D-Link®

User Manual

WIRELESS N 150無線寬頻路由器

Wireless N150 Home Router

DIR-610

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2012 by D-Link Systems, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

Table of Contents

Preface i
Trademarks i

Table of Contents ii

Product Overview 1
Package Contents 1
System Requirements 2
Features 3
Hardware Overview 4
Front Panel 4
Back Panel 5

Hardware Installation 6
Before You Begin 6
Wireless Installation Considerations 7
Connect to Cable/DSL/Satellite Modem 8

Configuration 9
Web-based Configuration Utility 9
Setup Wizard 10
Internet Connection 10
Internet Connection(Setup Wizard) 11
Manual Configuration 18
Wireless Settings 27
Network Settings 36
IPv6 40
Advanced Category 62
Virtual Server 63
Port Forwarding 65
Application Rules 66
QoS Engine 67
Network Filter 69
Access Control 70
Website Filter 73
Inbound Filter 74
Firewall Settings 75
Routing 77
Advanced Wireless 78
Wi-Fi Protected Setup 79
Advanced Network 81
Tools Category 83
Admin 84
Time 86
Syslog 87
Email Settings 88
System 90
Firmware 91
Dynamic DNS 92
System Check 95

Schedules 96
Status Category 97
Device Info 98
Logs 100
Statistics 101
Internet Sessions 102
Wireless 102
IPv6 103
Support Category 104

Knowledge Base 105
Wireless Basics 105
Wireless Modes 107
Wireless Security 108
What is WPA? 108
Networking Basics 109
Connect to a Wireless Network 111
Using Window 7 111
Using Window 7 and WPS 113
Using Window Vista 116
Using Window XP 118

Troubleshooting 119

Technical Specifications 121

Product Overview

Package Contents

Check for the supplied accessories below:

DIR-610 Wireless N150 Home Router

Power Adapter

Ethernet Cable

Quick Installation Guide

Note: Using a power supply with a different voltage rating than the one included with the product, will cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n or 802.11g wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher (with Java 1.3.1 or higher) **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
CD Installation Wizard Requirements	**Computer with the following:** • Windows® 7, Vista®, or XP with Service Pack 2 • An installed Ethernet adapter

Features

- **Internet Connectivity -** In conjunction with a DSL or Cable Modem, this device provides high-speed Internet connectivity to your local network for up to four wired devices.

- **Wireless LAN functionality -** This router supports features like WMM, RF Output Level Control, WPS, and much more.

- **Networking -** This router comes with one WAN port and four LAN ports that enable up to four computers on your local network to be connected.

- **Wireless Distribution System (WDS) mode-** The router supports WDS where it can extend the network coverage from another router.

- **Advanced Security -** The router also supports a range of security features like Network Filtering, Access Control, Website Filtering, Inbound Filtering, and SPI.

- **IPv6 -** This router supports local IPv6 support and IPv6 Internet Connection.

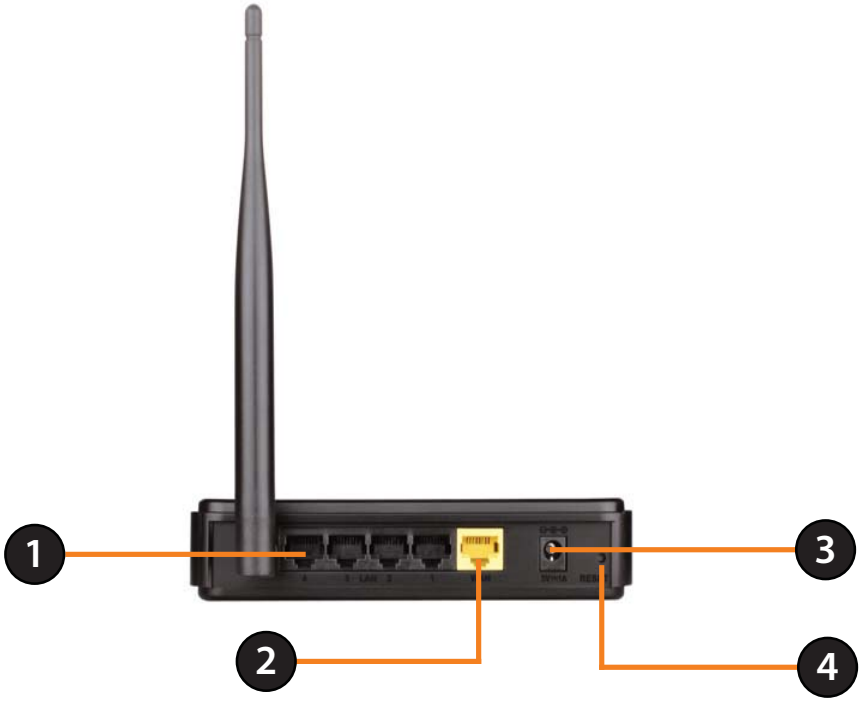
- **User-friendly Setup Wizard -** The DIR-610's easy-to-use Web-based user interface lets you manage and configure your router qickly and conveniently.

Hardware Overview

Front Panel

1	Power LED	The LED lights solid green to indicate the power is on.
2	WAN LED	A solid light indicates connection on the Internet port. This LED blinks during data transmission.
3	Wireless LED	A solid light indicates that the wireless segment is ready. This LED blinks during wireless data transmission.
4	LAN LEDs (1-4)	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.

Back Panel



1	Ethernet Ports (1 to 4)	Connect to Ethernet devices such as computers, switches, and hubs.
2	Internet Port	Connects to a DSL or Cable modem.
3	Power Receptor	Receptor for the supplied power adapter.
4	Reset	Pressing the Reset button restores the router to its original factory default settings.

Hardware Installation

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

Before You Begin

- The router is designed for use with the Ethernet port on your broadband modem. If you were using the USB connection before using the router, you must turn off your modem and disconnect the USB cable. Connect an Ethernet cable to the WAN/Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change your connection type (USB to Ethernet).

- If you have DSL and are connecting via PPPoE, be sure to disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer. Otherwise you will not be able to connect to the Internet.

Wireless Installation Considerations

The router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or office. The key to maximizing the wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters.) Position your devices so that the number of walls and/or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick. Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Try to position access points, wireless routers, and computers so that the signal passes through open doorways and drywall. Materials such as glass, metal, brick, insulation, concrete and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors and aluminum studs may also have a negative effect on range.

4. Keep your product at least 3 to 6 feet (1-2 meters) away from electrical devices or appliances that generate RF noise.

5. If you are using 2.4 GHz cordless phones, make sure that the 2.4 GHz phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone in not in use. In some cases, cordless phones, X-10 wireless devices, and electronic equipment such as ceiling fans, fluorescent lights, and home security systems may dramatically degrade wireless connectivity.

Connect to Cable/DSL/Satellite Modem

If you are connecting the router to a Cable/DSL/Satellite Modem, please follow the steps below:

1. Place the router in an open and central location. Do not plug the power adapter into the router.
2. Turn the power off on your modem. If there is no on/off switch, unplug the modem's power adapter. Shut down your computer.
3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the Internet port on the router.
4. Plug an Ethernet cable into one of the LAN ports on the router. Plug the other end into the Ethernet port on your computer.
5. Turn on or plug in your modem. Wait for the modem to boot (about 30 seconds).
6. Plug the power adapter into the router and connect to an outlet or power strip. Wait about 30 seconds for the router to boot up.
7. Turn on your computer.
8. Verify that the Power LED on the router is lit. If the Power LED does not light up, make sure your computer, modem, and router are powered, on and verify that the cables connected correctly.
9. In a later section in this manual we'll discuss the Web GUI configuration of the router in more detail..

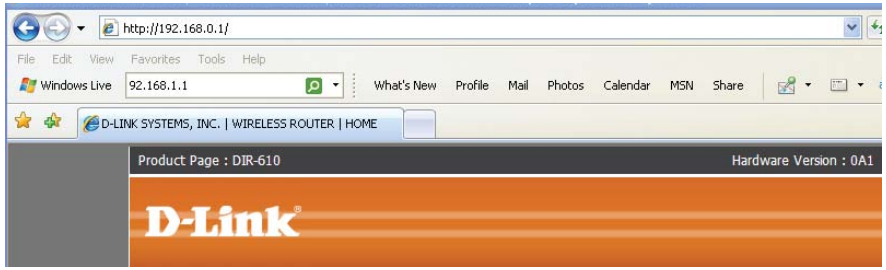
Configuration

This section will show you how to configure your new D-Link wireless router using the web-based configuration utility.

Web-based Configuration Utility

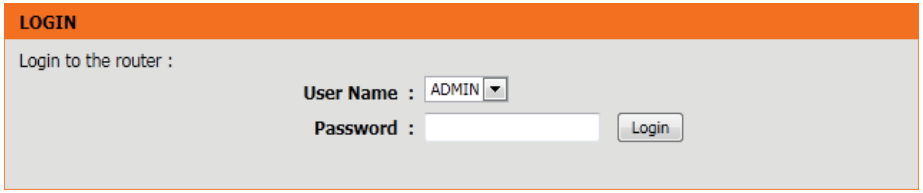
To access the configuration utility, open a web browser such as Internet Explorer and enter the IP address of the router (192.168.0.1).

You may also connect using the NetBIOS name in the address bar (**http://dlinkrouter**).



Enter your password. **Admin** is the default username and cannot be changed. The password is left blank by default.
If you get a **Page Cannot be Displayed** error message, please refer to the **Troubleshooting** section for assistance.

Click **Login** to log into the Router.

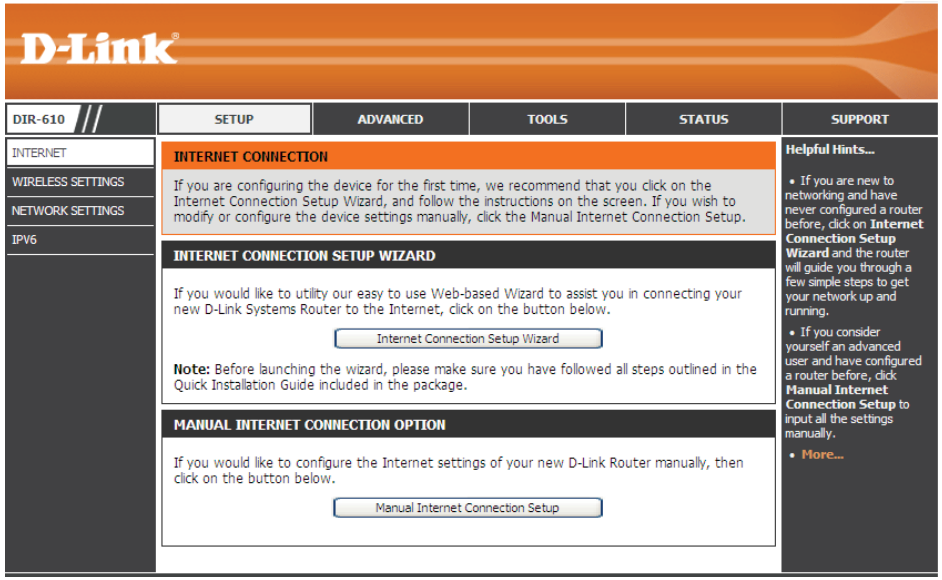


Setup Wizard

Internet Connection

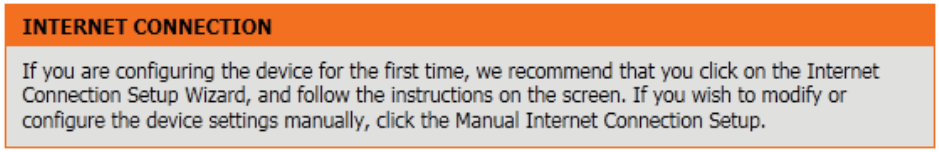
Click **Internet Connection Setup Wizard** to quickly configure your router. Skip to the next page.

If you want to enter your settings without running the wizard, click **Manual Configuration** and skip to page 20.



Internet Connection(Setup Wizard)

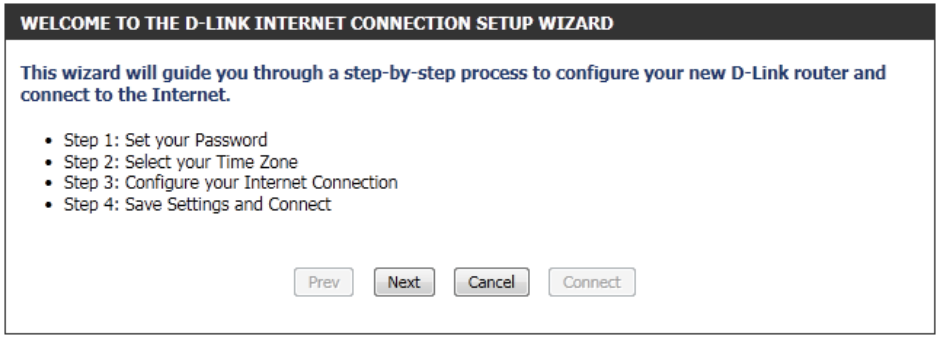
When configuring the router for the first time, we recommend that you click **Internet Connection Setup Wizard,** and follow the instructions on the screen. This wizard is designed to assist user with a quick and easy method to configure the Internet connection of this router.



Anytime during the Internet Connection Setup Wizard, you can click on **Cancel** to discard any changes made and return to the main Internet page. Also you can click on **Prev** to return to the previous window for re-configuration.

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

Click **Next** to continue.



Step 1: Set Your Password

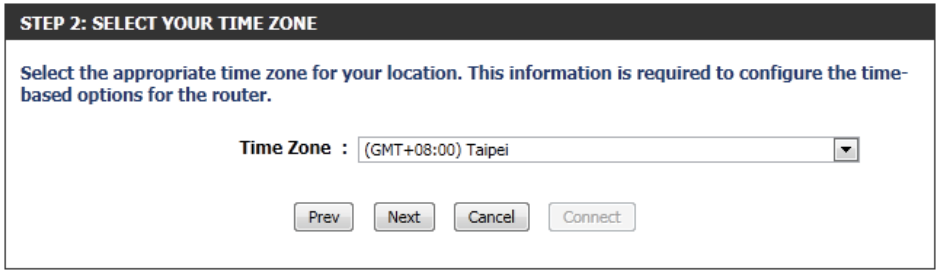
By default, the D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please enter and verify a password in the spaces provided. The two passwords must match.

Click **Next** to continue.

Step 2: Select Your Time Zone

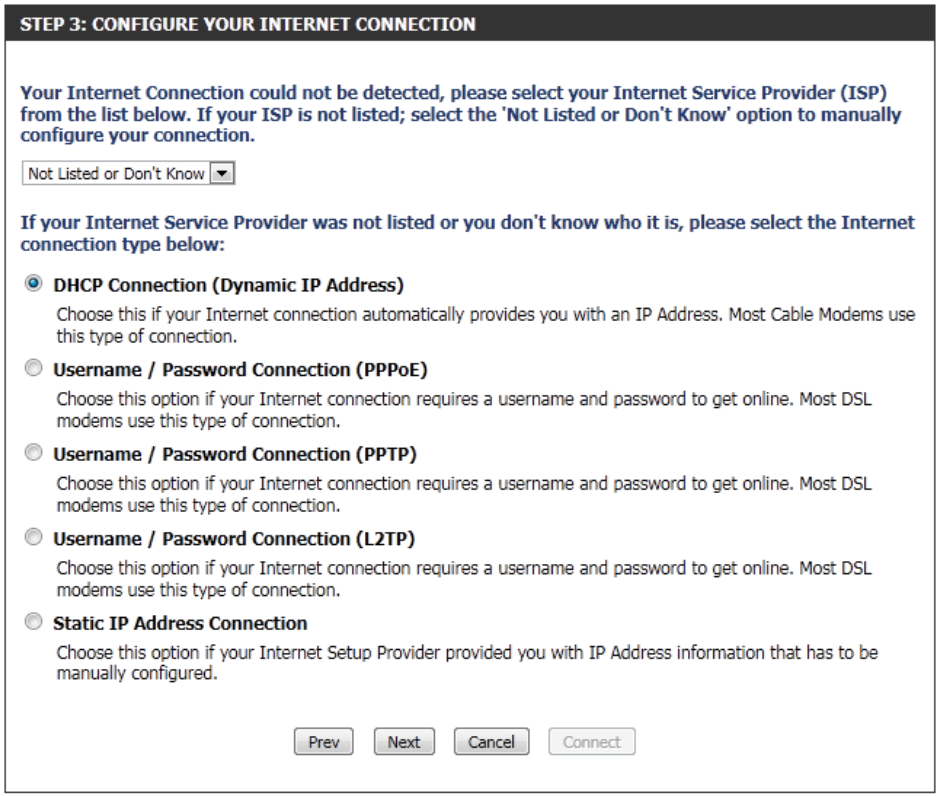
Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

Click **Next** to continue.



Step 3: Internet Connection

Here the user will be able to configure the Internet Connectivity used by this device. If your ISP connection is listed in the drop-down menu select it and click **Next.** If your ISP connection is not listed then you can proceed to select any of the other manual Internet Connection methods listed below.



Dynamic IP Address: Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

PPPoE: Choose this option if your Internet connection requires a PPPoE username and password to get online. Most DSL modems use this type of connection.

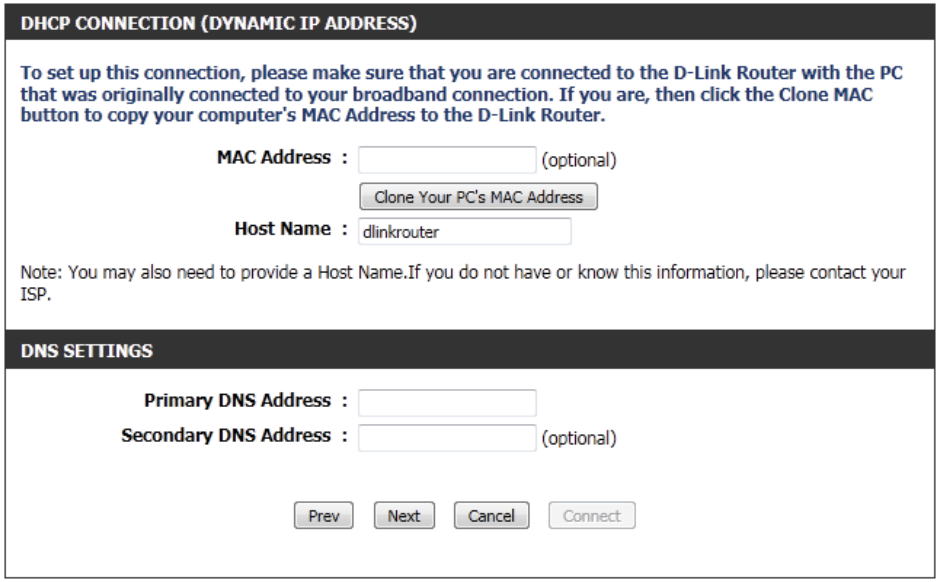
PPTP: Choose this option if your Internet connection requires a PPTP username and password to get online.

L2TP: Choose this option if your Internet connection requires an L2TP username and password to get online.

Static IP Address: Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

Step 3: Internet Connection (Dynamic IP Address)

After selecting the Dynamic IP Address Internet connection method, the following page will appear.



MAC Address: Enter the MAC address of the Internet gateway (plugged into the Internet port of this device).

Clone Button: If the configuration PC also acts as the Internet gateway, then click on the Clone Your PC's MAC Address button to copy the PC's MAC address into the space provided. If you're not sure, leave the MAC Address field blank.

Host Name: Enter the host name used. You may also need to provide a Host Name. If you do not have or know this information, please contact your ISP.

Primary DNS Address: Enter the Primary DNS IP address used.

Secondary DNS Address: Enter the Secondary DNS IP address used. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

Step 3: Internet Connection (PPPoE)

After selecting the PPPoE Internet connection method, the following page will appear:

Address Mode: The user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. PPPoE usually requires a Dynamic IP configuration.

IP Address: Enter the PPPoE IP address used. This option is only available if Static IP is selected.

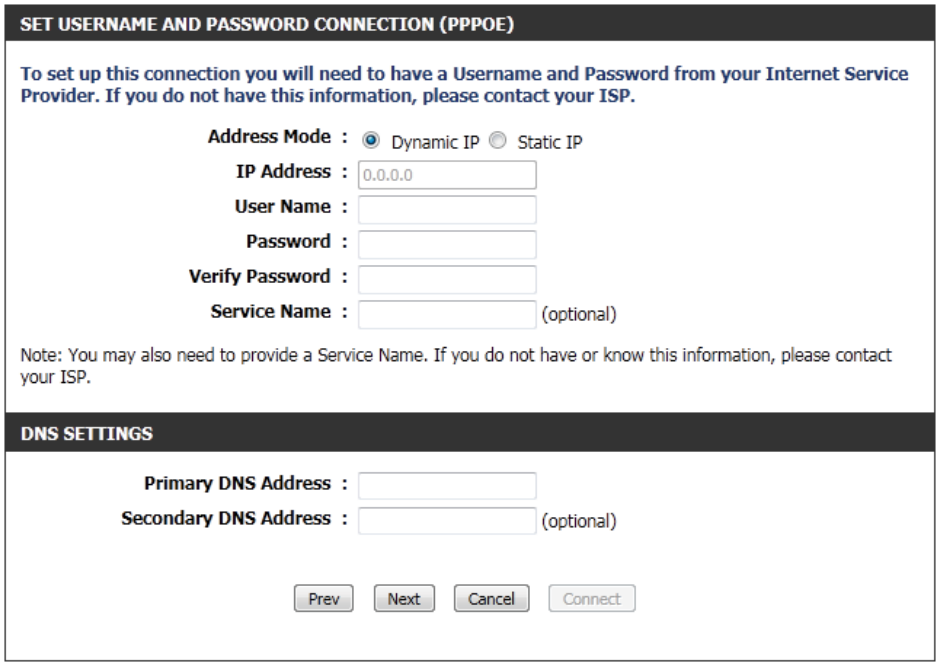
User Name: Enter the PPPoE account user name used. This information is given by the ISP.

Password: Enter the PPPoE account password used. This information is given by the ISP.

Verify Password: Re-enter the PPPoE account password used.

Service Name: This optional field enables the user to enter a service name to identify this Internet connection.

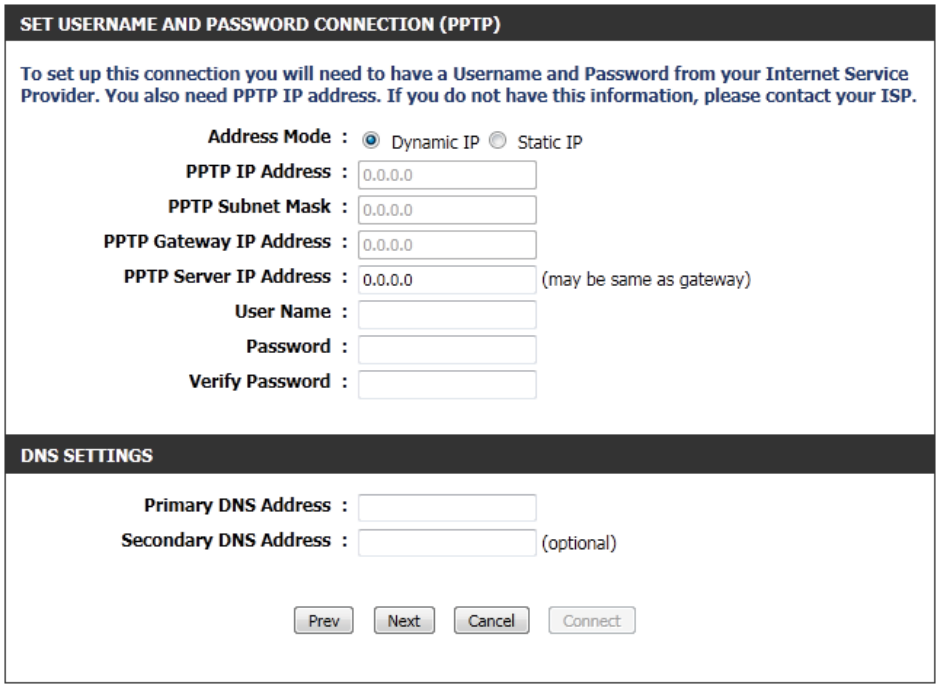
Primary DNS Address: Enter the Primary DNS IP address used.



Click **Next** to continue.

Step 3: Internet Connection (PPTP)

After selecting the PPTP Internet connection method, the following page will appear:



Address Mode: Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. PPTP usually requires a Dynamic IP configuration.

PPTP IP Address: Enter the PPTP IP address used here. This option is only available if Static IP is selected.

PPTP Subnet Mask: Enter the PPTP Subnet Mask used.

PPTP Gateway IP Address: Enter the PPTP Gateway IP address used.

PPTP Server IP Address: Enter the PPTP Server IP address used. This is normally the same as the PPTP Gateway IP address.

User Name: Enter the PPTP username used.

Password: Enter the PPTP password used.

Verify Password: Re-enter the PPTP password used.

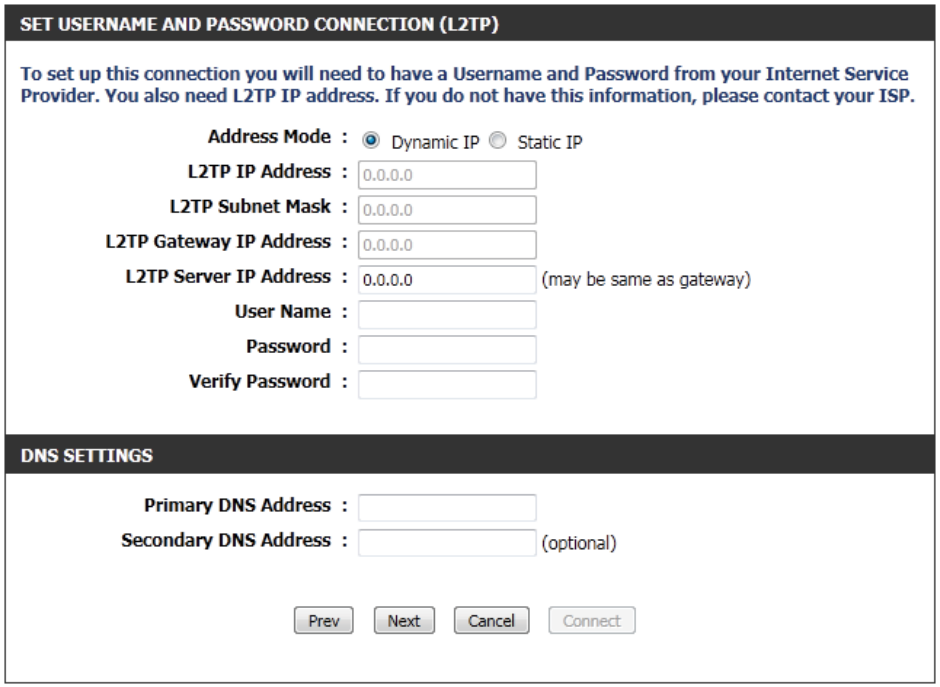
Primary DNS Address: Enter the Primary DNS IP address used.

Secondary DNS Address: Enter the Secondary DNS IP address used. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

Step 3: Internet Connection (L2TP)

After selecting the L2TP Internet connection method, the following page will appear:



Address Mode: Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. L2TP usually requires a Dynamic IP configuration.

L2TP IP Address: Enter the L2TP IP address used here. This option is only available if Static IP is selected.

L2TP Subnet Mask: Enter the L2TP Subnet Mask used.

L2TP Gateway IP Address: Enter the L2TP Gateway IP address used.

L2TP Server IP Address: Enter the L2TP Server IP address used. This is normally the same as the L2TP Gateway IP address.

User Name: Enter the L2TP username used.

Password: Enter the L2TP password used.

Verify Password: Re-enter the L2TP password used.

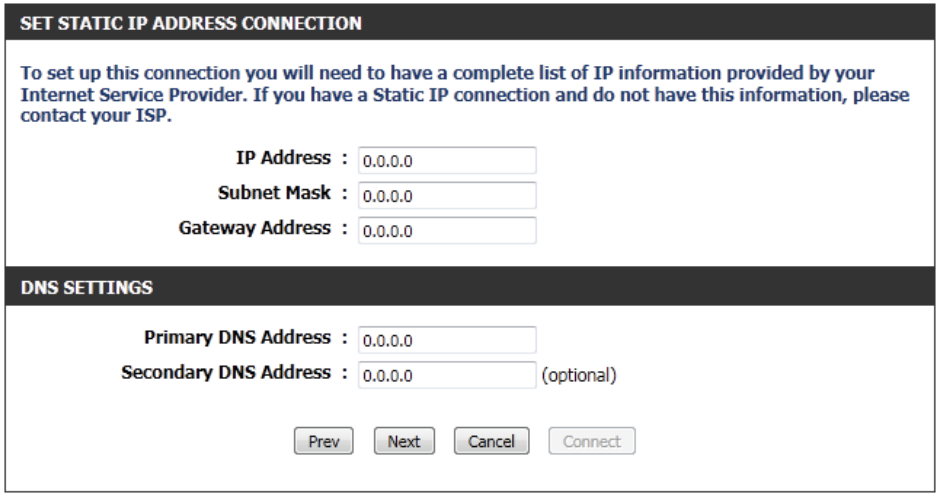
Primary DNS Address: Enter the Primary DNS IP address used.

Secondary DNS Address: Enter the Secondary DNS IP address used. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

Step 3: Internet Connection (Static IP Address)

After selecting the Static IP Address Internet connection method, the following page will appear:



IP Address: Enter the Static IP address provided by the ISP.

Subnet Mask: Enter the Subnet Mask provided by the ISP.

Gateway Address: Enter the Gateway IP address provided by the ISP.

Primary DNS Address: Enter the Primary DNS IP address used.

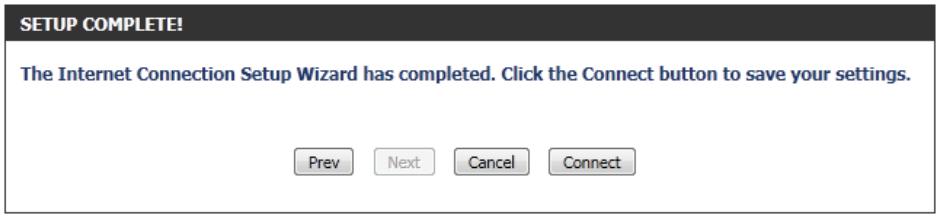
Secondary DNS Address: Enter the Secondary DNS IP address used. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

Setup Complete!

This is the last page of the Internet Connection Setup Wizard.

Click the **Connect** button to save your settings.



Manual Configuration

On this page the user can configure the Internet Connection settings manually. To access the Manual Internet Connection Setup page, click on the **Manual Internet Connection Setup** button. On this page there are multiple parameters that can be configured regarding the Internet Connection setup. We'll discuss them from top to bottom.

At any given point the user can save the configuration done by clicking on the **Save Settings** button. If you choose to discard the changes made, click on the **Don't Save Settings**.

Internet Connection Type

In this section, the user can select from a list of Internet Connection types that can be configured and used on this router. Options to choose from are Static IP, Dynamic IP, PPPoE, PPTP, L2TP, and DS-Lite.
After selecting a specific Internet Connection type, this page will automatically refresh and display unique fields to configure related to the specified Internet Connection type.

My Internet Connection is: Dynamic IP (DHCP)

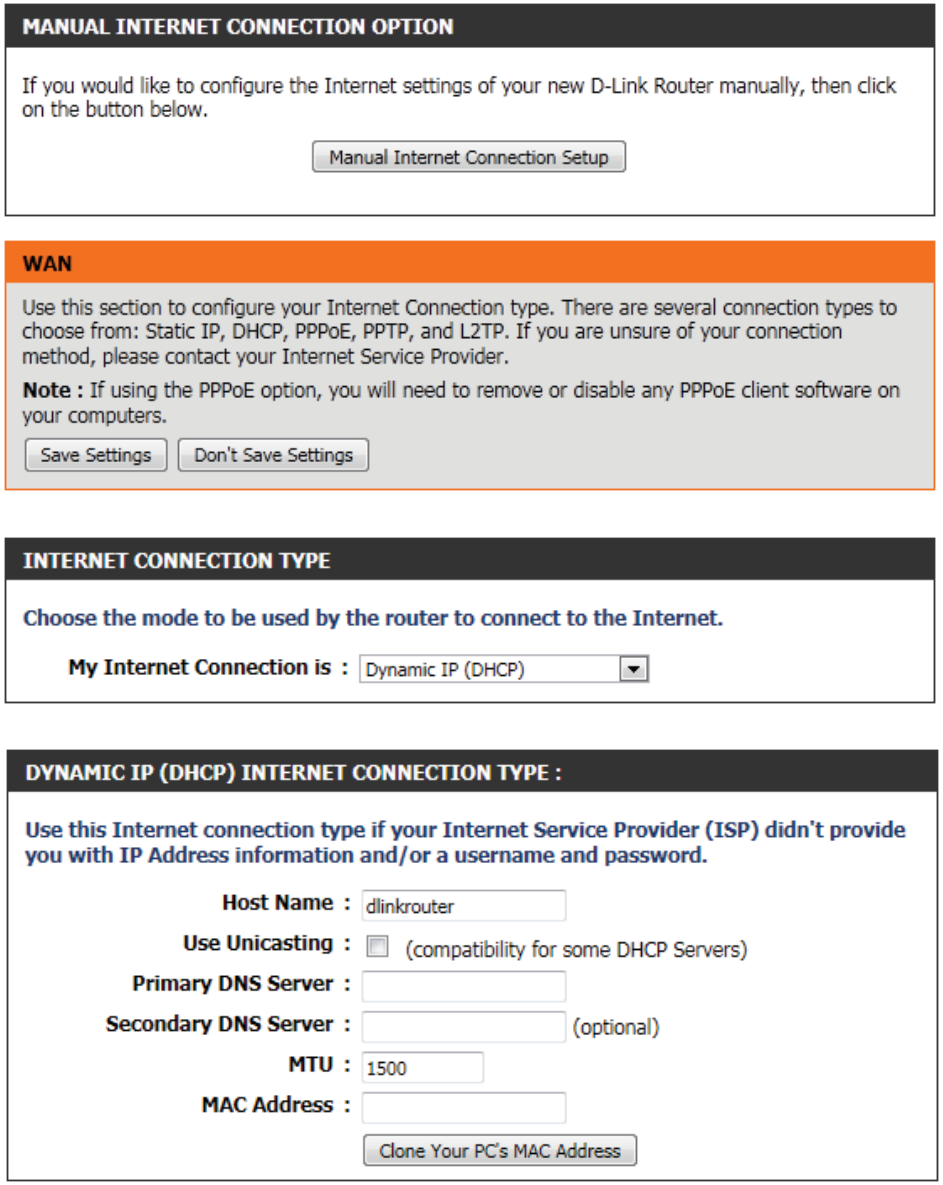
The default WAN configuration for this router is Dynamic IP (DHCP). This option allows the router to obtain an IP address automatically from the device that is connected to the Internet port.

Note: If you're not sure about the type of Internet Connection you have, please contact your Internet Service Provider (ISP) for assistance.

Host Name: The Host Name is optional but may be required by some ISPs. Leave it blank if you are not sure.

Use Unicasting: Tick this option if your ISP uses the unicast method to provide IP addresses.

Primary DNS: Enter the Primary DNS IP address used.



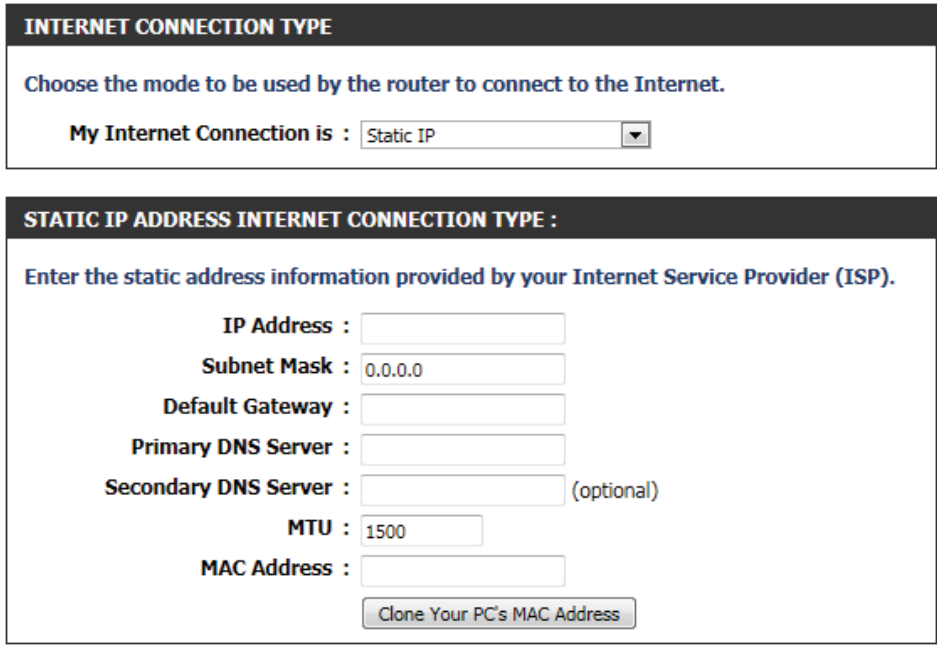
Secondary DNS: Enter the Secondary DNS IP address used. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

My Internet Connection is: Static IP

Another Internet Connection type is Static IP. This option allows the user to manually configure the Static IP Internet Connection type. Normally the information entered will be supplied by your ISP.



IP Address: Enter the Static IP address provided by the ISP.

Subnet Mask: Enter the Subnet Mask provided by the ISP.

Default Gateway: Enter the Gateway IP address provided by the ISP.

Primary DNS: Enter the Primary DNS IP address used.

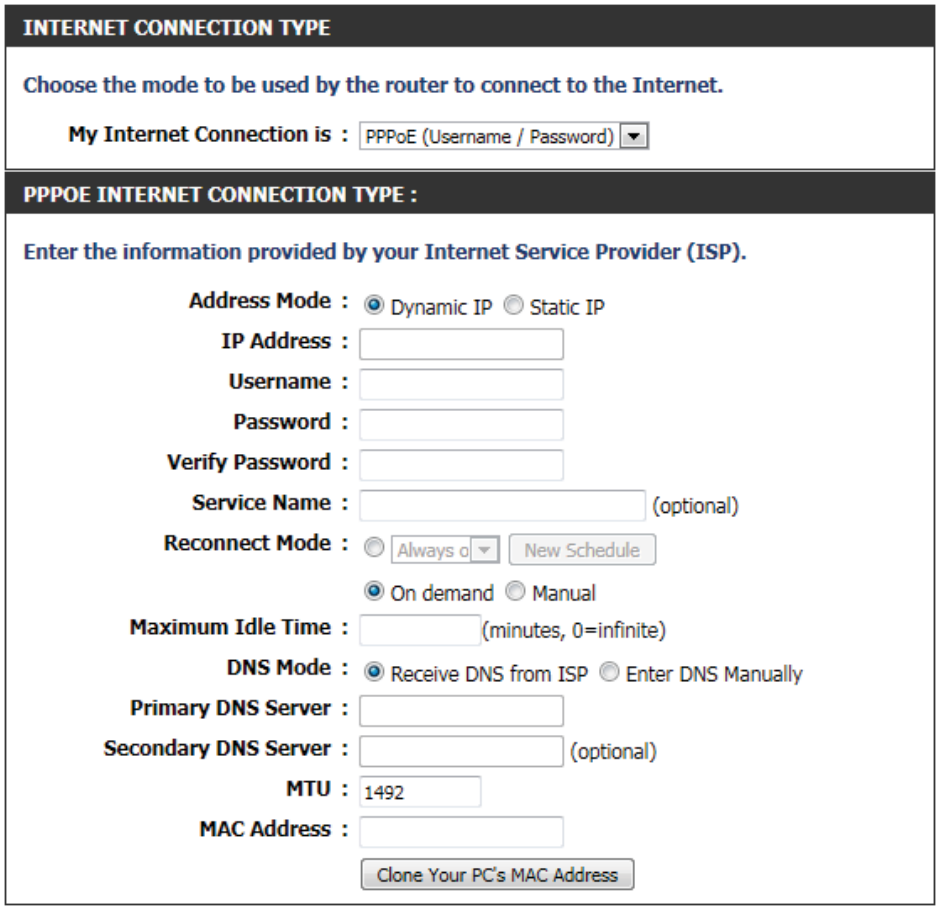
Secondary DNS: Enter the Secondary DNS IP address used. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the Clone Your PC's MAC Address button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

My Internet Connection is: PPPoE (Username/Password)

Another Internet Connection type is PPPoE. This option is typically used if you have a DSL Internet Connection. Make sure to remove the PPPoE software installed on your computer first before using this connection type. Most of the information needed for this connection type is provided to you by your ISP.



Address Mode: Here you can specify whether the Internet connection requires the use of a **Dynamic** or **Static IP** address. PPPoE usually requires a Dynamic IP configuration.

IP Address: Enter the PPPoE IP address used here. This option is only available if Static IP is selected.

Username: Enter the PPPoE account user name used. This information is given by the ISP.

Password: Enter the PPPoE account password used. This information is given by the ISP.

Verify Password: Re-enter the PPPoE account password used.

Service Name: This optional field enables the user to enter a service name to identify this Internet connection.

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the New Schedule button to open the Schedules page. Schedules will be discussed later.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity.

DNS Mode: This option allow the router to obtain the DNS IP addresses from the ISP, when **Receive DNS from ISP** is selected, or allows the user to enter the DNS IP address manually, when **Enter DNS Manually** is selected.

Primary DNS Server: Enter the Primary DNS IP address used here.

Secondary DNS Server: Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

My Internet Connection is: PPTP (Username/Password)

Another Internet Connection type is PPTP. This option is typically used if you have a secure DSL Internet Connection. Most of the information needed for this connection type is provided to you by your ISP.

Address Mode: Here the user can specify whether this Internet connection requires the use of a **Dynamic** or **Static IP** address. PPTP usually requires a Dynamic IP configuration.

PPTP IP Address: Enter the PPTP IP address used. This option is only available if Static IP is selected.

PPTP Subnet Mask: Enter the PPTP Subnet Mask used.

PPTP Gateway IP Address: Enter the PPTP Gateway IP address used.

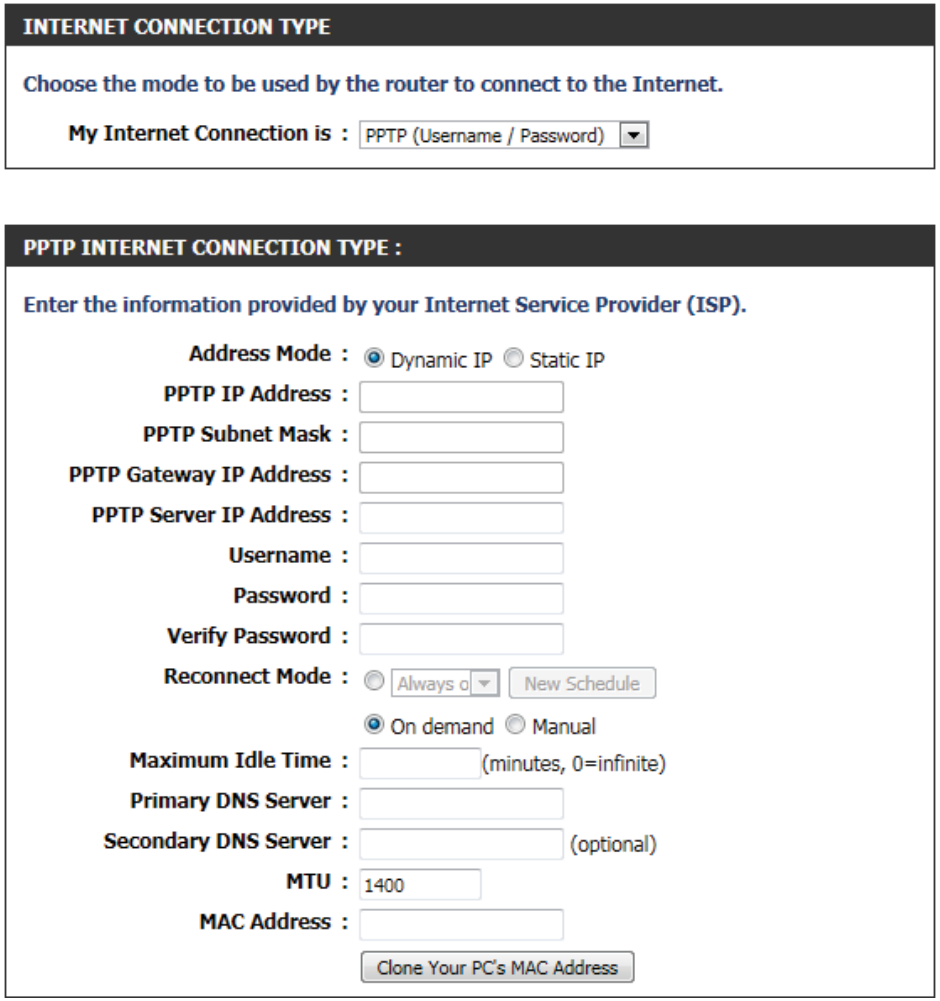
PPTP Server IP Address: Enter the PPTP Server IP address used. This is normally the same a the PPTP Gateway IP address.

Username: Enter the PPTP username used.

Password: Enter the PPTP password used.

Verify Password: Re-enter the PPTP password used.

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click **New Schedule** to open the Schedules page. Schedules will be discussed later.



Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

Primary DNS Server: Enter the Primary DNS IP address used.

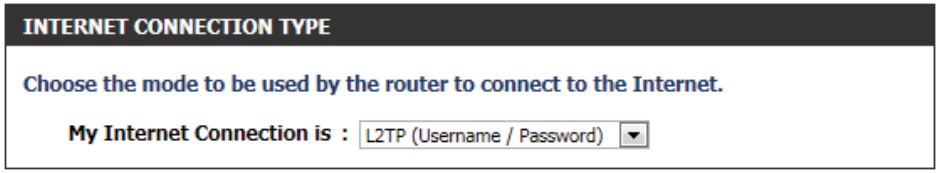
Secondary DNS Server: Enter the Secondary DNS IP address used. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

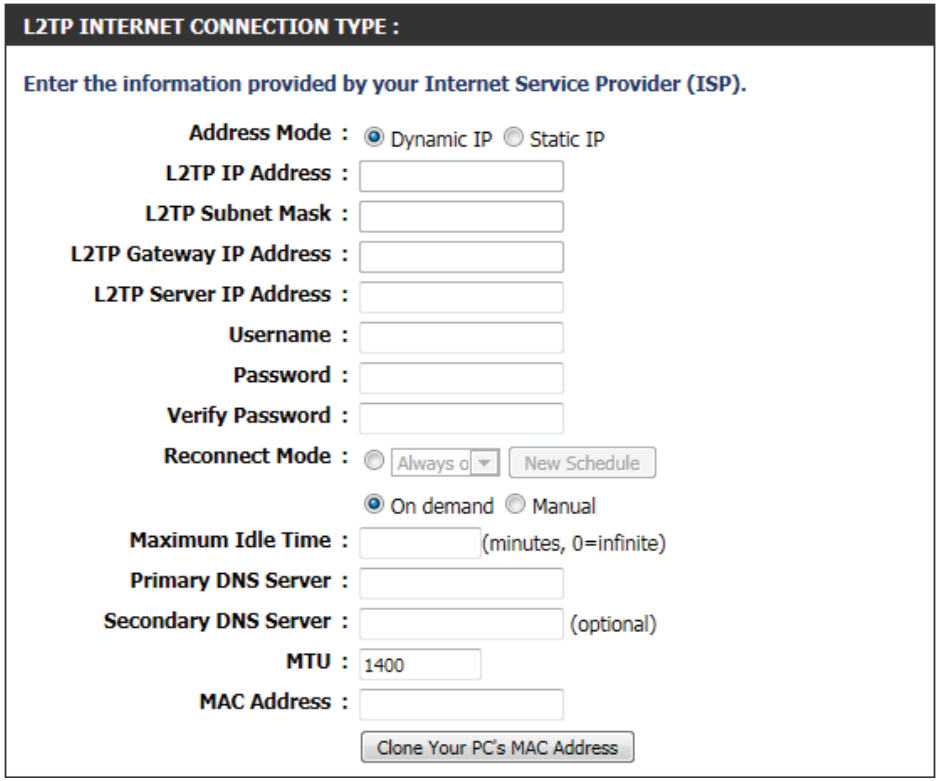
MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

My Internet Connection is: L2TP (Username/Password)

Another Internet Connection type is L2TP. This option is typically used if you have a secure DSL Internet Connection. Most of the information needed for this connection type is provided to you by your ISP.





Address Mode: The user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. L2TP usually requires a Dynamic IP configuration.

L2TP IP Address: Enter the L2TP IP address used. This option is only available if Static IP is selected.

L2TP Subnet Mask: Enter the L2TP Subnet Mask used.

L2TP Gateway IP Address: Enter the L2TP Gateway IP address used.

L2TP Server IP Address: Enter the L2TP Server IP address used. This is normally the same as the L2TP Gateway IP address.

Username: Enter the L2TP username used.

Password: Enter the L2TP password used.

Verify Password: Re-enter the L2TP password used.

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the **New Schedule** to open the Schedules page. Schedules will be discussed later.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

Primary DNS Server: Enter the Primary DNS IP address used.

Secondary DNS Server: Enter the Secondary DNS IP address used. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

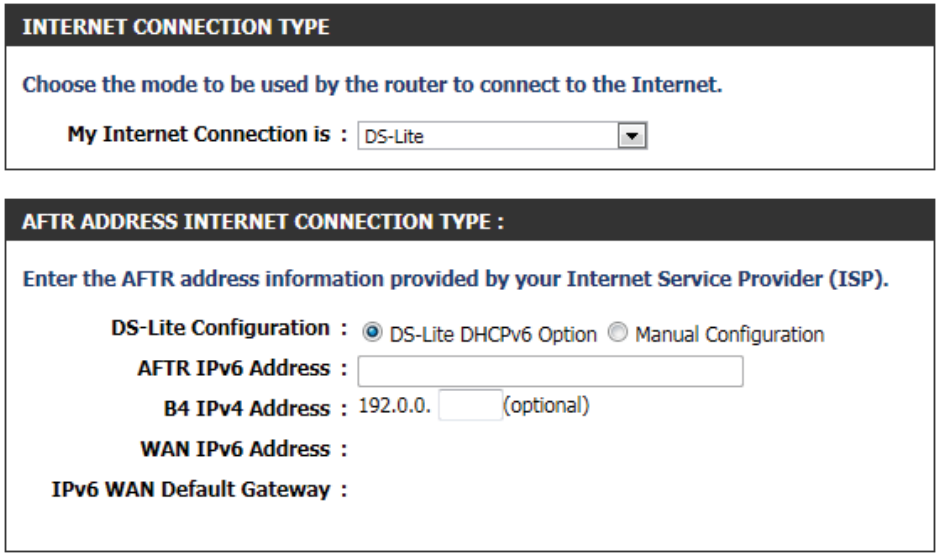
MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

My Internet Connection is: DS-Lite)
Another Internet Connection type is DS-Lite.

After selecting DS-Lite, the following parameters will be available for configuration:

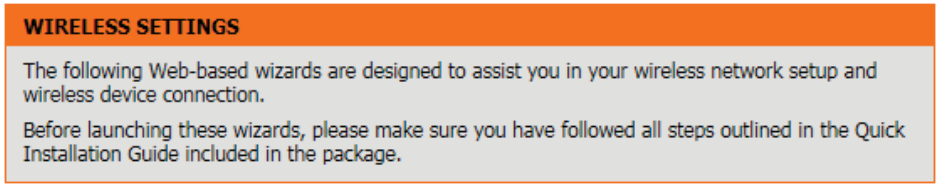
DS-Lite Configuration:	Select the **DS-Lite DHCPv6 Option** to let the router allocate the AFTR IPv6 address automatically. Select the **Manual Configuration** to enter the AFTR IPv6 address in manually.
AFTR IPv6 Address:	After selecting the Manual Configuration option above, the user can enter the AFTR IPv6 address used.
B4 IPv4 Address:	Enter the B4 IPv4 address value used.
WAN IPv6 Address:	Once connected, the WAN IPv6 address will be displayed.
IPv6 WAN Default Gateway	Once connected, the IPv6 WAN Default Gateway address will be displayed.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Wireless Settings

On this page the user can configure the Wireless settings for this device. There are 3 ways to configure Wireless using this router. Firstly, the user can choose to make use for the quick and easy **Wireless Connection Setup Wizard**. Secondly, the user can choose to make use Wi-Fi Protected Setup. Lastly, the user can configure the Wireless settings manually.

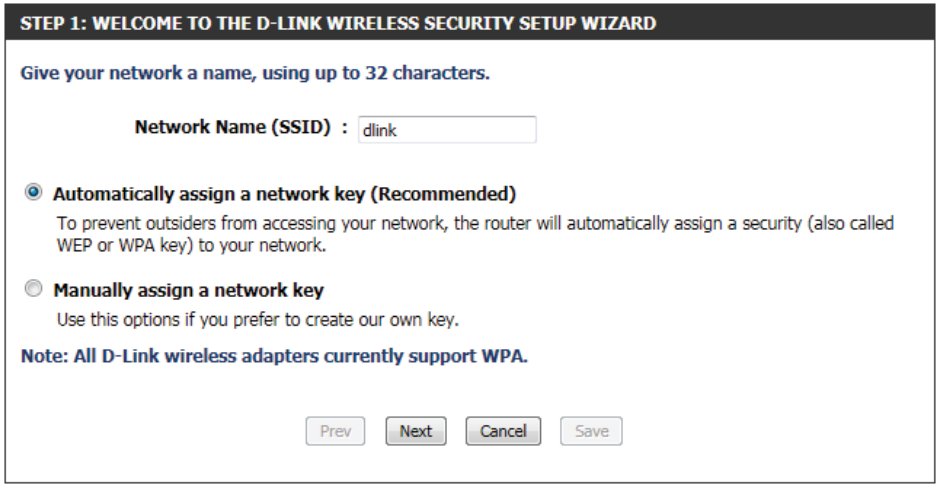


Wireless Settings: Wireless Connection Setup Wizard

The Wireless Connection Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to configure the wireless settings of this router. It is highly recommended to customized the wireless network settings to fit into your environment and to add higher security.

To initiate the **Wireless Connection Setup Wizard** click on the Wireless Connection Setup Wizard button.

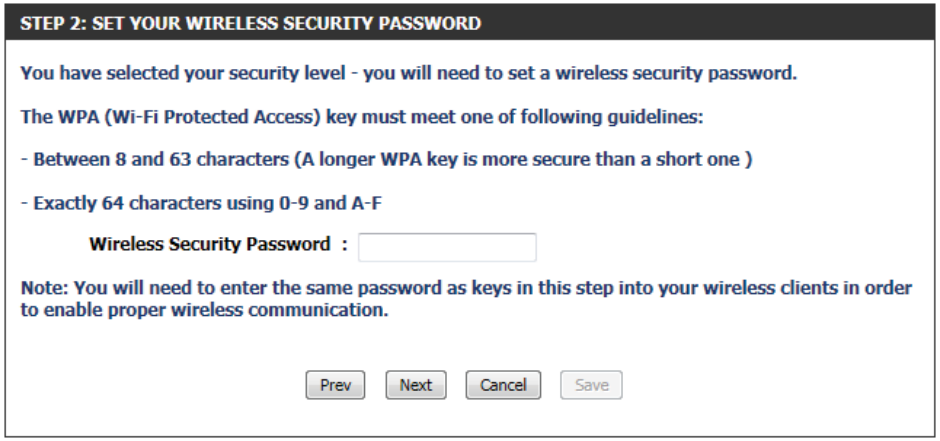
Step 1: In this step, the user must enter a custom Wireless Network Name or SSID. Enter the new **SSID name** in the appropriate space provided. Secondly the user can choose between two wireless security wizard configurations. The user can select '**Automatically assign a network key**', by which the router will automatically generate a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods; or the user can select '**Manually assign a network key**', by which the user will be prompt to manually enter a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods.



Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

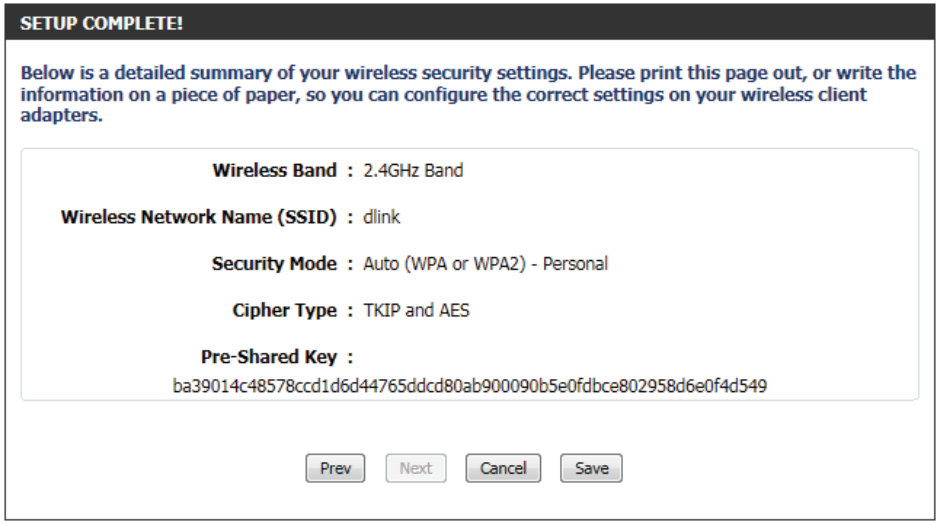
Step 2: This step will only be available if the user selected 'Manually assign a network key' in the previous step. Here the user can manually enter the WPA/WPA2 pre-shared key in the **Wireless Security Password** space provided. The key entered must be between 8 and 63 characters long. Remember, this key will be used when wireless clients wants to connect to this device. So please remember this key to prevent future troubleshooting.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

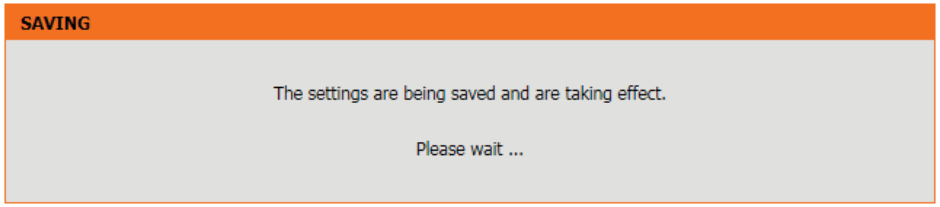


Setup Complete: On this page the user can view the configuration made and verify whether they are correct.

Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard the changes made and return to the main wireless page. Click on the **Save** button to accept the changes made.

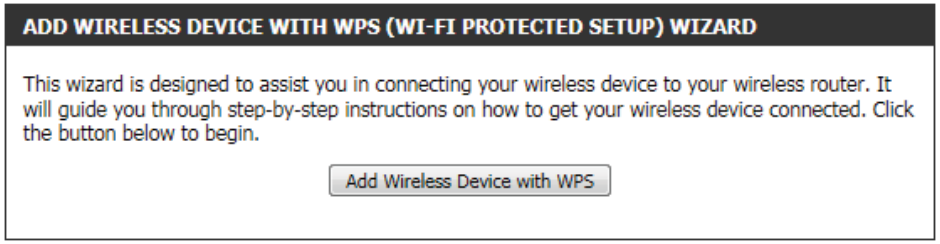


After click the **Save** button the device will save the settings made and return to the main wireless page.



Wireless Settings: Wi-Fi Protected Setup Wizard

If your Wireless Clients support the WPS connection method, this Wi-Fi Protected Setup Wizard can be used to initiate a wireless connection between this device and Wireless clients with a simple click of the WPS button. The Wi-Fi Protected Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to connect wireless clients to this router using the WPS method.



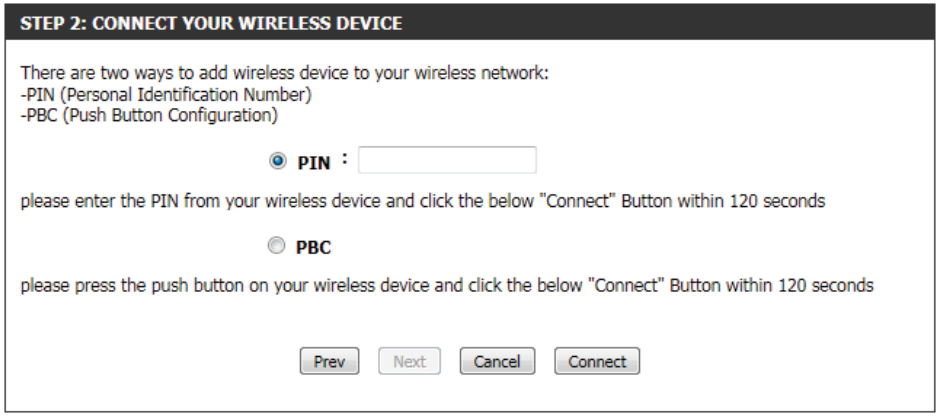
To initiate the Wi-Fi Protected Setup Wizard click on the **Add Wireless Device with WPS** button.

Step 1: In this step the user have two options to choose from. You can choose **Auto** if the wireless client supports WPS, or **Manual** if the wireless client does not support WPS.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

Step 2: After selecting Auto, the following page will appear. There are two ways to add a wireless device, that supports WPS. Firstly, there is the Personal Identification Number (**PIN**) method. Using this method will prompt the user to enter a PIN code. This PIN code should be identical on the wireless client. Secondly, there is the Push Button Configuration (**PBC**) method. Using this method will allow the wireless client to connect to this device by similarly pressing the PBC button on it.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

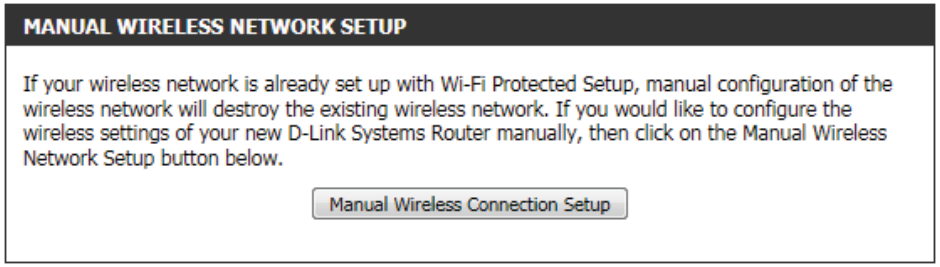


Step 2: After selecting Manual, the following page will appear. On this page to user can view the wireless configuration of this router. The wireless clients should configure their wireless settings to be identical to the settings displayed on this page for a successful connection. This option is for wireless clients that can't use the WPS method to connect to this device.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page. Click on the **Wireless Status** button to navigate to the Status > Wireless page to view what wireless client are connected to this device.

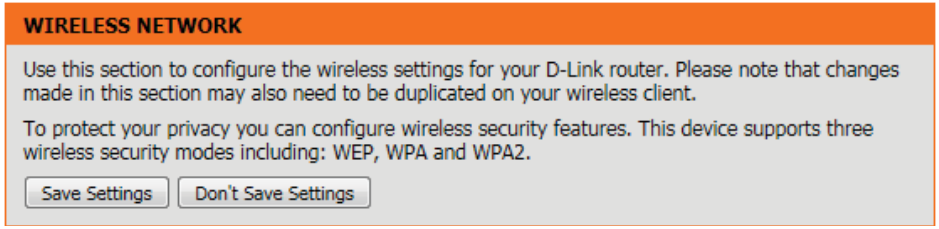
Wireless Settings: Manual Wireless Network Setup

The manual wireless network setup option allows users to configure the wireless settings of this device manually. This option is for the more advanced user and includes all parameters that can be configured for wireless connectivity.

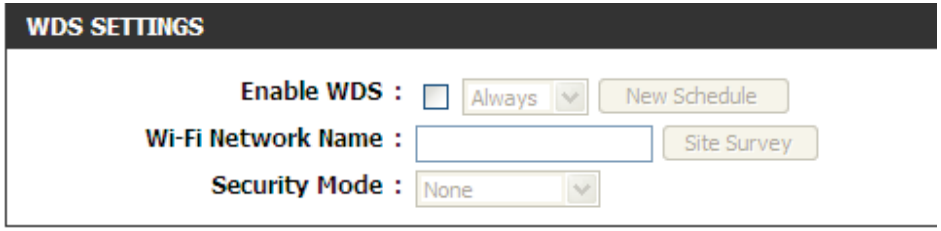


To initiate the Manual Wireless Setup page, click on the **Manual Wireless Connection Setup** button.

On this page the user can configure all the parameters related to the wireless connectivity of this router.



The following parameters will be available for wireless distribution system (WDS) configuration:

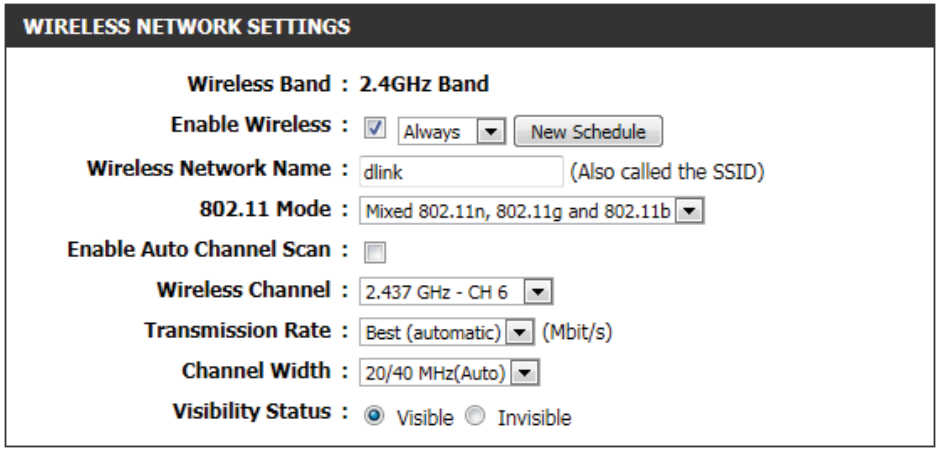


Enable WDS: Check the box to enable the WDS function. If you do not want to use WDS, uncheck the box to disable the service. Select the time frame that you would like your WDS enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click **New Schedule** to create a new schedule.

Wi-Fi Network Name: The Service Set Identifier (SSID) is the name of your wireless network. Click **Site Survey** to select an existing SSID or create a name using up to 32 characters. The SSID is case-sensitive.

Security Mode: Select either WEP or WPA-Personal for security encryption.

The following parameters will be available for configuration:



Wireless Band: Displays the wireless band being configured. In this option we find that the following parameters will be regarding the 2.4GHz band.

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click New Schedule to create a new schedule.

Wireless Network Name: The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.

802.11 Mode: Here the user can manually select the preferred frequency band to use for this wireless network.

Enable Auto Channel Scan: The auto channel selection setting can be selected to allow this device to choose the channel with the least amount of interference.

Wireless Channel: By default the channel is set to 1. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.

Transmission Rate: Select the transmit rate. It is strongly suggested to select Best (Automatic) for best performance.

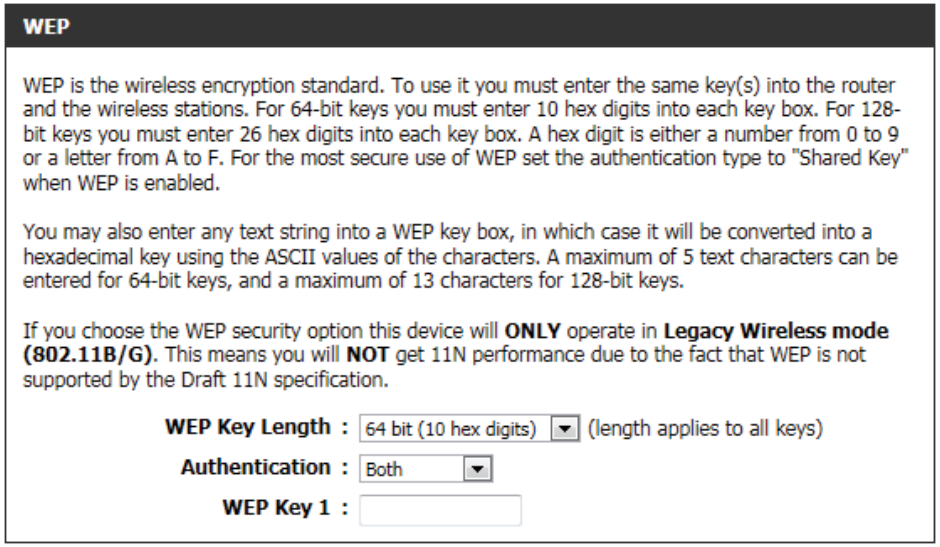
Channel Width: When using the 802.11n frequency band, the user have an option to choose between a 20MHz or 20/40MHz bandwidth.

Visibility Status: The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcasted to anyone within the range of your signal. If you are not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

By default the wireless security of this router will be disabled. In this next option the user can enabled or disable wireless security for the frequency band 2.4GHz. There are two types of encryption that can be used- WEP or WPA/WPA2.

Wireless Security Mode: WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. Even though it is known as a 'weak' security method, it is better than no security at all. Older wireless adapter sometimes only supports WEP encryption and thus we still find this encryption method used today.



WEP Key Length: Here the user can specify to either use a 64Bit or a 128Bit encrypted key.

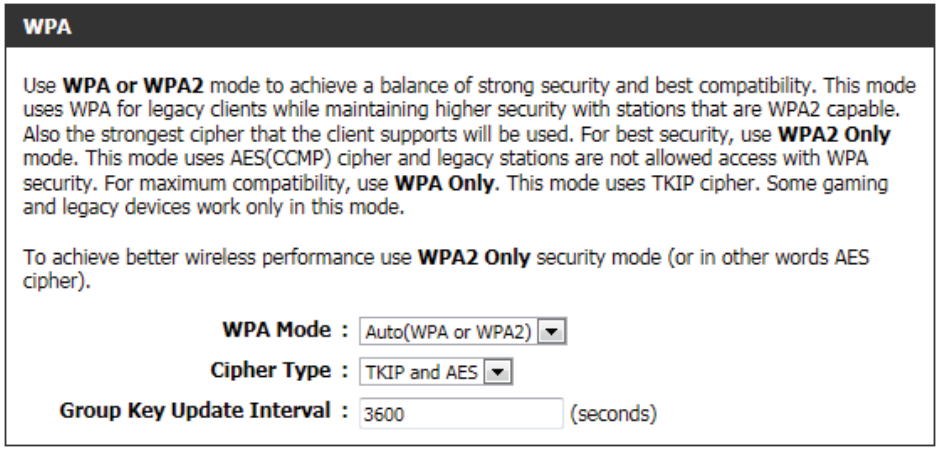
Authentication: Authentication is a process by which the router verifies the identity of a network device that is attempting to join the wireless network. There are two types authentication for this device when using WEP. **Open System** allows all wireless devices to communicate with the router before they are required to provide the encryption key needed to gain access to the network. **Shared Key** requires any wireless device attempting to communicate with the router to provide the encryption key needed to access the network before they are allowed to communicate with the router.

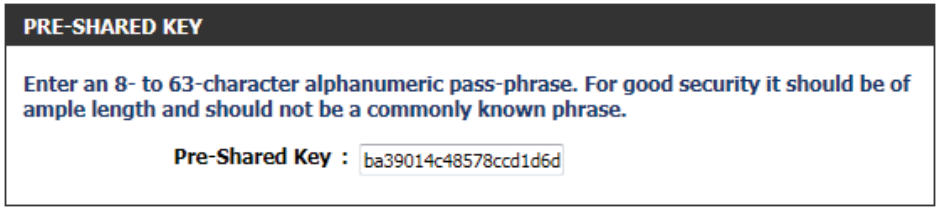
WEP Key 1: Enter the WEP key used here. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.

Wireless Security Mode: WPA-Personal

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a pass-phrase (Shared Secret) for security.

The following parameters will be available for configuration:





WPA Mode: WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (**TKIP**), Advanced Encryption Standard (**AES**), and Both (**TKIP and AES**).

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Pre-Shared Key: Enter the shared secret used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

Wireless Security Mode: WPA-Enterprise

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a pass-phrase (Shared Secret) for security.

WPA Mode: WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

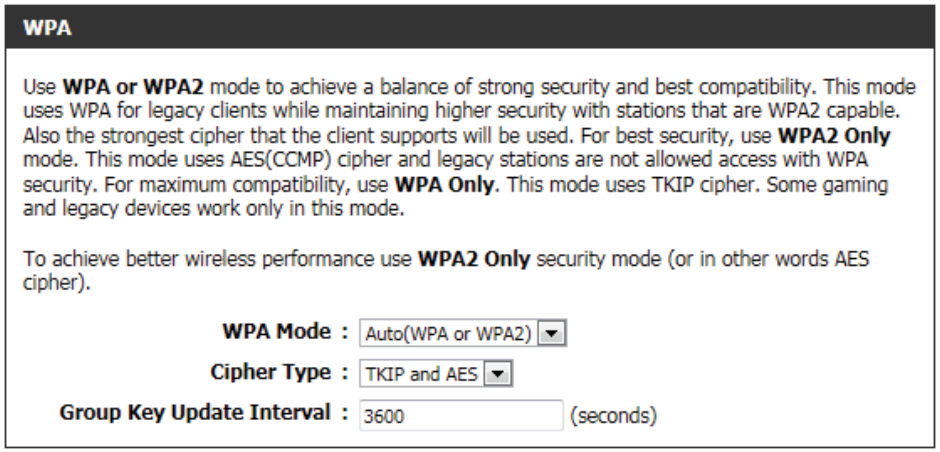
Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (**TKIP**), Advanced Encryption Standard (**AES**), and Both (**TKIP and AES**).

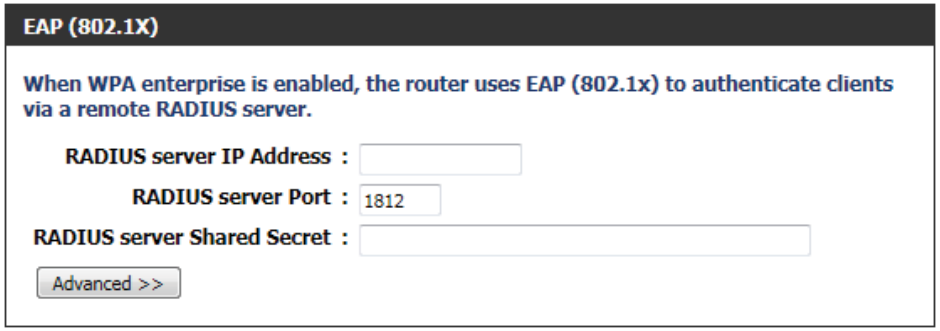
Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

RADIUS Server IP Address: When the user chooses to use the EAP authentication framework, the RADIUS server's IP address can be entered here.

RADIUS Server Port: When the user chooses to use the EAP authentication framework, the RADIUS server's port number can be entered here.

RADIUS Server Shared Secret: Enter the shared secret used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.





Network Settings

On this page the user can configure the internal network settings of the router and also able to configure the built-in DHCP server to assign IP addresses to computers on the network. The IP address that is configured here is the IP address that is used to access the Web-based management interface. If you change the IP address in this section, you may need to adjust your PC's network settings to access the network again.

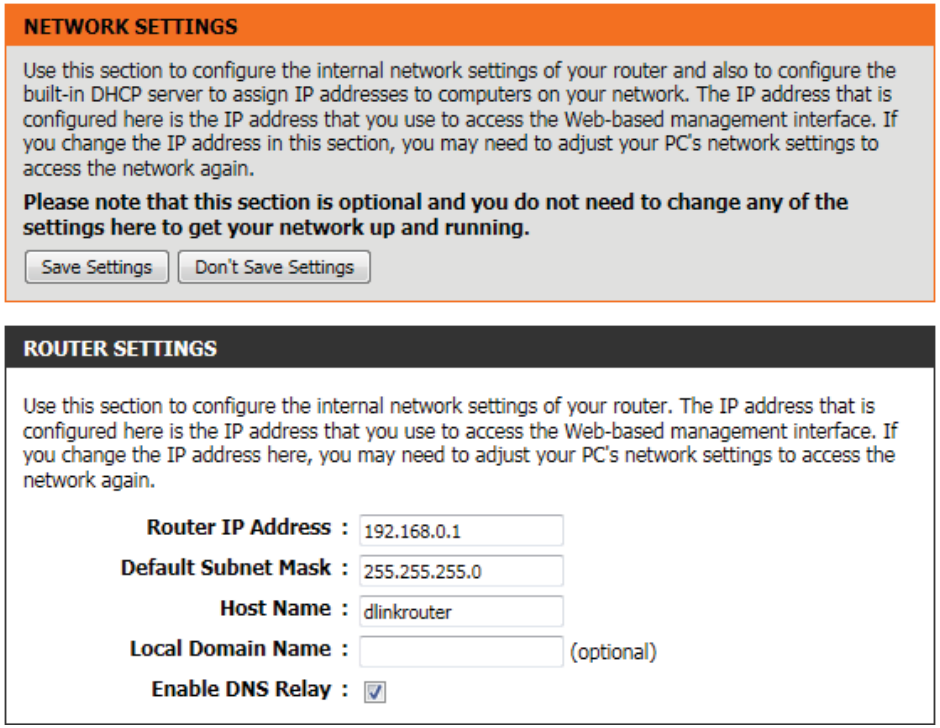
Router IP Address: Enter the IP address of the router. The default IP address is 192.168.0.1. If you change the IP address, once you click Apply, you will need to enter the new IP address in your browser to get back into the configuration utility.

Default Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

Host Name: Enter a Host Name to identify this device.

Local Domain Name: Enter the local domain name used here. (Optional).

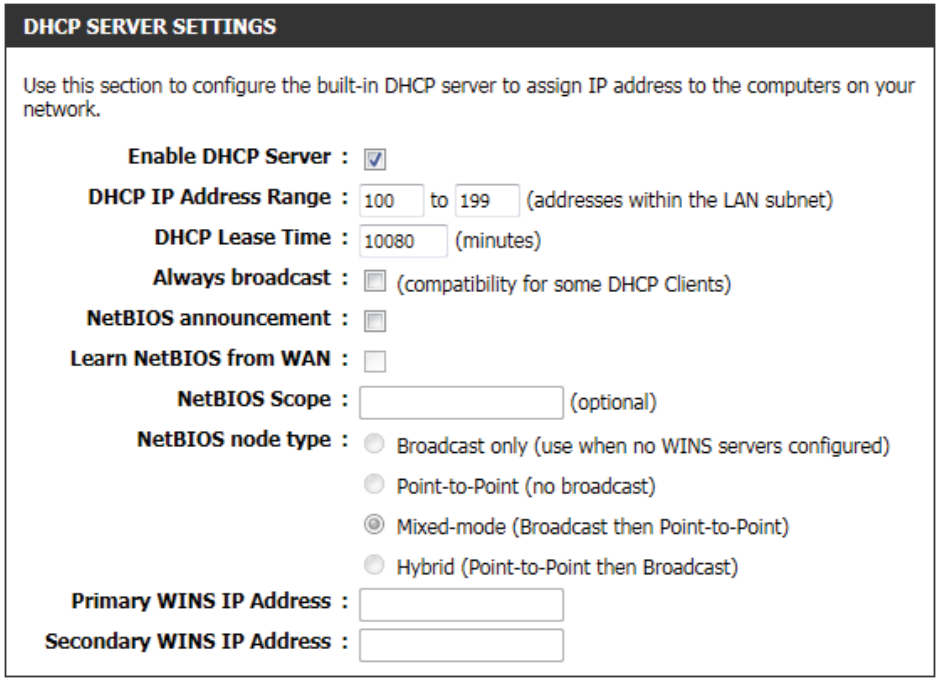
Enable DNS Relay: Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.



DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. This device has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the router. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

The following parameters will be available for configuration:



Enable DHCP Server: Check this box to enable the DHCP server on your router. Uncheck to disable this function.

DHCP IP Address Range: Enter the starting and ending IP addresses for the DHCP server's IP assignment.

DHCP Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

Always Broadcast: If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

NetBIOS announcement: Check this box to allow the DHCP Server to offer NetBIOS configuration settings to the LAN hosts. NetBIOS allow LAN hosts to discover all other computers within the network, e.g. within Network Neighborhood.

Learn NetBIOS from WAN: If NetBIOS announcement is switched on, it will cause WINS information to be learned from the WAN side, if available. Turn this setting off to configure manually.

NetBIOS Scope: This is an advanced setting and is normally left blank. This allows the configuration of a NetBIOS 'domain' name under which network hosts operate. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

NetBIOS node type: This field indicates how network hosts are to perform NetBIOS name registration and discovery. H-Node, this indicates a Hybrid-State of operation. First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers. M-Node (default), this indicates a Mixed-Mode of operation. First Broadcast operation is performed to register hosts and discover other hosts, if broadcast operation fails, WINS servers are tried, if any. This mode favours broadcast operation which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN. P-Node, this indicates to use WINS servers ONLY. This setting is useful to force all NetBIOS operation to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server. B-Node, this indicates to use local network broadcast ONLY. This setting is useful where there are no WINS servers available, however, it is preferred you try M-Node operation first. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

Primary WINS Server IP address: Configure the IP address of the preferred WINS server. WINS Servers store information regarding network hosts, allowing hosts to 'register' themselves as well as discover other available hosts, e.g. for use in Network Neighborhood. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

Secondary WINS Server IP address: Configure the IP address of the backup WINS server, if any. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

Add/Edit DHCP Reservation

This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the D-Link router. The D-Link router will provide the device the same IP address every time. DHCP Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option.

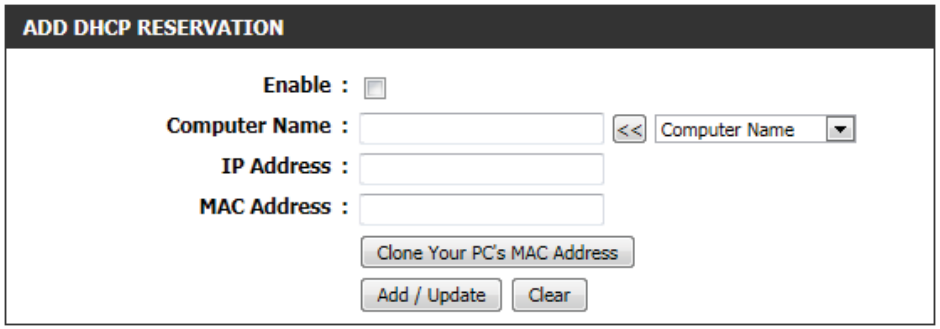
The following parameters will be available for configuration:

Enable: Check this box to enable the reservation.

Computer Name: Enter the computer name. Alternatively, select a computer that currently has a DHCP lease from the drop down menu and click << to automatically populate the Computer Name, IP Address, and MAC Address fields.

IP Address: Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.

MAC Address: Enter the MAC address of the computer or device.



DHCP Reservations List

This shows clients that you have specified to have reserved DHCP addresses. An entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the 'Edit DHCP Reservation' section is activated for editing.

Number of Dynamic DHCP Clients

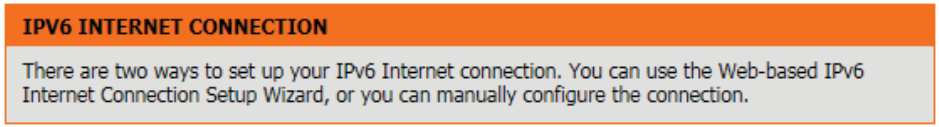
In this section you can see what LAN devices are currently leasing IP addresses.

IPv6

On this page, the user can configure the IPv6 Connection type. There are two ways to set up the IPv6 Internet connection. You can use the Web-based IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.

IPv6 Internet Connection Setup Wizard

For the beginner user that have not configured a router before, click on the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running.

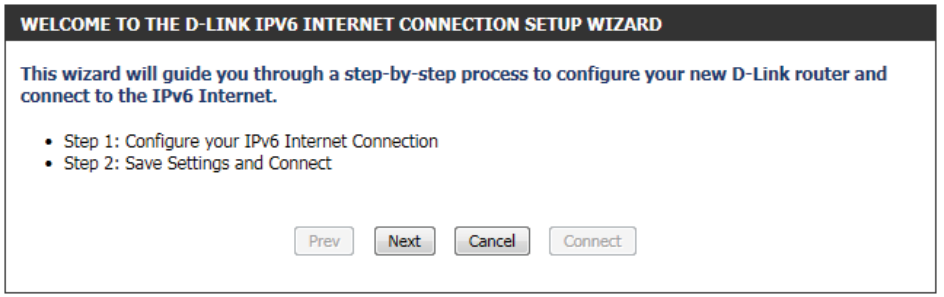


After clicking on the IPv6 Internet Connection Setup Wizard button, this page will appear.

Welcome to the D-Link IPv6 Internet Connection Setup Wizard

This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the IPv6 Internet.

Click **Next** to continue to the next page. Click **Cancel** to discard the changes made and return to the main page.



Step 1: Configure Your IPv6 Internet Connection

The router will try and detect whether its possible to obtain the IPv6 Internet Connection type automatically. If this succeeds then the user will be guided through the input of the appropriate parameters for the connection type found.

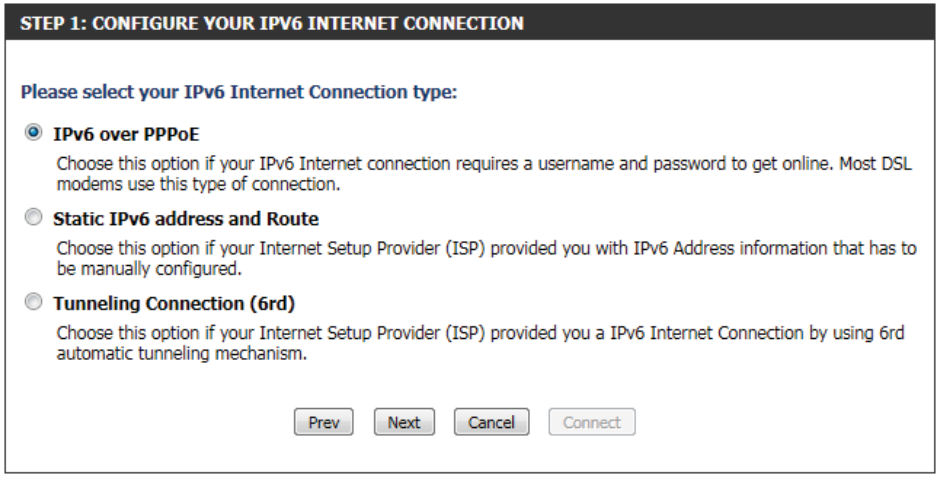
However, if the automatic detection fails, the user will be prompt to either **Try again** or to click on the **Guide me through the IPv6 settings** button to initiate the manual continual of the wizard.

Step 1: Configure Your IPv6 Internet Connection

There are several connection types to choose from. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled. The 3 options available on this page is **IPv6 over PPPoE**, **Static IPv6 address and Route**, and **Tunneling Connection**.

Choose the required IPv6 Internet Connection type and click on the **Next** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.



Set Username and Password Connection (PPPoE)

After selecting the IPv6 over PPPoE option, the user will be able to configure the IPv6 Internet connection that requires a username and password to get online. Most DSL modems use this type of connection.

The following parameters will be available for configuration:

PPPoE Session: Select the PPPoE Session value used here. This option will state that this connection shares it's information with the already configured IPv6 PPPoE connection, or the user can create a new PPPoE connection here.

User Name: Enter the PPPoE username used here. This information is obtainable from the ISP.

Password: Enter the PPPoE password used here. This information is obtainable from the ISP.

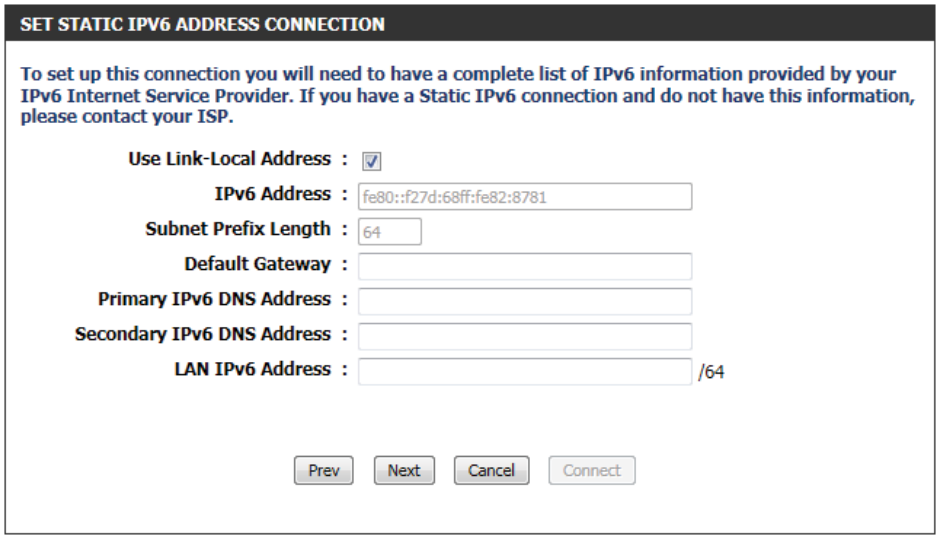
Verify Password: Re-enter the PPPoE password used here.

Service Name: Enter the service name for this connection here. This option is optional.

Click on the **Next** button to continue. Click on the **Prev** button to return to the previous page.
Click on the **Cancel** button to discard all the changes made and return to the main page.

Set Static IPv6 Address Connection

This mode is used when your ISP provides you with a set IPv6 addresses that does not change. The IPv6 information is manually entered in your IPv6 configuration settings. You must enter the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP provides you with all this information.



Use Link-Local Address: The Link-local address is used by nodes and routers when communicating with neighboring nodes on the same link. This mode enables IPv6-capable devices to communicate with each other on the LAN side.

IPv6 Address: Enter the WAN IPv6 address for the router here.

Subnet Prefix Length: Enter the WAN subnet prefix length value used here.

Default Gateway Enter the WAN default gateway IPv6 address used here.

Primary IPv6 DNS Address: Enter the WAN primary DNS Server address used here.

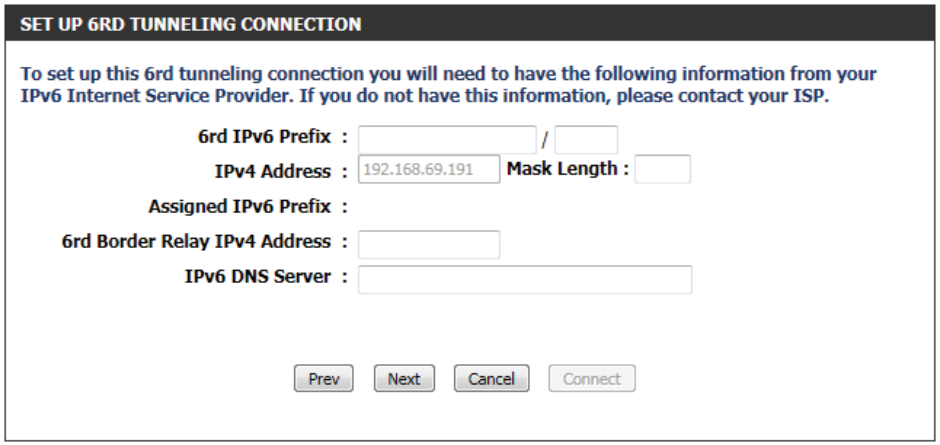
Secondary IPv6 DNS Address: Enter the WAN secondary DNS Server address used here.

LAN IPv6 Address: These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 Address and Subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)

Click on the **Next** button to continue. Click on the **Prev** button to return to the previous page.
Click on the **Cancel** button to discard all the changes made and return to the main page.

Tunneling Connection (6rd)

After selecting the Tunneling Connection (6rd) option, the user can configure the IPv6 6rd connection settings.



The following parameters will be available for configuration:

6rd IPv6 Prefix: Enter the 6rd IPv6 address and prefix value used here.

IPv4 Address: Enter the IPv4 address used here.

Mask Length: Enter the IPv4 mask length used here.

Assigned IPv6 Prefix: Displays the IPv6 assigned prefix value here.

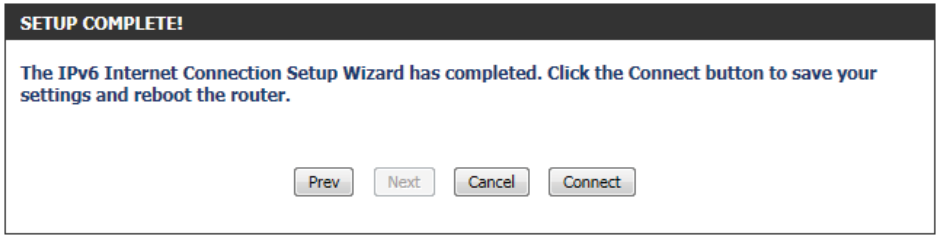
6rd Border Relay IPv4 Address: Enter the 6rd border relay IPv4 address used here.

IPv6 DNS Server: Enter the primary DNS Server address used here.

Click on the **Next** button to continue. Click on the **Prev** button to return to the previous page.
Click on the **Cancel** button to discard all the changes made and return to the main page.

Setup Complete

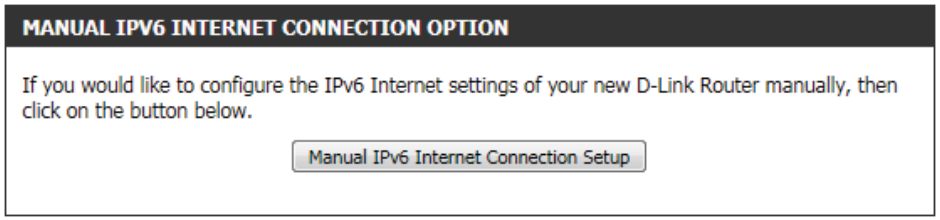
The IPv6 Internet Connection Setup Wizard was completed.



Click on the **Connect** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

Manual IPv6 Internet Connection Option

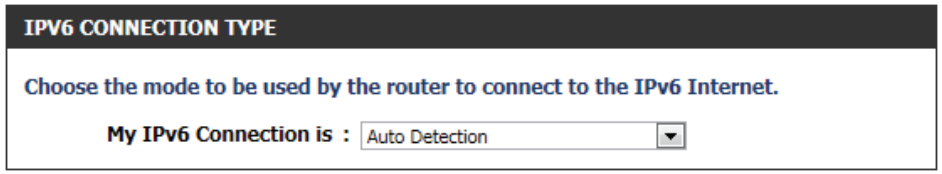
For the advanced user that have configured a router before, click on the **Manual IPv6 Internet Connection Setup** button to input all the settings manually.

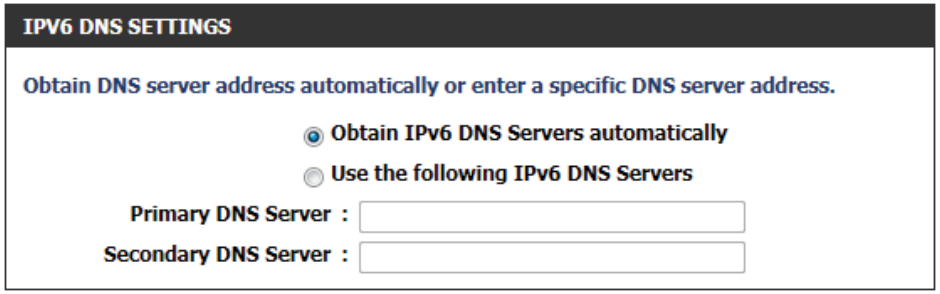


On this page the user can manually configure the mode that the Router will use to access an IPv6 Internet connection. There are several connection types to choose from: Link-local, Static IPv6, DHCPv6, Stateless Auto-Configuration, PPPoE, IPv6 over IPv4 Tunnel and 6to4. If you are unsure of your connection method, please contact your IPv6 ISP.

IPv6 Connection Type: Auto Detection

In the following section we'll discuss the parameters that can be configured when setting up an Auto Detection (Stateless/DHCPv6) connection. This is a method of connection where the ISP assigns your IPv6 address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the IPv6 Internet.





Obtain IPv6 DNS Server automatically: Select this option to obtain the DNS Server addresses automatically.

Use the following IPv6 DNS Servers: Select this option to manually enter the DNS Server addresses used.

Primary DNS: Enter the primary DNS Server address used here.

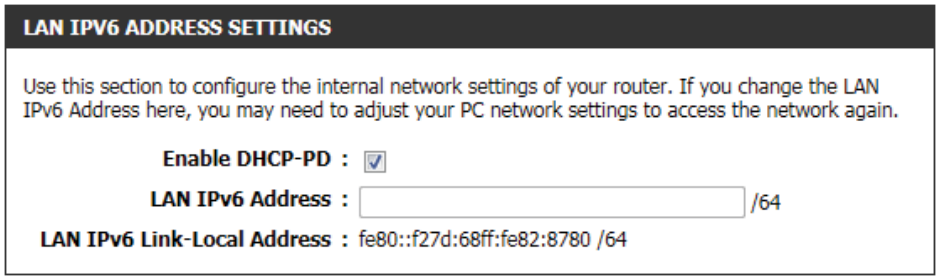
Secondary DNS: Enter the secondary DNS Server address used here.

Use the section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. DHCP-PD can be used to acquire a IPv6 prefix for the LAN interface.

Enable DHCP-PD: Select this option to enable DHCP PD.

LAN IPv6 Address: Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.

LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-Local address used here.



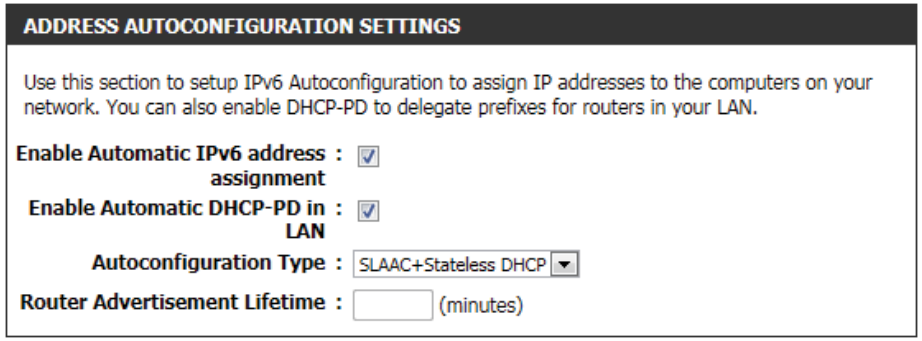
The following parameters will be available for configuration:

Enable Automatic IPv6 address: The user can tick this option to enable the auto-configuration feature.

Enable Automatic DHCP-PD in LAN: Autoconfiguration Tick this option to enable the automatic DHCP-PD on the LAN.

Autoconfiguration Type: The user can select the auto-configuration type used here.

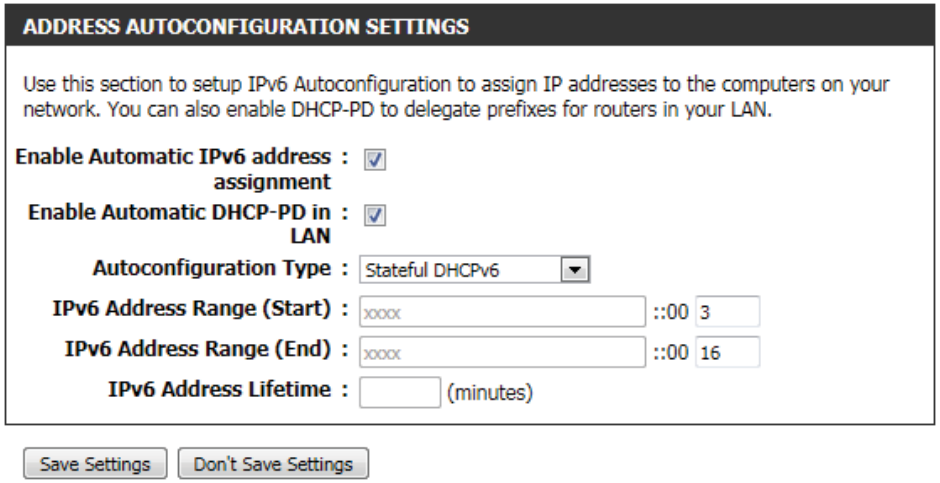
Router Advertisement Lifetime: This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.



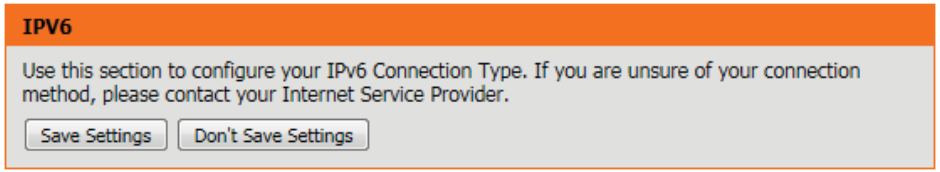
IPv6 Address Range (Start): This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range (End): This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).



Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



IPv6 Connection Type: Static IPv6

In the following section we'll discuss the parameters that can be configured when setting up an Static IPv6 connection. This mode is used when your ISP provides you with a set IPv6 addresses that does not change. The IPv6 information is manually entered in your IPv6 configuration settings. You must enter the **IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server,** and **Secondary DNS Server.** Your ISP provides you with all this information.

The following parameters will be available for configuration:

Use Link-Local Address: The Link-local address is used by nodes and routers when communicating with neighboring nodes on the same link. This mode enables IPv6-capable devices to communicate with each other on the LAN side.

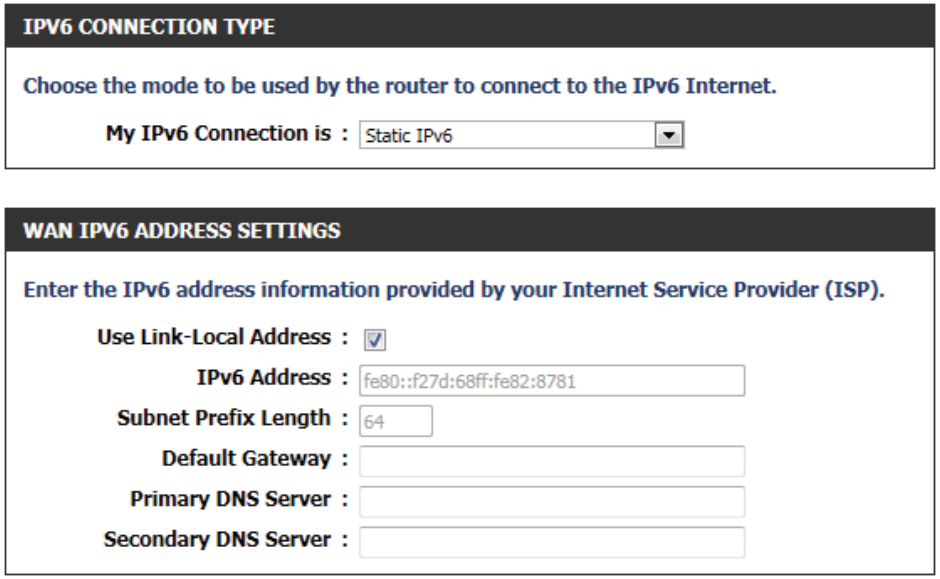
IPv6 Address: Enter the WAN IPv6 address for the router here.

Subnet Prefix Length:

Default Gateway: Enter the WAN default gateway IPv6 address used here.

Primary DNS Server: Enter the WAN primary DNS Server address used here.

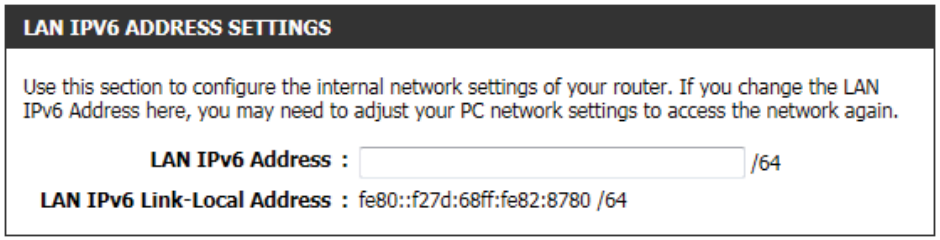
Secondary DNS Servers: Enter the WAN secondary DNS Server address used here.



The following parameters will be available for configuration:

LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router here.

LAN IPv6 Link-Local Address: Displays the Router's LAN Link-Local Address here.



The following parameters will be available for configuration:

Enable Automatic IPv6 address: The user can tick this option to enable the auto-configuration feature.

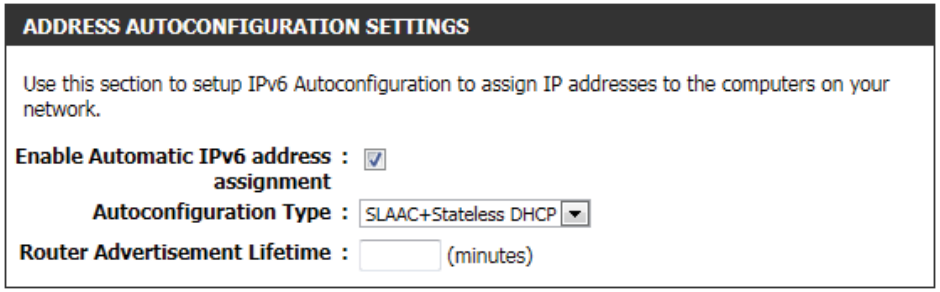
Autoconfiguration Type: The user can select the auto-configuration type used here.

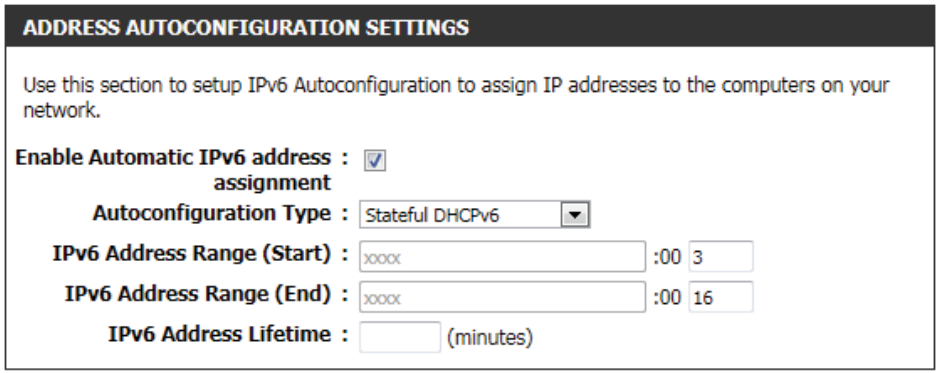
Router Advertisement Lifetime: This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.

IPv6 Address Range (Start): This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range (End): This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).





Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

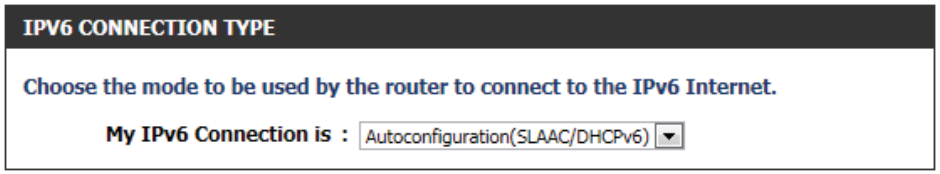
IPv6 Connection Type: Autoconfiguration (SLAAC/DHCPv6)

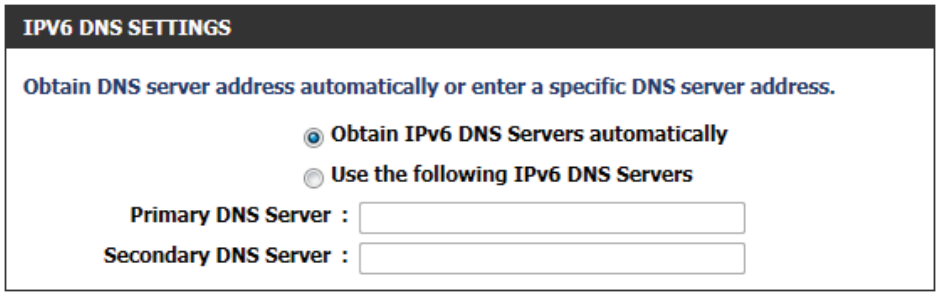
In the following section we'll discuss the parameters that can be configured when setting up an Autoconfiguration (SLAAC/DHCPv6) connection. This is a method of connection where the ISP assigns your IPv6 address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the IPv6 Internet.

The following parameters will be available for configuration:

Obtain IPv6 DNS Servers automatically: Select this option to obtain the DNS Server addresses automatically.

Use the following IPv6 DNS Servers: Select this option to manually enter the DNS Server addresses used.





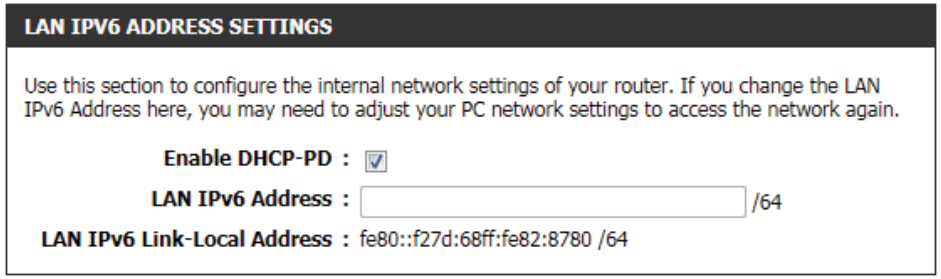
Primary DNS Server: Enter the WAN primary DNS Server address used here.

Secondary DNS Server: Enter the WAN secondary DNS Server address used here.

Enable DHCP-PD: Select this option to enable DHCP PD.

LAN IPv6 Address: Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.

LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-Local address used here.



The following parameters will be available for configuration:

Enable Automatic IPv6 address: The user can tick this option to enable the auto-configuration feature.

Enable Automatic DHCP-PD in LAN: Tick this option to enable the automatic DHCP-PD on the LAN.

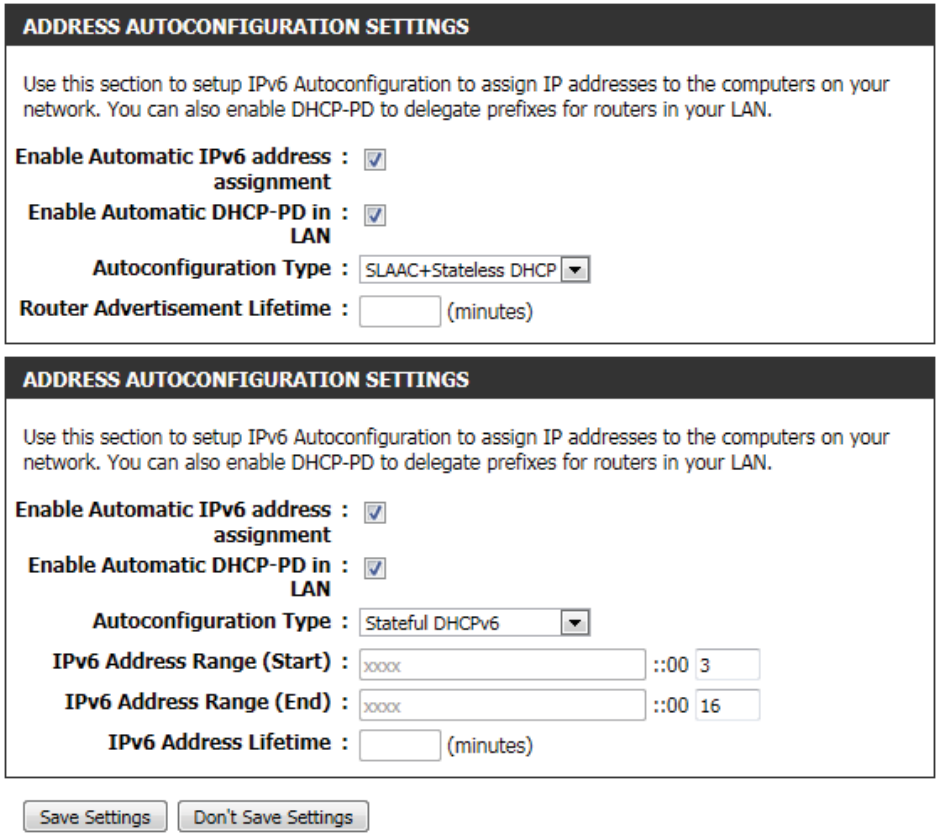
Autoconfiguration Type: The user can select the auto-configuration type used here.

Router Advertisement Lifetime: This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.

IPv6 Address Range (Start): This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range (End): This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address for the DHCPv6 range for your local computers.

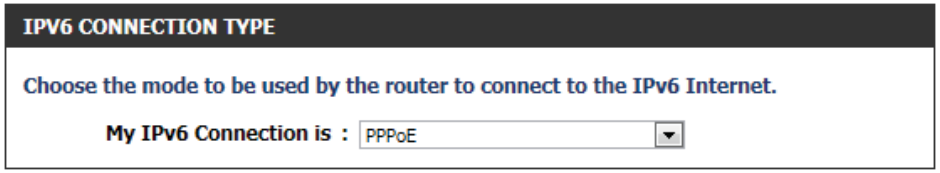
IPv6 Address Lifetime: This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).



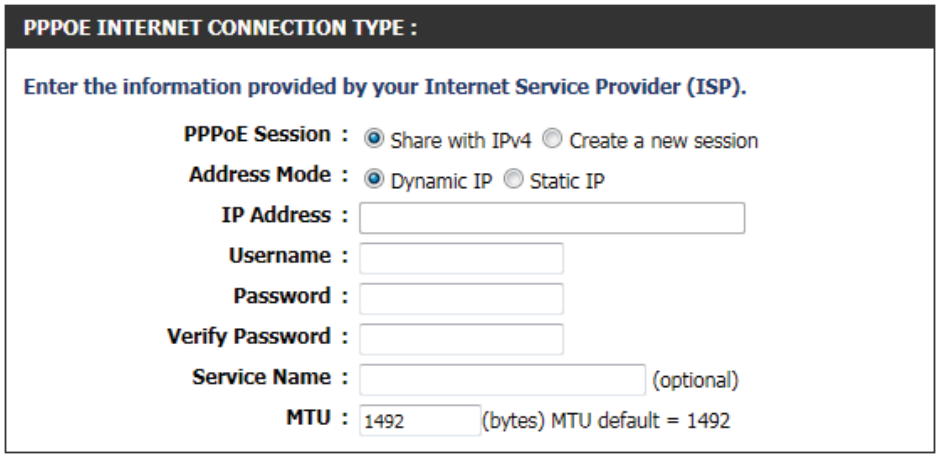
Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: PPPoE

Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection to IPv6 Internet. DSL providers typically use this option. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the IPv6 Internet. The supported authentication protocols are PAP and CHAP.



The following parameters will be available for configuration:



PPPoE Session: Select the PPPoE Session value used here. This option will state that this connection shares it's information with the already configured IPv6 PPPoE connection, or the user can create a new PPPoE connection here.

Address Mode: Select the appropriate address mode used here. Select **Dynamic IP** if the ISP's servers assign the router's WAN IPv6 address upon establishing a connection. If your ISP has assigned a fixed IPv6 address, select **Static IP**. The ISP provides the value for the IPv6 Address.

IP Address: Enter the ISP PPPoE IP address in here.

Username: Enter the PPPoE username used here. This information is obtainable from the ISP.

Password: Enter the PPPoE password used here. This information is obtainable from the ISP.

Verify Password: Re-enter the PPPoE password used here.

Service Name: Enter the service name for this connection here. This option is optional.

MTU: Enter the MTU value used here. The default value is 1492.

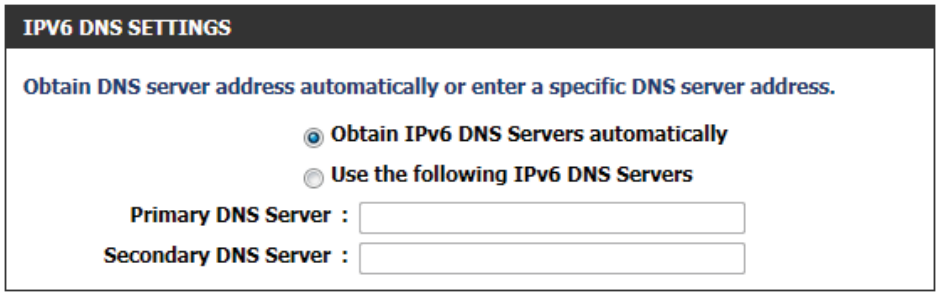
The following parameters will be available for configuration:

Obtain IPv6: Select this option to obtain the DNS Server addresses automatically.

Use IPv6: Select this option to manually enter the DNS Server addresses used.

Primary DNS: Enter the primary DNS Server address used here.

Secondary DNS: Enter the secondary DNS Server address used here.

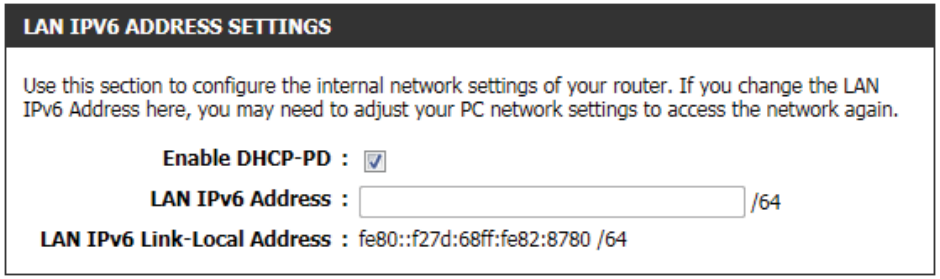


The following parameters will be available for configuration:

Enable DHCP-PD: Select this option to enable DHCP PD.

LAN IPv6 Address: Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.

LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-Local address used here.



The following parameters will be available for configuration:

Enable Automatic IPv6 address: The user can tick this option to enable the auto-configuration feature.

Enable Automatic DHCP-PD in LAN: Tick this option to enable the automatic DHCP-PD on the LAN.

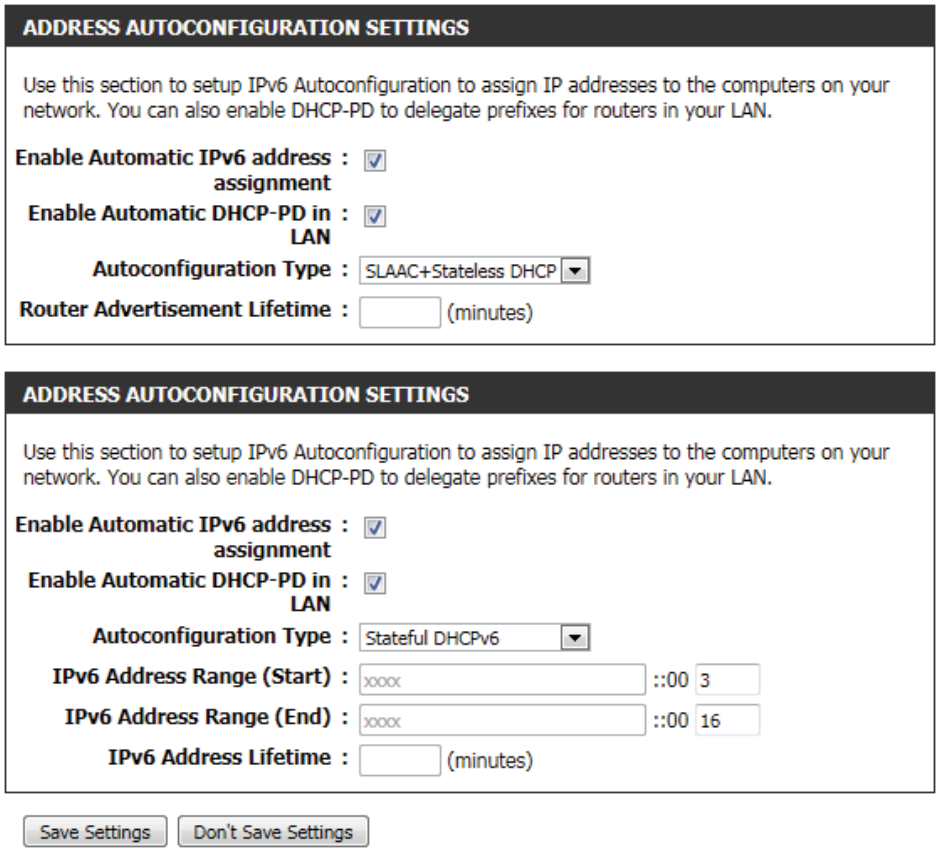
Autoconfiguration Type: The user can select the auto-configuration type used here.

Router Advertisement Lifetime: This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.

IPv6 Address Range (Start): This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range (End): This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address for the DHCPv6 range for your local computers.

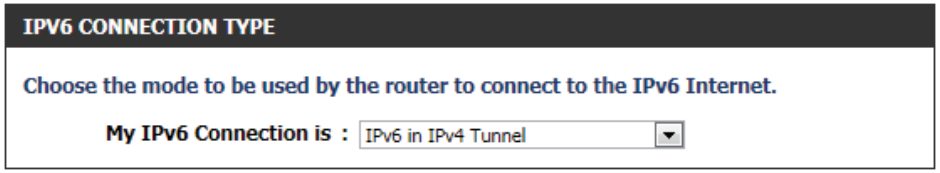
IPv6 Address Lifetime: This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).



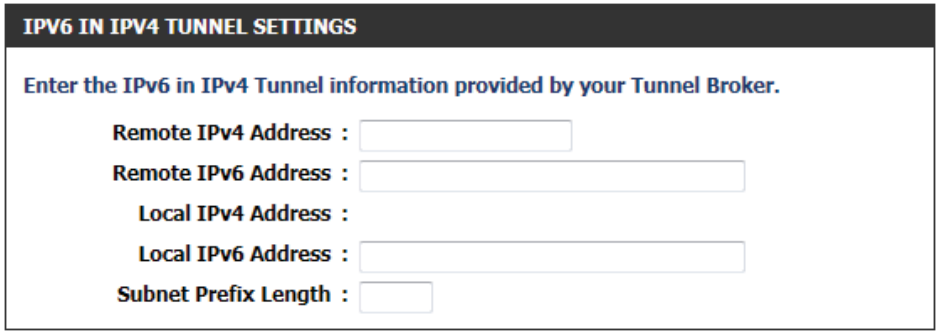
Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: IPv6 in IPv4 Tunnel

In section to the user can configure the IPv6 connection to run in IPv4 Tunnel mode. IPv6 over IPv4 tunneling encapsulates IPv6 packets in IPv4 packets so that IPv6 packets can be sent over an IPv4 infrastructure.



The following parameters will be available for configuration:



Remote IPv4 Address: Enter the remote IPv4 address used here.

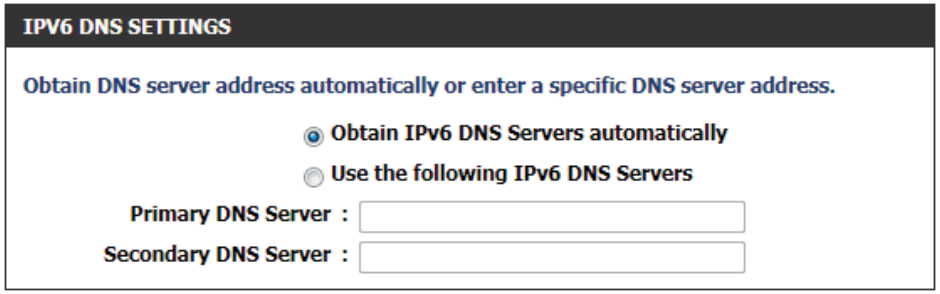
Remote IPv6 Address: Enter the remote IPv6 address used here.

Local IPv4 Address: Enter the local IPv4 address used here.

Local IPv6 Address: Enter the local IPv6 address used here.

Subnet Prefix Length: Enter the Subnet prefix length value used here.

The following parameters will be available for configuration:



Obtain IPv6 DNS Servers automatically: Select this option to obtain the DNS Server addresses automatically.

Use the following IPv6 DNS Servers: Select this option to manually enter the DNS Server addresses used.

Primary DNS Server: Enter the WAN primary DNS Server address used here.

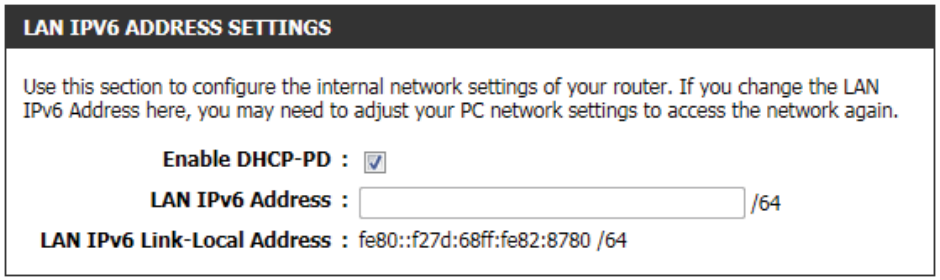
Secondary DNS Server: Enter the WAN secondary DNS Server address used here.

The following parameters will be available for configuration:

Enable DHCP-PD: Select this option to enable DHCP PD.

LAN IPv6 Address: Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.

LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-Local address used here.



The following parameters will be available for configuration:

Enable Automatic IPv6 address: The user can tick this option to enable the auto-configuration feature.

Enable Automatic DHCP-PD in LAN: Tick this option to enable the automatic DHCP-PD on the LAN.

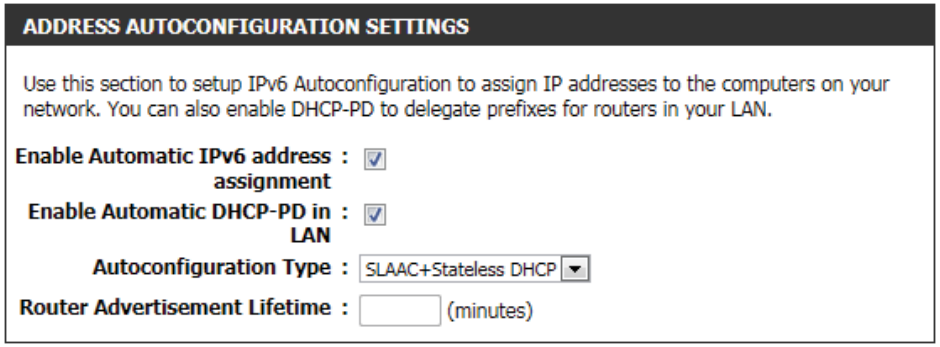
Autoconfiguration Type: The user can select the auto-configuration type used here.

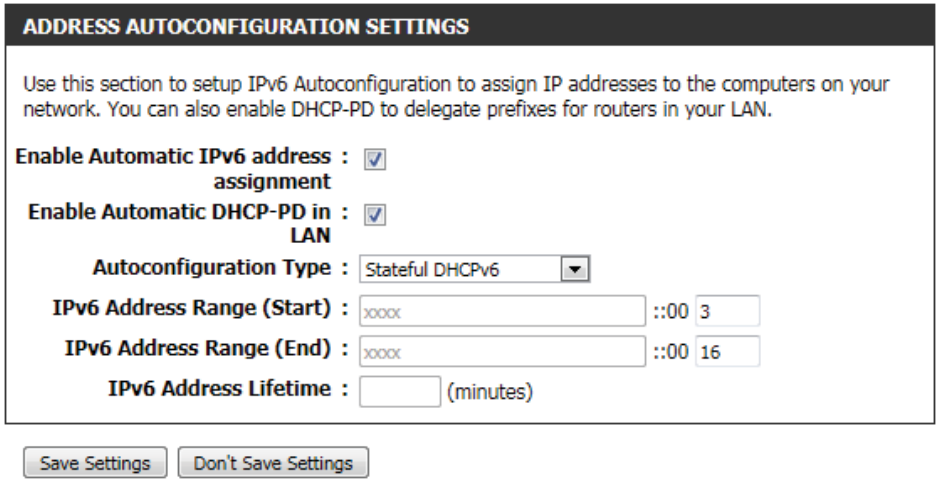
Router Advertisement Lifetime: This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.

IPv6 Address Range (Start): This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range (End): This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).

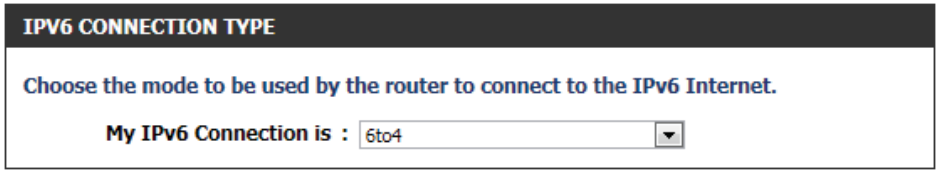




Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: 6to4

In this section the user can configure the IPv6 6to4 connection settings. 6to4 is an IPv6 address assignment and automatic tunneling technology that used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet.



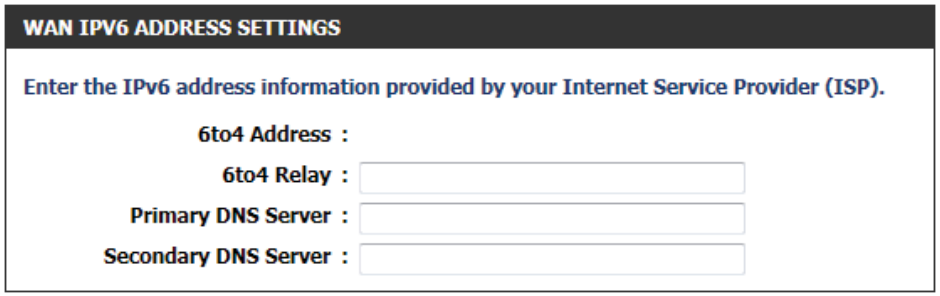
The following parameters will be available for configuration:

6to4 Address: Here the 6to4 configured address will be displayed.

6to4 Relay: Enter the 6to4 relay address used here.

Primary DNS Server: Enter the primary DNS Server address used here.

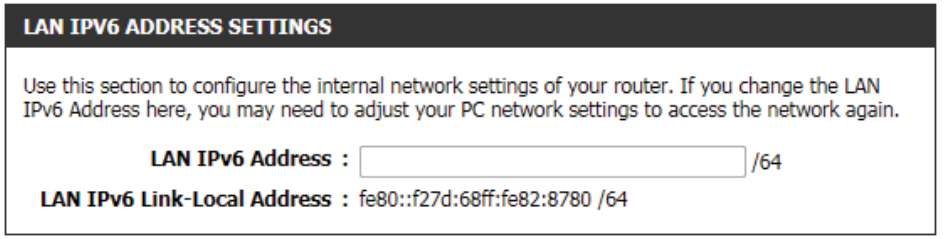
Secondary DNS Server: Enter the secondary DNS Server address used here.



The following parameters will be available for configuration:

LAN IPv6 Address: Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.

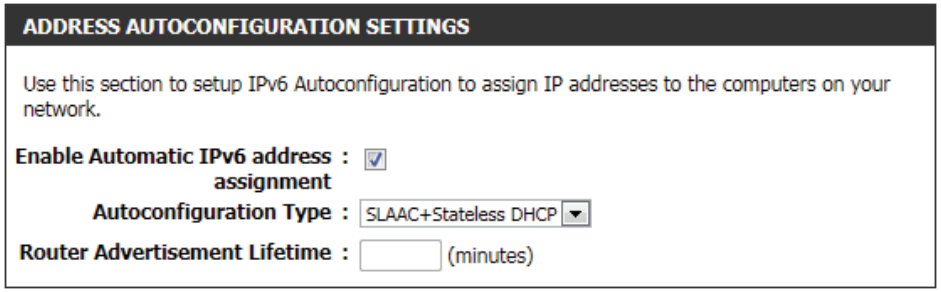
LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-Local address used here.



Enable Automatic IPv6 address The user can tick this option to enable the auto-configuration feature.

Autoconfiguration Type: The user can select the auto-configuration type used here.

Router Advertisement Lifetime: This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here



The following parameters will be available for configuration:

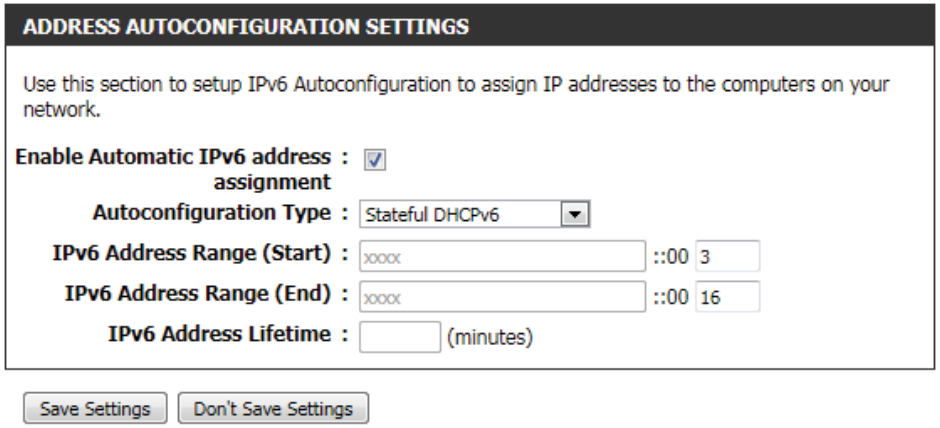
Enable Automatic IPv6 address: The user can tick this option to enable the auto-configuration feature.

Autoconfiguration Type: The user can select the auto-configuration type used here.

IPv6 Address Range (Start): This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range (End): This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address for the DHCPv6 range for your local computers.

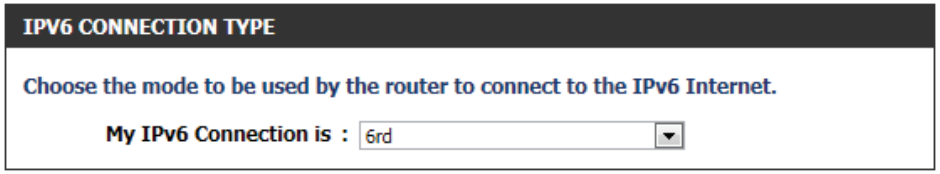
IPv6 Address Lifetime: This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).



Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

IPv6 Connection Type: 6rd

In this section the user can configure the IPv6 6rd connection settings.



The following parameters will be available for configuration:

6rd Configuration: Select the desired 6rd configuration option here.

6rd IPv6 Prefix: Enter the 6rd IPv6 address and prefix value used here.

IPv4 Address: Enter the IPv4 address used here.

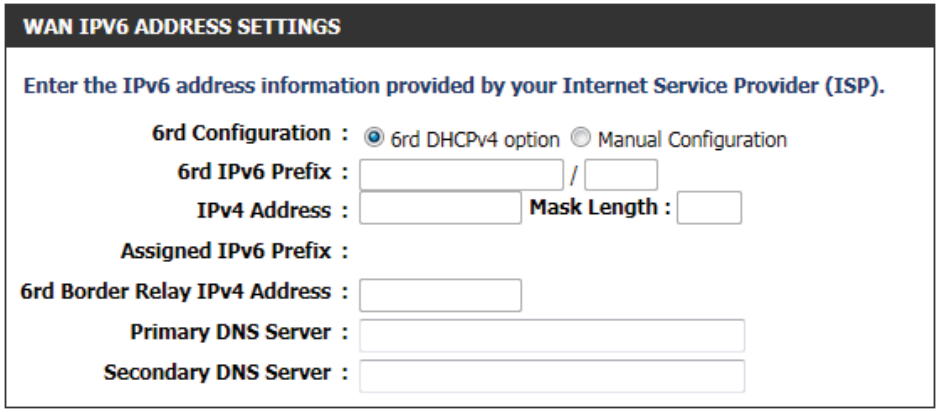
Mask Length: Enter the IPv4 mask length used here.

Assigned IPv6 Prefix: Displays the IPv6 assigned prefix value here.

6rd Border Relay IPv4 Address: Enter the 6rd border relay IPv4 address used here.

Primary DNS Server Enter the primary DNS Server address used here.

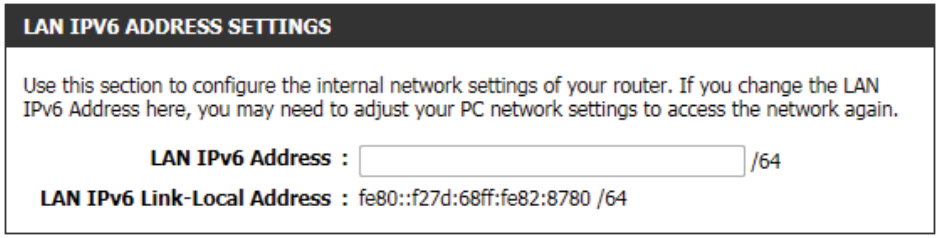
Secondary DNS Server: Enter the secondary DNS Server address uses here.



The following parameters will be available for configuration:

LAN IPv6 Address: Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.

LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-Local address used here.



The following parameters will be available for configuration:

Enable Automatic IPv6 address: The user can tick this option to enable the auto-configuration feature.

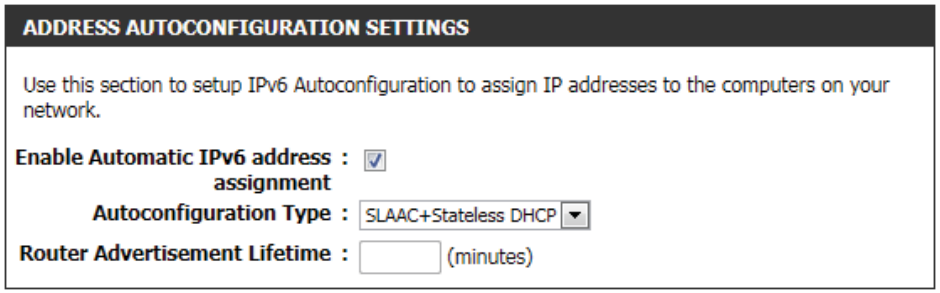
Autoconfiguration Type: The user can select the auto-configuration type used here.

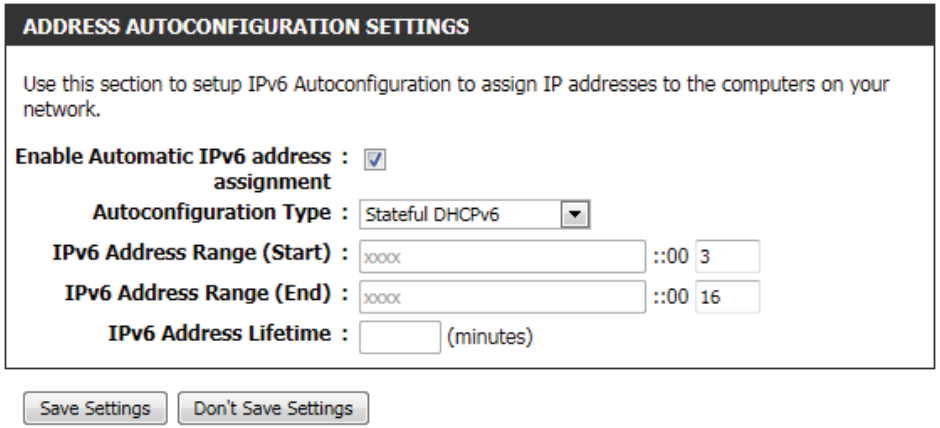
Router Advertisement Lifetime: This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.

IPv6 Address Range (Start): This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Range (End): This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).





Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

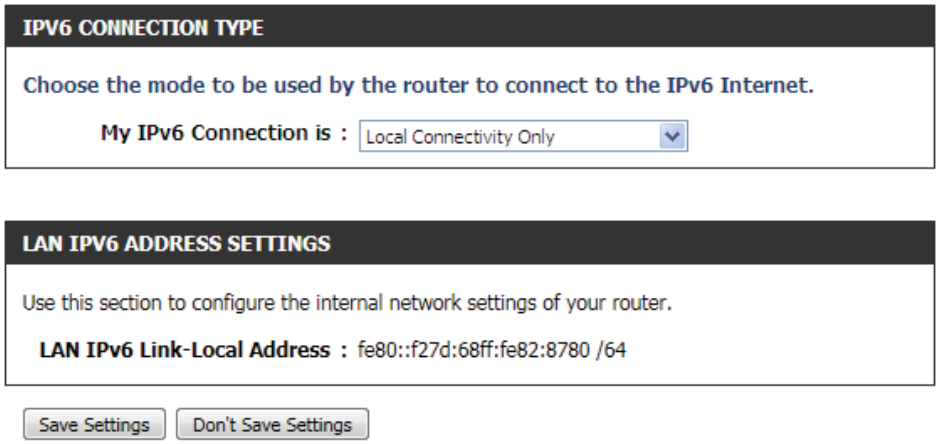
IPv6 Connection Type: Local Connection Only

The Link-local address is used by nodes and routers when communicating with neighboring nodes on the same link. This mode enables IPv6-capable devices to communicate with each other on the LAN side.

The following parameters will be available for configuration:

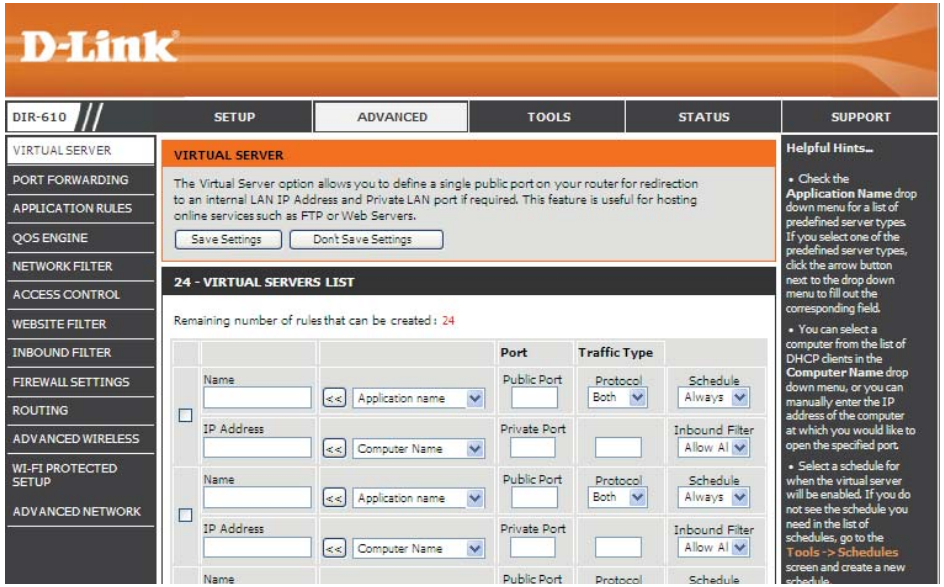
LAN IPv6 Link-Local Address: Displays the LAN IPv6 Link-Local address used here.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



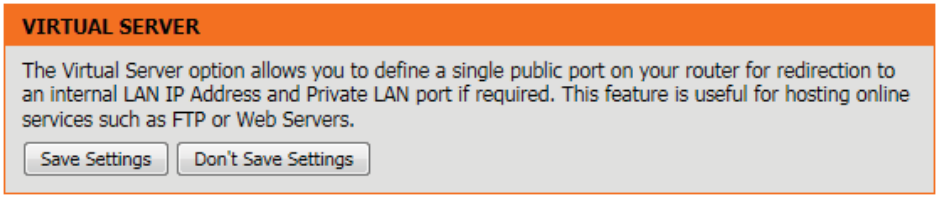
Advanced Category

This section allows the user to configure the more advanced features that can be done by this router. Features like **Port Forwarding, Firewall settings, Quality of Service** settings and more.

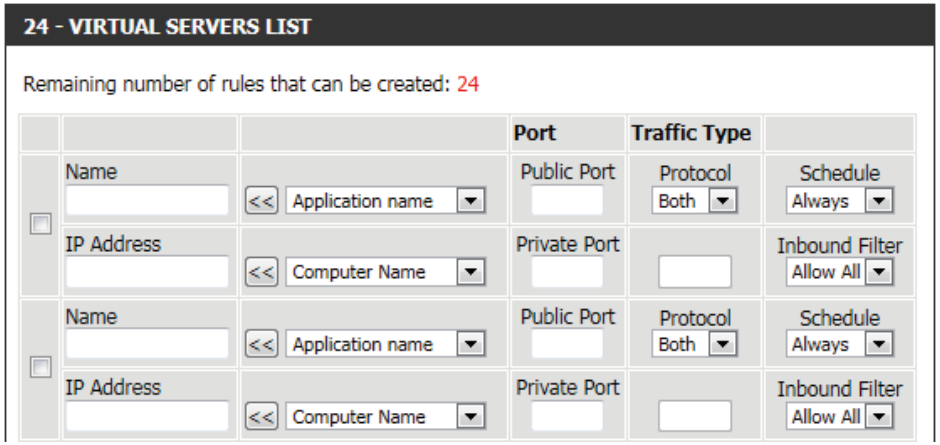


Virtual Server

This router can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network). The router's firewall feature filters out unrecognized packets to protect the LAN network so all computers networked with the router are invisible to the outside world. The user can make some of the LAN computers accessible from the Internet by enabling Virtual Server.



Depending on the requested service, the router redirects the external service request to the appropriate server within the LAN network. The router is also capable of port-redirection, meaning that incoming traffic to a particular port may be redirected to a different port on the server computer.



Checkbox: Check the box on the left side to enable the Virtual Server rule.

Name: Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the Computer Name drop-down menu. Select your computer and click <<.

Port: Enter the port that you want to open next to Public Port and Private Port. The public and private ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.

Traffic Type: Select TCP, UDP, or All from the Protocol drop-down menu.

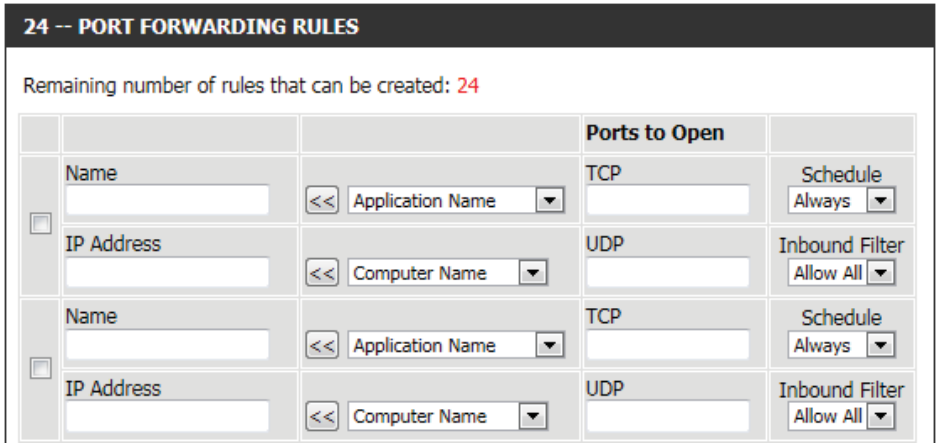
Schedule: Use the drop-down menu to schedule the time that the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

Port Forwarding

The Port Forwarding option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web or game servers. For each entry, you define a public port on your router for redirection to an internal LAN IP Address and LAN port. This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in the format, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689). This option is only applicable to the INTERNET session.

The following parameters will be available for configuration:



Checkbox: Tick the checkbox on the left side to enable the Port Forwarding rule.

Name: Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

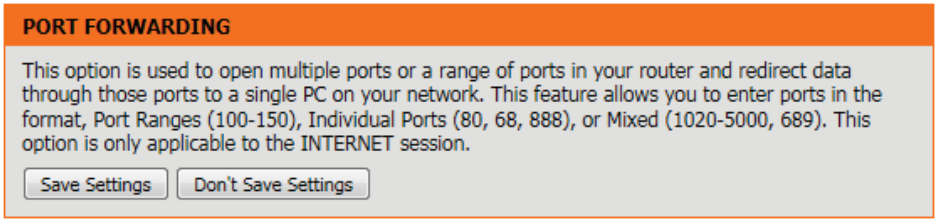
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the Computer Name drop-down menu. Select your computer and click <<.

Ports to Open: Enter the external port number in the appropriate space provided. If the port number is TCP then enter the number in the TCP space, and if the port number is UDP than enter it in the UDP space.

Schedule: Use the drop-down menu to schedule the time that the Port Forwarding rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.

Inbound Filter: Select the inbound filter rule here. Options to choose from are Allow All, Deny All, and any other custom rule created.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the router. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The following parameters will be available for configuration:

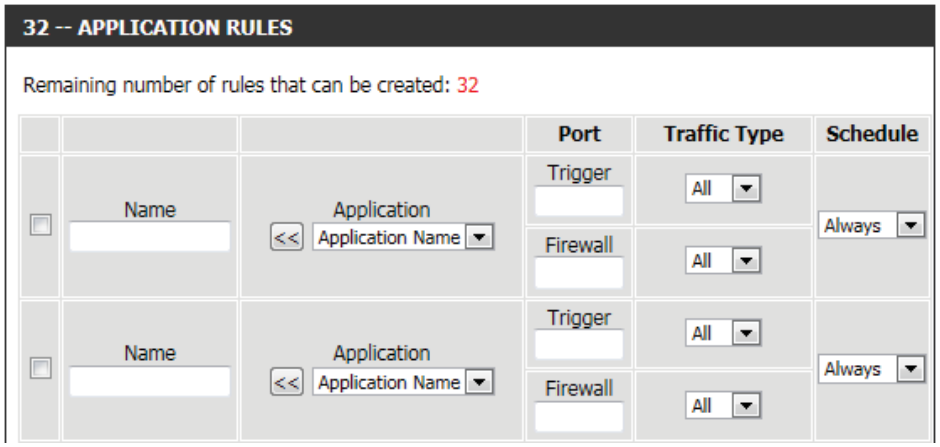
Checkbox: Check the box on the left side to enable the Application Rule.

Name: Enter a name for the rule. You may select a predefined application from the Application drop-down menu and click <<.

Application: Displays a list of predefined application to use in the rules.

Port (Trigger): This is the port used to trigger the application. It can be either a single port or a range of ports.

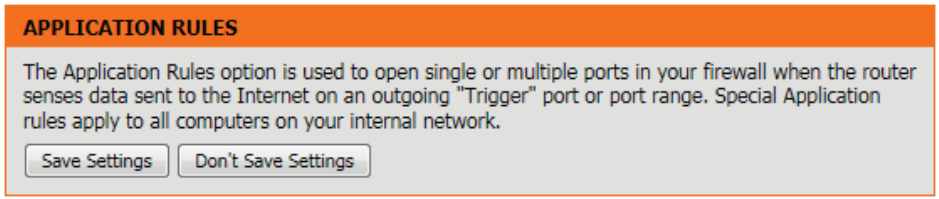
Port (Firewall): This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.



Traffic Type: Select the protocol of the firewall port (TCP, UDP, or All).

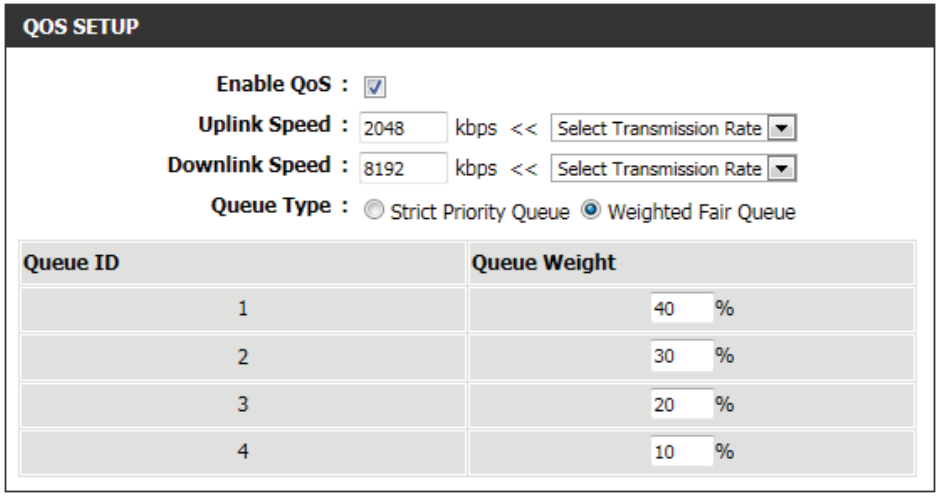
Schedule: The schedule of time when the Application Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



QoS Engine

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically. The QoS section contains a queuing mechanism, traffic shaping and classification. It supports two kinds of queuing mechanisms. Strict Priority Queue (SPQ) and Weighted Fair Queue (WFQ). SPQ will process traffic based on traffic priority. Queue1 has the highest priority and Queue4 has the lowest priority. WFQ will process traffic based on the queue weight. Users can configure each queue's weight. The sum of all the queue's weight must be 100. When surfing the Internet, the system will do traffic shaping based on the uplink and downlink speed. The classification rules can be used to classify traffic to different queues, then SPQ or WFQ will do QoS based on the queue's priority or weight.



Enable QoS: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

Uplink Speed: The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.

Downlink Speed: The speed at which data can be transferred from the ISP to the router. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5Mbits/284Kbits.

Using this example, you would enter 1500. Alternatively you can test your downlink speed with a service such as www.dslreports.com.

Queue Type: Here the user can specify the queue type used. When choosing the option Strict Priority Queue, the router will apply QoS based on the internal specification for the queue ID's listed. When choosing the option Weight Fair Queue, the router will apply QoS based on the user defined percentage in the Queue Weight column.

Queue ID: In this column the Queue ID used will be displayed.

Queue Priority: In this column the Queue Priority used will be displayed.

Queue Weight: After choosing to use the Weight Fair Queue option, under Queue Type, the user will be able to manual enter the Queue Weight for each individual Queue ID.

After specifying the QoS framework used, in the QoS setup section, the user can now create individual rules for scenarios that require the use of traffic control and data priority manipulation.

The following parameters will be available for configuration:

Checkbox: Tick this option to enable the rule specified.

Name: Enter a custom name for the rule being created here. This name is used for identification.

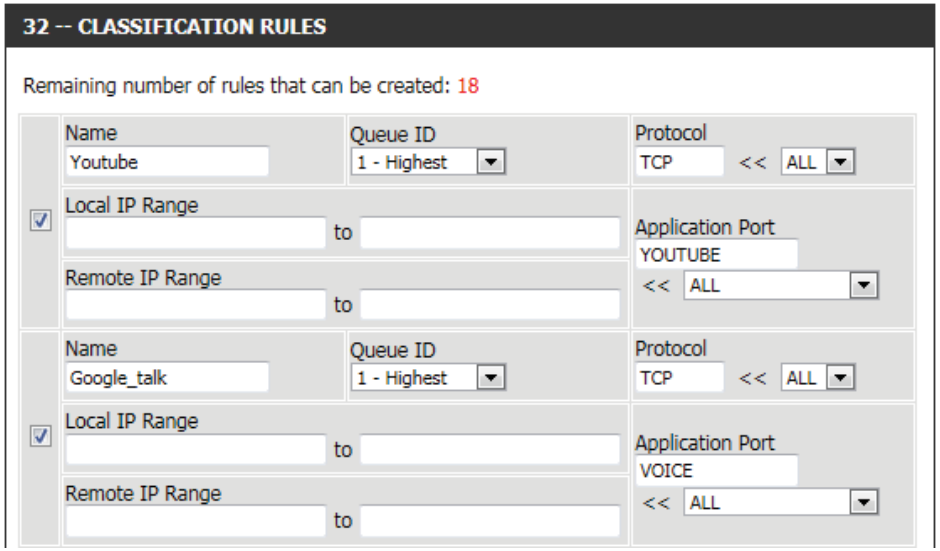
Queue ID: Select the appropriate priority requirement from the drop-down menu that will be applied to this rule. Option to choose from are Highest, Higher, Normal, and Best Effort.

Protocol: Select the protocol used for the application for in the drop-down menu and it will automatically place it in the Protocol field.

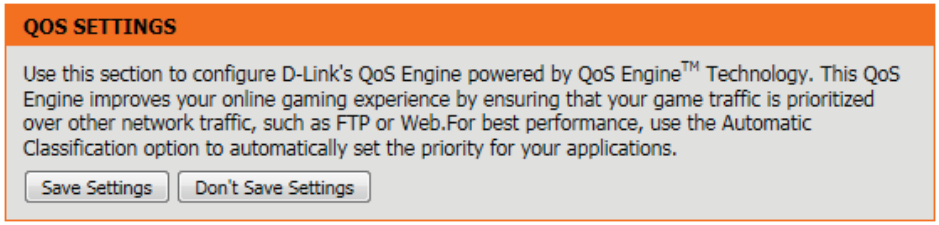
Local IP Range: Enter the local IP range used here. This is the IP range of you Local Area Network. The Router's IP cannot be included in this range.

Remote IP Range: Enter the remote IP range used here. This is the IP range of the public network from the Internet Port side. To apply this rule to any IP addresses from the public side, enter the range 0.0.0.1 to 255.255.255.254.

Application Port: Enter the application port number used here.



Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Network Filter

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/ Internet access.

In the MAC Filtering Rules section, the user can create and edit Network filter rules. This maximum amount of rules that can be created are 24 rules.

The following parameters will be available for configuration:

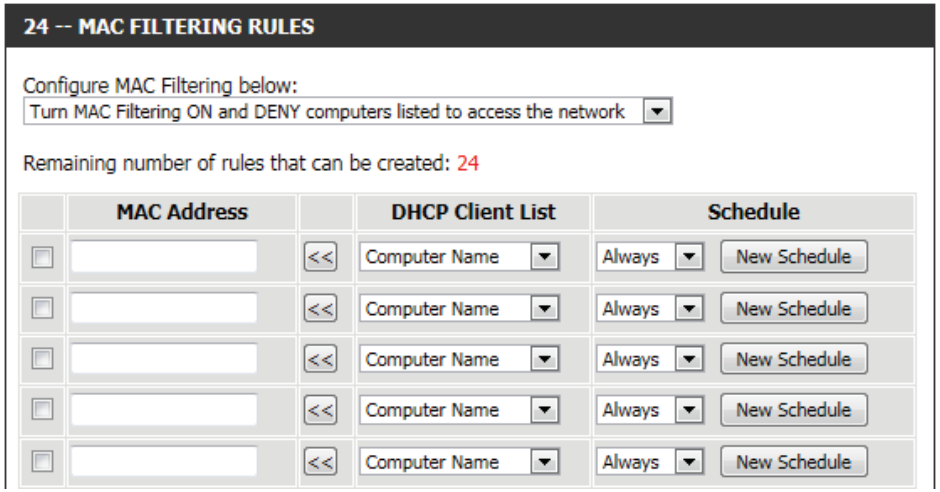
Configure MAC Filtering below: Select **Turn MAC Filtering OFF**, **Turn MAC Filtering ON and ALLOW computers listed to access the network**, or **Turn MAC Filtering ON and DENY computers listed to access the network** from the drop-down menu.

Checkbox: Check the box on the left side to enable the Network Filter.

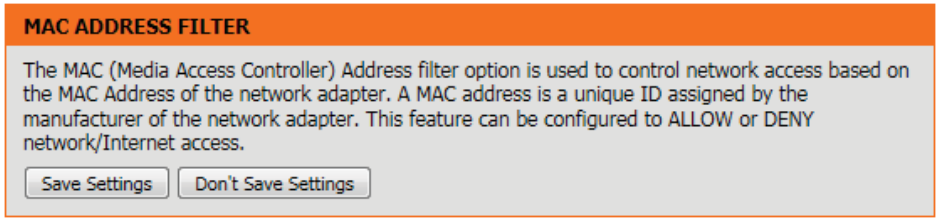
MAC Address: Enter the MAC address you would like to use in this filtering rule.

DHCP Client List: Select a DHCP client from the Computer Name drop-down menu and click << to copy that MAC Address.

Schedule: The schedule of time when the Network Filter will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the New Schedule button to create your own times in the Schedules page.



Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



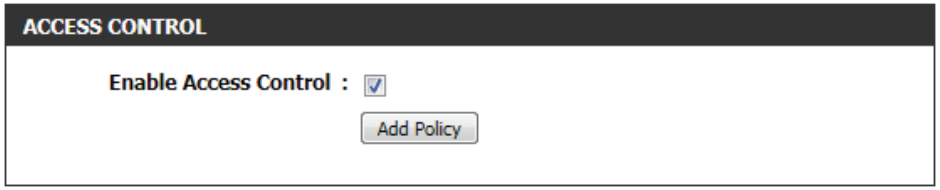
Access Control

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

The following parameters will be available for configuration:

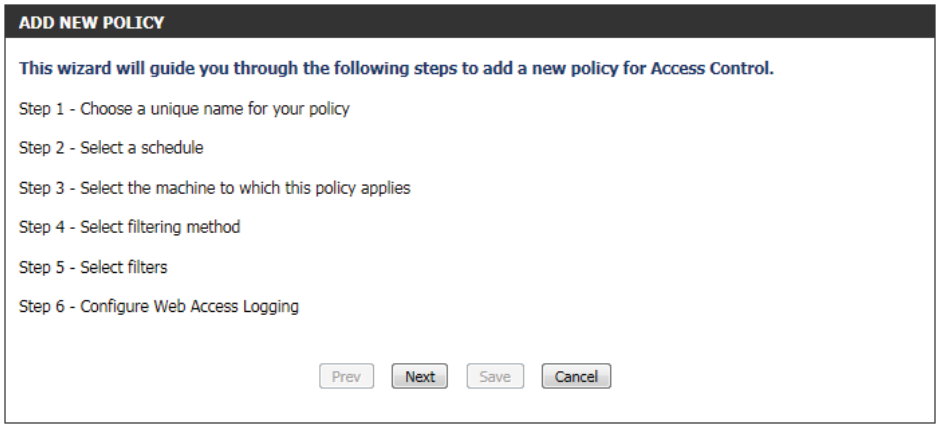
Enable Access Control: Tick this option to enable the Access Control feature.

Add Policy: Click on this button to add a new Access Control Policy.



After clicking on the Add Policy button, the add policy wizard will guide you through the step-by-step process in adding a new policy. The first window explains the process.

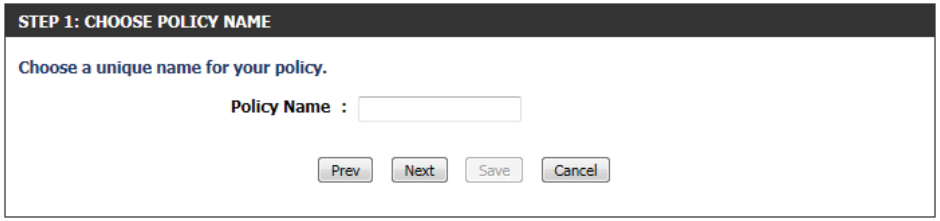
Throughout this wizard the user will be able to:
Click on the **Prev** button to return to the previous window.
Click on the **Next** button to continue to the next window.
Click on the **Cancel** button to discard the changes made and return to the main Access Control window.



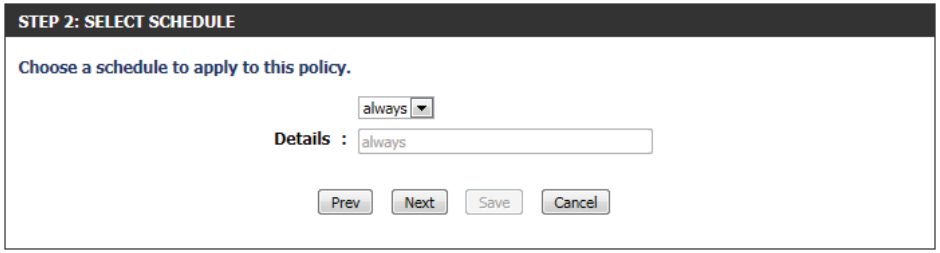
Step 1: In the first step, the user can enter the policy name used.

The following parameters will be available for configuration:

Policy Name: Enter the new policy name used for this rule here.



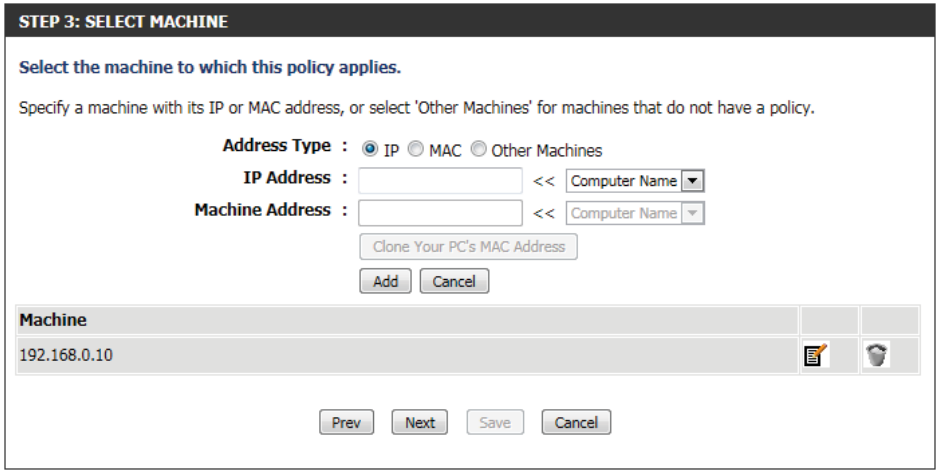
Step 2: In the second step, the user can configure the schedule settings for this rule.



The following parameters will be available for configuration:

Details: Select the appropriate predefined schedule rule to apply to this rule from the drop-down menu.

Step 3: In the third step, the user can configure the address type and IP address of the machines used in this rule.



The following parameters will be available for configuration:

Address Type: Specify a machine with its IP or MAC address, or select 'Other Machines' for machines that do not have a policy.

IP Address: After selecting the IP address type, the user can enter the IP address of the machines used in this rule here. Alternatively, the user can select a Computer from the Computer Name list.

Machine Address: After selecting the MAC address type, the user can enter the MAC address of the machine used in this rule here. Alternatively, the used can select a Computer from the Computer Name list.

Add: Click on this button to add the machine to the list.

Update: After clicking the option, the user will be able to update the machine information.

Delete: If the user chooses to remove a machine from the list, click on the icon.

Step 4: In the fourth step, the user can select the filtering method used for this rule.

The following parameters will be available for configuration:

Method: Here the user can select the filtering method used. Options to choose from are '**Log Web Access Only**', 'B**lock All Access**', and '**Block Some Access**'.

The following parameters will be available for configuration:

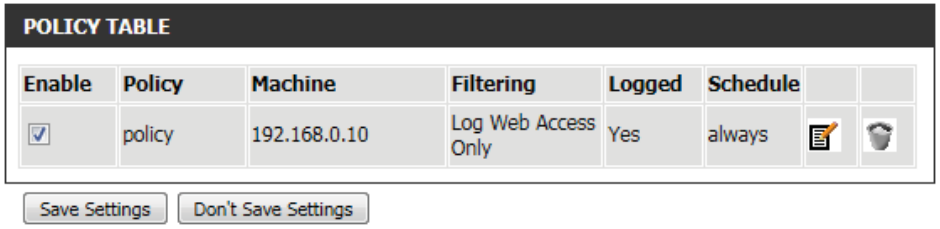
Apply Web Filter: After selecting the '**Block Some Access**' option, the user will be able to select this option. Selecting this option will allow the web filter access control feature to be applied to this rule.

Apply Advanced Port Filters: After selecting the '**Block Some Access**' option, the user will be able to select this option. Selecting this option will allow the advanced port filters access control feature to be applied to this rule.

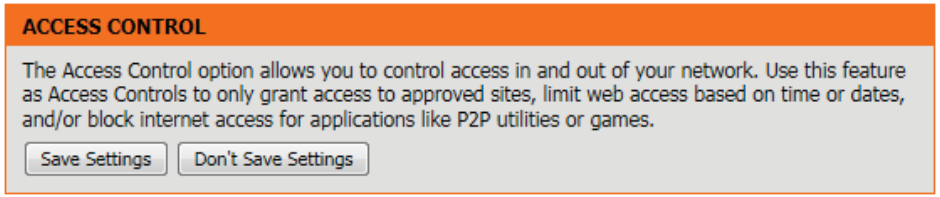
Click on the **Save** button to accept the changes made and return to the main Access Control window.

In the **Policy Table** section a list on access control rules will be displayed.

To edit a specific rule, click on the icon.
To remove a specific rule, click on the icon.



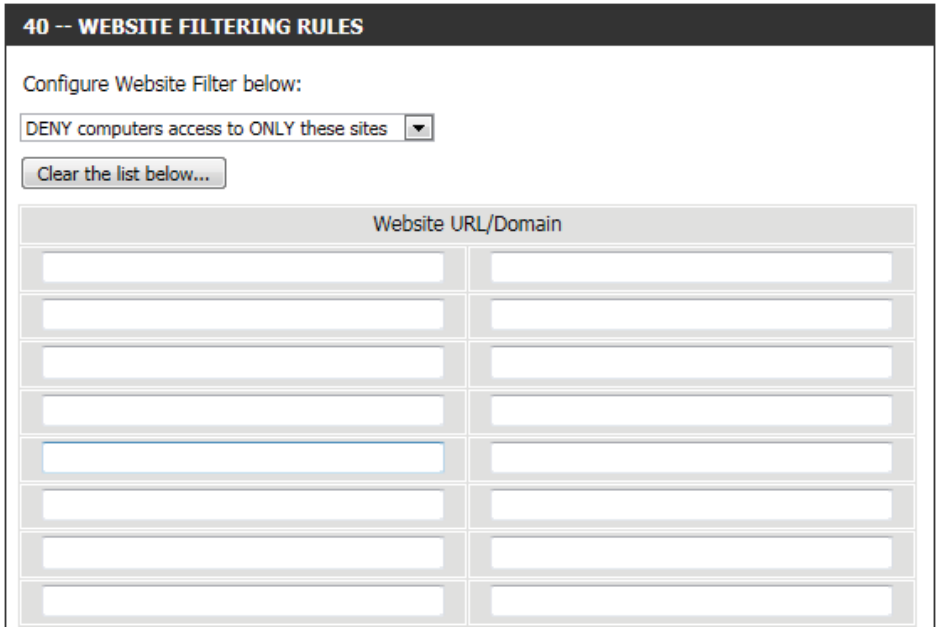
Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Website Filter

Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network.

Website Filter is used to allow or deny computers on your network from accessing specific web sites by keywords or specific Domain Names. Select '**ALLOW computers access to ONLY these sites**' in order only allow computers on your network to access the specified URLs and Domain Names. '**DENY computers access to ONLY these sites**' in order deny computers on your network to access the specified URLs and Domain Names.

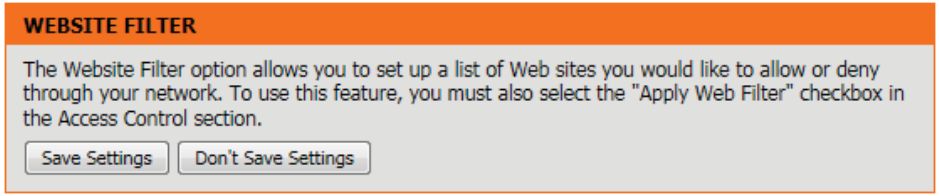


The following parameters will be available for configuration:

Website URL/ Domain: Enter the URL or Domain name that you want to allow or block here.
An example of an URL is: http://www.facebook.com/
An example of a domain name is: facebook.com

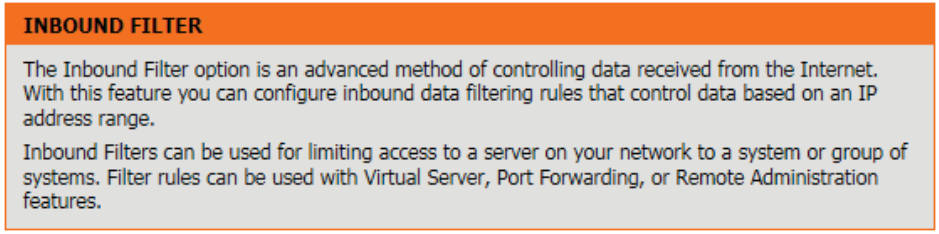
Click on the **Clear the list below...** button to remove all the entries from the spaces in the list.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Inbound Filter

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range. Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features. The user can add new Inbound filter rule in the next section.



The following parameters will be available for configuration:

Name: The user can enter a custom name for the inbound filter rule here.

Action: Select an action that will take place when this rule is initiated. Options to choose from are **Allow** and **Deny**.

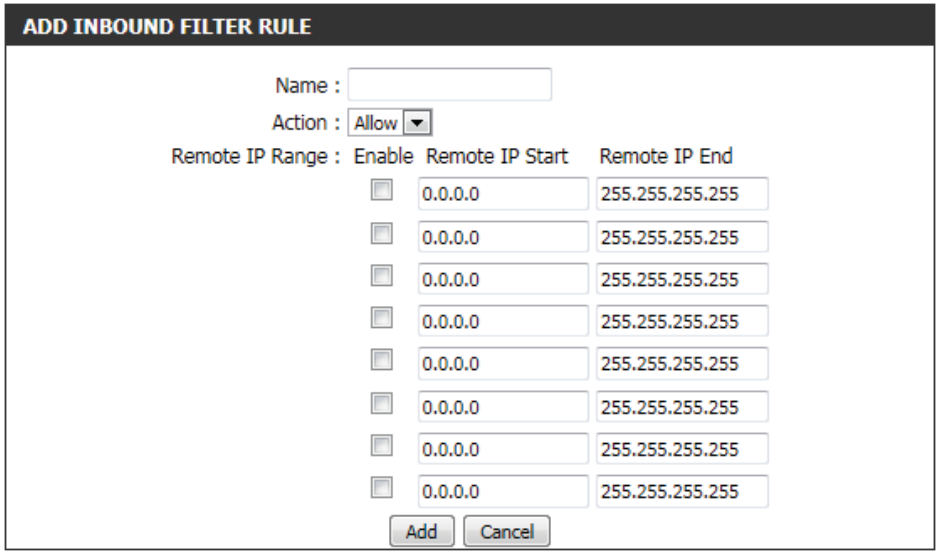
Enable: Tick this option to enable the specified IP range for this rule.

Remote IP Start: Enter the remote starting IP address here in the range.

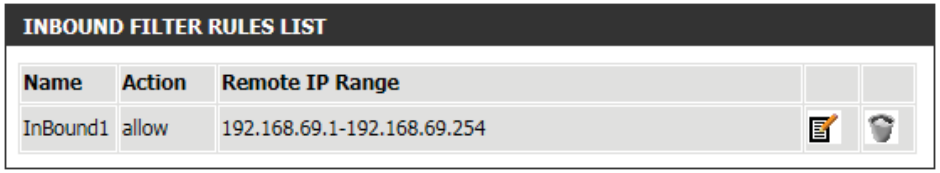
Remote IP End: Enter the remote ending IP address here in the range.

Add: Click this button to add the new inbound filter rule.

Cancel: Click this button to discard the new inbound filter rule.



In the **Inbound Filter Rules List** section, the user can view a list of the inbound filter rules already created. To edit a specific rule, click on the icon. The delete a specific rule, click on the icon.



Firewall Settings

A firewall protects your network from the outside world. The router offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

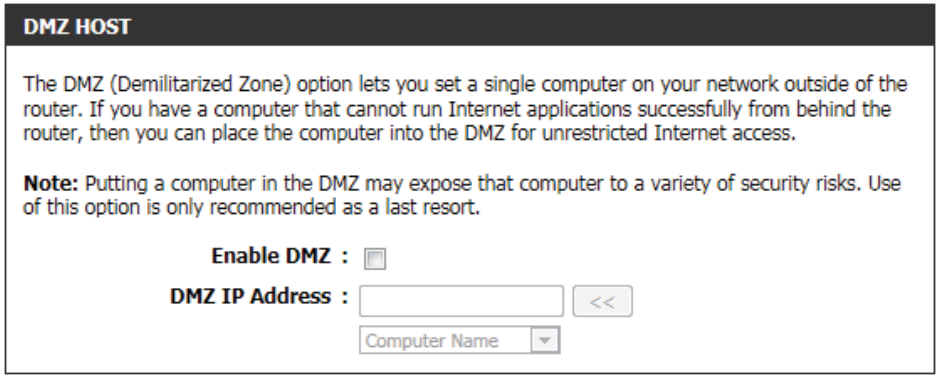
The following parameters will be available for configuration:

Enable SPI: Check the **Enable SPI** box to enable the SPI (Stateful Packet Inspection, also known as dynamic packet filtering) feature. Enabling SPI helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.

The following parameters will be available for configuration:

Enable anti-spoof checking: Tick this option to enable the anti-spoof checking feature.

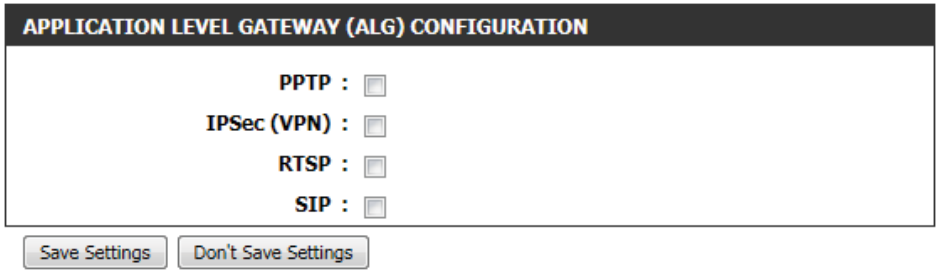
Firewall rules can be used to allow or deny traffic passing through the router. You can specify a single port by utilizing the input box at the top or a range of ports by utilizing both input boxes. DMZ means "Demilitarized Zone". DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers and others.



The following parameters will be available for configuration:

Enable DMZ: Tick this option to enable the DMZ feature.

DMZ IP Address: Enter the IP address of the computer on the LAN that you want to have unrestricted Internet communication in the DMZ IP address field. To specify an existing DHCP client, use the Computer Name drop-down to select the computer that you want to make a DMZ host. If selecting a computer that is a DHCP client, be sure to make a static reservation in the Setup > Network Settings page so that the IP address of the DMZ machine does not change.



The following parameters will be available for configuration:

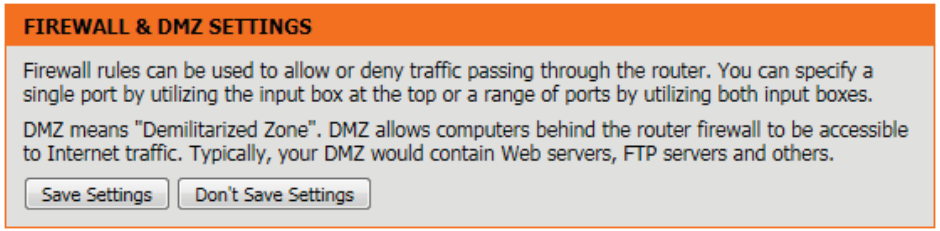
PPTP: Tick this option to allow PPTP access to the LAN network.

IPSec (VPN): Tick this option to allow IPSec (VPN) access to the LAN network.

RSTP: Tick this option to allow RSTP access to the LAN network.

SIP: Tick this option to allow SIP access to the LAN network.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Routing

The Routing option is an advanced method of customizing specific routes of data through your network.

In the **Routing List** section, the user can configure routing rules used by this router. The maximum amount of rules that can be configured is 32.

The following parameters will be available for configuration:

Checkbox: To enable a route, check the box that is on the left side of the route.

Name: Enter a name for the rule used here.

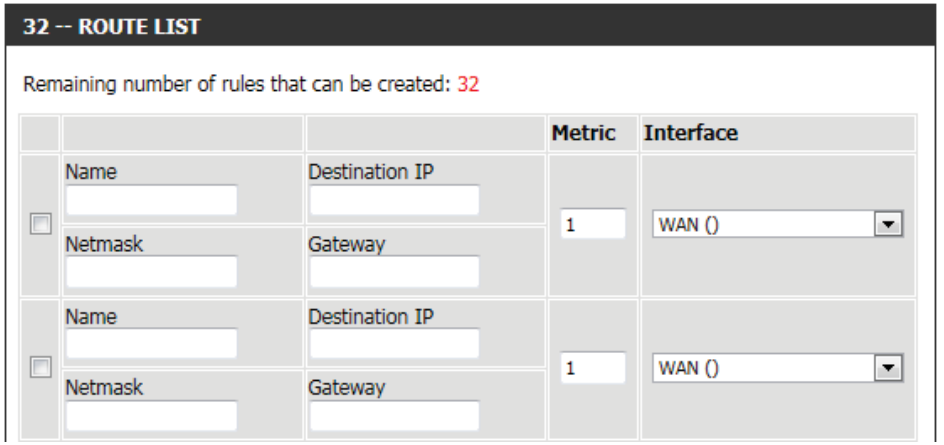
Destination IP: Enter the IP address of the packets that will take this route.

Netmask: Enter the netmask to specify the subnet of the IP packets that will take this route.

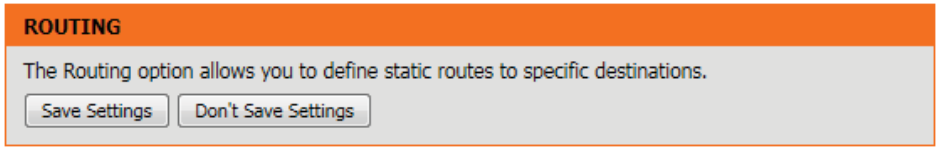
Gateway: Enter the next hop that will be taken if this route is used.

Metric: Enter the metric value that this route will use here.

Interface: Use the drop-down menu to specify if the IP packet must use the WAN or LAN interface to transit out of the Router.



Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Advanced Wireless

These options are for users that wish to change the behavior of their 802.11n wireless radio from the standard settings. We do not recommend changing these settings from the factory defaults. Incorrect settings may impact the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

The following parameters will be available for configuration:

Wireless Band: Here the user can view the wireless frequency band being configured. In the case 2.4GHz.

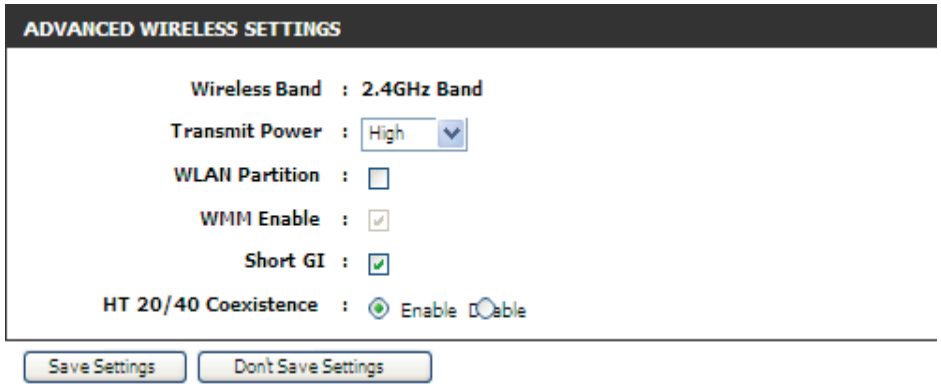
Transmit Power: This option sets the transmit power of the antennas.

WLAN Partition: Check this box to enable WLAN Partition.

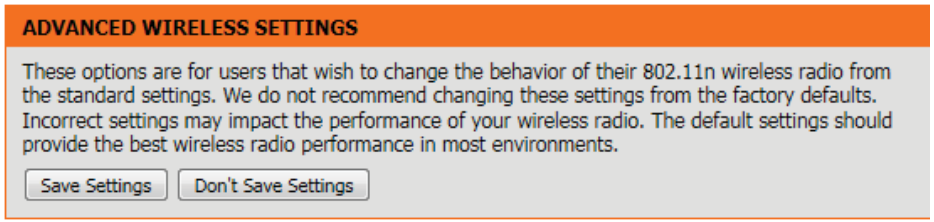
WMM Enable: Check this box to enable the WMM feature.

Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

HT 20/40 Coexistence:



Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the "Initial setup" as well as the "Add New Device" processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy, as depressing a button for the Push-Button Method or correctly entering the 8-digit code for the Pin-Code Method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

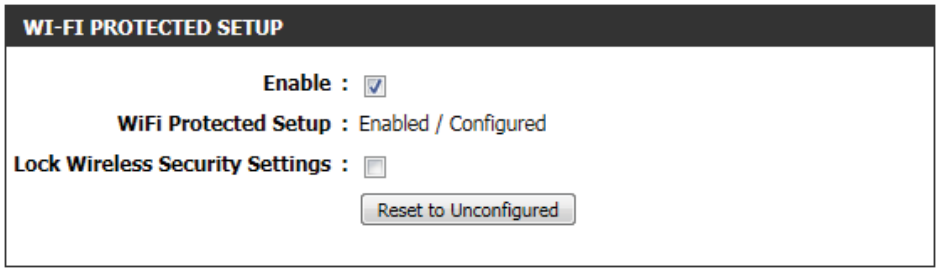
In the Wi-Fi Protected Setup section, the user can enable the WPS feature of this router.

The following parameters will be available for configuration:

Enable: Tick this option to enable the Wi-Fi Protected Setup feature.

WiFi Protected Setup: This parameter displays the WPS setup status.

Lock Wireless Security Settings: Tick this option to lock the configured wireless security settings.



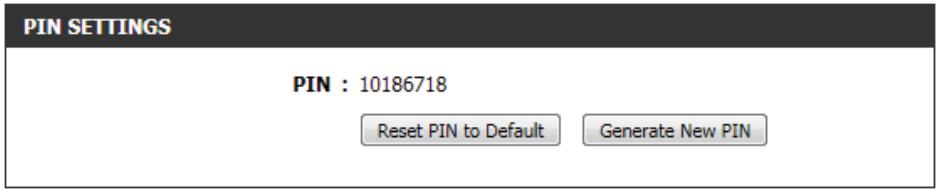
In the PIN Settings section, the user not only will be able to view the PIN code, but will also be able to reset the PIN to default or to generate a new PIN code. A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

The following parameters will be available for configuration:

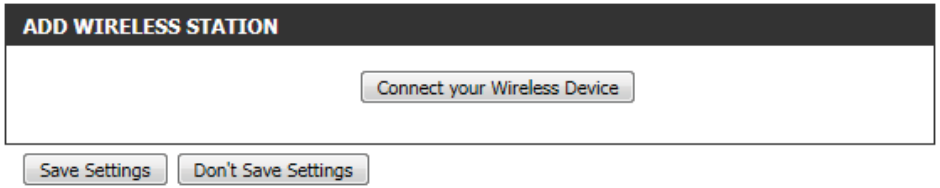
PIN: Shows the current value of the router's PIN.

Reset PIN to Default: Click this button to restore the default PIN of the router.

Generate New PIN: Click this button to create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to the user interface of the registrar.



Click the '**Connect your Wireless Device**' button to start Wireless Connection Setup Wizard. This wizard helps you add wireless devices to the wireless network.

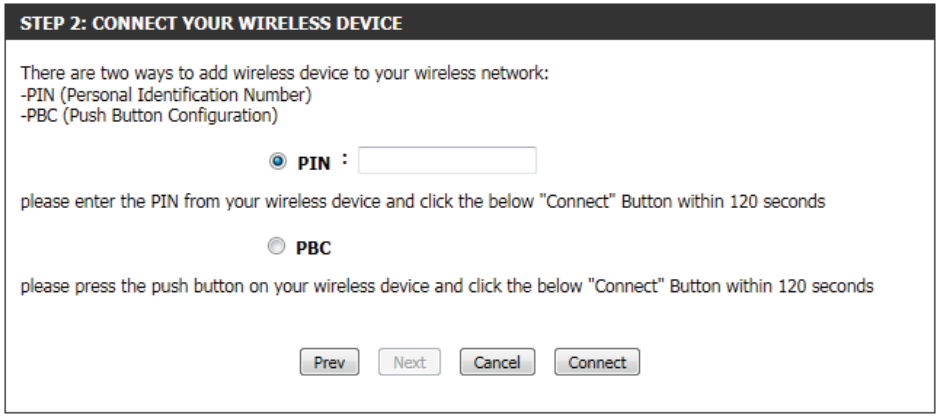


Step 1: In this step the user have two options to choose from. You can choose **Auto** if the wireless client supports WPS, or **Manual** if the wireless client does not support WPS.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

Step 2: After selecting Auto, the following page will appear. There are two ways to add a wireless device, that supports WPS. Firstly, there is the Personal Identification Number (**PIN**) method. Using this method will prompt the user to enter a PIN code. This PIN code should be identical on the wireless client. Secondly, there is the Push Button Configuration (**PBC**) method. Using this method will allow the wireless client to connect to this device by similarly pressing the PBC button on it.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.



Step 2: After selecting **Manual**, the following page will appear. On this page to user can view the wireless configuration of this router. The wireless clients should configure their wireless settings to be identical to the settings displayed on this page for a successful connection. This option is for wireless clients that can't use the WPS method to connect to this device.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page. Click on the **Wireless Status** button to navigate to the Status > Wireless page to view what wireless client are connected to this device.

Advanced Network

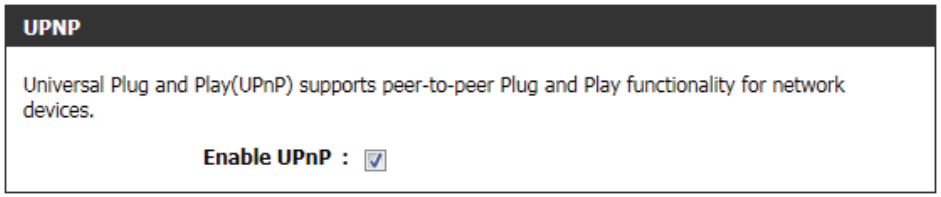
This section contains settings which can change the way the router handles certain types of traffic. We recommend that you not change any of these settings unless you are already familiar with them or have been instructed to change them by one of our support personnel.

UPnP

UPnP is short for Universal Plug and Play which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The device is a UPnP enabled router, meaning it will work with other UPnP devices/software. If you do not want to use the UPnP functionality, it can be disabled by selecting "Disabled".

The following parameters will be available for configuration:

Enable UPnP: Tick this option to enable the UPnP feature of the router.

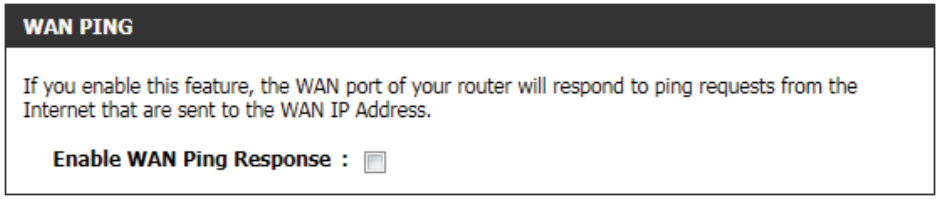


WAN Ping

When you Enable WAN Ping response, you are causing the public WAN (Wide Area Network) IP address on the device to respond to ping commands sent by Internet users. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

The following parameters will be available for configuration:

Enable WAN Ping Response: Tick this option to enable the WAN Ping Response option of the router.

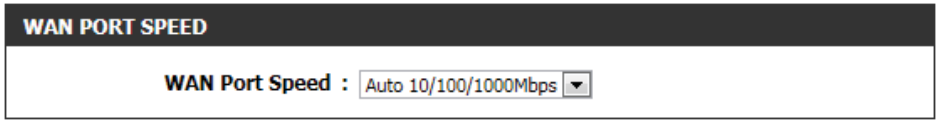


WAN Port Speed

This allows you to select the speed of the WAN interface of the router. Option to choose from are Auto 10/100/1000Mbps, 10Mbps, 100Mbps, or 1000Mbps.

The following parameters will be available for configuration:

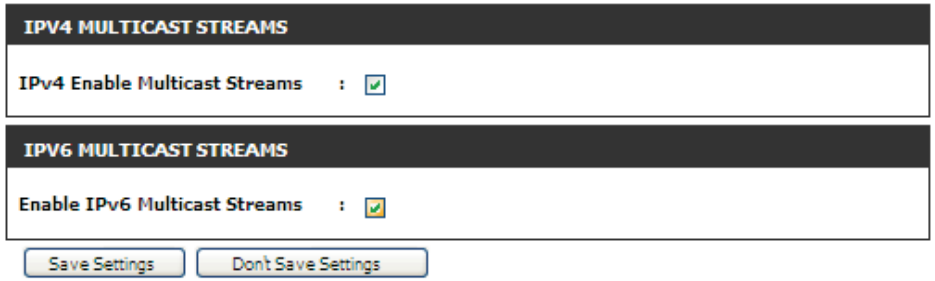
WAN Port Speed: You may set the port speed of the Internet port to **Auto 10/100/1000Mbps**, **10Mbps**, **100Mbps,** or **1000Mbps**. Some older cable or DSL modems may require you to set the port speed to 10Mbps.



Multicast Streams

This section enables the user to allow IPv4 or IPv6 Multicast traffic to pass from the Internet to your network more efficiently.

The following parameters will be available for configuration:

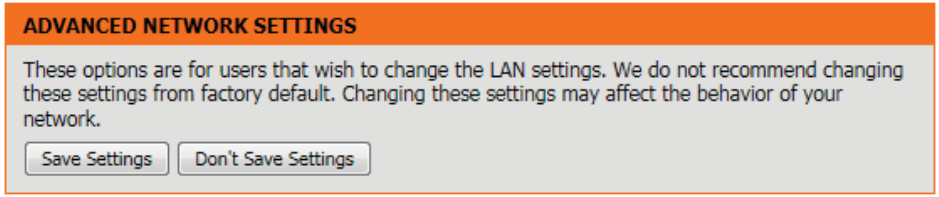


IPv4 Enable Multicast Streams

Enable IPv6 Multicast Streams

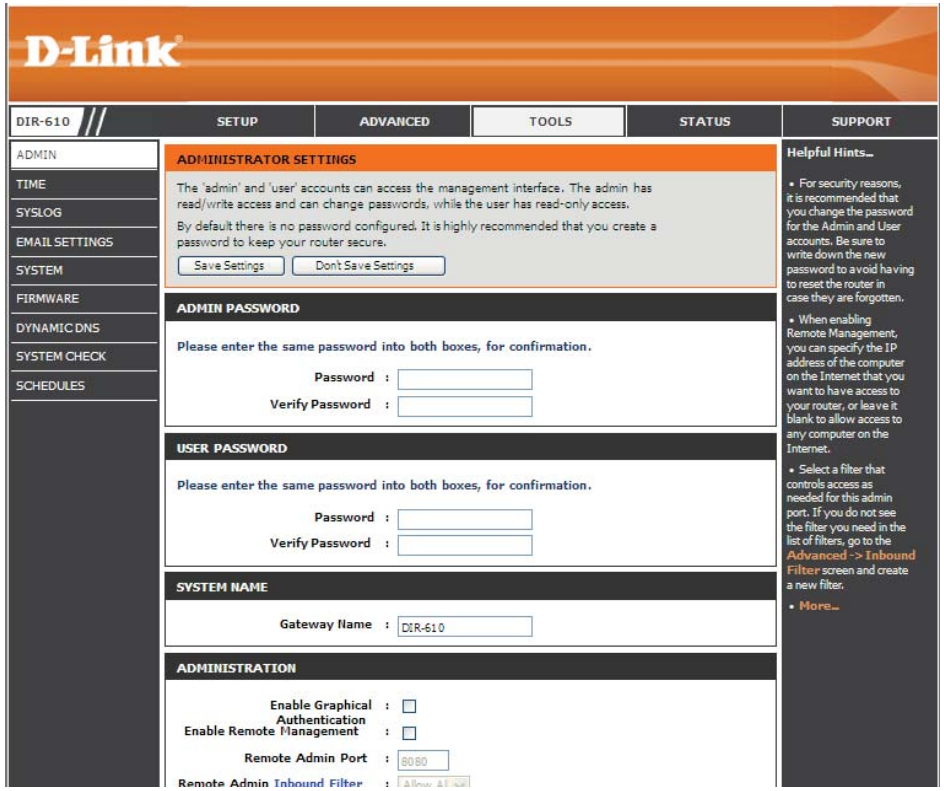
Enable Multicast Streams: Enable this option if you are receiving video on demand type of service from the Internet. The router uses the IGMP protocol to support efficient multicasting transmission of identical content, such as multimedia, from a source to a number of recipients. This option must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling this option.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Tools Category

In this category the user will be able to configure features that are related to the router itself. Features like the time settings, login accounts, firmware update and more.



Admin

This page will allow you to change the Administrator password and configure the authentication settings. This window also allows you to enable Remote Management, via the Internet. For security reasons, it is recommended that you change the password for the Admin and User accounts. Be sure to write down the new password to avoid having to reset the router in case they are forgotten.

In the **Admin Password** section, the user can change the Administrator login password used for this device.

The following parameters will be available for configuration:

Password: Enter the new login password used here.

Verify Password: Re-enter the new login password here.

In the **User Password** section, the user can change the User login password used for this device.

The following parameters will be available for configuration:

Password: Enter the new login password used here.

Verify Password: Re-enter the new login password here.

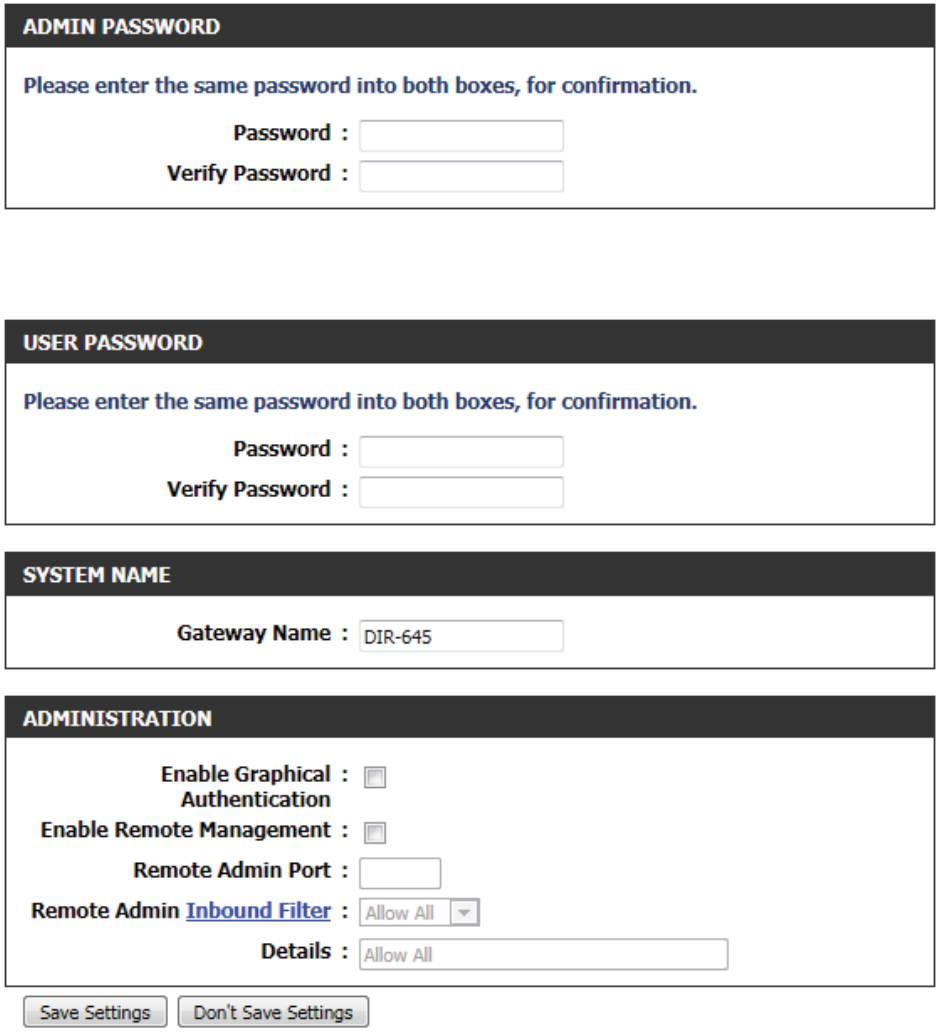
In the **System Name** section, the user can change the gateway name used for this device.

The following parameters will be available for configuration:

Gateway Name: Enter the router gateway name used here.

The following parameters will be available for configuration:

Enable Graphical Authentication: Tick this option to enable the graphical image confirmation when the user login to the web configuration.



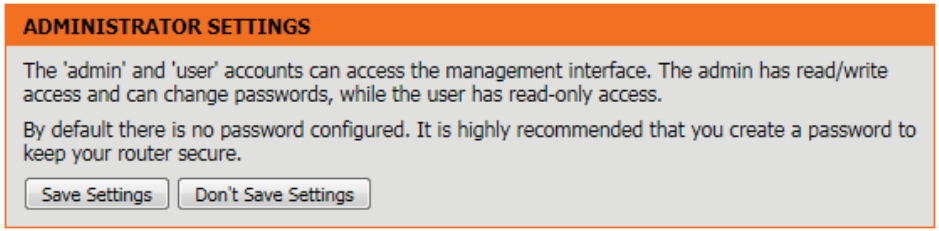
Enable Remote Management: Tick this option to enable remote management. This option will enable the router to be accessible from the Internet port.

Remote Admin Port: Enter the remote administration port number used here. Sometimes services like an internal web server will occupy the port number 80. In this option the user can change the remote administration port to 8080 for example.

Remote Admin Inbound Filter: Select the appropriate remote admin inbound filter behavior here. Options to choose from are **Allow All** and **Deny All**.

Details: Enter the remote admin inbound filter detail description used here.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



Time

The Time window 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 Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Time and Date Configuration

Here the user can configure the time zone as well as the daylight savings settings used for this router.

The following parameters will be available for configuration:

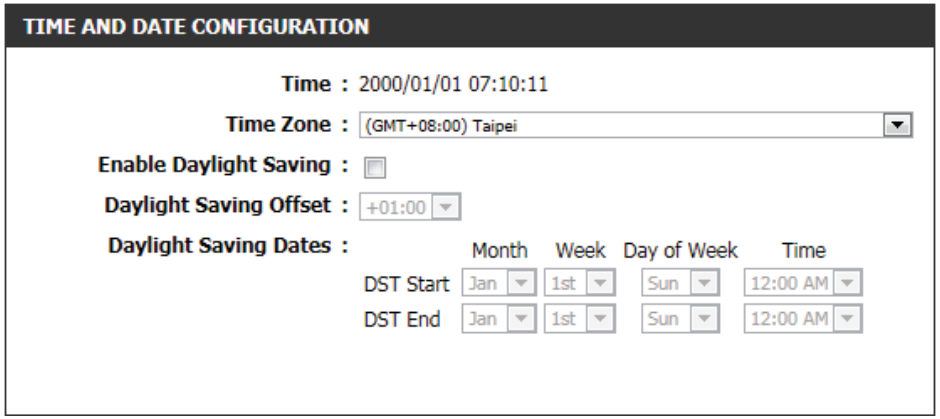
Time: Here will be displayed the current time configuration running on this device.

Time Zone: Select the appropriate time zone used on this device here.

Enable Daylight Saving: Check this box if the country your are located in uses Daylight Saving time.

Daylight Saving Offset: Select the daylight savings offset used here.

Daylight Saving Dates: Select the start date and end date for daylight saving time.



Automatic Time and Date Configuration

Here the user can configure whether this router will automatically synchronize it's time and date with a public time server.

The following parameters will be available for configuration:

Automatically synchronize: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Tick this option to enable automatic time and date synchronizing.

NTP Server Used: Select the appropriate time server used here. The interval at which the router will communicate with the NTP server is set to 7 days.

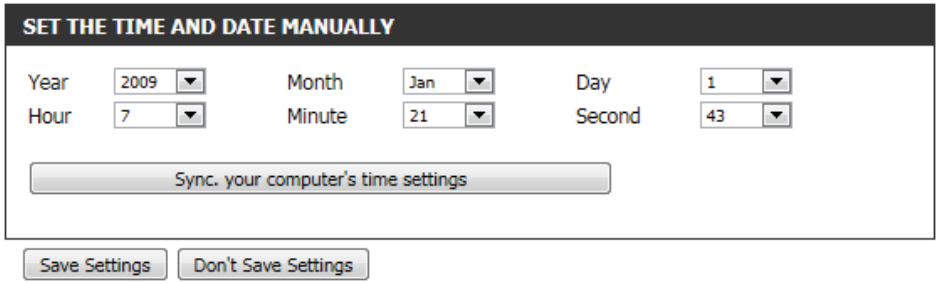
Update Now: After selecting the appropriate time server and enabling the automatic synchronization option, click on this button to update the current time and date of the router.

Set the Time and Date Manually

Here the user can configure the time and date values, used by this router, manually. Here the user can also synchronize the router's time with the configuration computer's time.

The following parameters will be available for configuration:

Set Manually: Here the user can manually configure the date and time used by this device. Options to configure are Year, Month, Day, Hour, Minute, and Second.



Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

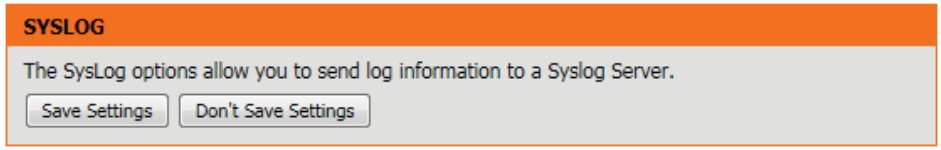
Syslog

The Syslog options allow you to send log information to a System Log Server.

The following parameters will be available for configuration:

Enable Logging To SysLog Server: Tick this option to enable the Syslog feature.

Syslog Server IP Address: Enter the Syslog Server IP address used here.



Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

Email Settings

The Email feature can be used to send the system log files and router alert messages to your email address.

Email Notification

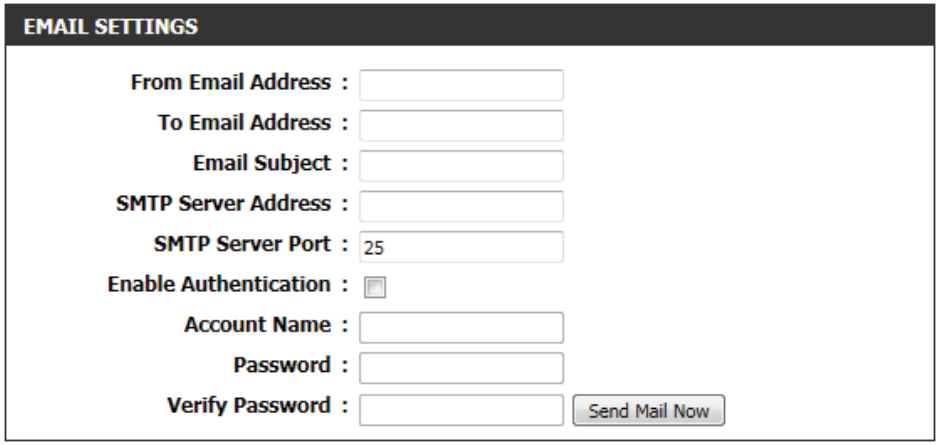
When this option is enabled, router activity logs or firmware upgrade notifications can be emailed to a designated email address.

The following parameters will be available for configuration:

Enable Email Notification: Tick this option to enable the Email notification feature.

Email Settings

Here this user can manually enter the email settings required to enable the email notification feature.



The following parameters will be available for configuration:

From Email Address: This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

To Email Address: Enter the email address where you want the email sent.

Email Subject: Enter the text that you want to appear in the subject line of the e-mail that is sent.

SMTP Server Address: Enter the SMTP server address for sending email. If your SMTP server requires authentication, select this option.

SMTP Server Port: Enter the SMTP server port number used for sending email.

Enable Authentication: Tick this option if the SMTP server requires authentication for sending mail.

Account Name: Enter your account for sending email.

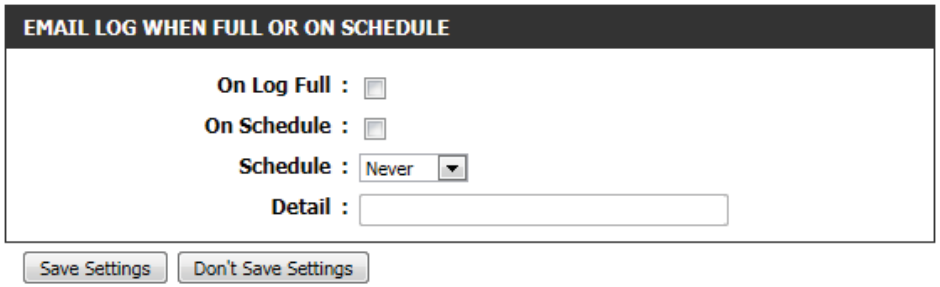
Password: Enter the password associated with the account.

Verify Password: Re-enter the password associated with the account here.

Send Mail Now: Click this button to send a test email from the Router to verify that the email settings have been configured correctly.

Email Log When Full or on Schedule

Normally emails are sent at the starting and ending time defined in the schedule. However, rebooting the router during the schedule period will cause additional emails to be sent.



The following parameters will be available for configuration:

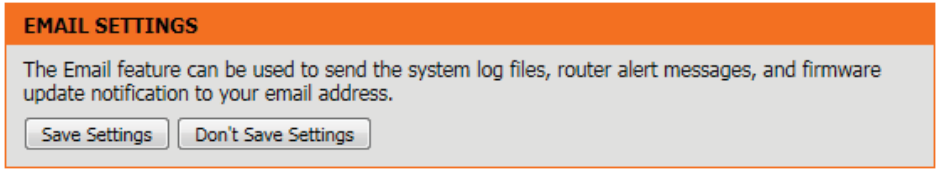
On Log Full: Select this option if you want logs to be sent by email when the log is full.

On Schedule: Select this option if you want logs to be sent by email according to a schedule.

Schedule: If you selected the '**On Schedule**' option, select one of the defined schedule rules. If you do not see the schedule you need in the list of schedules, go to the Tools > Schedules screen and create a new schedule.

Detail: Enter a detailed description here.

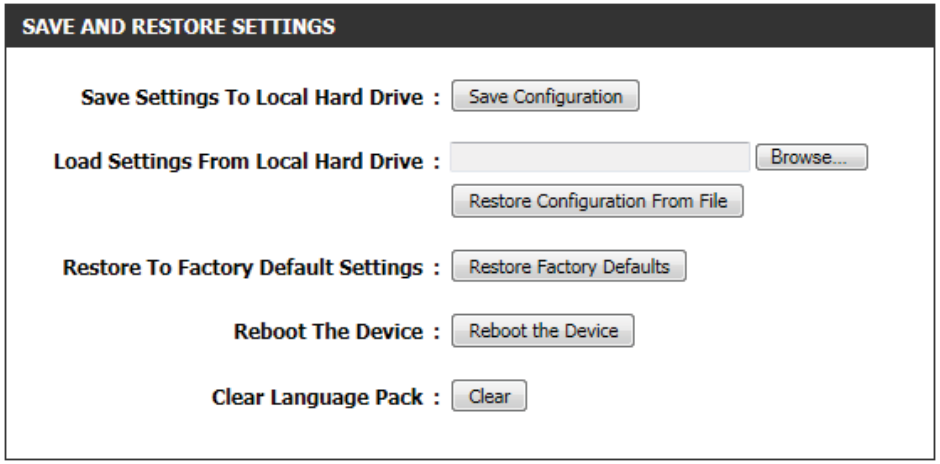
Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.



System

This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

The following parameters will be available for configuration:



Save Settings To Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. A file dialog will appear, allowing you to select a location and file name for the settings.

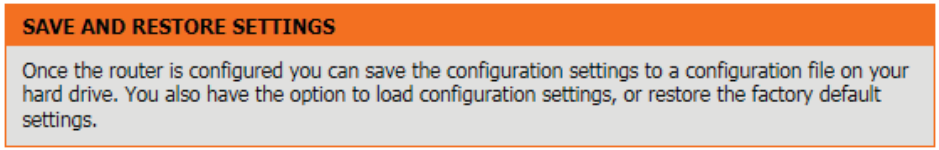
Load Settings From Local Hard Drive: Use this option to load previously saved router configuration settings. First, use the **Browse** option to find a previously saved file of configuration settings. Then, click the **Restore Configuration From File** button below to transfer those settings to the router.

Restore To Factory Default Settings: This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the Save button above.

Reboot The Device: Click to reboot the router.

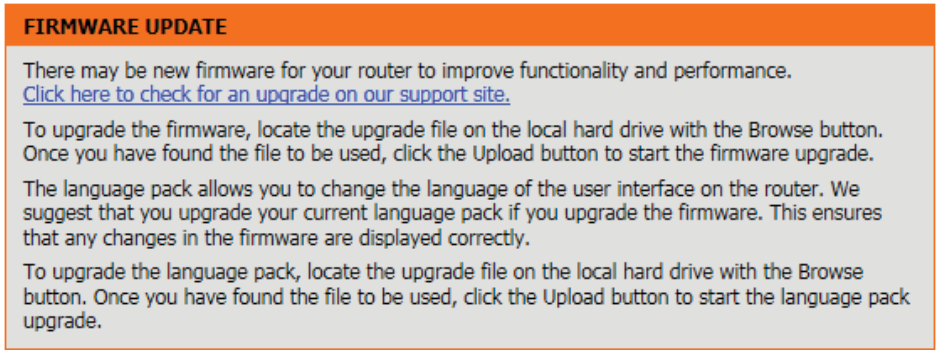
Clear Language Pack: If you previously installed a language pack and want to revert all the menus on the Router interface back to the default language settings, click the **Clear** button.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

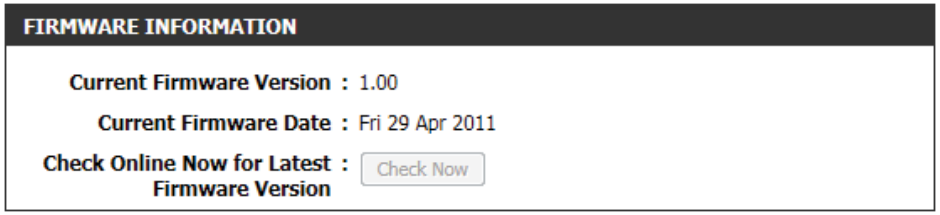


Firmware

Use the Firmware window to upgrade the firmware of the Router and install language packs. If you plan to install new firmware, make sure the firmware you want to use is on the local hard drive of the computer. If you want to install a new language pack, make sure that you have the language pack available. Please check the support site for firmware updates. You can download firmware upgrades to your hard drive from the support site.

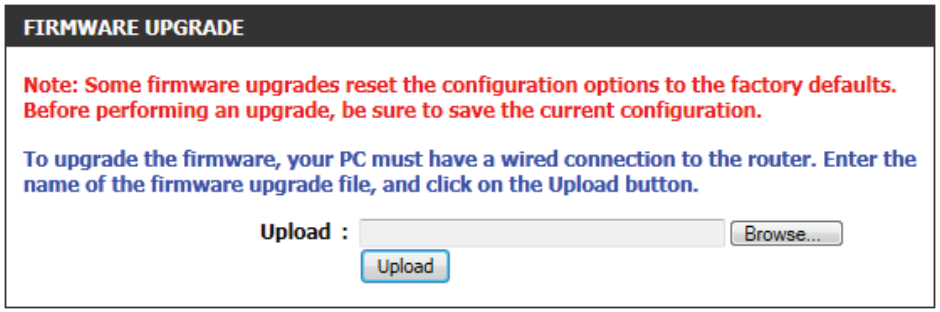


In the **Firmware Information** section the user can view the **Current Firmware Version** number running on this device, the **Current Firmware Date** of this same firmware version running on this device, and a button to click that will Check Online Now for Latest Firmware Version.

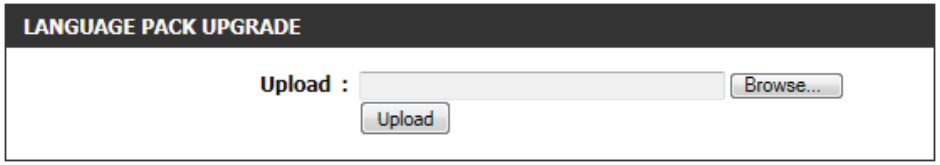


In the **Firmware Upgrade** section the user can physically upgrade the firmware of this device clicking on the **Browse** button and navigating to the firmware file, saved on the local hard drive. After locating the file, click on the **Upload** button to initiate the firmware upgrade.

Note: Some firmware upgrades will reset the configuration, of the device, to factory defaults. Be sure to save the current configuration first before any firmware update.



In the **Language Pack Upgrade** section, the user can change the router's language pack by clicking on the **Browse** button and navigating to the language pack, downloaded to the computer. After navigating to the language pack file, click on the **Upload** button to initiate the language pack upload and configuration. Always keep a close lookout on the local vendor's website for new firmware upgrades and language packs.



Note: Always update the firmware or language packs for this device using the wired connection. Never upgrade using a wireless connection.

Dynamic DNS

The DDNS 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 in your domain name to connect to your server no matter what your IP address is.

The following parameters will be available for configuration:

Enable Dynamic DNS: Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.

Server Address: Choose your DDNS provider from the drop down menu.

Host Name: Enter the Host Name that you registered with your DDNS service provider.

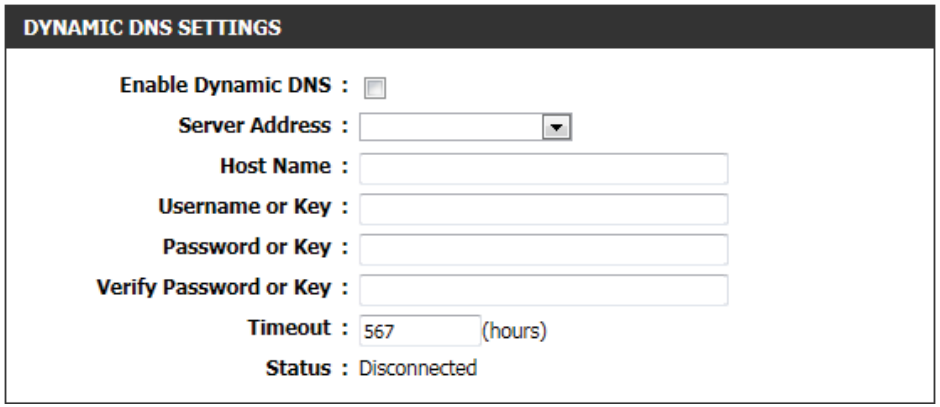
Username or Key: Enter the Username or Key for your DDNS account.

Password or Key: Enter the Password or Key for your DDNS account.

Verify Password or Key: Re-enter the Password or Key for your DDNS account.

Timeout: Enter the timeout value used for the DDNS account here.

Status: Displays the DDNS connection status here.



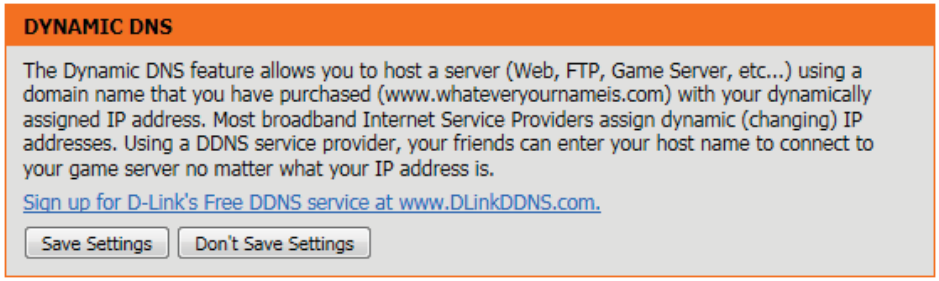
The following parameters will be available for configuration:

Enable: Tick this option to enable the Dynamic DNS feature for IPv6 hosts.

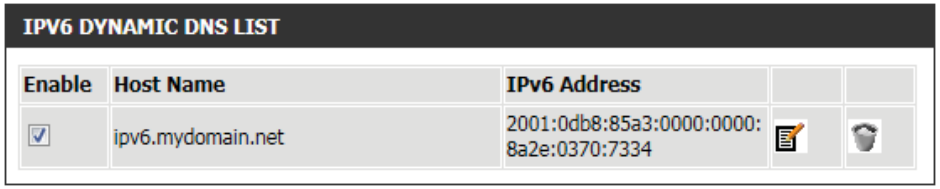
IPv6 Address: Enter the IPv6 Address used here. Alternatively, the user can select the Computer Name for the drop-down list and click on the << button to add it the IPv6 Address field.

Host Name: Enter the IPv6 host name used for the DDNS account here.

Click on the **Save** button to add the IPv6 host to the IPv6 Dynamic DNS List.
Click on the **Clear** button to clear the information entered in the fields.



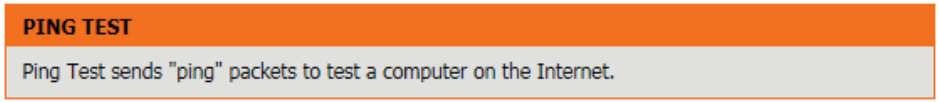
In the **IPv6 Dynamic DNS List** section, a list of IPv6 hosts will be displayed. Tick the **Enable** checkbox to make the host active. To edit a specific entry click on the icon. To remove a specific entry, click on the icon.



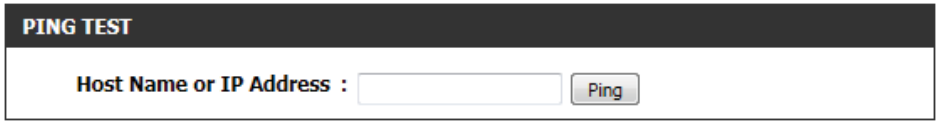
Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

System Check

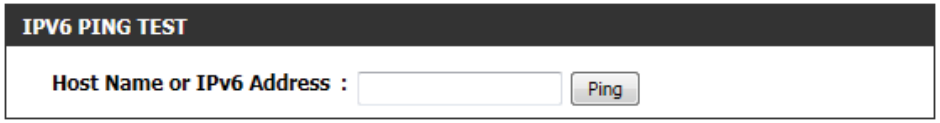
This useful diagnostic utility can be used to check if a computer is on the Internet. It sends ping packets and listens for replies from the specific host.



In the **Ping Test** section the user can test the Internet connectivity by entering in a host name or the IP address that you want to Ping and click on the **Ping** button. The status of your Ping attempt will be displayed in the Ping Result box.



In the **IPv6 Ping Test** section the user can test the Internet connectivity by entering in a host name or the IPv6 address that you want to Ping and click on the **Ping** button. The status of your Ping attempt will be displayed in the Ping Result box.



In the Ping Result section the results of the attempted ping will be displayed.

Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

The following parameters will be available for configuration:

Name: Enter the custom name for the new schedule rule here. This name is used for identification.

Day(s): To use every day in the week for this rule, select the **All Week** option. To use only selected days for this rule, select the **Select Day(s)** option and tick the appropriate days used for this rule.

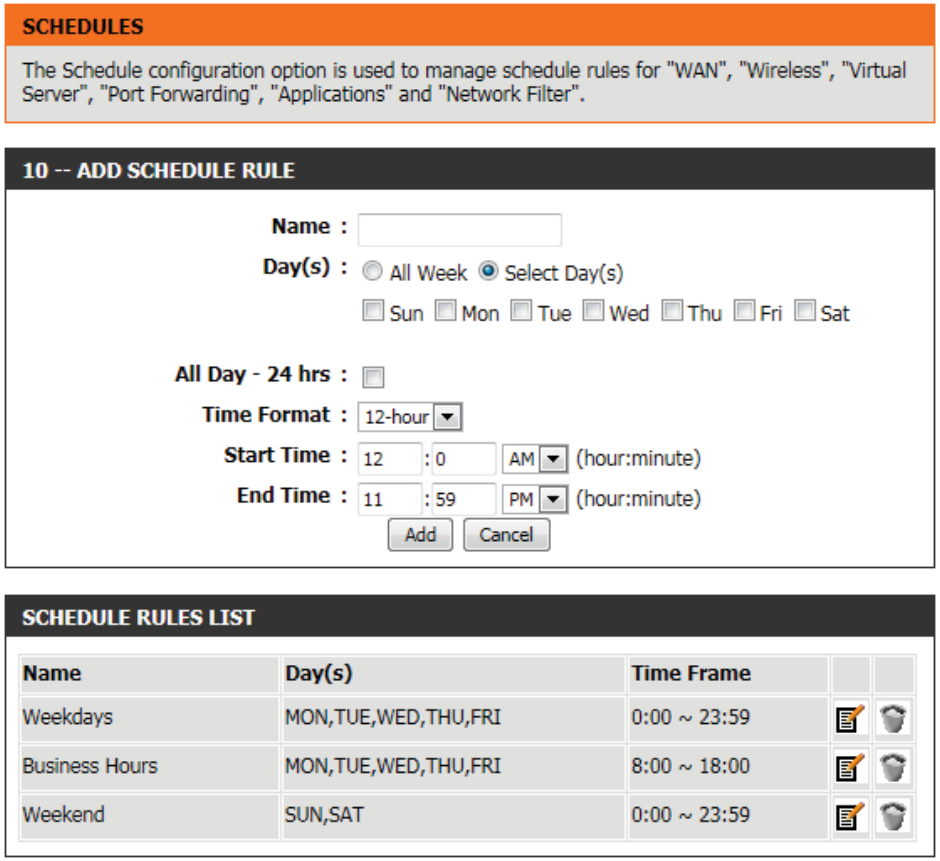
All Day - 24 hrs: To enable this rule to run 24 hours instead of only a certain part of the day, tick this option.

Time Format: Select the appropriate time format to use here.

Start Time: If the All Day option is not selected, the user can enter the starting time here.

End Time: If the All Day option is not selected, the user can enter the ending time here.

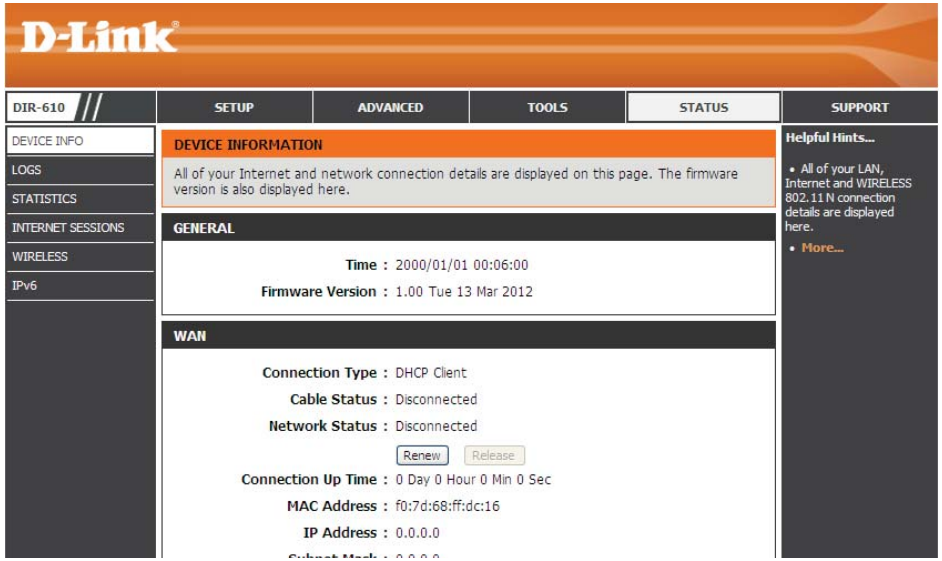
Click on the **Add** button to add this new rule to the schedule rules list. Click on the **Cancel** button to discard the information and cancel the rule addition.



In the **Schedule Rules List** section, the user can view the available schedule rules created. To edit an existing rule, click on the icon of the specific entry, To remove an existing rule, click on the icon of the specific entry.

Status Category

In this category the user will be able to view information regarding the configuration and functionality of this device. The information includes WAN, LAN and Wireless configurations, System, Firewall, Router logs, and more.



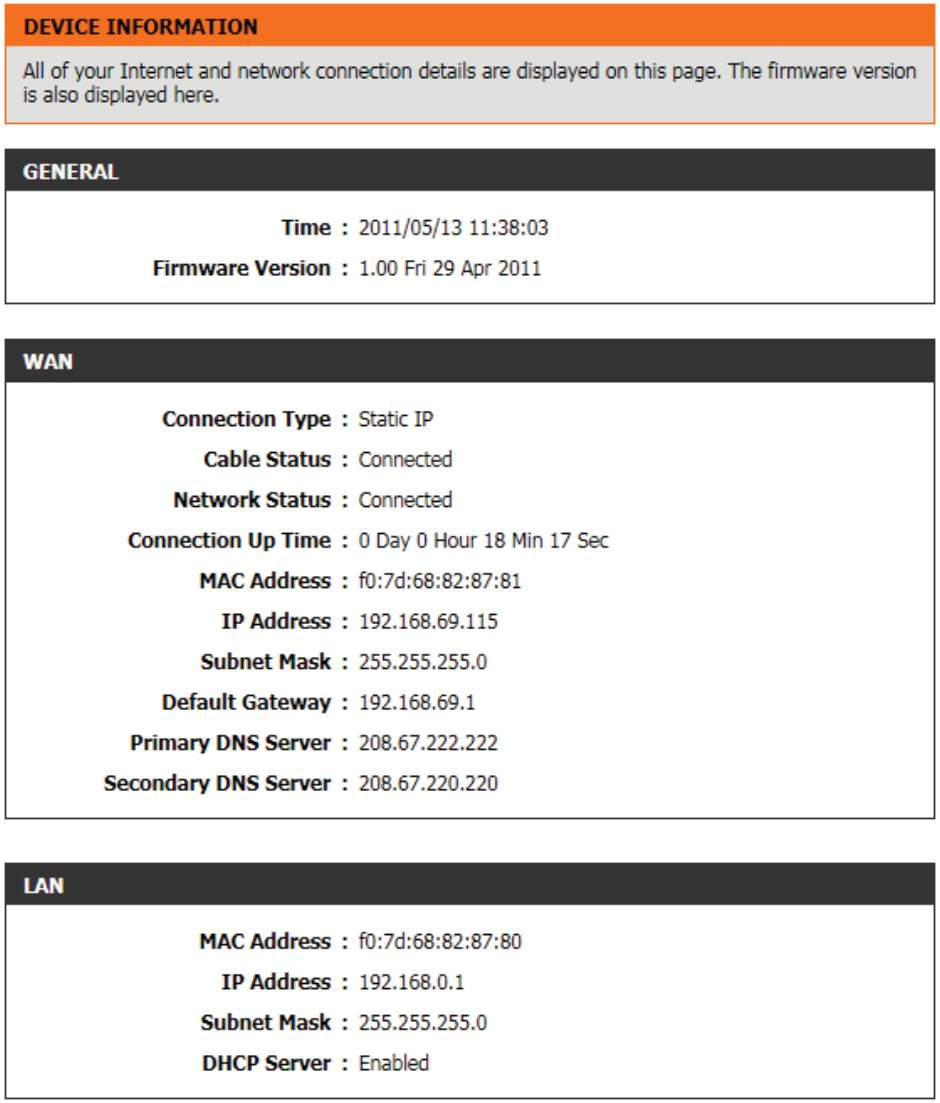
Device Info

This page displays the current information for the router. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a Release button and a Renew button will be displayed. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

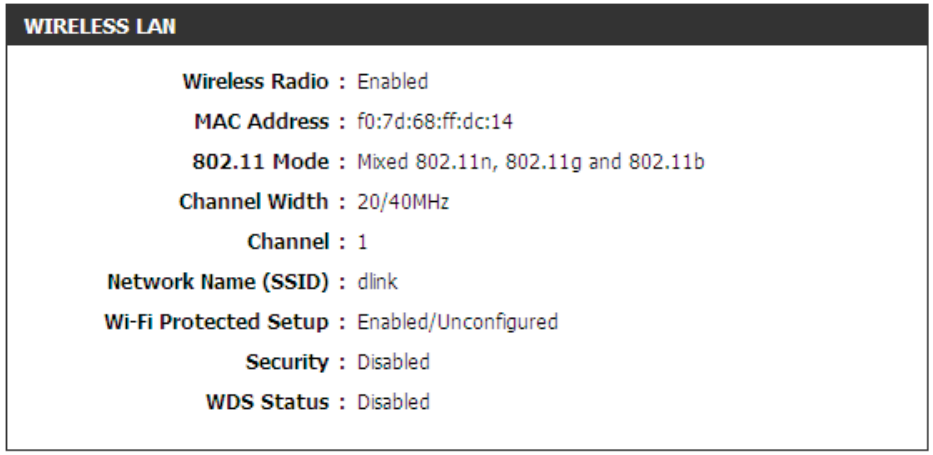
In the **General** section, information about the time and firmware is being displayed.

In the **WAN** section, information about the Internet connection is being displayed.

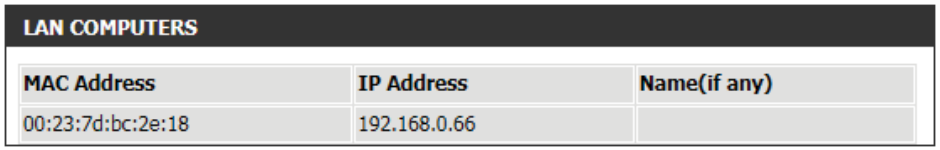
In the **LAN** section, information about the Local Area Network configuration is being displayed.



In the **Wireless LAN** section, information about the Wireless Local Area Network configuration is being displayed.



In the **LAN Computers** section, a list of actively connected nodes are being displayed.

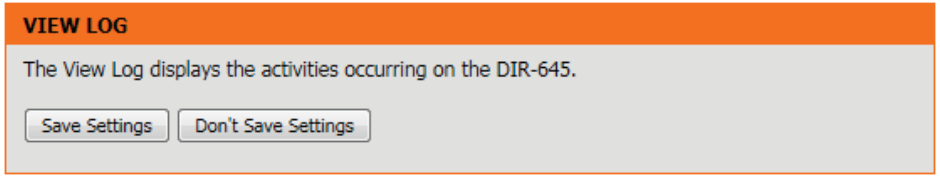


In the **IGMP Multicast Memberships** section, a list of Multicast Group Addresses are being displayed.

Logs

The router automatically logs (records) events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

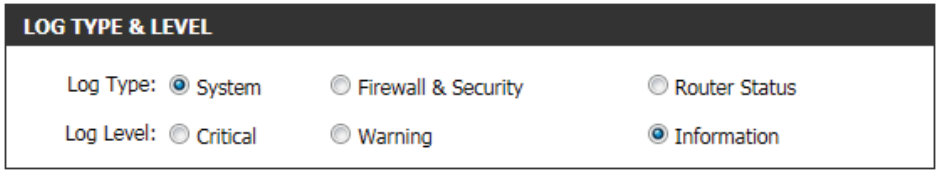
In the **Save Log File** section, the user can click on the **Save** button save the Router's log entries to a log file on your computer.



The following parameters will be available for configuration:

Log Type: Use the radio buttons to select the types of messages that you want to display from the log. System, Firewall & Security, and Router Status messages can be selected.

Log Level: There are three levels of message importance: Critical, Warning, and Information. Select the levels that you want displayed in the log.



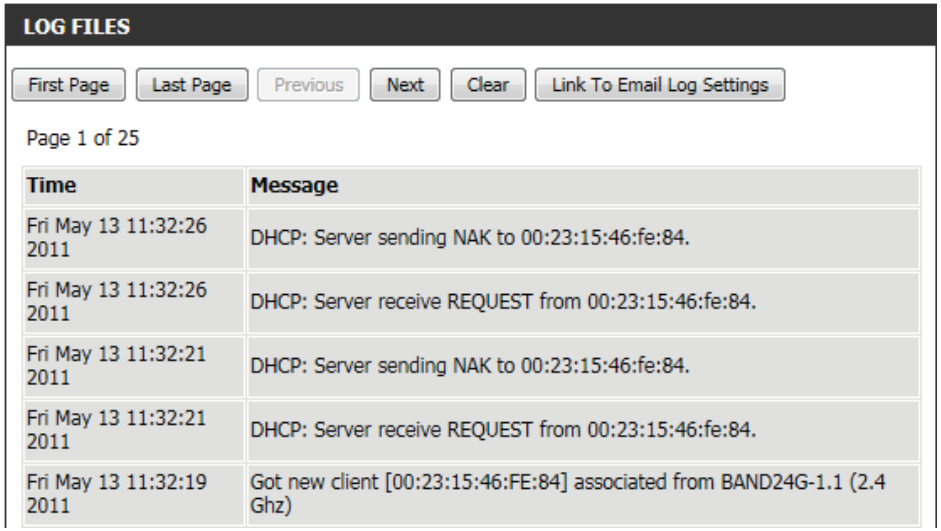
The following parameters will be available for configuration:

First - Last Page: Use these buttons to navigate to the first or last page of the router logs.

Previous - Next: Use these buttons to navigate to the next or previous page of the router logs.

Clear: Click on this button to clear all the contents from the log.

Link to Email Log Settings: Click this button to open the Email Settings screen so that you can change the Email configuration for sending logs.



Statistics

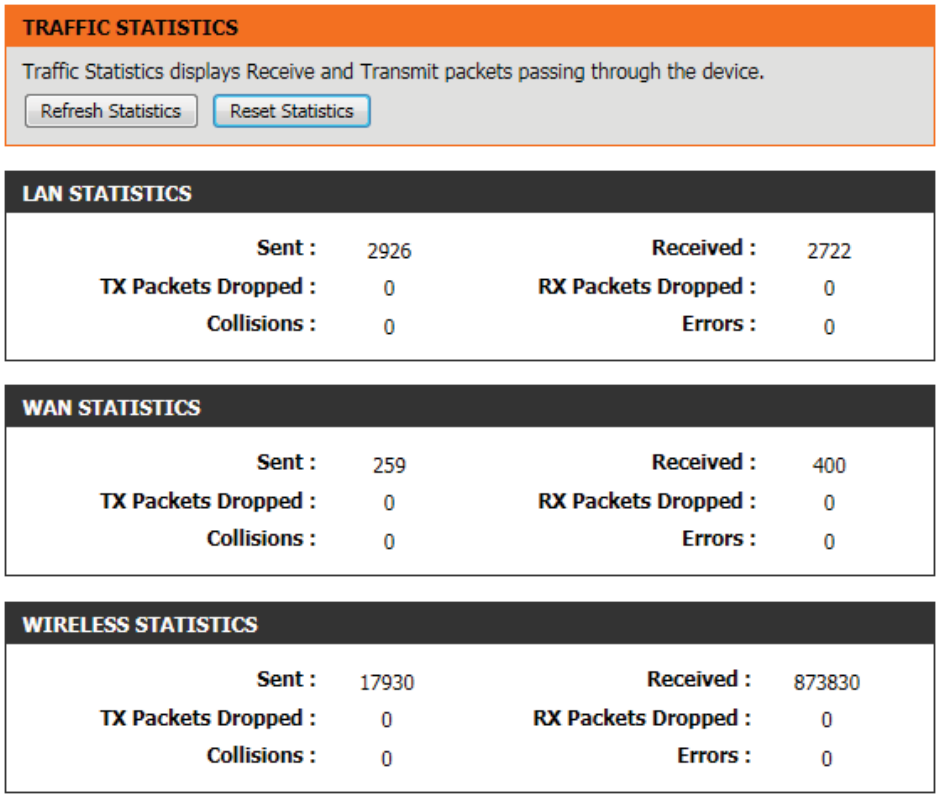
The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the router on both the WAN, LAN ports and the 802.11n/g (2.4GHz) wireless band. The traffic counter will reset if the device is rebooted.

In the **LAN Statistics** section, the user can view the traffic statistics that occurred on the LAN interface. Information that is displayed includes the packets sent and received, packets dropped, collisions that occurred, and error packets sent and received.

In the **WAN Statistics** section, the user can view the traffic statistics that occurred on the WAN interface. Information that is displayed includes the packets sent and received, packets dropped, collisions that occurred, and error packets sent and received.

In the **Wireless Statistics** section, the user can view the traffic statistics that occurred on the Wireless interface. Information that is displayed includes the packets sent and received, packets dropped, collisions that occurred, and error packets sent and received.

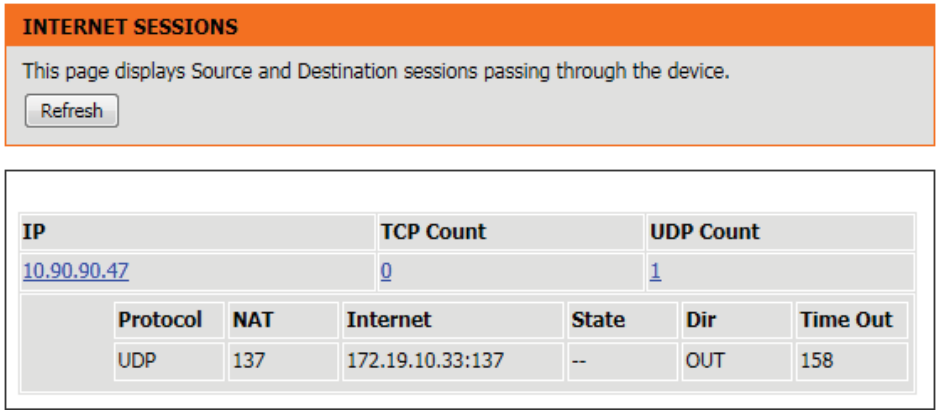
Click on the **Refresh Statistics** button to refresh the display page.
Click on the **Reset Statistics** button to clear all the statistic information for all the fields displayed.



Internet Sessions

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

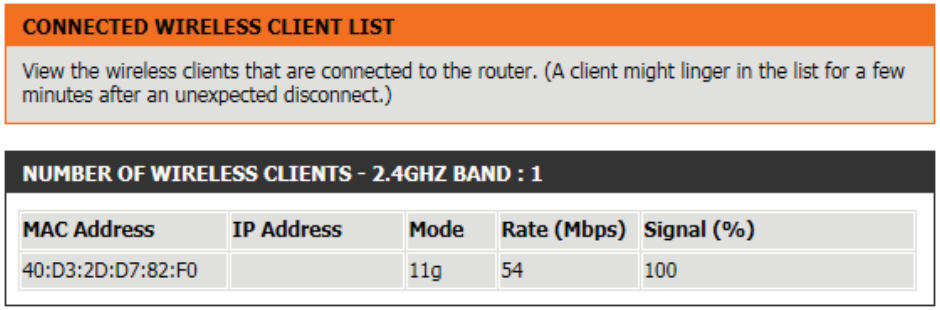
In the section all the active Internet sessions will be displayed.



Wireless

The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.

In the **Number of Wireless Clients - 2.4GHz Band** section a list of 2.4GHz active wireless clients will be displayed.

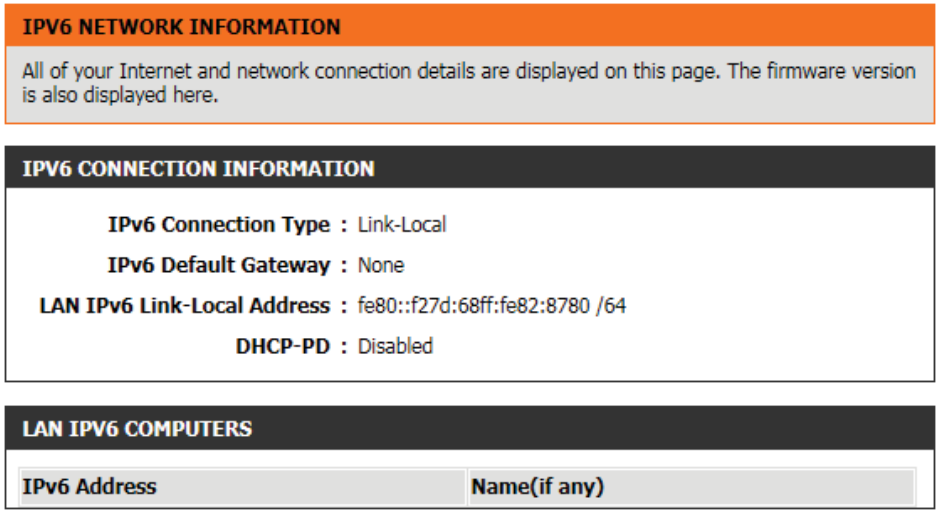


IPv6

The IPv6 page displays a summary of the Router's IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.

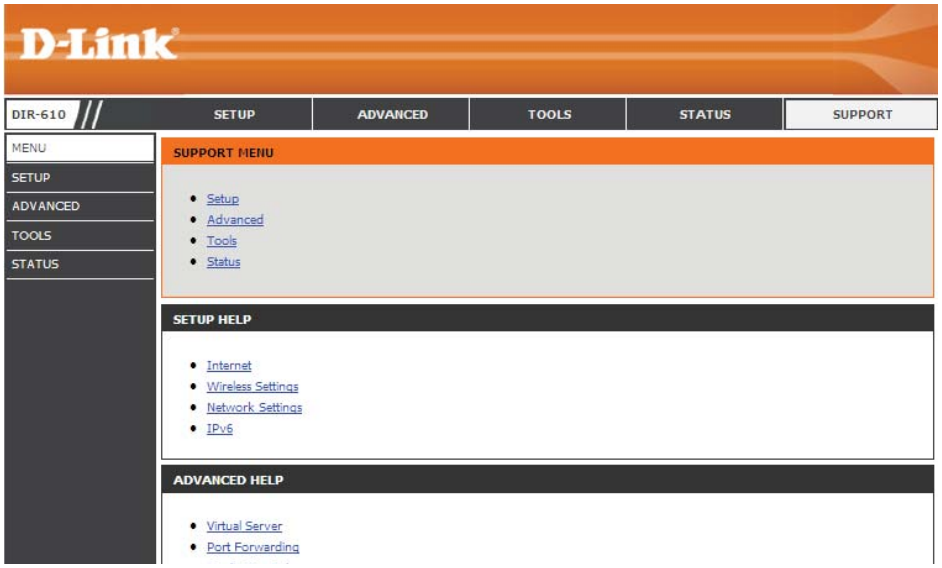
In the **IPv6 Connection Information** section, more information about the IPv6 connection will be displayed. Information like the connection type, gateway address, Link-Local address, DNS Servers, and more.

In the **LAN IPv6 Computers** section, a list of actively connected LAN IPv6 computers will be displayed.



Support Category

In this section, the user will have access to a portal of information regarding each and every page that exists on this device. This information gives the basic description of parameter and uses for the pages.



Knowledge Base

Wireless Basics

Wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

How does Wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away. Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology as become so popular in recent years that almost everyone is using it, whether it's for home, office, business, we have a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a Wireless Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- Infrastructure – All wireless clients will connect to an access point or wireless router.
- Ad-Hoc – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless Cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The router offers wireless security options like WPA/WPA2 PSK/EAP.

What is WPA?

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

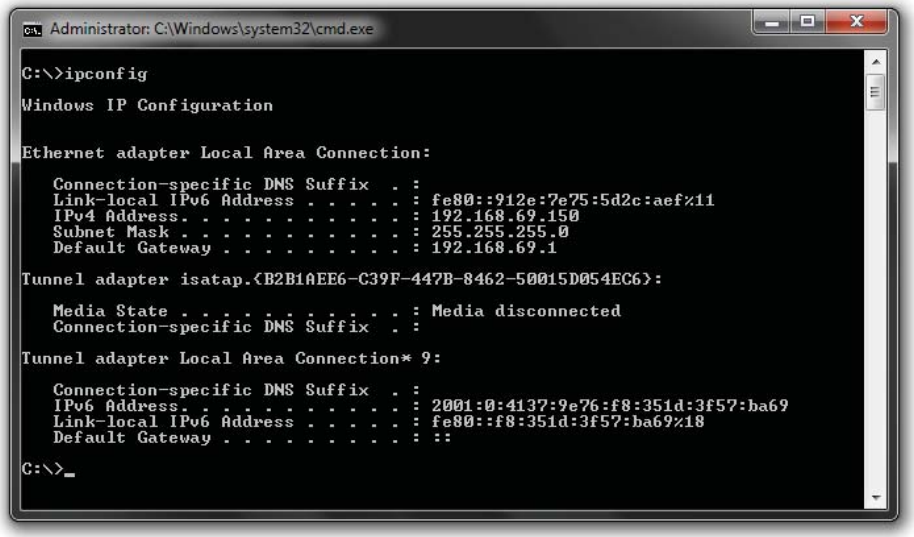
WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Networking Basics

Check your IP address

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



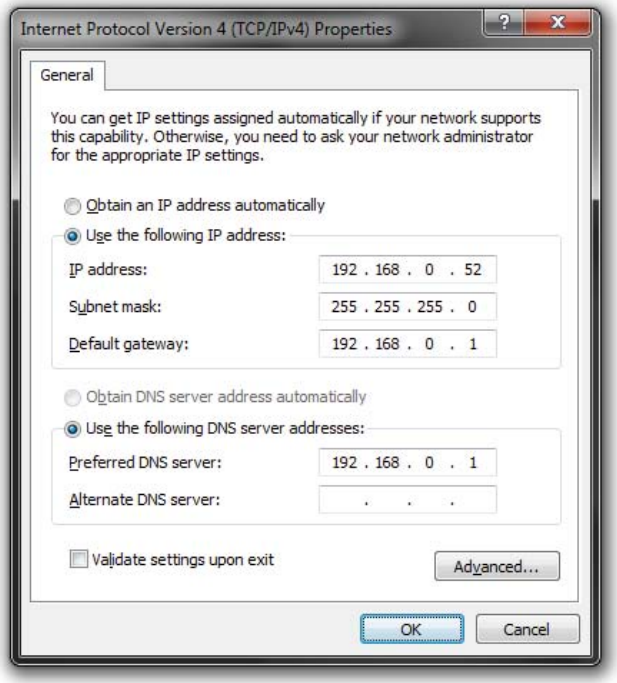
Click on Start > Run. In the run box type cmd and click OK. (Windows® 7/Vista® users type cmd in the Start Search box.) At the prompt, type ipconfig and press Enter.

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

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

Statically Assign an IP address

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



Step 1

- Windows® 7 - Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Setting.
- Windows Vista® - Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.
- Windows® XP - Click on Start > Control Panel > Network Connections.
- Windows® 2000 - From the desktop, right-click My Network Places > Properties.

Step 2

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

Step 3
Highlight Internet Protocol (TCP/IP) and click Properties.

Step 4
Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example:
If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.

Set Default Gateway the same as the LAN IP address of your router (192.168.0.1). Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5
Click **OK** twice to save your settings.

Connect to a Wireless Network

Using Window 7

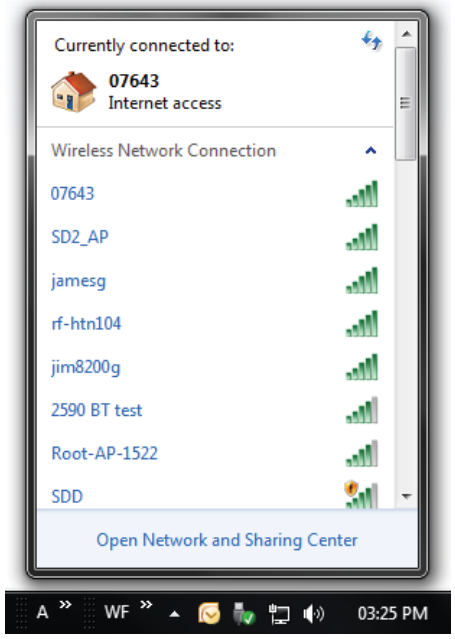
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).

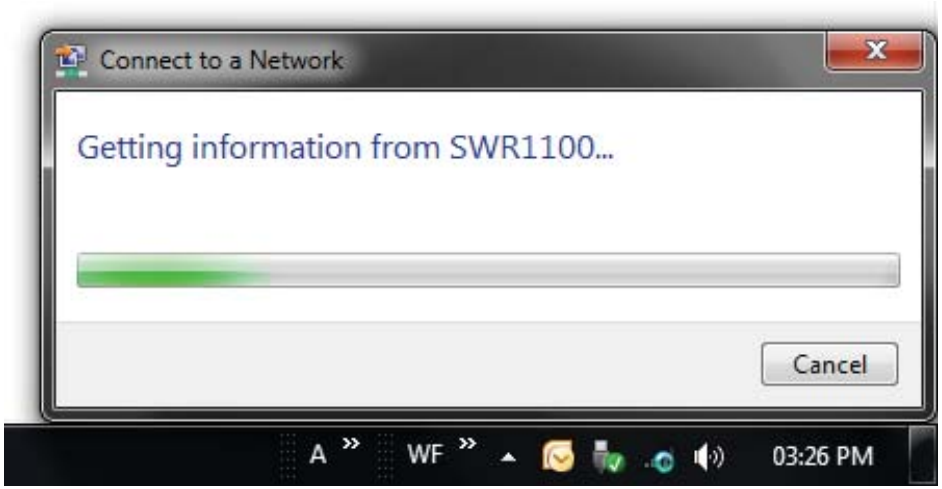
2. The utility will display any available wireless networks in your area.

3. Highlight the wireless network (SSID) you would like to connect to and click the Connect button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase that is on your router and click Connect. You can also connect by pushing the WPS button on the router.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

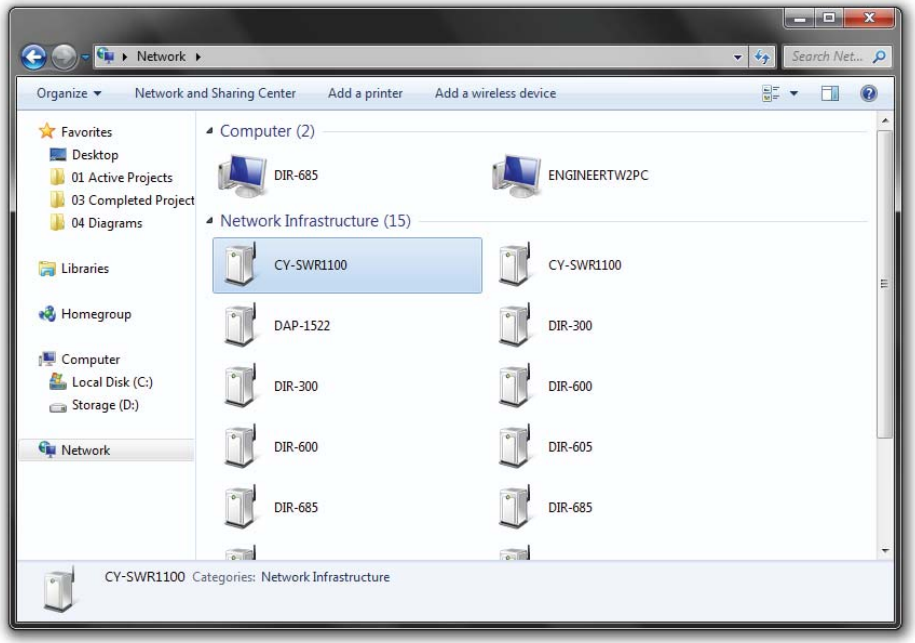
Using Window 7 and WPS

The WPS feature of the router can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature of the router:

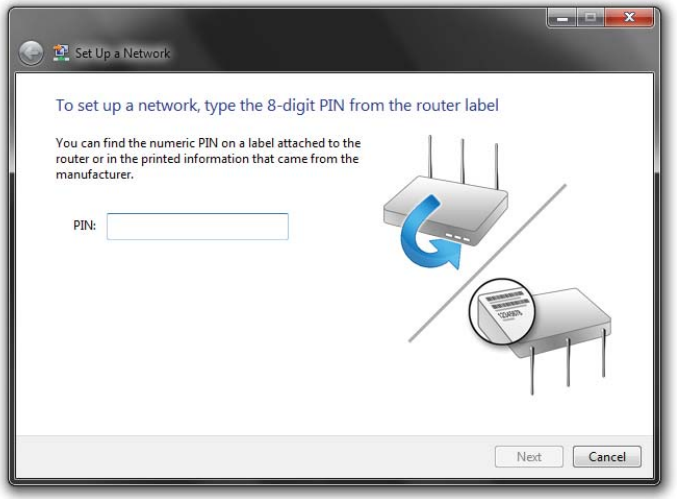
1. Click the Start button and select Computer from the Start menu.

2. Click the Network option.

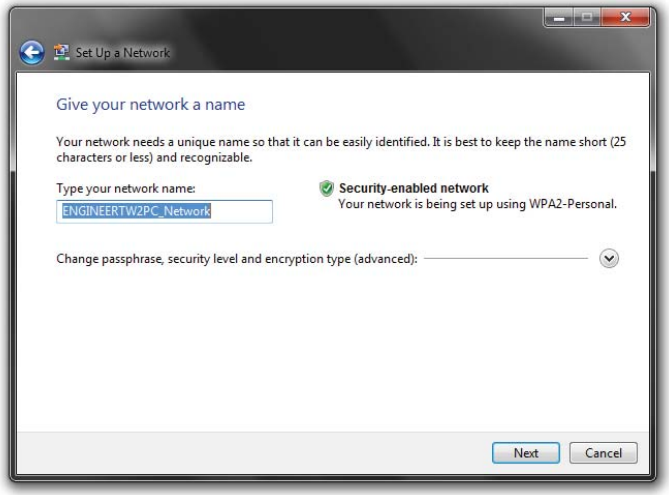
3. Double-click the Router.



4. Input the WPS PIN number and click Next.

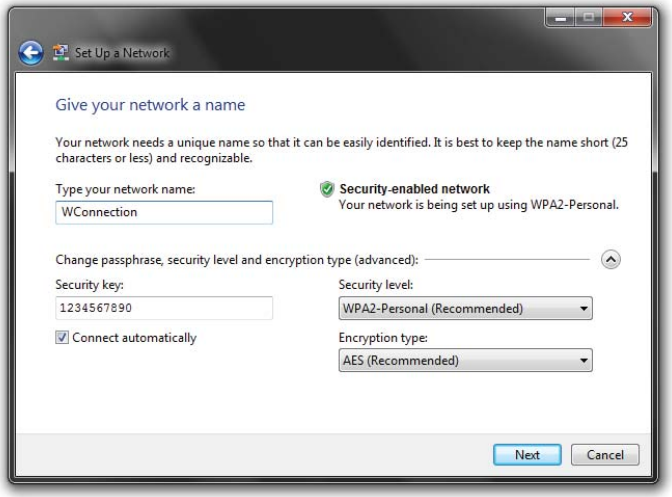


5. Type a name to identify the network.



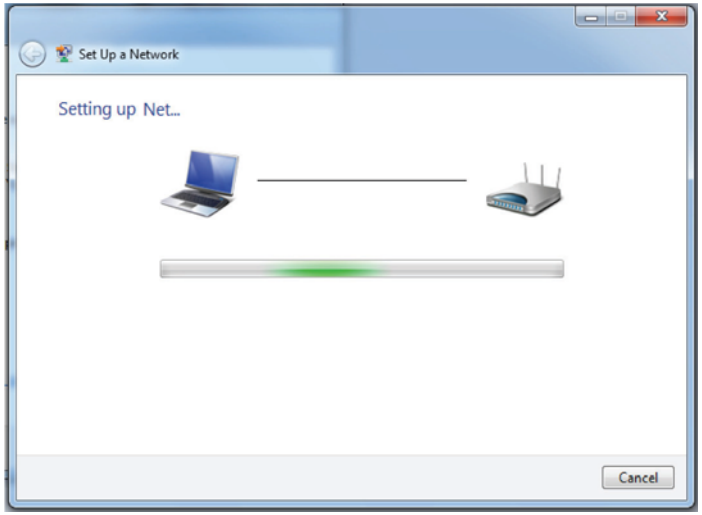
6. To configure advanced settings, click on the drop-down icon.

Click Next to continue.



7. The following window appears while the Router is being configured.

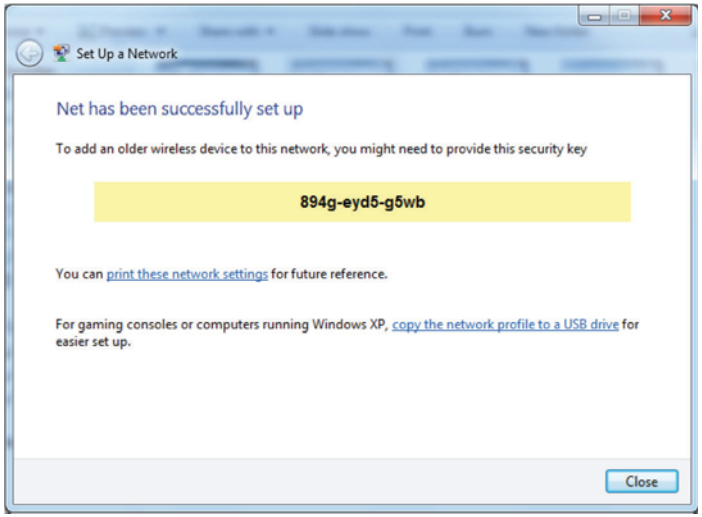
Wait for the configuration to complete.



8. The following window informs you that WPS on the Router has been setup successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click Close to complete WPS setup.



Using Window Vista

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

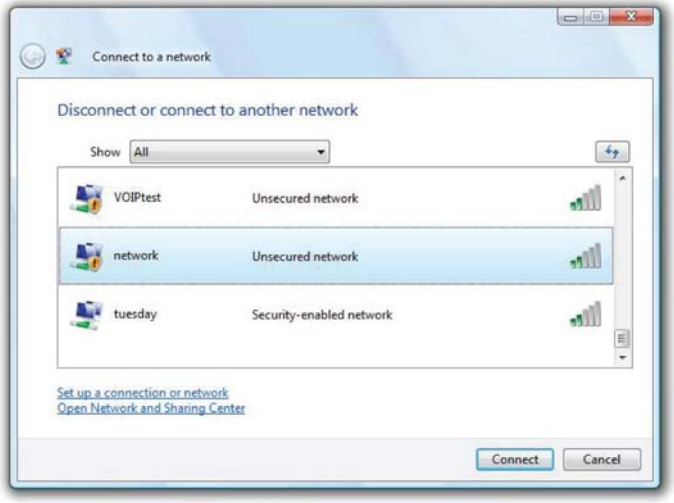
If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility or right-click on the wireless computer icon in your system tray (lower-right corner next to the time).

Select Connect to a network.

The utility will display any available wireless networks in your area.

Click on your wireless network (displayed using the SSID) and click the Connect button.

If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select Connect to a network.

2. Highlight the wireless network (SSID) you would like to connect to and click Connect.

3. Enter the same security key or passphrase that is on your router and click Connect.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

Using Window XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the center of the bubble to access the utility or right-click on the wireless computer icon in your system tray (lower right corner next to the time). Select View Available Wireless Networks.

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the Connect button.

If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

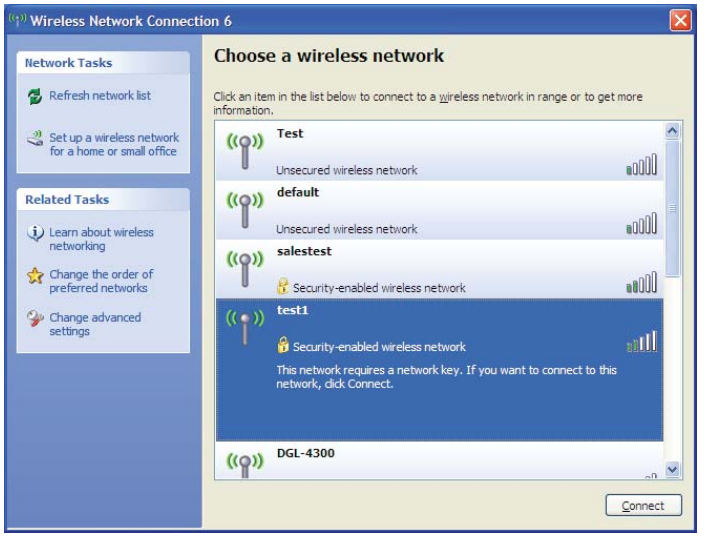
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select View Available Wireless Networks.

2. Highlight the wireless network (SSID) you would like to connect to and click Connect.

3. The Wireless Network Connection box will appear. Enter the WPA-PSK passphrase and click Connect.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the router. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screen captures on your computer will look similar to the following examples.

Why can't I access the web-based configuration utility?

When entering the IP address of the router (192.168.0.1 for example), you are not connecting to a website nor do you have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

Make sure you have an updated Java-enabled web browser. We recommend the following:

- Microsoft Internet Explorer® 6.0 and higher
- Mozilla Firefox 3.0 and higher
- Google™ Chrome 2.0 and higher
- Apple Safari 3.0 and higher

Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

Configure your Internet settings:

- Go to Start > Settings > Control Panel. Double-click the Internet Options Icon. From the Security tab, click the button to restore the settings to their defaults.
- Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK.
- Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.
- Close your web browser (if open) and open it.

Access the web management. Open your web browser and enter the IP address of your router in the address bar. This should open the login page for your web management.

If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the bottom panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is admin and leave the password box empty.

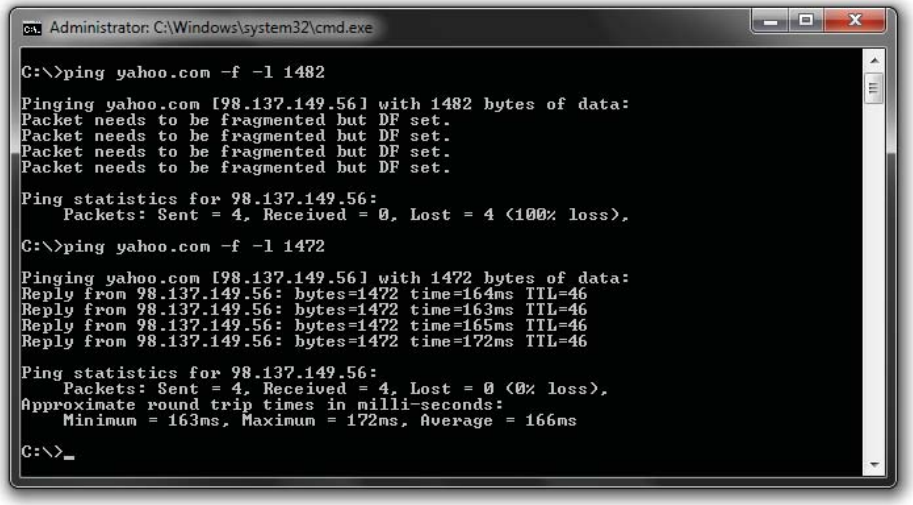
Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on Start and then click Run.
- Windows® 95, 98, and Me users type in command (Windows® NT, 2000, and XP users type in cmd) and press Enter (or click OK).
- Once the window opens, you'll need to do a special ping. Use the following syntax: ping [url] [-f] [-l] [MTU value]

Example: ping yahoo.com -f -l 1472



You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.0.1) and click OK.
- Enter your username (admin) and password (blank by default). Click OK to enter the web configuration page for the device.
- Click on Setup and then click Manual Configure.
- To change the MTU enter the number in the MTU field and click Save Settings to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Technical Specifications

Standards

- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.3
- IEEE 802.3u

Security

- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise
- Wi-Fi protected set-up (PBC/PIN)

Wireless Signal Rates*

- 150 Mbps
- 54 Mbps
- 36 Mbps
- 18 Mbps
- 11 Mbps
- 6 Mbps
- 2 Mbps
- 48 Mbps
- 24 Mbps
- 12 Mbps
- 9 Mbps
- 5.5 Mbps
- 1 Mbps

Frequency Range

- 2.4 GHz to 2.483 GHz

LEDs

- Power
- WPS
- WLAN
- WAN
- LAN

Operating Temperature

- 32°F to 131°F (0°C to 55°C)

Humidity

- 95% maximum (non-condensing)

Safety & Emissions

- FCC
- CSA International

Dimensions

- L = 4.4 inches
- W = 5.8 inches
- H = 1.2 inches

Warranty

- 1 Year

* Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

CE Mark Warning:
This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

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

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

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

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement
This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
Radiation Exposure Statement:
This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

IMPORTANT NOTE:
Radiation Exposure Statement:
The product comply with the US/Canada portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

NOTE IMPORTANTE:
Déclaration d'exposition aux radiations:
Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

NOTE IMPORTANTE: (Pour l'utilisation des appareils portables)
Déclaration d'exposition aux radiations:
Le produit est conforme aux limites d'exposition pour les appareils portables RF pour les Etats-Unis et le Canada établies pour un environnement non contrôlé.
Le produit est sûr pour un fonctionnement tel que décrit dans ce manuel. La réduction aux expositions RF peut être augmentée si l'appareil peut être conservé aussi loin que possible du corps de l'utilisateur ou que le dispositif est réglé sur la puissance de sortie la plus faible si une telle fonction est disponible.

以下警語適用台灣地區

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。