **Services** and **CAPTCHA**.



ACCESS CONTROLS -- ACCOUNT PASSWORD

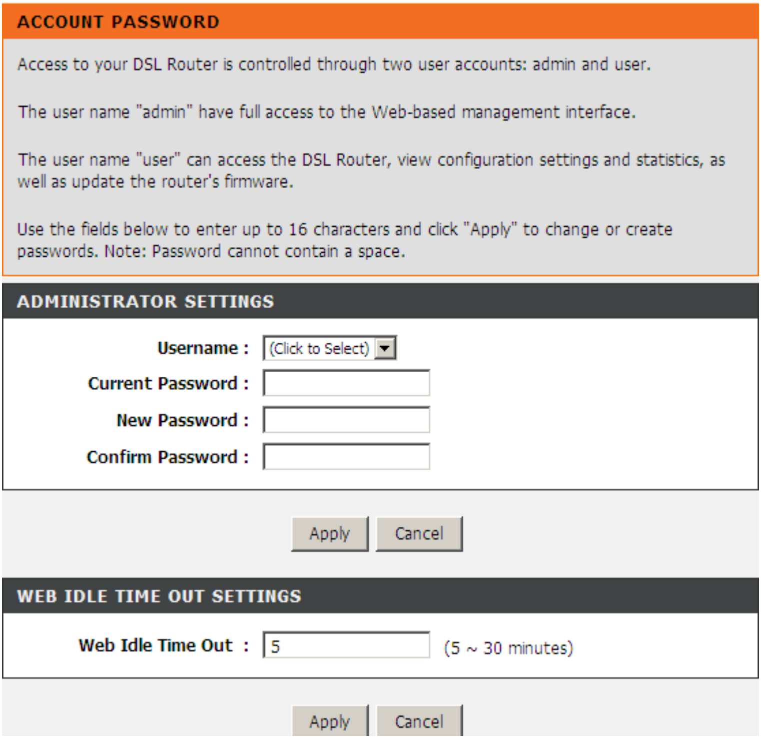
Manage DSL Router user accounts.

ACCESS CONTROLS -- SERVICES

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

4.4.3.1 Account Password

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



ACCOUNT PASSWORD

Access to your DSL Router is controlled through two user accounts: admin and user.

The user name "admin" have full access to the Web-based management interface.

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)

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.

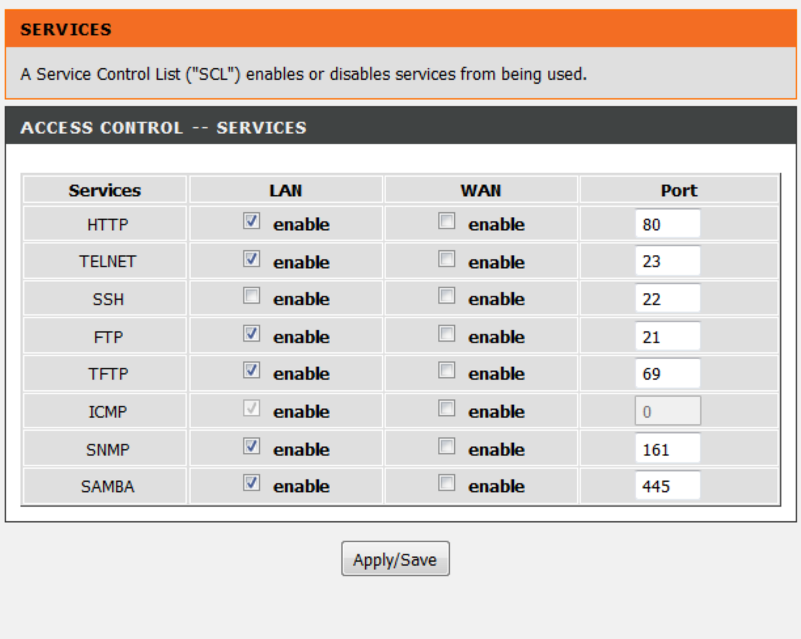
Select the **Username** from the drop-down list. You can select **admin**, **support**, or **user**.

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

Click **Apply** to apply the settings.

4.4.3.2 Services

In the **Access Controls** page, click **Services**. The page is shown as the following figure appears.



SERVICES

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

ACCESS CONTROL -- SERVICES

Services	LAN	WAN	Port
HTTP	☑ enable	□ enable	80
TELNET	☑ enable	□ enable	23
SSH	□ enable	□ enable	22
FTP	☑ enable	□ enable	21
TFTP	☑ enable	□ enable	69
ICMP	☑ enable	□ enable	0
SNMP	☑ enable	□ enable	161
SAMBA	☑ enable	□ enable	445

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 do not need to change the settings.

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

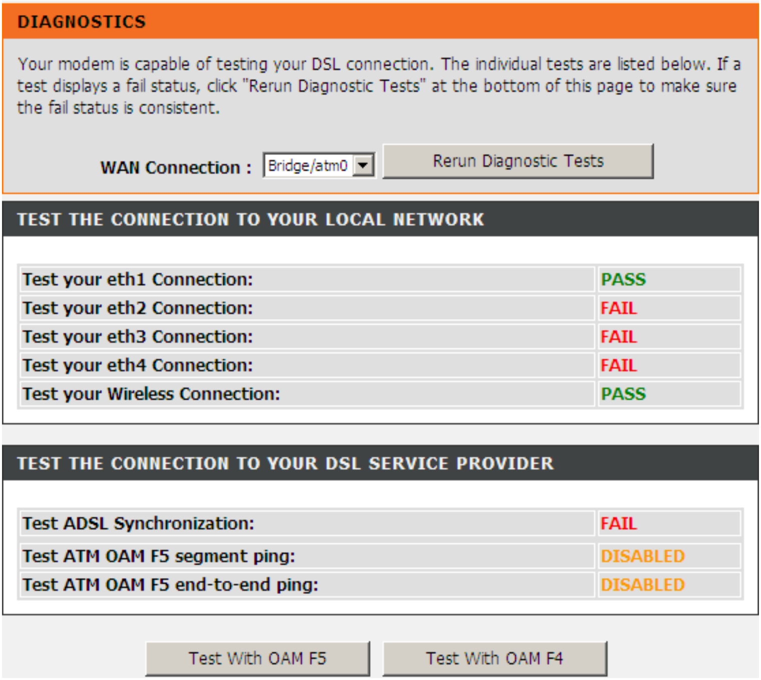
Click **Apply** to apply the settings.

Note:

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

4.4.4 Diagnostics

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



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 : Bridge/atm0 ▼ Rerun Diagnostic Tests

TEST THE CONNECTION TO YOUR LOCAL NETWORK

Test your eth1 Connection:	PASS
Test your eth2 Connection:	FAIL
Test your eth3 Connection:	FAIL
Test your eth4 Connection:	FAIL
Test your Wireless Connection:	PASS

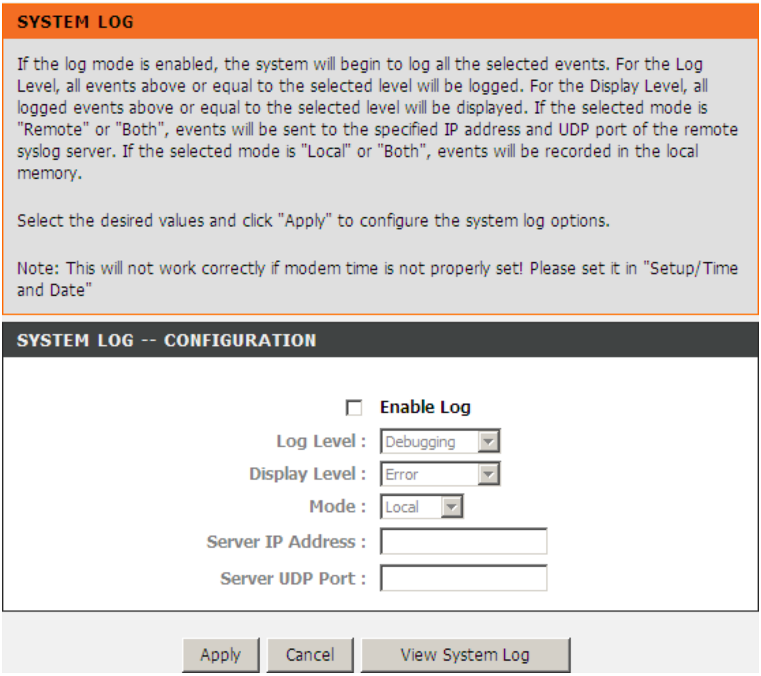
TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER

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

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.

4.4.5 System Log

Choose **MAINTENANCE** > **System Log**. The **System Log** page is shown as 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 procedures for logging the events are as follows:

Step 1 Select **Enable Log** check box.

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

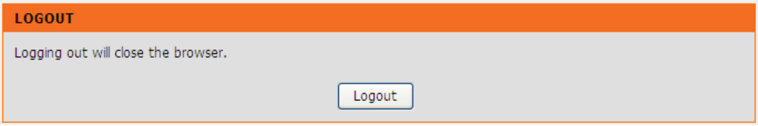
Step 3 Enter the **Server IP Address** and **Server UDP Port** if the **Mode** is set to **Both** or **Remote**.

Step 4 Click **Apply** to apply the settings.

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

4.4.6 Logout

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



LOGOUT

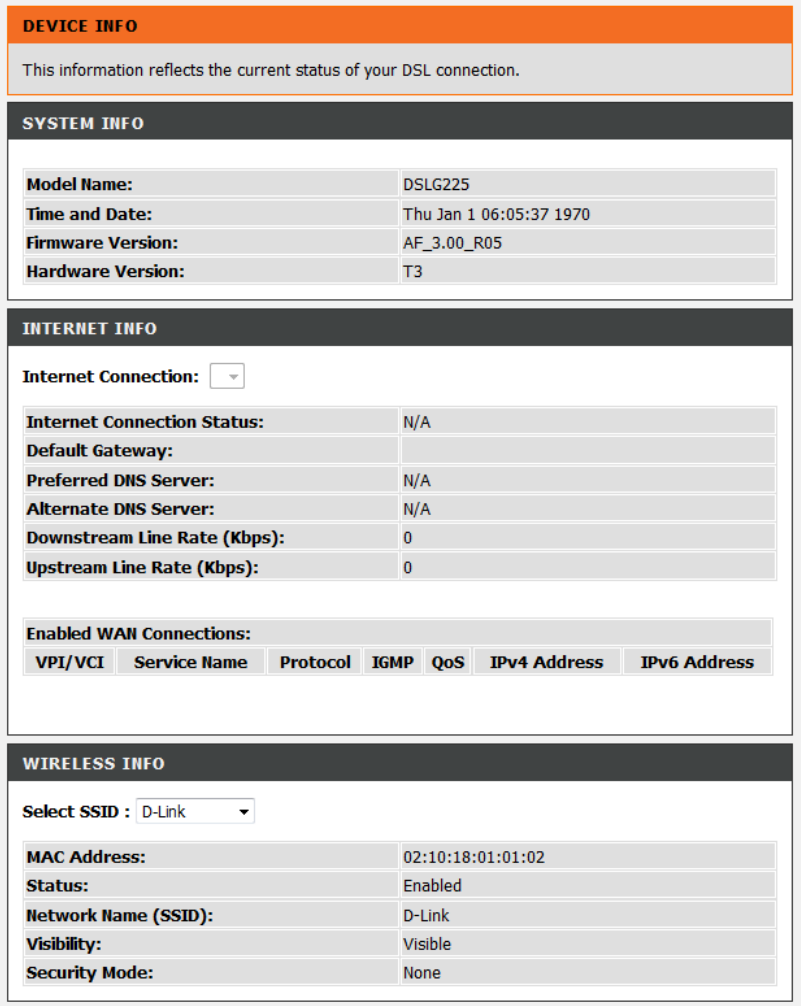
Logging out will close the browser.

4.5 Status

You can view the system information and monitor performance.

4.5.1 Device Info

Choose **STATUS** > **Device Info**. The page is shown as the following figure appears.



DEVICE INFO

This information reflects the current status of your DSL connection.

SYSTEM INFO

Model Name:	DSLG225
Time and Date:	Thu Jan 1 06:05:37 1970
Firmware Version:	AF_3.00_R05
Hardware Version:	T3

INTERNET INFO

Internet Connection:

Internet Connection Status:	N/A
Default Gateway:	
Preferred DNS Server:	N/A
Alternate DNS Server:	N/A
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0

Enabled WAN Connections:

VPI/VCI	Service Name	Protocol	IGMP	QoS	IPv4 Address	IPv6 Address

WIRELESS INFO

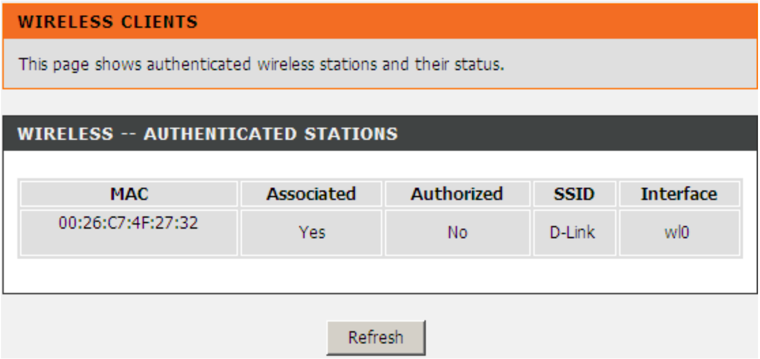
Select SSID : D-Link

MAC Address:	02:10:18:01:01:02
Status:	Enabled
Network Name (SSID):	D-Link
Visibility:	Visible
Security Mode:	None

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

4.5.2 Wireless Clients

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



WIRELESS CLIENTS

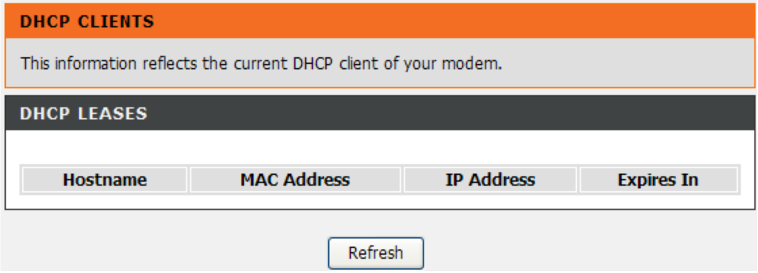
This page shows authenticated wireless stations and their status.

WIRELESS -- AUTHENTICATED STATIONS

MAC	Associated	Authorized	SSID	Interface
00:26:C7:4F:27:32	Yes	No	D-Link	wl0

4.5.3 DHCP Clients

Choose **STATUS** > **DHCP Clients**. The page shown in the following page appears.



DHCP CLIENTS

This information reflects the current DHCP client of your modem.

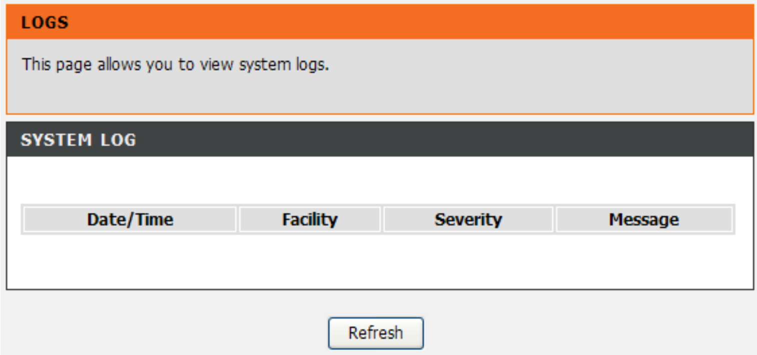
DHCP LEASES

Hostname	MAC Address	IP Address	Expires In

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).

4.5.4 Logs

Choose **STATUS** > **Logs**. The page is shown as the following figure appears.



LOGS

This page allows you to view system logs.

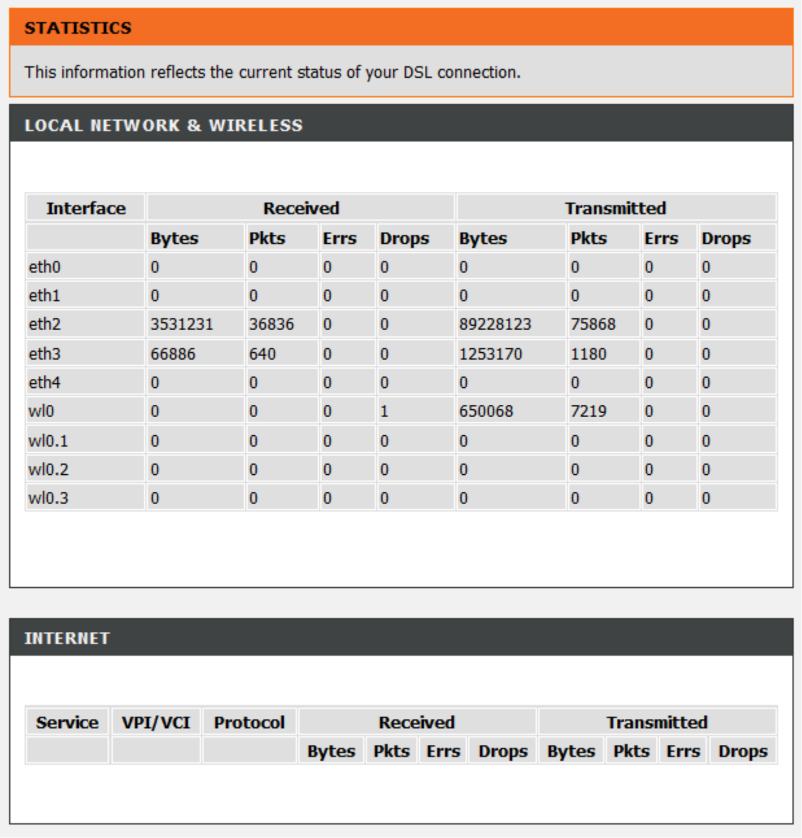
SYSTEM LOG

Date/Time	Facility	Severity	Message

This page lists the system log. Click **Refresh** to refresh the system log shown in the table.

4.5.5 Statistics

Choose **STATUS** > **Statistics**. The page is shown as the following figures appears.



STATISTICS

This information reflects the current status of your DSL connection.

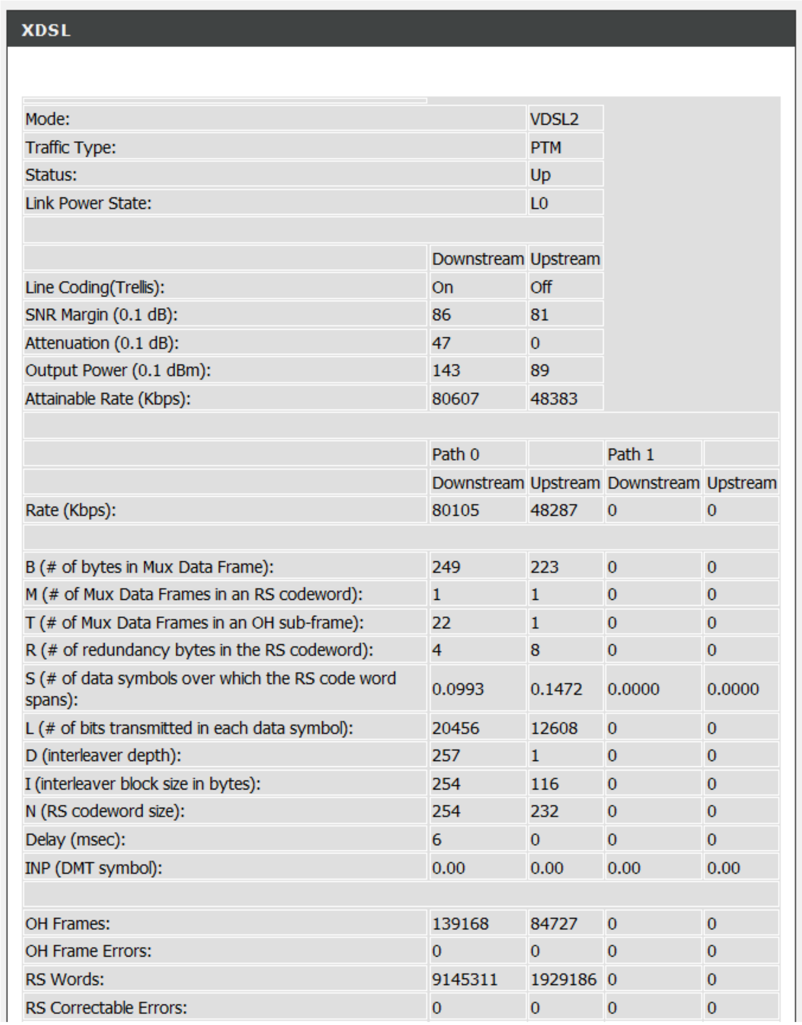
LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	0	0	0	0
eth1	0	0	0	0	0	0	0	0
eth2	3531231	36836	0	0	89228123	75868	0	0
eth3	66886	640	0	0	1253170	1180	0	0
eth4	0	0	0	0	0	0	0	0
wl0	0	0	0	1	650068	7219	0	0
wl0.1	0	0	0	0	0	0	0	0
wl0.2	0	0	0	0	0	0	0	0
wl0.3	0	0	0	0	0	0	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

Figure 23



XDSL

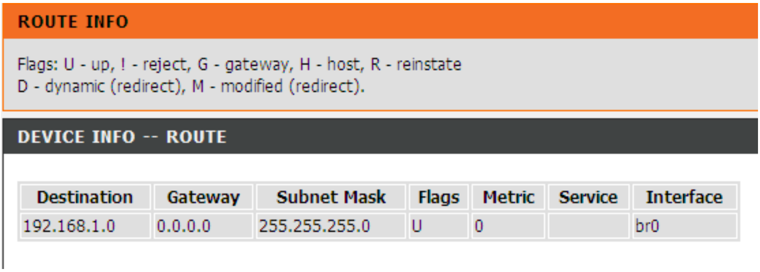
Mode:		VDSL2		
Traffic Type:		PTM		
Status:		Up		
Link Power State:		L0		
	Downstream	Upstream		
Line Coding(Trellis):	On	Off		
SNR Margin (0.1 dB):	86	81		
Attenuation (0.1 dB):	47	0		
Output Power (0.1 dBm):	143	89		
Attainable Rate (Kbps):	80607	48383		
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	80105	48287	0	0
B (# of bytes in Mux Data Frame):	249	223	0	0
M (# of Mux Data Frames in an RS codeword):	1	1	0	0
T (# of Mux Data Frames in an OH sub-frame):	22	1	0	0
R (# of redundancy bytes in the RS codeword):	4	8	0	0
S (# of data symbols over which the RS code word spans):	0.0993	0.1472	0.0000	0.0000
L (# of bits transmitted in each data symbol):	20456	12608	0	0
D (interleaver depth):	257	1	0	0
I (interleaver block size in bytes):	254	116	0	0
N (RS codeword size):	254	232	0	0
Delay (msec):	6	0	0	0
INP (DMT symbol):	0.00	0.00	0.00	0.00
OH Frames:	139168	84727	0	0
OH Frame Errors:	0	0	0	0
RS Words:	9145311	1929186	0	0
RS Correctable Errors:	0	0	0	0

Figure 24

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.

4.5.6 Route info

Choose **STATUS** > **Route Info**. The page is shown as the following figure appears.



ROUTE INFO

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

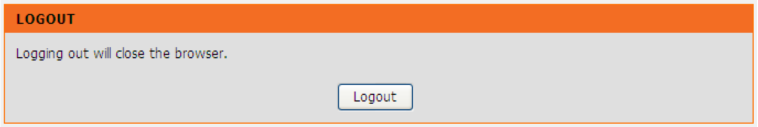
DEVICE INFO -- ROUTE

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

The table shows a list of destination routes commonly accessed by the network.

4.5.7 Logout

Choose **STATUS** > **Logout**. The page is shown as 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 whether the power connection is correct. ● Check whether the power switch is turned on.
Why is the LAN indicator off?	● Check whether the connections between the device and the PC, the hub, or the switch are correct. ● Check whether the running statuses of the computer, hub, or switch are normal. ● The cables that connects the device and other devices: –If the device connects to a computer, use the crossover 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 10.0.0.2** (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 15-20 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: 10.0.0.2 ● Subnet mask: 255.255.255.0. ● User name and password: admin/admin